



Fundamentos teóricos de la ciberseguridad en los sistemas de información: una
revisión conceptual

Modalidad: Monografía Teórica

YESID RODRIGUEZ TAVERA

CC: 1007678713

YULIETH JULIANA FLOREZ

CC: 1193547580

UNIDADES TECNOLÓGICAS DE SANTANDER
Facultad de Ciencias Socioeconómicas y Empresariales
Contaduría Pública - Virtual
Bucaramanga (14/09/2026)



Fundamentos teóricos de la ciberseguridad en los sistemas de información: una
revisión conceptual

Modalidad: Monografía Teórica

YESID RODRIGUEZ TAVERA

CC: 1007678713

YULIETH JULIANA FLOREZ

CC: 1193547580

**Trabajo de Grado para optar al título de
Contador Público**

DIRECTOR

Mg. Omar Hernán Nova Jaimes

Grupo de investigación E-INNOVARE

**UNIDADES TECNOLÓGICAS DE SANTANDER
Facultad de Ciencias Socioeconómicas y Empresariales
Contaduría Pública - Virtual
Bucaramanga (14/09/2026)**

F-DC-125

INFORME FINAL DE TRABAJO DE GRADO EN MODALIDAD DE PROYECTO
DE INVESTIGACIÓN, DESARROLLO TECNOLÓGICO, MONOGRAFÍA,
EMPRENDIMIENTO Y SEMINARIO

VERSIÓN: 2.0

Este informe final de trabajo de grado,
en modalidad de Monografía, fue APROBADO
en cumplimiento de uno de los requisitos exigidos por
las Unidades Tecnológicas de Santander para optar
el Título de Contador Público según acta No. 16 del
14 de septiembre del 2026,
del Comité de Trabajo de Grado

Dedcy Latorre

Firma del Evaluador
Dedcy Latorre Jácome



Firma del Director

DEDICATORIA

Dedicamos este trabajo de grado, en primer lugar, a Dios, por brindarnos la fortaleza, sabiduría y perseverancia necesarias para culminar esta etapa de nuestra formación profesional.

A nuestras familias, por su amor, apoyo incondicional, comprensión y confianza durante todo este proceso. Gracias por acompañarnos en cada desafío y por ser una fuente permanente de motivación para alcanzar nuestras metas.

A nuestros docentes y director de trabajo de grado, por compartir sus conocimientos, orientarnos y contribuir a nuestro crecimiento académico y profesional.

Finalmente, nos dedicamos este logro a nosotros mismos, por la constancia, el esfuerzo y el compromiso que nos permitieron superar cada dificultad y llegar hasta este momento. Este trabajo representa no solo el cierre de una etapa académica, sino también el inicio de nuevos sueños y oportunidades.

AGRADECIMIENTOS

Expresamos nuestro más sincero agradecimiento a Dios, por brindarnos la fortaleza, sabiduría y perseverancia necesarias para culminar satisfactoriamente esta etapa de nuestra formación profesional.

A nuestras familias, por su amor, apoyo incondicional, comprensión y confianza durante todo el proceso académico. Su acompañamiento y motivación fueron fundamentales para superar cada reto y continuar trabajando por nuestras metas.

A nuestro director de trabajo de grado, Mg. Omar Hernán Nova Jaimes, por su orientación, disposición, conocimientos y acompañamiento durante el desarrollo de esta investigación, aportando valiosas recomendaciones para fortalecer nuestro trabajo.

A los docentes de las Unidades Tecnológicas de Santander, por los conocimientos, enseñanzas y experiencias compartidas a lo largo de nuestra formación como profesionales.

A las Unidades Tecnológicas de Santander, por brindarnos los espacios, herramientas y oportunidades necesarias para nuestra formación académica y profesional.

Finalmente, agradecemos a todas las personas que, de manera directa o indirecta, contribuyeron al desarrollo y culminación de este trabajo de grado. A todos, muchas gracias por hacer parte de este logro.

TABLA DE CONTENIDO

<u>INTRODUCCIÓN</u>	<u>11</u>
<u>1. DESCRIPCIÓN DEL TRABAJO DE INVESTIGACIÓN</u>	<u>14</u>
1.1. PLANTEAMIENTO DEL PROBLEMA	14
1.2. OBJETIVOS	15
1.2.1. OBJETIVO GENERAL	15
1.2.2. OBJETIVOS ESPECÍFICOS	15
<u>2. MARCO REFERENCIAL</u>	<u>17</u>
2.1. MARCO TEÓRICO	17
2.1.1 FUNDAMENTO TEÓRICO DE CIBERSEGURIDAD	17
2.1.3 FUNDAMENTO TEORICO MODELO CIA (CONFIDENTIALITY, INTEGRITY, AVAILABILITY)	19
2.1.4 RIESGOS EN LA CONTABILIDAD ASOCIADOS A LA FALTA DE CIBERSEGURIDAD	20
2.2 MARCO LEGAL	22
NORMATIVA INTERNACIONAL	22
NORMATIVA NACIONAL	23
2.3 MARCO CONCEPTUAL	24
<u>3 DISEÑO DE LA INVESTIGACION</u>	<u>36</u>
<u>4 DESARROLLO DEL TRABAJO DE GRADO</u>	<u>39</u>
<u>5 RESULTADOS</u>	<u>44</u>
<u>6 CONCLUSIONES</u>	<u>138</u>
<u>7 RECOMENDACIONES</u>	<u>140</u>
<u>8 REFERENCIAS BIBLIOGRÁFICAS</u>	<u>142</u>
<u>9. APÉNDICES</u>	<u>154</u>

LISTA DE FIGURAS

No se encuentran elementos de tabla de ilustraciones.

LISTA DE TABLAS

Tabla 1. Riesgos en la contabilidad asociados a la falta de ciberseguridad	21
Tabla 2. Conceptos fundamentales de ciberseguridad.	49
Tabla 3. Antecedentes sobre el impacto de la ciberseguridad en la contabilidad.	56
Tabla 4. Antecedentes automatización contable y riesgos cibernéticos	57
Tabla 5. Análisis de estudios previos sobre la ciberseguridad en la contabilidad.	58
Tabla 6 Cumplimiento normativo en procesos contables y su relación con la ciberseguridad	68
Tabla 7. Casos reales y análisis de impacto	71
Tabla 8 Controles desde el desarrollo de conceptos clave y la evolución de la ciberseguridad en los sistemas de información	73
Tabla 9 Base conceptual estructurada de la ciberseguridad en los sistemas de información, ...	75
Tabla 10 Matriz de relación entre ciberseguridad y cumplimiento normativo en los sistemas de información	98
Tabla 11 Matriz de identificación, relación y cumplimiento normativo.....	99
Tabla 12 Matriz integral de conceptos, ciberseguridad y cumplimiento normativo.....	103
Tabla 13 Matriz comparativa de ventajas y desventajas	123
Tabla 14 Síntesis de las ventajas y desventajas de la implementación de medidas de ciberseguridad en los sistemas de información financieros.....	128
Tabla 15 Evaluación del impacto de las medidas de ciberseguridad en los sistemas financieros y contables.....	135
Tabla 16 Sin tesis de los resultados	137

RESUMEN EJECUTIVO

El presente trabajo tuvo como objetivo establecer los fundamentos teóricos de la ciberseguridad aplicables a los sistemas de información, mediante la revisión de conceptos, principios, amenazas, riesgos y mecanismos de protección relacionados con la seguridad de la información. Asimismo, buscó identificar los principales enfoques utilizados para preservar la confidencialidad, integridad y disponibilidad de los datos, considerando la evolución de los riesgos derivados de la transformación digital. De acuerdo con ISO/IEC 27001:2022, la seguridad de la información requiere un enfoque sistemático para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información.

La metodología correspondió a una revisión documental de enfoque cualitativo y alcance descriptivo, sustentada en el análisis de literatura académica, estándares internacionales y documentos técnicos publicados entre 2021 y 2026, priorizando fuentes especializadas y organismos reconocidos en ciberseguridad. Se analizaron referentes como el NIST Cybersecurity Framework 2.0, que estructura la gestión del riesgo mediante resultados orientados a comprender, evaluar, priorizar y comunicar los riesgos de ciberseguridad (NIST, 2024).

Los resultados permitieron identificar que la ciberseguridad comprende dimensiones tecnológicas, organizacionales y de gestión del riesgo. Además, se evidenció la presencia de amenazas como ransomware, malware, ingeniería social, ataques a los datos, denegación de servicio y ataques a la cadena de suministro, señaladas por ENISA (2024).

Se concluye que la ciberseguridad constituye un componente estratégico de los sistemas de información y requiere integrar controles tecnológicos, gestión de riesgos, gobernanza, capacitación y mejora continua para fortalecer la protección de los activos de información.

PALABRAS CLAVE: Ciberseguridad; Sistemas de información; Gestión de riesgos; Seguridad de la información; Protección de datos.

INTRODUCCIÓN

El rápido avance tecnológico a nivel global, incluido Colombia, ha transformado la manera en que las organizaciones gestionan, almacenan, procesan y transmiten información. Esta creciente dependencia de los sistemas de información también ha incrementado la exposición a ciberataques, vulnerabilidades y fallas de seguridad que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos. En este contexto, la ciberseguridad se consolida como un componente fundamental para la protección de los recursos tecnológicos, la continuidad operativa y el desarrollo de las actividades organizacionales. En el ámbito colombiano, los reportes de la Superintendencia Financiera de Colombia (2023) evidencian la importancia de fortalecer la seguridad de la información y la gestión de incidentes cibernéticos en las entidades financieras.

Los riesgos asociados a la ciberseguridad pueden generar consecuencias significativas para las organizaciones, entre ellas interrupciones operativas, pérdidas económicas, afectaciones a los activos de información y deterioro de la confianza de los usuarios. De acuerdo con Otonne et al. (2023), los fraudes cibernéticos y otras interrupciones tecnológicas representan desafíos para la continuidad y el desempeño empresarial. Asimismo, Ulloa (2021) destaca la relevancia de la seguridad digital frente al crecimiento de las amenazas cibernéticas y sus posibles repercusiones en las organizaciones. Estos planteamientos permiten comprender que la protección de los sistemas de información requiere una perspectiva integral que trascienda la implementación aislada de herramientas tecnológicas.

En particular, los sistemas de información contable constituyen un componente relevante de las organizaciones, debido a que procesan y administran datos financieros necesarios para la toma de decisiones. Bushman (2021) resalta la importancia de la

información financiera y de los mecanismos que contribuyen a garantizar su confiabilidad. Por consiguiente, las vulnerabilidades que afectan los sistemas contables pueden comprometer la exactitud, disponibilidad y seguridad de los registros financieros, lo que evidencia la necesidad de incorporar fundamentos de ciberseguridad en su diseño, operación y supervisión.

Desde una perspectiva estratégica, la ciberseguridad no solo comprende la prevención de ataques, sino también la identificación de riesgos, la aplicación de controles, la gestión de incidentes y el fortalecimiento de las capacidades organizacionales. Gomero y Sánchez (2024) destacan la importancia de la ciberseguridad en entornos caracterizados por la transformación tecnológica y la necesidad de proteger la información frente a nuevas amenazas. En consecuencia, el estudio de sus fundamentos teóricos permite relacionar los componentes tecnológicos con los procesos de gestión, las personas, las políticas institucionales y los mecanismos de protección de los activos de información.

A pesar de la existencia de investigaciones y documentos especializados sobre seguridad digital, persiste la necesidad de organizar conceptualmente los principales fundamentos de la ciberseguridad en los sistemas de información, especialmente en lo relacionado con sus definiciones, principios, amenazas, vulnerabilidades, riesgos y controles de protección. Esta situación justifica el desarrollo del presente trabajo, cuyo aporte consiste en integrar y sistematizar conocimientos teóricos que faciliten la comprensión de la ciberseguridad desde una perspectiva organizacional y tecnológica.

Por lo anterior, el objetivo de esta investigación es analizar los fundamentos teóricos de la ciberseguridad en los sistemas de información mediante una revisión conceptual de literatura especializada, con el propósito de identificar sus principales componentes, riesgos y mecanismos de protección. Para alcanzar este objetivo, se emplea una metodología de enfoque cualitativo, alcance descriptivo y diseño

documental, basada en la búsqueda, selección, análisis e interpretación de fuentes académicas, técnicas y normativas relacionadas con el tema. El desarrollo metodológico permitirá profundizar en los fundamentos conceptuales y establecer una base teórica organizada que contribuya a la comprensión de la ciberseguridad y a futuras investigaciones sobre la protección de los sistemas de información.

1. DESCRIPCIÓN DEL TRABAJO DE INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

En el marco del proyecto titulado “El rol de la ciberseguridad en los sistemas de información un análisis teórico”, resulta fundamental analizar cómo el crecimiento de los riesgos digitales que impacta directamente la gestión contable y financiera. El avance tecnológico, tanto a nivel global como en Colombia, ha dado lugar a un aumento en los ciberataques, superando en ocasiones los progresos alcanzados. Esto ha generado la necesidad de que diversas organizaciones implementen medidas de protección para mitigar su impacto en el funcionamiento de la sociedad y en el desarrollo financiero (Ulloa, 2021). En Latinoamérica, sectores productivos, comerciales, financieros y bancario, las telecomunicaciones y las inversiones entre otros han sido afectados por delitos cibernéticos, resultando en la pérdida de información y la vulneración de la seguridad (Robles, 2024).

El aumento de los ciberataques es una tendencia global que afecta a todos los países, con altos niveles de incidencia en la región. Ecuador presenta un 75%, seguido de Perú (71%), Panamá (60%), Guatemala (43%) y Venezuela (29%), mientras que Colombia registra un número significativo de intentos de infección. A nivel global, el malware genera en promedio 35 ataques por segundo, lo que evidencia la magnitud del problema (Diazgranados, 2021).

Esta situación expone la vulnerabilidad de los sistemas de información contable, comprometiendo la integridad, confidencialidad y disponibilidad de los datos financieros. Otonne et al. (2023) señalando que los fraudes cibernéticos afectan la productividad, la gestión y el crecimiento empresarial, generando pérdidas económicas y deterioro de la confianza.

En este contexto, la ciberseguridad se posiciona como un elemento clave dentro de los sistemas de información, ya que garantiza la protección de los activos, la continuidad operativa y la estabilidad financiera. Dada la creciente interdependencia entre la gestión tecnológica y los procesos contables, resulta fundamental comprender cómo esta disciplina resguarda la integridad de la información financiera frente a las amenazas digitales actuales.

Pregunta problema:

De acuerdo con lo anterior, se plantea la siguiente pregunta de investigación: ¿Cuál es el papel de la ciberseguridad en la protección de los activos y la estabilidad financiera dentro de los sistemas de información contable?

1.2. OBJETIVOS

1.2.1. Objetivo General

Analizar el rol de la ciberseguridad en los sistemas de información, mediante un estudio teórico que evalúe sus fundamentos y su impacto en la protección de los activos, la mitigación de fraudes y el cumplimiento normativo, con el fin de fortalecer la toma de decisiones estratégicas y garantizar la sostenibilidad financiera de las organizaciones.

1.2.2. Objetivos Específicos

Comprender los conceptos clave y la evolución de la ciberseguridad en los sistemas de información, mediante la revisión de literatura académica, para abarcar su aplicabilidad en los sistemas de información.

Identificar la relación entre la ciberseguridad y el cumplimiento normativo en los sistemas de información, a través del análisis teórico, con la finalidad de determinar su contribución a la integridad y legalidad de los procesos contables y financieros.

Describir las ventajas y desventajas de la implementación de medidas de ciberseguridad en los sistemas de información financieros, mediante un estudio bibliográfico, con el fin de evaluar su impacto en la protección de la información, la eficiencia operativa y el cumplimiento regulatorio.

2. MARCO REFERENCIAL

2.1. MARCO TEÓRICO

2.1.1 Fundamento Teórico de Ciberseguridad

La habilidad de una organización para enfrentar amenazas y vulnerabilidades está estrechamente relacionada con los niveles de formación y concienciación en ciberseguridad de su personal. Según (Ortega, 2024) la ciberseguridad se enfoca en la protección de los activos digitales, que abarcan no solo redes, hardware y software, sino también la información que se procesa, almacena y transporta en entornos interconectados. En este sentido, la ciberseguridad implica un conjunto de técnicas, sistemas de gestión y diversas medidas que tienen como objetivo salvaguardar la información digital contra accidentes, tanto deliberados como intencionales.

Es importante considerar la ciberseguridad como un componente de la seguridad de la información en general. De este modo, podemos definir la ciberseguridad como la protección de los activos de información, abordando las amenazas que pueden afectar a la información procesada, almacenada y transportada a través de estos sistemas interconectados. En un mundo cada vez más digital, esta protección es esencial para garantizar la integridad y la confidencialidad de la información.

En el marco de ciberseguridad, (Ortega, 2024) identifica cinco (5) funciones que son cruciales para proteger los activos digitales de las organizaciones. Estas se alinean con las metodologías de gestión de incidentes e incluyen las siguientes actividades:

Identificar: usar el entendimiento de la organización para minimizar el riesgo de los sistemas, activos, datos y capacidades (Ortega, 2024)

Proteger: diseñar salvaguardas para limitar el impacto de los eventos potenciales en servicios e infraestructuras críticos (Ortega, 2024).

Detectar: aplicar acciones para identificar la presencia de eventos de ciberseguridad.

Responder: tomar medidas adecuadas tras conocerse un evento de seguridad.

Recuperar: planificar para tener resiliencia y recuperar de forma oportuna los servicios y capacidades que pudieran haber sido comprometidos (Ortega, 2024)

La confidencialidad es el principio que establece que solo los usuarios autorizados pueden acceder a los recursos de un sistema. Por otro lado, la integridad se refiere a la propiedad de la información que garantiza la precisión de los datos almacenados o transportados, asegurando que no se hayan alterado, perdido o destruido, ya sea de manera accidental o intencionada, debido a errores de software, hardware o factores ambientales. Lo anterior, significa que solo los usuarios autorizados pueden modificar los recursos del sistema. Por último, la disponibilidad se relaciona con la capacidad de un servicio, sistema o información para ser accesible y utilizable por los usuarios o procesos autorizados cuando lo necesiten. Así mismo, los recursos del sistema deben estar siempre disponibles para quienes tienen permiso para utilizarlos (Ortega, 2024).

2.1.2 Fundamento Teórico de Dominios de la ciberseguridad

Mantener un cierto nivel de seguridad requiere, de hecho, un proceso continuo de mejora que abarque las siguientes fases: análisis, prevención, detección y respuesta. Estas etapas son complementarias entre sí y, si se llevan a cabo correctamente, forman un ciclo que permite preservar la seguridad a lo largo del tiempo (Ortega, 2024).

La primera fase, el análisis de riesgos, implica que el nivel de riesgo varía con el tiempo, ya que continuamente se identifican nuevas vulnerabilidades en los sistemas y las amenazas también evolucionan. Además, las organizaciones no pueden permanecer

inalteradas; sus mercados, productos, servicios y objetivos cambian (Ortega, 2024). Las otras tres fases, cuando se realizan adecuadamente, facilitarán la detección de intentos de intrusión y la reacción ante ellos, minimizando el impacto. Al mismo tiempo, permitirán aprender y mejorar los mecanismos y procedimientos relacionados con la seguridad en todos los sistemas administrativos de la empresa (Ortega, 2024).

Según (Ortega, 2024) los cuatro ámbitos de la ciberseguridad son:

- Conceptos de ciberseguridad
- Principios de arquitectura de ciberseguridad
- Seguridad de redes, sistemas, aplicaciones y datos
- Respuestas a incidentes

2.1.3 Fundamento Teorico Modelo CIA (Confidentiality, Integrity, Availability)

Tres conceptos fundamentales en la seguridad de la información son la confidencialidad, la integridad y la disponibilidad, conocidos colectivamente como la tríada de la seguridad de la información. Este modelo, conocido como la tríada CIA, ha sido utilizado durante más de 20 años y proporciona un marco que facilita la reflexión y el debate sobre los aspectos de seguridad, con un énfasis particular en la protección de los datos (Vega, 2021).

El modelo CIA está diseñado para proteger tanto la información como los sistemas de información. Al abordar estos tres principios, las organizaciones pueden desarrollar estrategias efectivas para garantizar que sus datos permanezcan seguros y accesibles solo para los usuarios autorizados, que se mantengan intactos y precisos, y que estén disponibles cuando se necesiten (Vega, 2021).

2.1.4 Riesgos en la Contabilidad asociados a la falta de Ciberseguridad

Los riesgos asociados a la falta de ciberseguridad constituyen una preocupación importante en el contexto actual, por tanto, así, la creciente digitalización y la adopción de tecnologías de la información han expuesto a las organizaciones a un mayor número de vulnerabilidades. Este panorama se vuelve aún más alarmante considerando que los datos financieros y contables son objetivos atractivos a ciberataques (García, 2021).

Dentro de los principales riesgos, encontramos el fraude y la manipulación de datos; esto hace referencia a que la ausencia de medidas de ciberseguridad efectivas puede facilitar el acceso no autorizado a los sistemas contables, que permite a los ciberdelincuentes llevar a cabo acciones fraudulentas, como modificar los registros financieros o generar transacciones falsas (Caamaño & Gil, 2020). Otro riesgo importante es la pérdida de confidencialidad, ya que los ataques cibernéticos pueden exponer información financiera sensible, comprometiendo no solo la integridad de la organización, sino también la confianza de clientes y socios comerciales (Almario, 2022).

También se encuentra el riesgo la interrupción operativa, porque un ciberataque exitoso tiene el potencial de paralizar las operaciones contables y financieras, afectando la capacidad de la organización para llevar a cabo sus funciones diarias y cumplir con sus obligaciones legales y fiscales (García, 2021). Por último, los costos económicos asociados a estos ataques pueden ser significativos, llegando a representar hasta el 6% del PIB en algunos países, debido a pérdidas directas e indirectas relacionadas con la interrupción del negocio y el robo de datos.

Tabla 1. Riesgos en la contabilidad asociados a la falta de ciberseguridad.

RIESGO	DESCRIPCIÓN	FACTORES	INVOLUCRADOS
Robo de datos financieros	Acceso no autorizado a datos financieros sensibles, como balances, facturas o reportes financieros.	Falta de cifrado en la transmisión y almacenamiento de datos; contraseñas débiles; falta de autenticación.	Contadores, departamento TI, gerencia.
Alteración de informes contables	Modificación de registros contables o financieros que afectan la integridad de los informes y las decisiones.	Acceso no controlado a sistemas; falta de monitoreo y registros de auditoría; permisos excesivos de acceso.	Contadores, auditores, departamento TI.
Pérdida de datos	Eliminación accidental o malintencionada de registros contables, lo que afecta el análisis financiero.	Ausencia de copias de seguridad; falta de planes de recuperación; vulnerabilidades en el almacenamiento de datos.	Contadores, gerencia, equipo de recuperación de datos.
Fraude contable	Manipulación de información contable para ocultar actividades fraudulentas.	Falta de controles internos; ausencia de revisiones periódicas; falta de autenticación y autorización.	Contadores, auditores internos, gerencia.
Phishing y robo de credenciales	Obtención fraudulenta de credenciales de acceso mediante engaño, comprometiendo los sistemas contables.	Falta de capacitación en ciberseguridad; filtrado de correos electrónicos inadecuado; políticas débiles de autenticación.	Contadores, personal administrativo, TI.
Infección de malware y ransomware	Software malicioso que cifra datos o interrumpe el acceso a sistemas contables, requiriendo un rescate.	Ausencia de software antivirus y antimalware; falta de actualizaciones de seguridad; accesos remotos inseguros.	Departamento TI, contadores, gerencia.
Cumplimiento normativo	Incumplimiento de regulaciones de protección de datos (como GDPR) debido a falta de seguridad en datos contables.	Desconocimiento de las normativas; falta de controles y auditorías; deficiencias en políticas de protección de datos e información general.	Contadores, equipo legal, departamento TI, reguladores.

Fuente: (elaboración propia, 2024).

2.2 MARCO LEGAL

Normativa Internacional

- Organización Internacional de Normalización y Comisión Electrotécnica Internacional (2022), propone ISO/IEC 27001 que es un estándar internacional que establece un marco para la gestión de la seguridad de la información (SGSI). Su objetivo es ayudar las empresas a proteger sus activos de información, garantizando la confidencialidad, integridad y disponibilidad de datos (International Organization for Standardization, 2022). La norma se basa en un enfoque sistemático que incluye la evaluación de riesgos, la propuesta de políticas de seguridad, la asignación de responsabilidades, la capacitación del personal e implementación de controles técnicos y administrativos (Culot et al., 2021).

- Organización Internacional de Normalización y Comisión Electrotécnica Internacional (2018), establece ISO/IEC 27005 que se enfoca en la gestión de riesgos de seguridad de la información, proporcionando directrices específicas sobre cómo identificar, evaluar y tratar los riesgos asociados a la seguridad de la información (Culot et al., 2021). Esta norma es complementaria a la ISO/IEC 27001 y se centra en el proceso de gestión de riesgos, ayudando a las organizaciones a comprender mejor sus vulnerabilidades y a priorizar las medidas de seguridad en función de la evaluación del riesgo. Incluye metodologías para realizar análisis de riesgos y ofrecer recomendaciones sobre cómo mitigar las amenazas y gestionar las oportunidades (International Organization for Standardization, 2022).

- Naciones Unidas: el documento llamado *“fomento de la confianza en el comercio electrónico: cuestiones jurídicas del uso internacional de métodos de autenticación y firmas electrónicas de la Comisión de las Naciones Unidas para el*

desarrollo Mercantil Internacional de 2009” (Organización de las Naciones Unidas, 2022), se busca establecer las directrices para facilitar el uso de métodos de autenticación y firmas electrónicas en transacciones comerciales a nivel global.

Normativa Nacional

- Ley 527 de 1999, Ley de Comercio electrónico: reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación (Congreso de la República, 1999).
- Ley 1266 de 2008 Habeas Data: por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de los datos e información contenida en las bases de datos personales, en especial, de carácter financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones (Congreso de la República, 2008).
- Ley 1273 de 2009: por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Esta ley tipifica delitos informáticos y establece sanciones para quienes vulneren la seguridad informática, afectando la protección de datos, incluida la información contable (Congreso de la República, 2009).
- Ley 1581 de 2012: por la cual se dictan disposiciones generales para la protección de datos personales. Esta ley establece principios para la recolección y tratamiento de información, importante para la seguridad de los datos financieros (Congreso de la República, 2012).

- Decreto 2364 de 2012: por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones. además, Este decreto establece el régimen de protección de datos personales y complementa la Ley 1581 de 2012, que es la norma principal sobre la protección de datos en el país (Congreso de la República, 2012).

2.3 MARCO CONCEPTUAL

Amenaza

Es una situación adversa que puede presentarse y, al ocurrir, genera efectos negativos sobre los activos, provocando su falta de disponibilidad, mal funcionamiento o disminución de su valor. Es un acto o situación que puede explotar una vulnerabilidad de un sistema o infraestructura, causando daños directos o indirectos a la integridad de la información (Calle & Andrade, 2024).

Arquitectura de Confianza Cero (Zero Trust)

La teoría de Zero Trust rompe con el modelo tradicional de "perímetro de red", asumiendo que ninguna entidad interna o externa debe ser confiable por defecto. Todo acceso debe ser verificado continuamente mediante autenticación robusta y segmentación de red. Este enfoque es vital para proteger los sistemas de información modernos ante ataques de movimiento lateral. (Rose , & Et al., 2024)

Auditoría de Sistemas de Información

La auditoría es el examen y evaluación de los controles de TI. Teóricamente, busca proporcionar seguridad razonable de que los sistemas están alineados con los objetivos de la organización. ISACA establece los estándares para que el auditor pueda verificar que la información financiera sea precisa, confidencial y que los sistemas posean la resiliencia adecuada ante fallas o ataques. (Rodriguez, 2024)

Análisis de Vulnerabilidades y Pentesting

El análisis de vulnerabilidades es un examen sistemático para detectar fallos de seguridad. El Pentesting (prueba de penetración) es un paso más allá, donde se simula un ataque real. Teóricamente, estos procesos permiten validar la efectividad de los controles de seguridad implementados, identificando brechas que podrían ser explotadas para acceder a información financiera sensible. (OSTEC GROUP, 2021)

Blockchain para la Integridad de Datos

Blockchain ofrece un registro inmutable y descentralizado, lo que teóricamente garantiza la integridad total de los datos. En auditoría, esta tecnología permite la creación de pistas de auditoría transparentes y resistentes a la manipulación. La revisión conceptual debe explorar cómo los contratos inteligentes pueden automatizar controles y validaciones contables. (Meneses, 2024)

Base de datos: Colección ordenada de datos interconectados y se guardan de forma estructurada, permite un acceso y una gestión eficiente (Bermúdez, 2020). Existen varios tipos de bases de datos según la estructura de los datos y el uso previsto:

- **Relacionales:** Almacenan los datos en tablas relacionadas y utilizan SQL (Structured Query Language) para gestionar la información (MySQL y Oracle) (Bermúdez, 2020).
- **NoSQL:** Diseñadas para datos no estructurados, como los documentos o registros en grandes volúmenes, ideales para el big data y redes sociales (Bermúdez, 2020).
- **Bases de datos en la nube:** Las bases de datos alojadas en servidores remotos y accesibles a través de internet, utilizadas por empresas para reducir costos y mejorar la escalabilidad, permiten que las organizaciones almacenen, gestionen y recuperen grandes volúmenes de información de forma rápida y segura, siendo

esenciales en áreas como finanzas, comercio, salud y redes sociales (Bermúdez, 2020).

Biometría: Es el uso de las características físicas y de comportamiento únicas de una persona para su identificación y autenticación. Este sistema de seguridad está basado en que cada individuo tiene patrones únicos en sus huellas dactilares, rostro, iris, voz y firma. La biometría se emplea en áreas, desde desbloquear dispositivos móviles hasta sistemas de control de acceso en empresas y lugares públicos (García, 2021). Existen dos tipos principales de biometría:

- **Biometría física:** Incluye rasgos físicos como huellas dactilares, el reconocimiento facial, el iris o el patrón de la retina.
- **Biometría conductual:** Se basa en patrones de comportamiento, como la forma de teclear o la firma, mejora la seguridad y la eficiencia en el control de acceso, ya que ofrece un nivel de autenticación difícil de falsificar que las contraseñas tradicionales.

Ciberataque

Acción dirigida a comprometer la seguridad, integridad o disponibilidad de sistemas informáticos, redes y datos mediante medios digitales. Estos ataques pueden estar motivados por el robo de información, el fraude, la interrupción de servicios, o incluso el espionaje y sabotaje a nivel estatal. Los métodos de ciberataque son variados e incluyen técnicas como el phishing (engaño por medio de correos electrónicos o sitios falsos para robar información personal), ransomware (secuestro de datos mediante encriptación, donde el atacante exige un rescate para liberarlos), DDoS (ataque de denegación de servicio distribuido que inunda un servidor con solicitudes para que deje de funcionar) y malware (software malicioso), entre otros. Los ciberataques afectan tanto a individuos como a organizaciones, e

incluso infraestructuras críticas como la energía, el agua y la salud pública (García, 2021).

Ciberdelincuente

Estos pueden ser personas, organizaciones estructuradas o incluso gobiernos que emplean tecnologías para llevar a cabo acciones ilegales. Estas acciones abarcan desde el hurto de información y fraudes económicos hasta ataques a cualquier tipo de infraestructura y actividades de ciber espionaje (Jiménez, 2022).

Cifrado

Es un procedimiento criptográfico que utiliza un algoritmo matemático para "envolver" un mensaje de manera que solo el receptor autorizado pueda acceder a su contenido, usando una clave única que permite "desenvolver" el mensaje. El propósito del cifrado es garantizar que el mensaje sea ininteligible para cualquier persona que no esté involucrada en la comunicación (Álvarez, 2019).

Ciberseguridad.

La ciberseguridad se constituye como un conjunto multidimensional de políticas, tecnologías y prácticas orientadas a salvaguardar la integridad, confidencialidad y disponibilidad de los sistemas de información frente a amenazas emergentes. Dada su naturaleza estratégica, el Foro Económico Mundial la cataloga como un riesgo global capaz de comprometer infraestructuras críticas y la estabilidad económica. En este entorno de vulnerabilidad sistémica, la adopción de estándares internacionales, tales como la norma ISO 27001, resulta imperativa para formalizar sistemas de gestión de seguridad robustos, permitiendo a las organizaciones mitigar riesgos y garantizar la continuidad operativa de sus activos digitales. (PIRANI, 2026)

Ciberdelincuencia y Fraude Financiero

Este tema aborda la criminalidad en entornos digitales. La teoría del fraude (como el Triángulo de Cressey) se adapta al mundo digital: oportunidad, presión y racionalización. Los atacantes utilizan ransomware, phishing y fraude de CEO (BEC) para extraer capital. Es un tema fundamental para analizar cómo el cibercrimen afecta la estabilidad financiera de las pymes. (Financial Crimen Academy Org, 2026)

Ciberseguridad en el Sector Financiero (Fintech)

El sector financiero es el objetivo número uno de los ciberataques. La teoría en Fintech se enfoca en la seguridad de las APIs, la protección contra fraude en tiempo real y el cumplimiento de estándares como PCI-DSS para el manejo de tarjetas. Es un área que combina estrictos controles regulatorios con innovaciones tecnológicas de alta velocidad y riesgo. (MOONFLOW, 2025)

Continuidad del Negocio y Recuperación (BCP/DRP)

Los planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP) no son puramente técnicos, sino de gestión. Teóricamente, se basan en el Análisis de Impacto al Negocio (BIA), que determina la importancia de los procesos. En contabilidad, esto garantiza que, ante un ciberataque, la organización pueda recuperar sus estados financieros y registros en un tiempo aceptable. (ISO ORG, 2022)

Control de acceso

Es el proceso de otorgar permisos a usuarios o grupos para acceder a recursos como archivos en una red. Este proceso se fundamenta en tres conceptos clave: identificación, autenticación y autorización. El control de acceso puede aplicarse tanto para regular el acceso a áreas físicas como para gestionar el acceso a la información dentro de un sistema (Oliveira, 2020).

Criptografía y Seguridad de Datos

La criptografía es la ciencia de proteger la información mediante técnicas matemáticas (cifrado). Es fundamental para garantizar la confidencialidad y autenticidad en las transmisiones de datos. En el ámbito financiero, el cifrado de extremo a extremo es el estándar para proteger transacciones y datos sensibles contra interceptaciones maliciosas durante el tránsito o reposo en bases de datos. (Stallings, 2021)

Defensa en Profundidad

La teoría de la "defensa en profundidad" sostiene que una sola capa de seguridad es insuficiente. Se basa en el despliegue de múltiples controles defensivos superpuestos (físicos, técnicos y administrativos). Si un atacante vulnera una barrera, las capas subsiguientes deben detener o mitigar la amenaza. Este principio es análogo al control interno contable, donde existen múltiples filtros de validación para prevenir errores. (Group Fortinet, 2026)

Ética en la Seguridad de la Información

La ética en la ciberseguridad trasciende la legalidad; se refiere a la responsabilidad social de los profesionales de seguridad. Teóricamente, aborda dilemas sobre la privacidad versus la seguridad, el uso responsable de herramientas de hacking y la transparencia en la divulgación de vulnerabilidades. Es un eje fundamental para cualquier profesional contable que maneje información confidencial. (Gomez, 2024)

Gestión de Identidades y Accesos (IAM)

IAM se basa en el principio de "mínimo privilegio": los usuarios solo deben tener acceso a lo estrictamente necesario para su función. Teóricamente, esto incluye autenticación multifactor (MFA), gestión de ciclos de vida de usuarios y control de acceso basado en roles (RBAC). Es un pilar fundamental para evitar que una sola cuenta comprometida ponga en peligro todo el sistema contable. (Entrust, 2026)

Gestión de Incidentes de Seguridad

Este tema trata el proceso estructurado de respuesta ante una brecha (detección, contención, erradicación y recuperación). Teóricamente, busca reducir el impacto y el costo financiero de un incidente. Para una empresa, tener un protocolo definido y probado reduce significativamente las pérdidas operativas y reputacionales tras un ataque exitoso. (Cardenas, Peña, & Cardenas, 2024)

Gestión de Riesgos (COSO ERM)

El marco COSO ERM es la referencia global para la gestión de riesgos empresariales. Su relevancia en la ciberseguridad radica en integrar la gestión del riesgo tecnológico con la estrategia de negocio. Al identificar las amenazas cibernéticas como riesgos operativos y financieros, las organizaciones pueden cuantificar su impacto y asignar recursos para su mitigación efectiva dentro de los sistemas contables. (Torres, 2023)

Gobernanza de TI (COBIT)

COBIT proporciona un marco integral que permite a las empresas alcanzar sus metas de negocio mediante el gobierno y la gestión efectiva de la información y la tecnología. En ciberseguridad, COBIT ayuda a asegurar que los controles tecnológicos estén alineados con los requisitos de cumplimiento legal y de negocio, garantizando la transparencia y la rendición de cuentas en los procesos. (Joseph, 2024)

Ingeniería Social (El factor humano)

A diferencia de los ataques técnicos, la ingeniería social manipula la psicología humana para obtener acceso o información. Este tema es crucial teóricamente porque reconoce que el usuario final es el eslabón más débil. Las estrategias de mitigación incluyen capacitación continua y políticas de concienciación, siendo un

pilar necesario para proteger los sistemas de información frente al fraude.
(Cibersafety, 2025)

Inteligencia de Amenazas (Threat Intelligence)

La inteligencia de amenazas es la recolección y análisis de información sobre atacantes y sus tácticas. Teóricamente, transforma datos reactivos en conocimiento proactivo. Permite a las organizaciones anticipar ataques basándose en indicadores de compromiso (IoC) conocidos. Para una empresa, esto significa pasar de ser una víctima pasiva a una entidad preparada y alerta ante riesgos específicos. (Kosinski, 2026)

Inteligencia Artificial en Detección de Amenazas

La IA permite procesar volúmenes masivos de datos en tiempo real para identificar anomalías que el ojo humano o los sistemas de reglas tradicionales ignorarían. Teóricamente, la IA en ciberseguridad se divide en aprendizaje supervisado (detección de patrones conocidos) y no supervisado (detección de comportamientos inusuales). Es una herramienta potente contra el fraude financiero sofisticado. (Zscaler Company, 2026)

Malware

Malware, o software malicioso, engloba un programa o código diseñado al dañar, robar información o causar efectos negativos en dispositivos, redes y sistemas informáticos, puede propagarse con múltiples enlaces, archivos adjuntos, aplicaciones infectadas, o sitios web comprometidos (Jiménez, 2022). Algunos tipos comunes son:

- **Virus:** Son programas que se replican y se insertan en otros programas o archivos, propagándose cuando el usuario ejecuta esos programas (Jiménez, 2022).

- **Troyanos:** Programas legítimos, pero ocultan funciones maliciosas que permiten al atacante controlar el sistema afectado (Jiménez, 2022).
- **Ransomware:** Cifra los datos del usuario y exige un pago para restaurar el acceso y devolver las contraseñas de acceso que han sido cambiadas (Jiménez, 2022).
- **Spyware:** Programa que se instala en el dispositivo para espiar la actividad del usuario y robar información sensible. El malware es una de las principales amenazas a la seguridad digital y puede ocasionar desde la pérdida de datos personales hasta daños significativos en redes empresariales (Jiménez, 2022).

Marco de Ciberseguridad del NIST (NIST CSF)}

El NIST CSF proporciona un lenguaje común para gestionar el riesgo de ciberseguridad. Sus cinco funciones Identificar, Proteger, Detectar, Responder y Recuperar ofrecen un enfoque estructurado y flexible que permite a las organizaciones alinear sus actividades de ciberseguridad con las metas de negocio. Es fundamental en la gestión de auditoría tecnológica para medir la madurez de los controles implementados. (NIST CSF, 2026)

Modelo CIA (Confidentiality, Integrity, Availability).

En la literatura especializada sobre seguridad de la información, el modelo de la tríada CID o CIA, que comprende la Confidencialidad, la Integridad y la Disponibilidad se erige como el eje transversal para el diseño, implementación y evaluación de sistemas de seguridad robustos. Esta estructura conceptual no solo facilita la segmentación de objetivos de protección, sino que proporciona una metodología sistemática para el diagnóstico de vulnerabilidades y la formulación de estrategias de mitigación. En el ámbito organizacional, la preservación equilibrada de estos tres pilares es determinante para garantizar la continuidad operativa y la resiliencia de los sistemas; por tanto, cuando una entidad alcanza un nivel de

cumplimiento óptimo en estos criterios, su arquitectura de seguridad se consolida, dotándola de una mayor capacidad de respuesta técnica y estratégica frente a incidentes o ciber amenazas emergentes. (Fortinet, 2026)

Privacidad de Datos y Normativas (GDPR / Ley 1581)

La protección de datos personales es un imperativo legal. La teoría se centra en el consentimiento, la minimización de datos y el derecho al olvido. Para un sistema de información, esto implica implementar controles técnicos como el anonimato, la seudonimización y el cifrado, garantizando que el tratamiento de datos cumpla con la regulación colombiana (Ley 1581) y estándares internacionales. (Superintendencia de Industria y Comercio, 2026)

Resiliencia Cibernética

La resiliencia cibernética es la capacidad de una organización para resistir, absorber, recuperarse y adaptarse ante un incidente adverso. Teóricamente, va más allá de la "seguridad" tradicional, aceptando que las brechas son inevitables. Se enfoca en minimizar el tiempo de inactividad y mantener las operaciones críticas — como la facturación o nómina— funcionando, aunque sea en modo degradado. (Gonzalez, 2025)

Riesgos en las finanzas y la contabilidad asociados a la falta de Ciberseguridad

La carencia de ciberseguridad en sistemas contables trasciende lo técnico, convirtiéndose en un riesgo financiero crítico que compromete la integridad de los estados financieros y la continuidad operativa. Amenazas como el fraude por suplantación (BEC), la manipulación de registros y el secuestro de datos (ransomware) impactan directamente la liquidez y el cumplimiento legal. En consecuencia, la gestión de riesgos cibernéticos debe integrarse al control interno

organizacional para asegurar la sostenibilidad y salvaguardar la veracidad de la información financiera. (Pihel, 2025)

Sistema de Gestión de Seguridad de la Información (ISO/IEC 27001)

La norma ISO 27001 establece los requisitos para un SGSI. Su valor teórico reside en el enfoque basado en procesos y la mejora continua mediante el ciclo Plan-Do-Check-Act (PDCA). Para una entidad, adoptar este estándar significa sistematizar la seguridad, convirtiéndola en una práctica de gestión auditable y medible, lo cual es esencial para demostrar cumplimiento frente a terceros. (ISO ORG, 2022)

Sistemas de información

Los sistemas de información constituyen un entramado estructurado de personas, procesos y recursos tecnológicos orientados a la administración integral de datos. Su función principal radica en la recolección, clasificación y procesamiento de información, transformándola en un activo recuperable y de fácil consulta. Mediante la interacción organizada de sus componentes, estos sistemas optimizan el flujo informativo, siendo indispensables para la gestión estratégica tanto en organizaciones empresariales como gubernamentales. Su adaptabilidad permite su despliegue en diversos entornos, garantizando la disponibilidad y utilidad del conocimiento. (Grupo Concepto, 2026)

Seguridad del Internet de las Cosas (IoT)

El IoT introduce riesgos sin precedentes debido a la vasta superficie de ataque que generan millones de dispositivos interconectados con capacidad de procesamiento limitado. La teoría de la seguridad en IoT se enfoca en autenticación de dispositivos, actualización de firmware y segmentación para evitar que un dispositivo comprometido (ej. una cámara) sirva de puerta de entrada a la red contable. (Sikdar, 2021)

Seguridad en la Nube (Cloud Security)

La adopción de servicios en la nube requiere una revisión teórica sobre el "modelo de responsabilidad compartida". En este esquema, el proveedor (como AWS o Azure) se encarga de la seguridad *de* la nube, mientras que el cliente es responsable de la seguridad *en* la nube (datos, identidades, configuraciones). Comprender esta distinción es vital para la auditoría de sistemas alojados en plataformas externas. (Fortinet, 2026)

Seguridad en Redes y Protocolos

La seguridad de redes protege la infraestructura que transporta la información. Los fundamentos teóricos incluyen el uso de Firewalls, sistemas de detección de intrusos (IDS), sistemas de prevención (IPS) y VPNs. En contabilidad, asegurar la red es indispensable para proteger el flujo de datos entre sucursales o hacia la nube, garantizando que no haya intercepciones no autorizadas. (Kurose & Ross, 2023)

Tecnologías financieras

Aplicación de tecnologías en el ámbito de los servicios. También, describen esta variable como empresas tecnológicas financieras que ofrecen soluciones e innovaciones al sector financiero, con el objetivo de proporcionar nuevos productos y servicios que se alineen con la transformación digital (Castellanos, 2020).

3 DISEÑO DE LA INVESTIGACION

3.1 TIPO DE INVESTIGACIÓN

La investigación es de tipo exploratorio y descriptivo, debido a que busca profundizar en la comprensión de los fundamentos teóricos de la ciberseguridad aplicados a los sistemas de información, identificando conceptos, características, riesgos, amenazas y mecanismos de protección presentes en la literatura especializada. El carácter exploratorio permite aproximarse a un campo de estudio en constante evolución, mientras que el alcance descriptivo facilita la identificación y organización de sus principales componentes y características (Vizcaíno et al., 2023). A su vez, la investigación descriptiva permitirá sistematizar los conocimientos encontrados sobre la relación entre ciberseguridad, sistemas de información, gestión de riesgos y protección de los activos de información (Arias & Covinos, 2021).

3.2 ENFOQUE DE INVESTIGACIÓN

El proyecto adopta un enfoque cualitativo, debido a que se fundamenta en la revisión, interpretación y análisis de información documental relacionada con los fundamentos de la ciberseguridad en los sistemas de información. Este enfoque permitirá comprender los conceptos, principios, amenazas, vulnerabilidades, riesgos y mecanismos de protección a partir de diferentes perspectivas teóricas y técnicas. Para ello, se analizarán artículos científicos, libros académicos, normas, estándares internacionales, informes técnicos y documentos institucionales que permitan comprender la evolución y aplicación de la ciberseguridad en los sistemas de información (Arias & Covinos, 2021).

3.3 MÉTODO DE INVESTIGACIÓN

El método de investigación será analítico, dado que permitirá descomponer la información recopilada en sus principales elementos conceptuales para posteriormente establecer relaciones entre ciberseguridad, sistemas de información, activos de información, amenazas, vulnerabilidades, riesgos y controles de seguridad. Este procedimiento facilitará la identificación de semejanzas, diferencias y aportes de los diferentes referentes consultados, permitiendo construir una visión integrada de los fundamentos teóricos de la ciberseguridad (Vizcaíno et al., 2023).

Asimismo, el análisis de fuentes secundarias permitirá interpretar los planteamientos encontrados en la literatura especializada y establecer categorías conceptuales relacionadas con la identificación de riesgos, protección de la información, prevención de incidentes, gestión de la seguridad y continuidad de las operaciones. De esta manera, el método analítico contribuirá a organizar los conocimientos existentes y determinar los principales fundamentos que sustentan la ciberseguridad dentro de los sistemas de información (Arias & Covinos, 2021).

3.4 TÉCNICAS DE INVESTIGACIÓN

La principal técnica de investigación será la revisión documental, mediante la recopilación, selección, clasificación y análisis de fuentes secundarias relacionadas con la ciberseguridad y los sistemas de información. Se consultarán artículos científicos, libros, documentos académicos, informes técnicos, estándares internacionales, normativas y publicaciones de organismos especializados, priorizando fuentes pertinentes y actualizadas que permitan sustentar conceptualmente el objeto de estudio (Vizcaíno et al., 2023).

La información recopilada será organizada de acuerdo con categorías previamente definidas, entre ellas: fundamentos de ciberseguridad, sistemas de información, activos de información, amenazas, vulnerabilidades, riesgos, controles de

seguridad y mecanismos de protección. Posteriormente, se realizará un proceso de análisis e interpretación de los contenidos con el propósito de identificar los principales aportes teóricos y establecer relaciones entre las diferentes categorías estudiadas. Este procedimiento permitirá construir una base conceptual organizada que contribuya a comprender el papel de la ciberseguridad en la protección y funcionamiento de los sistemas de información (Arias & Covinos, 2021).

4 DESARROLLO DEL TRABAJO DE GRADO

El desarrollo del trabajo de grado “Fundamentos teóricos de la ciberseguridad en los sistemas de información: una revisión conceptual” se estructura en tres etapas, articuladas con los objetivos específicos planteados. El desarrollo se fundamenta en una revisión bibliográfica y documental orientada a identificar, analizar, organizar e interpretar los principales conceptos relacionados con la ciberseguridad, su evolución, su relación con el cumplimiento normativo y sus efectos en la protección de la información y el funcionamiento de los sistemas de información financieros.

ETAPA I. FUNDAMENTOS CONCEPTUALES Y EVOLUCIÓN DE LA CIBERSEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Objetivo relacionado

Comprender los conceptos clave y la evolución de la ciberseguridad en los sistemas de información, mediante la revisión de literatura académica, para abarcar su aplicabilidad en los sistemas de información.

En esta primera etapa se realizará una revisión de literatura académica, técnica e institucional con el propósito de establecer los fundamentos conceptuales de la ciberseguridad. Se abordarán conceptos como ciberseguridad, seguridad de la información, sistemas de información, activos de información, amenazas, vulnerabilidades, riesgos, incidentes de seguridad y controles de protección.

El análisis permitirá diferenciar la ciberseguridad de conceptos relacionados, pero no necesariamente equivalentes, como seguridad informática y seguridad de la información. De esta manera, se busca construir una base conceptual que permita comprender la función de la ciberseguridad dentro de las organizaciones y su relación con la protección de los recursos tecnológicos y de información.

Posteriormente, se estudiará la evolución de la ciberseguridad, considerando la transición desde enfoques centrados principalmente en la protección de infraestructura tecnológica hacia modelos integrales de gestión del riesgo. Esta evolución permitirá reconocer la influencia de fenómenos como la transformación digital, la computación en la nube, la interconexión de sistemas, la inteligencia artificial y el crecimiento de las amenazas cibernéticas.

También se analizarán los principios fundamentales de protección de la información, especialmente la confidencialidad, integridad y disponibilidad, junto con otros elementos relacionados con autenticidad, trazabilidad y continuidad operativa.

Como resultado de esta etapa se elaborará un marco conceptual de los fundamentos de la ciberseguridad, acompañado de una matriz de revisión bibliográfica y un esquema que represente la relación entre sistemas de información, activos, amenazas, vulnerabilidades, riesgos y controles de seguridad.

ETAPA II. CIBERSEGURIDAD Y CUMPLIMIENTO NORMATIVO

Objetivo relacionado

Identificar la relación entre la ciberseguridad y el cumplimiento normativo en los sistemas de información, a través del análisis teórico, con la finalidad de determinar su contribución a la integridad y legalidad de los procesos contables y financieros.

En la segunda etapa se analizará la relación existente entre la ciberseguridad y el cumplimiento de disposiciones legales, normativas y estándares relacionados con la protección de la información. El análisis permitirá identificar cómo los mecanismos de seguridad contribuyen a establecer condiciones de control sobre los sistemas de información y sobre los datos utilizados en los procesos organizacionales.

La revisión considerará referentes normativos y técnicos relacionados con la seguridad de la información, la protección de datos, la gestión de riesgos y los controles tecnológicos. Se estudiará especialmente la manera en que estos instrumentos orientan a las organizaciones en aspectos como gestión de accesos, protección de datos, gestión de incidentes, continuidad operativa, identificación de riesgos, monitoreo y control.

En el ámbito de los sistemas de información financieros y contables, se analizará la importancia de garantizar que los datos sean íntegros, confiables, disponibles y trazables. La aplicación de controles de ciberseguridad puede contribuir a reducir riesgos asociados con alteraciones no autorizadas, pérdida de información, accesos indebidos, fraude y fallas que afecten la generación de información financiera.

Esta etapa permitirá establecer una relación conceptual entre ciberseguridad, control interno, cumplimiento normativo, protección de datos e integridad de la información financiera, sin limitar el análisis a una única normativa o sector económico.

El resultado de esta etapa será una matriz de relación entre ciberseguridad y cumplimiento normativo, en la cual se establecerán las principales categorías normativas, riesgos asociados, controles de seguridad y contribuciones a la integridad, confiabilidad y protección de la información contable y financiera.

ETAPA III. VENTAJAS Y DESVENTAJAS DE LAS MEDIDAS DE CIBERSEGURIDAD

Objetivo relacionado

Describir las ventajas y desventajas de la implementación de medidas de ciberseguridad en los sistemas de información financieros, mediante un estudio bibliográfico, con el fin de evaluar su impacto en la protección de la información, la eficiencia operativa y el cumplimiento regulatorio.

En la tercera etapa se realizará un análisis bibliográfico orientado a identificar las principales ventajas y desventajas asociadas con la implementación de medidas de ciberseguridad en los sistemas de información, con especial atención a aquellos utilizados para gestionar información financiera y contable.

Entre las ventajas se analizarán aspectos relacionados con la protección de los activos de información, reducción de riesgos, prevención de accesos no autorizados, fortalecimiento de la integridad de los datos, continuidad operativa, confianza de los usuarios, cumplimiento de requisitos y apoyo a la toma de decisiones.

De igual manera, se estudiarán las posibles limitaciones y desafíos derivados de la implementación de estas medidas. Entre ellos se podrán considerar los costos de implementación y mantenimiento, necesidad de capacitación, complejidad tecnológica, resistencia al cambio, actualización permanente de controles, dependencia de personal especializado y posibles dificultades de integración entre sistemas.

El análisis no buscará establecer una valoración general, sino identificar, a partir de la literatura revisada, las diferentes perspectivas existentes sobre los efectos de las medidas de ciberseguridad. De esta manera, se podrá comprender que su implementación implica tanto oportunidades para fortalecer los sistemas de información como desafíos organizacionales, tecnológicos y económicos que deben ser gestionados.

Como producto final se elaborará una matriz de ventajas y desventajas de la ciberseguridad en los sistemas de información financieros, organizada en las dimensiones de protección de la información, eficiencia operativa y cumplimiento regulatorio.

INTEGRACIÓN DE LAS TRES ETAPAS

Las tres etapas se desarrollarán de manera articulada. La Etapa I permitirá establecer los fundamentos conceptuales y comprender la evolución de la ciberseguridad; la Etapa II permitirá relacionar dichos fundamentos con el cumplimiento normativo y la protección de la información contable y financiera; finalmente, la Etapa III permitirá identificar las ventajas y desventajas asociadas con la implementación de medidas de ciberseguridad en los sistemas de información financieros.

Como resultado de la integración de las tres etapas, se obtendrá una revisión conceptual estructurada de los fundamentos de la ciberseguridad en los sistemas de información, que permitirá comprender sus principales componentes, su relación con el cumplimiento normativo y sus implicaciones para la protección de la información y el funcionamiento de los sistemas financieros y contables.

5 RESULTADOS

El presente trabajo de grado, titulado “Fundamentos teóricos de la ciberseguridad en los sistemas de información: una revisión conceptual”, se desarrolla mediante tres fases articuladas que permiten abordar de manera progresiva el objeto de estudio. La primera fase está orientada a comprender los conceptos fundamentales y la evolución de la ciberseguridad en los sistemas de información, a partir de la revisión de literatura académica. La segunda fase busca identificar la relación entre la ciberseguridad y el cumplimiento normativo, considerando su importancia para la integridad y legalidad de los procesos contables y financieros. Finalmente, la tercera fase se centra en describir las ventajas y desventajas de implementar medidas de ciberseguridad, con el propósito de analizar sus efectos sobre la protección de la información, la eficiencia operativa y el cumplimiento regulatorio. En conjunto, estas fases permiten construir una revisión conceptual integral que contribuya a comprender la importancia de la ciberseguridad en la gestión y protección de los sistemas de información.

FASE I

La primera etapa del trabajo de grado se orienta a establecer los fundamentos teóricos y conceptuales que permiten comprender la ciberseguridad dentro de los sistemas de información. Para ello, se realiza una revisión documental de fuentes académicas, técnicas e institucionales recientes, con énfasis en publicaciones posteriores a 2021. El análisis parte de reconocer que los sistemas de información constituyen estructuras en las cuales interactúan personas, procesos, tecnologías, datos y recursos destinados a recopilar, procesar, almacenar y distribuir información. En este contexto, la ciberseguridad debe comprenderse como un componente transversal de la gestión del riesgo y de la protección de los activos de información.

La ISO/IEC 27001:2022 establece requisitos para los sistemas de gestión de seguridad de la información y plantea un enfoque orientado a establecer, implementar,

mantener y mejorar continuamente la seguridad de la información dentro de las organizaciones. Desde esta perspectiva, la protección no se limita a los recursos tecnológicos, sino que comprende los procesos organizacionales y las medidas necesarias para gestionar los riesgos que pueden afectar la información (International Organization for Standardization [ISO], 2022).

CONCEPTOS FUNDAMENTALES Y EVOLUCIÓN DE LA CIBERSEGURIDAD.

Importancia de la ciberseguridad en el contexto actual

La ciberseguridad constituye un componente fundamental para la protección de los sistemas de información, especialmente en un contexto caracterizado por la creciente digitalización de los procesos organizacionales. Su evolución ha estado estrechamente relacionada con el desarrollo de nuevas tecnologías y con la incorporación de sistemas digitales para el almacenamiento, procesamiento y transmisión de información. En este escenario, las organizaciones han incrementado su dependencia de los sistemas de información, generando la necesidad de establecer mecanismos que permitan proteger los datos y garantizar su adecuado funcionamiento frente a las diferentes amenazas cibernéticas (Calle & Andrade, 2024).

La transformación digital ha generado nuevas oportunidades para mejorar la eficiencia y disponibilidad de la información; sin embargo, también ha incrementado la exposición de las organizaciones a riesgos asociados con ataques informáticos, robo de información, ransomware, fraudes electrónicos y accesos no autorizados. Estas amenazas pueden afectar principios fundamentales de la seguridad de la información, particularmente la confidencialidad, integridad y disponibilidad de los datos, ocasionando consecuencias operativas, financieras, legales y reputacionales para las organizaciones (Castellanos, 2020). Por esta razón, el estudio de la ciberseguridad requiere comprender

no solamente las amenazas existentes, sino también los fundamentos conceptuales, mecanismos de protección y estrategias utilizadas para gestionar los riesgos asociados con los sistemas de información.

Desde esta perspectiva, los sistemas de información representan un elemento esencial para la gestión organizacional, debido a que permiten recopilar, procesar, almacenar y distribuir información necesaria para el desarrollo de las actividades empresariales y para la toma de decisiones. En particular, los sistemas vinculados con procesos contables y financieros manejan información de carácter sensible, cuya alteración, pérdida o divulgación no autorizada puede afectar la confiabilidad de los registros, la toma de decisiones y el cumplimiento de las obligaciones legales y regulatorias. En consecuencia, la ciberseguridad adquiere especial importancia como mecanismo para fortalecer la protección de la información y reducir los riesgos derivados del entorno digital (Rivera, 2019).

En este sentido, los fundamentos teóricos de la ciberseguridad comprenden conceptos relacionados con la protección de activos de información, gestión de riesgos, controles de seguridad, prevención de incidentes y respuesta ante amenazas. Su estudio permite establecer una base conceptual para comprender cómo las organizaciones pueden enfrentar los desafíos derivados de la transformación digital y fortalecer la seguridad de sus sistemas de información. Asimismo, el análisis de la literatura permite identificar la evolución del concepto de ciberseguridad y su aplicación en diferentes contextos organizacionales, incluyendo los procesos contables y financieros.

Por lo anterior, el presente apartado tiene como propósito desarrollar una revisión conceptual de los fundamentos teóricos de la ciberseguridad en los sistemas de información, abordando su definición, evolución, principales conceptos asociados, riesgos y mecanismos de protección. De esta manera, se busca establecer una base teórica que permita comprender la importancia de la ciberseguridad para la protección de

la información, la continuidad de los procesos organizacionales y el fortalecimiento de la gestión de los sistemas de información.

Conceptos fundamentales de la ciberseguridad

En efecto, la evolución de la ciberseguridad ha estado estrechamente relacionada con el desarrollo de las tecnologías de la información, la transformación digital y la creciente interconexión de los sistemas organizacionales. A medida que las organizaciones incorporan plataformas digitales para almacenar, procesar y transmitir información, también aumenta su exposición a diferentes tipos de amenazas y vulnerabilidades. En este contexto, la ciberseguridad ha evolucionado desde enfoques centrados principalmente en la protección técnica de redes y equipos hacia perspectivas integrales que incorporan la gestión de riesgos, los controles organizacionales y la protección de los activos de información (Calle & Andrade, 2024).

Desde una perspectiva teórica, diferentes estándares y marcos internacionales han contribuido a consolidar los fundamentos para la gestión de la seguridad de los sistemas de información. Entre los principales referentes se encuentran:

ISO/IEC 27001: establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la identificación, evaluación y tratamiento de los riesgos que pueden afectar los activos de información. Este enfoque permite establecer políticas, controles y procesos orientados a preservar la seguridad de la información dentro de las organizaciones (Culot et al., 2021).

NIST: el National Institute of Standards and Technology ha desarrollado marcos de referencia para orientar a las organizaciones en la gestión de los riesgos de ciberseguridad. Su enfoque contempla funciones fundamentales relacionadas con la identificación de activos y riesgos, la implementación de medidas de protección, la detección de eventos, la respuesta ante incidentes y la recuperación de las capacidades

afectadas. Estas funciones permiten comprender la ciberseguridad como un proceso continuo de gestión y reducción del riesgo (Runtuwene et al., 2024).

CIS Controls: los controles desarrollados por el Center for Internet Security constituyen un conjunto de prácticas orientadas a fortalecer la protección de sistemas, redes y activos tecnológicos. Estos controles permiten abordar aspectos como la gestión de activos, la administración de vulnerabilidades, el control de accesos y la protección frente a diferentes amenazas cibernéticas (Sedano & Salman, 2021).

COBIT: el marco Control Objectives for Information and Related Technologies proporciona principios y prácticas para la gobernanza y gestión de las tecnologías de la información. Su importancia dentro de los fundamentos de la ciberseguridad radica en la articulación entre los objetivos organizacionales, la gestión de riesgos, los controles tecnológicos y el uso responsable de la información (Culot et al., 2021).

La existencia de estos marcos permite comprender que la ciberseguridad no constituye exclusivamente un conjunto de herramientas tecnológicas, sino un proceso integral que involucra personas, procedimientos, tecnologías, controles y mecanismos de gestión de riesgos. Desde esta perspectiva, la protección de los sistemas de información requiere establecer medidas que permitan anticipar, prevenir, identificar y responder ante situaciones que puedan comprometer los activos de información.

Dentro de los fundamentos conceptuales de la ciberseguridad adquieren especial relevancia los principios de confidencialidad, integridad y disponibilidad, conocidos como la tríada CIA (Confidentiality, Integrity and Availability). La confidencialidad busca evitar el acceso no autorizado a la información; la integridad procura preservar la exactitud y consistencia de los datos; y la disponibilidad pretende asegurar que la información y los sistemas se encuentren accesibles para los usuarios autorizados cuando sean requeridos. Estos principios constituyen una base conceptual para analizar las condiciones de seguridad de los sistemas de información (Calle & Andrade, 2024).

A estos principios se articulan otros conceptos fundamentales, entre ellos la autenticación, orientada a verificar la identidad de los usuarios; el control de acceso, relacionado con la autorización de recursos y operaciones; el no repudio, asociado con la posibilidad de demostrar la participación de un usuario en una determinada acción; y la gestión del riesgo, mediante la cual se identifican amenazas, vulnerabilidades y posibles impactos para establecer medidas de tratamiento. En conjunto, estos elementos permiten estructurar una visión integral de la ciberseguridad y comprender su importancia en la protección de los sistemas de información (Calle & Andrade, 2024).

Por consiguiente, la revisión conceptual de estos referentes permite establecer que los fundamentos de la ciberseguridad se sustentan en la articulación entre principios de seguridad de la información, gestión de riesgos, controles tecnológicos, gobernanza y respuesta ante incidentes. Esta perspectiva proporciona una base teórica para analizar la evolución de la ciberseguridad y su aplicación en los diferentes sistemas de información utilizados por las organizaciones, incluyendo aquellos relacionados con los procesos administrativos, contables y financieros.

Tabla 2. Conceptos fundamentales de ciberseguridad.

Concepto	Descripción
Confidencialidad	Asegurar que la información solo sea accesible por las entidades autorizadas. Evitar la divulgación no autorizada de datos (Gomero & Sánchez, 2024).
Integridad	Garantizar que la información y los sistemas se mantengan precisos, completos y sin alteraciones no autorizadas (Azcona, 2024).
Disponibilidad	Asegurar que los usuarios autorizados tengan acceso confiable a la información y los recursos cuando lo necesiten (Almario, 2022).
Autenticación	Verificar la identidad de un usuario, dispositivo o sistema para controlar el acceso a los recursos (Wang & Han, 2023).
No repudio	Impedir que una entidad pueda negar haber realizado una acción o transacción específica (Almario, 2022).
Gestión de riesgos	Identificar, analizar y mitigar los riesgos de seguridad a los que están expuestos los sistemas e información (Wang & Han, 2023).

Fuente: (elaboración propia, 2024).

Diferenciación entre seguridad informática y ciberseguridad.

Los fundamentos de la ciberseguridad en los sistemas de información se sustentan en un conjunto de principios orientados a preservar la protección y confiabilidad de los datos y recursos tecnológicos. Entre estos principios se encuentra la confidencialidad, entendida como la condición que permite restringir el acceso a la información únicamente a usuarios, procesos o entidades autorizadas. La integridad, por su parte, busca garantizar que los datos permanezcan completos, exactos y consistentes durante su almacenamiento, procesamiento y transmisión, evitando modificaciones, alteraciones, pérdidas o destrucciones no autorizadas. Finalmente, la disponibilidad hace referencia a la capacidad de los sistemas y de la información para permanecer accesibles y utilizables por los usuarios autorizados cuando sean requeridos (Ortega, 2024).

A estos principios se incorporan otros elementos esenciales para la protección de los sistemas de información. La autenticación constituye el proceso mediante el cual se verifica la identidad de un usuario o entidad antes de permitirle acceder a determinados recursos, utilizando mecanismos como credenciales, contraseñas u otros factores de autenticación (García, 2021). El no repudio permite disponer de mecanismos que aporten evidencia sobre la autoría o participación de una entidad en una determinada acción o transacción, dificultando que posteriormente pueda negar dicha participación. Por su parte, la gestión de riesgos comprende un proceso sistemático de identificación, análisis, evaluación y tratamiento de los riesgos que pueden afectar los activos de información, con el propósito de establecer medidas de protección acordes con las amenazas y vulnerabilidades identificadas (Ortega, 2024).

La articulación de estos principios permite comprender la ciberseguridad como un enfoque integral para la protección de los sistemas de información. Su aplicación no se limita a la implementación de herramientas tecnológicas, sino que involucra políticas, procedimientos, controles, personas y mecanismos de gestión orientados a prevenir, detectar y responder ante situaciones que puedan comprometer la información. Desde esta perspectiva, la confidencialidad, integridad y disponibilidad constituyen una base conceptual para evaluar las condiciones de seguridad de los sistemas y establecer medidas orientadas a fortalecer su protección.

Asimismo, resulta pertinente diferenciar los conceptos de seguridad informática y ciberseguridad. Caamaño y Gil (2020) señalan que la seguridad informática se encuentra principalmente relacionada con la protección de los sistemas tecnológicos, dispositivos, redes y recursos informáticos frente a diferentes riesgos. La ciberseguridad, en cambio, presenta un campo de acción más amplio frente a las amenazas originadas o desarrolladas en el entorno digital, incorporando aspectos relacionados con la protección de la información, la privacidad, la gestión de riesgos, el cumplimiento de requisitos y la capacidad de las organizaciones para responder y recuperarse ante incidentes cibernéticos.

En consecuencia, la revisión de estos conceptos permite establecer que la ciberseguridad en los sistemas de información debe comprenderse como un proceso multidimensional, en el que convergen principios de protección de la información, mecanismos de identificación y autenticación, control de accesos, gestión de riesgos y capacidad de respuesta. Esta perspectiva constituye uno de los fundamentos teóricos necesarios para analizar la evolución y aplicabilidad de la ciberseguridad en los diferentes contextos organizacionales y, posteriormente, comprender su relación con los procesos contables, financieros y administrativos.

Evolución de la ciberseguridad

La evolución de la ciberseguridad se encuentra estrechamente relacionada con el desarrollo de las tecnologías de la información y con el proceso de digitalización de las actividades organizacionales. Durante la década de 1980, la incorporación de los computadores personales representó un cambio significativo en la forma de almacenar, procesar y administrar información. En el ámbito empresarial, estos avances facilitaron la automatización de procesos administrativos, contables y financieros y sentaron las bases para el desarrollo de sistemas de información orientados a la gestión organizacional (Salazar & Rodríguez, 2020). Paralelamente, comenzaron a evidenciarse vulnerabilidades asociadas con la interconexión de los sistemas, generando la necesidad de establecer mecanismos para proteger la información y los recursos tecnológicos (Calle & Andrade, 2024).

Durante la década de 1990, la expansión de Internet incrementó significativamente la conectividad entre organizaciones, usuarios y sistemas de información. Esta transformación permitió mejorar el intercambio y disponibilidad de los datos, pero también amplió la superficie de exposición frente a amenazas digitales. En este periodo adquirieron mayor importancia mecanismos de protección como los firewalls, los programas antivirus y los controles de acceso, orientados a prevenir accesos no autorizados y reducir los riesgos asociados con la utilización de redes y sistemas conectados. La necesidad de preservar la confidencialidad, integridad y disponibilidad de la información se consolidó progresivamente como uno de los fundamentos de la seguridad de los sistemas de información (Muñoz et al., 2019).

A partir de la década de 2000, la expansión del comercio electrónico, las transacciones digitales y los servicios basados en Internet generó una mayor dependencia organizacional de los sistemas de información. En consecuencia, la protección de los datos dejó de considerarse exclusivamente un asunto técnico y

comenzó a relacionarse con la gestión de riesgos, el control interno, la privacidad y el cumplimiento de disposiciones legales y regulatorias. En este contexto, la ciberseguridad adquirió una dimensión organizacional, debido a que las amenazas podían afectar no solamente la infraestructura tecnológica, sino también la continuidad de las operaciones, la información financiera, las relaciones con los usuarios y la reputación institucional (Calle & Andrade, 2024).

Un referente importante de este proceso fue la promulgación de la Ley Sarbanes-Oxley (SOX) de 2002 en Estados Unidos, como respuesta a importantes escándalos corporativos y a la necesidad de fortalecer los controles relacionados con la información financiera. Aunque la norma no constituye propiamente un estándar de ciberseguridad, su énfasis en el control interno, la confiabilidad de la información financiera y la trazabilidad de los procesos contribuyó a fortalecer la necesidad de establecer controles sobre los sistemas que soportan los procesos empresariales y financieros (Motañez, 2019). De esta manera, la evolución de los sistemas de información ha generado una mayor integración entre tecnología, control interno, gestión de riesgos y confiabilidad de la información.

En relación con las Normas Internacionales de Información Financiera (NIIF), estas establecen principios y requerimientos para la preparación y presentación de información financiera útil, comparable y fiable para los usuarios de los estados financieros. Por tanto, su relación con la ciberseguridad puede analizarse de manera indirecta, en la medida en que los sistemas de información utilizados para generar información financiera deben permitir mantener registros confiables y trazables. En este sentido, la protección de los sistemas frente a modificaciones no autorizadas, pérdida de información o accesos indebidos constituye un elemento relevante para preservar la calidad de la información generada por los sistemas contables (Chai & Zolkipli, 2021; Oliveira, 2020).

A partir de la década de 2010, la ciberseguridad adquirió una dimensión aún más amplia debido a la aparición y consolidación de tecnologías como la computación en la nube, el análisis de grandes volúmenes de datos, la inteligencia artificial, el Internet de las cosas y blockchain. Paralelamente, las amenazas cibernéticas se hicieron más complejas, lo que llevó a las organizaciones a adoptar enfoques de seguridad basados en la gestión permanente del riesgo y en la necesidad de verificar continuamente los accesos y las actividades realizadas dentro de los sistemas. Dentro de estos enfoques se encuentra el modelo de confianza cero (Zero Trust), cuya premisa consiste en no asumir confianza implícita por la ubicación o procedencia de un usuario o dispositivo y en verificar de manera continua las solicitudes de acceso a los recursos (Oliveira, 2020).

En este proceso evolutivo, las nuevas tecnologías han generado tanto oportunidades como desafíos para la protección de los sistemas de información. La computación en la nube, por ejemplo, permite acceder a aplicaciones y datos desde diferentes ubicaciones y facilita la escalabilidad de los servicios tecnológicos. En el ámbito contable, las plataformas de software como servicio han permitido automatizar procesos y facilitar el acceso remoto a la información financiera. Sin embargo, también requieren mecanismos adecuados de autenticación, control de accesos, cifrado, gestión de vulnerabilidades y protección de datos, debido a la exposición que implica el procesamiento de información en entornos conectados (Kumar & Bhatia, 2020).

De igual manera, el desarrollo del Big Data y la inteligencia artificial ha transformado la capacidad de las organizaciones para procesar grandes volúmenes de información y detectar patrones que pueden ser utilizados en la gestión empresarial y financiera. Estas tecnologías pueden contribuir a la identificación de comportamientos inusuales, detección de posibles fraudes, automatización de procesos y apoyo a las actividades de auditoría (Almeida et al., 2024). No obstante, su utilización también plantea desafíos relacionados con la privacidad, seguridad, calidad y gobernanza de los datos,

particularmente cuando se procesan grandes cantidades de información sensible (Castellanos, 2020).

Por otra parte, la tecnología blockchain ha introducido nuevas posibilidades para el registro y trazabilidad de las transacciones mediante estructuras de información distribuidas. Su aplicación en procesos contables y de auditoría ha sido estudiada debido a características como la trazabilidad de las operaciones, la utilización de mecanismos criptográficos y la dificultad de modificar registros una vez incorporados a la cadena. Estas características han generado interés en su posible utilización para fortalecer determinados procesos de registro, verificación y auditoría de información (Vega, 2021).

En consecuencia, la evolución de la ciberseguridad puede comprenderse como un proceso que ha transitado desde la protección básica de computadores y redes hacia un enfoque integral de gestión de riesgos, protección de activos de información, gobernanza tecnológica, continuidad operativa y resiliencia digital. Este proceso ha sido impulsado tanto por la transformación tecnológica como por el crecimiento y sofisticación de las amenazas cibernéticas. En los sistemas de información actuales, la ciberseguridad requiere, por tanto, una visión que integre tecnologías, personas, procesos y controles organizacionales.

Desde la perspectiva de esta revisión conceptual, comprender dicha evolución resulta fundamental para establecer los fundamentos teóricos de la ciberseguridad y explicar su aplicabilidad en los sistemas de información contemporáneos. Asimismo, permite reconocer que tecnologías como la nube, la inteligencia artificial, Big Data y blockchain no deben analizarse únicamente por sus beneficios funcionales, sino también desde los riesgos de seguridad, privacidad, integridad y disponibilidad que pueden generar. De esta manera, la evolución histórica y tecnológica constituye una base para comprender los desafíos actuales de la protección de la información en las

organizaciones y, particularmente, en los sistemas que soportan procesos administrativos, contables y financieros.

Revisión de literatura sobre ciberseguridad en la contabilidad

Tabla 3. Antecedentes sobre el impacto de la ciberseguridad en la contabilidad.

TÍTULO	AUTOR(ES)	AÑO	RIESGOS CIBERNÉTICOS
RIESGOS INFORMÁTICOS Y ALTERNATIVAS PARA LA SEGURIDAD INFORMÁTICA EN SISTEMAS CONTABLES EN COLOMBIA.	Muñoz, H.; Zapata, L.; Requena, D.; Ricardo, L.	2019	Destaca los principales riesgos informáticos en sistemas contables y propone estrategias de mitigación en el contexto colombiano.
RIESGOS DE CIBERSEGURIDAD Y SUS CONSECUENCIAS EN LA PREVENCIÓN DE FRAUDES EN LAS EMPRESAS INDUSTRIALES DEL DISTRITO DE YANACANCHA – PASCO 2016.	Dávila, R.; Oscar, A.	2019	Examina cómo los ataques cibernéticos pueden facilitar el fraude en empresas industriales y la necesidad de controles robustos.
CIBERSEGURIDAD Y RIESGO OPERACIONAL EN LAS ORGANIZACIONES.	Martínez, N.	2019	Analiza la relación entre ciberseguridad y riesgos operacionales, destacando su impacto en la estabilidad contable.
GESTIÓN DEL RIESGO Y LA CIBERSEGURIDAD EN EL SECTOR FINANCIERO POPULAR Y SOLIDARIO DEL ECUADOR.	Ojeda, F.; Moreno, V.; Torres, M.	2020	Evalúa la importancia de la gestión de riesgos cibernéticos en entidades financieras del sector popular y solidario.
PREVENCIÓN DE RIESGOS POR CIBERSEGURIDAD DESDE LA AUDITORIA FORENSE: CONJUGANDO EL TALENTO HUMANO ORGANIZACIONAL.	Fernández, E.; Herrera, R.	2020	Resalta el papel de la auditoría forense en la prevención de riesgos cibernéticos dentro de organizaciones contables.
CIBERSEGURIDAD EN EL SECTOR FINANCIERO ¿CÓMO TRANSFORMAR UNA AMENAZA EN UNA OPORTUNIDAD?	García Wirton, C.	2021	Expone cómo las empresas pueden convertir las amenazas cibernéticas en oportunidades para mejorar sus procesos de seguridad contable.

CIBERSEGURIDAD POST COVID-19 Y SU IMPACTO EN LAS PYMES DEL ECUADOR.	Bueno, G.; Haz, L.	2022	Analiza el incremento de ataques cibernéticos en pymes y su repercusión en la contabilidad.
MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACIÓN DIGITAL-UN NUEVO ENFOQUE.	Salinas Tomapasca, A.	2022	Plantea un modelo de seguridad para proteger las transacciones contables en cajas municipales ante amenazas digitales.
GESTIÓN ESTRATÉGICA DEL PROGRAMA DE CIBERSEGURIDAD Y SU IMPACTO EN LA POSTURA DE SEGURIDAD DIGITAL DE CENTRIA, EN EL AÑO 2020.	Guevara, D.	2022	Evalúa cómo la gestión estratégica de ciberseguridad mejora la seguridad digital de las empresas en el ámbito contable.
ESTRATEGIAS DE AUDITORÍA EN CIBERSEGURIDAD Y SU IMPORTANCIA EN LAS EMPRESAS UNA REVISIÓN BIBLIOGRÁFICA.	Trujillo, M.; Morales, D.; Taipe, J.; Pallo, P.	2024	Destaca la auditoría en ciberseguridad como herramienta clave en la protección de datos contables y financieros.

Fuente: (Elaboración propia, 2026).

Tabla 4. Antecedentes automatización contable y riesgos cibernéticos.

Título	Autor(es)	Año	Riesgos Cibernéticos
Análisis de las características del sector microempresarial en Latinoamérica y sus limitantes en la adopción de tecnologías para la seguridad de la información.	Pruna, F.; Jeada, P.; Jumbo, J.	2020	Señala que las microempresas enfrentan barreras tecnológicas que limitan su capacidad de defensa ante ciberataques en procesos contables automatizados.
Automatización, ciberseguridad y ciencia de datos: la nueva estrategia empresarial.	Ulloa Mora, J.	2021	Expone cómo la automatización incrementa la exposición a riesgos cibernéticos y la necesidad de nuevas estrategias de seguridad.
Diseño de un sistema de ciberseguridad basado en Defense in Depth para protección del sistema de información de una empresa minera.	Collantes Maza, A.; Ramos Vilela, J.	2021	Analiza cómo la automatización en empresas mineras requiere capas de seguridad adicionales para evitar vulnerabilidades contables.

Título	Autor(es)	Año	Riesgos Cibernéticos
Diseño de controles de ciberseguridad para reducir los ciberataques en empresas distribuidoras de productos digitales basados en CIS control V8.	Dávila, M.; Muñoz, J.	2023	Presenta un modelo de control de ciberseguridad para reducir ataques en procesos automatizados de distribución de productos digitales.
Cultura de ciberseguridad, prevención y atención para las empresas mexicanas.	Landgrave Sandoval, M.	2023	Explica cómo la transformación digital ha aumentado la necesidad de fortalecer la cultura de ciberseguridad en empresas que implementan automatización en sus sistemas contables digitales.

Fuente: (Elaboración propia, 2026).

Tabla 5. Análisis de estudios previos sobre la ciberseguridad en la contabilidad.

Caso empresarial	Hallazgos clave	Relevancia contable
Smith & White (2021) - Cybersecurity Risks in Accounting Firms	Identifica los riesgos cibernéticos más comunes en firmas contables y su impacto financiero (Smith & White, 2021).	Destaca la importancia de medidas de ciberseguridad en la protección de datos financieros (Smith & White, 2021).
Johnson et al. (2022) - Digitalization and Cybersecurity in Accounting	Analiza cómo la transformación digital ha incrementado la exposición a ataques cibernéticos en la contabilidad (Johnson et al., 2022).	Propone estrategias para mitigar los riesgos mediante controles internos y auditoría digital (Johnson et al., 2022).
PwC (2023) - Global Economic Crime and Fraud Survey	Encuestas muestran que 75% de las firmas contables han sufrido ataques los últimos 3 años (PwC, 2023).	Sugiere inversión en formación en ciberseguridad y herramientas de detección de fraudes (PwC, 2023).
Deloitte (2023) - AI in Accounting: Cybersecurity Challenges	Impacto de la automatización contable y la IA en la ciberseguridad (Deloitte, 2023).	Destaca la necesidad de regulación y de sistemas de protección de datos (Deloitte, 2023).
KPMG (2022) - Cyber Risk in Financial Services	Un ataque encriptó archivos financieros, y la empresa no tenía copias de seguridad adecuadas, lo que resultó en pérdida de información crítica (KPMG, 2022).	La importancia de contar con protocolos de respaldo y recuperación ante desastres (KPMG, 2022).

Caso empresarial	Hallazgos clave	Relevancia contable
Brown & Lee (2021) - Financial Fraud and Cybersecurity	Hackers accedieron a sistemas contables y modificaron estados financieros antes de una auditoría (Brown & Lee, 2021).	Implementar herramientas de monitoreo continuo y auditoría en tiempo real (Brown & Lee, 2021).
EY (2022) - Data Security in the Accounting Sector	Fuga de datos en una empresa de auditoría: Una vulnerabilidad en el acceso remoto permitió la filtración de datos de clientes en la dark web (EY, 2022).	Importancia de políticas de acceso restringido y monitoreo de accesos (EY, 2022).
EY (2021) - Lessons from Cybersecurity Incidents	Caso de EY (2020): Un ciberataque expuso información confidencial de clientes debido a una configuración errónea en la nube (EY, 2021).	Relevancia de una gestión adecuada de seguridad en entornos cloud (EY, 2021).
Intuit Security Report (2022)	Caso QuickBooks (2021): Hackers explotaron credenciales robadas para acceder a datos financieros de pequeñas empresas (Milenio, 2021).	Necesidad de autenticación multifactor y supervisión de accesos (Milenio, 2021).

Fuente: (Elaboración propia, 2026).

La literatura revisada evidencia la necesidad de fortalecer los mecanismos de protección de los sistemas de información frente al incremento de las amenazas en los entornos digitales. La incorporación de tecnologías como la automatización, la inteligencia artificial, la computación en la nube y otras herramientas digitales ha transformado la manera en que las organizaciones gestionan, procesan y almacenan información, pero también ha generado nuevos escenarios de exposición a riesgos cibernéticos. En este contexto, resulta fundamental implementar controles de seguridad, mecanismos de gestión de riesgos y estrategias de protección que permitan preservar la confidencialidad, integridad y disponibilidad de los activos de información (Vaca et al., 2021).

Desde una perspectiva conceptual, los estudios analizados permiten reconocer que los incidentes de ciberseguridad pueden generar efectos sobre diferentes dimensiones de las organizaciones, entre ellas la continuidad de las operaciones, la confiabilidad de la información, la protección de los datos y la confianza de los usuarios. Por esta razón, la seguridad de los sistemas de información requiere un enfoque preventivo y sistemático que combine controles tecnológicos y administrativos, evaluación permanente de vulnerabilidades, mecanismos de autenticación y control de accesos, cifrado de información, copias de seguridad y procedimientos para la detección y respuesta ante incidentes.

Asimismo, la evidencia teórica señala que el factor humano constituye un elemento relevante dentro de la protección de los sistemas de información. El desconocimiento de las amenazas, el uso inadecuado de credenciales, los errores en la gestión de información y la exposición frente a técnicas de ingeniería social pueden incrementar los riesgos de seguridad. En consecuencia, la capacitación y sensibilización de los usuarios deben integrarse con las medidas tecnológicas para fortalecer una cultura organizacional orientada a la protección de la información.

En este sentido, la revisión conceptual permite establecer que la ciberseguridad no depende exclusivamente de la incorporación de herramientas tecnológicas, sino de la articulación entre personas, procesos, tecnologías, controles y gestión de riesgos. La adopción de estrategias de seguridad debe responder a las características de cada organización y a los riesgos asociados con los sistemas de información utilizados. Por tanto, el fortalecimiento de la ciberseguridad constituye un proceso continuo que requiere actualización, monitoreo y evaluación permanente frente a la evolución de las amenazas digitales (Vaca et al., 2021).

RELACIÓN DE LA CIBERSEGURIDAD Y EL CUMPLIMIENTO NORMATIVO EN LA INTEGRIDAD Y LEGALIDAD DE LOS PROCESOS CONTABLES.

La ciberseguridad y el cumplimiento normativo constituyen elementos fundamentales para la protección de los sistemas de información en un contexto caracterizado por la transformación digital y el incremento de la dependencia tecnológica de las organizaciones. La incorporación de plataformas digitales para almacenar, procesar y transmitir información ha generado nuevas oportunidades para mejorar los procesos organizacionales, pero también ha incrementado la exposición frente a amenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos. En consecuencia, las organizaciones requieren establecer controles y políticas de seguridad que permitan gestionar los riesgos tecnológicos y atender las disposiciones legales y regulatorias aplicables (Calle & Andrade, 2024).

Desde la perspectiva de los sistemas de información, el cumplimiento normativo comprende el conjunto de acciones mediante las cuales las organizaciones procuran ajustar sus procesos, procedimientos y controles a las leyes, reglamentos, estándares y demás disposiciones que regulan el tratamiento y protección de la información. En este sentido, la ciberseguridad se relaciona con el cumplimiento debido a que los controles implementados para proteger los sistemas pueden contribuir al cumplimiento de obligaciones relacionadas con la seguridad, privacidad, protección de datos y gestión de la información. La Universidad Nacional Abierta y a Distancia (2023) destaca la importancia de considerar los requerimientos normativos dentro de las estrategias de protección de la información, particularmente en escenarios caracterizados por una creciente digitalización.

En el contexto colombiano, la Ley 1273 de 2009 constituye un referente normativo relacionado con la protección de la información y los datos, al incorporar al ordenamiento

penal conductas asociadas con delitos informáticos. Esta disposición evidencia la importancia jurídica de proteger los sistemas de información frente a acciones que puedan afectar los datos y los recursos tecnológicos. De manera complementaria, la Ley 1581 de 2012 establece disposiciones generales para la protección de datos personales, por lo que las organizaciones que realizan tratamiento de información deben considerar principios y obligaciones relacionados con su adecuado manejo y protección.

En el ámbito internacional, la ISO/IEC 27001 constituye un referente para la gestión de la seguridad de la información mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Su enfoque se fundamenta en la identificación, evaluación y tratamiento de riesgos, así como en la implementación de controles orientados a proteger los activos de información. Por tanto, este estándar permite articular la gestión de la seguridad con los procesos organizacionales y con las necesidades de cumplimiento aplicables a cada entidad (Culot et al., 2021).

La relación entre ciberseguridad y cumplimiento normativo adquiere particular importancia en la protección de datos sensibles y sistemas críticos. Las organizaciones deben establecer mecanismos como controles de acceso, autenticación, cifrado, monitoreo, respaldo de información y gestión de incidentes, de acuerdo con las características de los sistemas y los riesgos identificados. Asimismo, las auditorías y evaluaciones periódicas permiten verificar la efectividad de los controles, identificar vulnerabilidades y determinar oportunidades de mejora en los procesos de protección de la información (Rodríguez, 2022).

En los sistemas de información utilizados para soportar procesos contables y financieros, esta relación adquiere especial relevancia debido a la naturaleza de la información procesada. Los registros contables, datos financieros, información de clientes, proveedores y demás documentos empresariales requieren condiciones adecuadas de seguridad para reducir el riesgo de accesos no autorizados,

modificaciones indebidas, pérdida de información o divulgación no autorizada. En este sentido, la ciberseguridad contribuye a preservar las condiciones necesarias para que la información utilizada en los procesos organizacionales mantenga niveles adecuados de confiabilidad e integridad (Calle & Andrade, 2024).

Asimismo, la integración de controles de ciberseguridad dentro de los sistemas de gestión y control organizacional permite establecer una relación entre la protección tecnológica, la gestión del riesgo y el cumplimiento de requisitos. Chai y Zolkipli (2021) señalan la importancia de incorporar mecanismos de seguridad en los entornos donde se administra información financiera y organizacional, debido a que la protección de los sistemas constituye un componente relevante para preservar la confiabilidad de los datos y reducir los riesgos asociados con su utilización.

En consecuencia, la revisión conceptual permite establecer que la relación entre ciberseguridad y cumplimiento normativo no debe entenderse únicamente como una obligación jurídica, sino como un componente de la gestión integral de los sistemas de información. La identificación de requisitos legales y regulatorios, junto con la evaluación de riesgos y la implementación de controles de seguridad, permite a las organizaciones fortalecer la protección de sus activos de información y establecer condiciones más adecuadas para la gestión de los datos. De esta manera, la ciberseguridad y el cumplimiento normativo se articulan como elementos complementarios para favorecer la integridad, protección, trazabilidad y uso adecuado de la información en los diferentes procesos organizacionales.

Importancia de la tecnología en la trazabilidad de transacciones

La trazabilidad constituye un elemento relevante dentro de la gestión y protección de los sistemas de información, debido a que permite registrar, identificar y reconstruir las acciones realizadas sobre los datos y recursos tecnológicos. En entornos

organizacionales cada vez más digitalizados, disponer de mecanismos que permitan conocer el origen, recorrido, modificación y utilización de la información contribuye al fortalecimiento de su integridad y facilita la identificación de actividades no autorizadas. En este sentido, la trazabilidad adquiere especial importancia en aquellos sistemas que gestionan información administrativa, financiera, contable y operativa (Bushman, 2021).

Desde una perspectiva de ciberseguridad, la trazabilidad se relaciona con la capacidad de los sistemas para generar registros de las actividades realizadas por usuarios, aplicaciones y dispositivos. Estos registros permiten establecer quién accedió a determinada información, cuándo se produjo una acción y qué modificaciones fueron efectuadas. De acuerdo con Caamaño y Gil (2020), la utilización de mecanismos tecnológicos orientados al registro y protección de los datos puede contribuir a disminuir los riesgos asociados con alteraciones no autorizadas y accesos indebidos.

El desarrollo de tecnologías digitales ha permitido fortalecer los mecanismos de trazabilidad mediante herramientas como registros de auditoría, bases de datos protegidas, sistemas de monitoreo, técnicas criptográficas y blockchain. Estas tecnologías ofrecen diferentes mecanismos para registrar y verificar operaciones, facilitando la generación de evidencias que pueden ser utilizadas para procesos de supervisión, auditoría y análisis de incidentes de seguridad. No obstante, su implementación debe considerar las características del sistema, los riesgos identificados y los requerimientos de seguridad y gobernanza de la información.

La trazabilidad también presenta una relación importante con el cumplimiento normativo, debido a que determinados entornos organizacionales requieren conservar evidencias sobre las operaciones y actividades realizadas sobre la información. La disponibilidad de registros confiables permite facilitar procesos de auditoría, supervisión y verificación, así como establecer responsabilidades frente a modificaciones o accesos no autorizados (García, 2021). De esta manera, los mecanismos de trazabilidad pueden

contribuir simultáneamente a la protección de la información y al fortalecimiento de los procesos de control.

Otro aspecto relevante corresponde al monitoreo y análisis de las actividades desarrolladas en los sistemas de información. La revisión de registros y patrones de comportamiento puede facilitar la identificación de actividades inusuales o potencialmente fraudulentas, permitiendo generar alertas y activar mecanismos de respuesta ante posibles incidentes. En consecuencia, la trazabilidad no solamente cumple una función documental, sino que puede constituirse en un componente preventivo y de detección dentro de una estrategia integral de ciberseguridad (Caamaño & Gil, 2020).

En el ámbito de los sistemas de información contable y financiero, la trazabilidad adquiere particular relevancia debido a la necesidad de conservar evidencia sobre las operaciones registradas y las modificaciones realizadas. Sin embargo, su utilidad trasciende estos sistemas, dado que puede aplicarse a diferentes procesos organizacionales en los que la integridad, autenticidad y disponibilidad de la información sean elementos relevantes.

En consecuencia, desde la perspectiva de los fundamentos teóricos de la ciberseguridad, la trazabilidad puede comprenderse como un mecanismo que contribuye a fortalecer la integridad, supervisión y control de los sistemas de información. Su articulación con tecnologías de registro, monitoreo y auditoría permite generar evidencias sobre las actividades realizadas y facilita la detección de comportamientos no autorizados. Por tanto, constituye un elemento complementario de la gestión de riesgos y de las estrategias orientadas a proteger los activos de información frente a las amenazas del entorno digital.

Herramientas de software contable con seguridad integrada

En el contexto de la transformación digital, la incorporación de mecanismos de ciberseguridad en los sistemas de información constituye un elemento fundamental para proteger los datos y garantizar la continuidad de las operaciones. Los sistemas de información utilizados en procesos administrativos, contables y financieros requieren medidas de protección que permitan reducir la exposición frente a amenazas y accesos no autorizados. Entre estas medidas se encuentran el cifrado de la información, la autenticación multifactor y el control de acceso basado en roles, mecanismos orientados a preservar la confidencialidad y contribuir a la integridad de los datos (Gomero & Sánchez, 2024).

Asimismo, los sistemas de información pueden incorporar registros de auditoría y mecanismos de monitoreo que permiten identificar, documentar y rastrear las acciones realizadas por los usuarios. Estos recursos favorecen la trazabilidad de la información y facilitan la detección de comportamientos anómalos o actividades potencialmente riesgosas. De igual manera, la incorporación de tecnologías como la inteligencia artificial y el aprendizaje automático permite fortalecer las capacidades de análisis de los sistemas mediante la identificación de patrones inusuales y la generación de alertas ante posibles eventos de seguridad (Gomero & Sánchez, 2024).

Desde una perspectiva de gestión de riesgos, la selección e implementación de sistemas de información debe considerar no solamente su funcionalidad, sino también las capacidades de protección incorporadas en su arquitectura y operación. Aspectos como las actualizaciones de seguridad, la protección frente a software malicioso, las copias de respaldo y los mecanismos de recuperación de información contribuyen a fortalecer la disponibilidad y resiliencia de los sistemas frente a incidentes cibernéticos (Vega, 2021).

En este sentido, la evolución de las amenazas digitales evidencia que la ciberseguridad debe abordarse como un componente transversal de los sistemas de

información, articulando personas, procesos, tecnologías y mecanismos de control. Su adecuada implementación contribuye a proteger los activos de información, fortalecer la continuidad operativa y reducir los riesgos asociados con la pérdida, alteración, divulgación o acceso no autorizado a los datos. Particularmente, en los sistemas contables y financieros, estas medidas adquieren relevancia debido a la importancia de la información que soporta los procesos de registro, análisis y toma de decisiones empresariales.

Mecanismos de ciberseguridad para garantizar el cumplimiento normativo

En este apartado se analiza la relación entre la ciberseguridad y el cumplimiento normativo en los sistemas de información, considerando las disposiciones legales, reglamentarias y técnicas orientadas a garantizar la adecuada protección de los datos y recursos digitales de las organizaciones. Desde una perspectiva conceptual, se examinan los principales referentes relacionados con la seguridad de la información, la protección de datos, el control de acceso, la gestión de riesgos y la trazabilidad de las operaciones, así como su importancia para fortalecer la integridad, confidencialidad y disponibilidad de la información.

El cumplimiento normativo constituye un componente relevante de la gestión de la ciberseguridad, debido a que permite establecer controles y procedimientos destinados a prevenir accesos no autorizados, pérdida o alteración de información y otros eventos que puedan afectar el funcionamiento de los sistemas. En este contexto, la adopción de políticas de seguridad, mecanismos de autenticación, controles de acceso, monitoreo, respaldo y gestión de incidentes contribuye a reducir la exposición a riesgos y a demostrar que los procesos organizacionales se desarrollan bajo criterios de protección y control.

De manera particular, los sistemas de información contables y financieros requieren especial atención debido a que procesan información necesaria para la gestión, control y

toma de decisiones. Por ello, la aplicación de principios de ciberseguridad y cumplimiento normativo contribuye a preservar la confiabilidad de los datos, fortalecer la trazabilidad de las operaciones y respaldar la transparencia de los procesos organizacionales. En consecuencia, la relación entre ciberseguridad y cumplimiento normativo constituye un elemento fundamental para comprender cómo los sistemas de información pueden gestionar de manera segura la información y responder adecuadamente a los riesgos derivados del entorno digital.

Tabla 6 Cumplimiento normativo en procesos contables y su relación con la ciberseguridad

NORMATIVA	DESCRIPCIÓN	IMPACTO EN LA CIBERSEGURIDAD
NORMAS INTERNACIONALES DE INFORMACIÓN FINANCIERA (NIIF)	Establecen principios para la presentación de información financiera confiable, exacta y comparable a nivel global (Quiñonez et al., 2021).	Exigen que la información contable sea íntegra y precisa, lo que implica la adopción de sistemas seguros para evitar manipulaciones y accesos no autorizados (Quiñonez et al., 2021).
NORMAS INTERNACIONALES DE AUDITORÍA (NIA)	Regulan los procesos de auditoría para garantizar la transparencia y confiabilidad de los estados financieros (Hernández et al., 2022).	Requieren la implementación de controles de seguridad en los sistemas de información para prevenir fraudes y garantizar la trazabilidad de los datos (Rivera, 2019).
LEY SARBANES-OXLEY (SOX)	Obliga a las empresas a garantizar la integridad de la información financiera y establecer controles internos sólidos (Huanca, 2021)	Impulsa el uso de herramientas de ciberseguridad como el cifrado, la autenticación multifactor y los registros inalterables para evitar fraudes contables (Huanca, 2021).
ISO 27001	Norma internacional para la gestión de la seguridad de la información en las organizaciones (Internacional Organization for Standardization, 2022).	Exige la implementación de políticas y procedimientos de seguridad en el manejo de datos contables, reduciendo el riesgo de ataques cibernéticos y fugas de información (Internacional Organization for Standardization, 2022).
REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (GDPR)	Protección de datos personales en la Unión Europea, aplicable a empresas con clientes o usuarios en la región (Europea, 2025).	La información financiera de clientes y empleados es gestionada con medidas de seguridad estrictas, incluyendo el control de accesos y el derecho al olvido (Europea, 2025).

**NORMATIVAS
LOCALES SOBRE
CIBERSEGURIDAD
Y CONTROL
CONTABLE**

Regulaciones específicas de cada país sobre la protección de datos y la seguridad de la información contable (Rivera, 2019).

Exigen la adopción de estándares nacionales de seguridad informática, auditoría y cumplimiento normativo en la gestión contable (Rivera, 2019).

Fuente: (Elaboración propia, 2026).

La tabla anterior, presenta el efecto normativo en la seguridad de la información en la contabilidad, subrayando la importancia de adoptar medidas de ciberseguridad para garantizar la transparencia y confiabilidad de los datos financieros.

Mecanismos de ciberseguridad para garantizar el cumplimiento normativo

Los mecanismos de ciberseguridad constituyen elementos fundamentales para fortalecer la protección de los sistemas de información y contribuir al cumplimiento de las disposiciones legales, reglamentarias y técnicas aplicables a las organizaciones. Desde una perspectiva conceptual, medidas como el cifrado de la información, la autenticación multifactor y el control de acceso permiten reducir la exposición frente a accesos no autorizados, modificaciones indebidas y divulgación de información, favoreciendo la confidencialidad, integridad y disponibilidad de los datos (Azcona, 2024; Castellanos, 2020).

De igual manera, las copias de seguridad y los mecanismos de recuperación de información representan componentes relevantes dentro de la gestión de la ciberseguridad, debido a que permiten responder ante incidentes, fallas técnicas o pérdida de datos. Estos mecanismos contribuyen a fortalecer la continuidad operativa y la capacidad de recuperación de los sistemas, al tiempo que facilitan la conservación y trazabilidad de los registros necesarios para procesos de auditoría y supervisión (Castellanos, 2020). En este contexto, la implementación de controles de seguridad debe

complementarse con procedimientos de monitoreo y evaluación de riesgos que permitan identificar vulnerabilidades y establecer medidas preventivas y correctivas.

Por otra parte, las tecnologías orientadas al análisis de información pueden fortalecer las capacidades de detección y respuesta frente a comportamientos anómalos. La inteligencia artificial, el análisis de grandes volúmenes de datos y las herramientas de auditoría digital permiten procesar información y reconocer patrones que podrían estar asociados con eventos de riesgo o actividades irregulares (Azcona, 2024). Estas aplicaciones adquieren especial importancia en los sistemas contables y financieros, donde el análisis automatizado puede contribuir a fortalecer los mecanismos de control y supervisión de las operaciones.

Asimismo, tecnologías como blockchain pueden aportar mecanismos de trazabilidad y verificación de los registros digitales mediante estructuras que dificultan su modificación no autorizada. Su aplicación en determinados procesos de información puede contribuir al fortalecimiento de la integridad y transparencia de los registros, aunque su utilidad y alcance dependen del contexto, la arquitectura del sistema y los requerimientos organizacionales y normativos (Sedano & Salman, 2021; García, 2021).

En consecuencia, la ciberseguridad en los sistemas de información requiere una articulación entre mecanismos tecnológicos, controles organizacionales, gestión de riesgos y cumplimiento normativo. La incorporación de estas medidas permite fortalecer la protección de los activos de información, mejorar la capacidad de respuesta ante incidentes y favorecer la confiabilidad y trazabilidad de los datos. En los sistemas contables y financieros, esta articulación adquiere particular relevancia debido a que la

seguridad de la información constituye un soporte para la transparencia, el control y la adecuada gestión de las operaciones organizacionales.

Casos reales y análisis de impacto

Como complemento del análisis conceptual, se presenta una tabla que reúne casos documentados de incidentes y vulnerabilidades de ciberseguridad en sistemas de información organizacionales. En ella se examinan sus principales efectos sobre la protección, integridad y disponibilidad de la información, así como las implicaciones operativas, económicas y normativas derivadas de estos eventos. Asimismo, se identifican las medidas y buenas prácticas de ciberseguridad adoptadas por las organizaciones para prevenir, gestionar y mitigar riesgos asociados con la seguridad de la información.

Tabla 7. Casos reales y análisis de impacto.

Caso	Análisis de impacto	Prácticas implementadas
Hackeo a Deloitte (2017)	Deloitte, una de las firmas de auditoría más grandes del mundo, sufrió un ciberataque que comprometió información confidencial de sus clientes debido a la falta de autenticación multifactor en su sistema de correos (Hopkins, 2017).	Implementación de autenticación multifactor, refuerzo en el cifrado de datos y auditorías de ciberseguridad más estrictas (Hopkins, 2017).
Ataque de ransomware a Maersk (2017)	La empresa de logística Maersk, que maneja operaciones contables globales, fue afectada por el ransomware NotPetya, causando pérdidas de aproximadamente \$300 millones. Los procesos financieros y contables quedaron paralizados durante semanas (Europa Press, 2018).	Estrategia de segmentación de redes, copias de seguridad redundantes y capacitación en ciberseguridad para empleados (Europa Press, 2018).
Fraude cibernético en la firma BDO (2018)	Hackers utilizaron correos electrónicos fraudulentos para engañar a empleados de BDO, obteniendo acceso a datos financieros sensibles y desviando fondos a cuentas externas (Petroff, 2017).	Refuerzo en la verificación de transacciones, educación sobre ataques de phishing y adopción de inteligencia artificial para detectar anomalías (Petroff, 2017).

Caso	Análisis de impacto	Prácticas implementadas
Ataque a la firma CPA Canada (2020)	La firma sufrió una filtración de datos que expuso información de más de 329,000 profesionales contables. El incidente afectó la reputación de la firma y llevó a investigaciones legales (La Nación, 2020).	Encriptación de datos confidenciales, monitoreo en tiempo real de accesos sospechosos y cumplimiento con regulaciones de privacidad (La Nación, 2020).
Fraude interno en Wirecard (2020)	Wirecard, una empresa fintech alemana, presentó un escándalo de fraude contable de más de \$1.9 mil millones, revelando vulnerabilidades en la trazabilidad de las transacciones (Suberg, 2020).	Implementación de blockchain para trazabilidad, auditorías independientes y mayor regulación en el sector fintech (Suberg, 2020).
Robo de credenciales en QuickBooks (2021)	Un grupo de ciberdelincuentes explotó vulnerabilidades en el software de contabilidad la entidad QuickBooks para acceder a datos de pequeñas y medianas empresas, afectando su gestión contable (Milenio, 2021).	Refuerzo en la autenticación de usuarios, actualizaciones de seguridad más frecuentes y notificaciones de actividad inusual (Milenio, 2021).

Fuente: (Elaboración propia, 2024).

Los casos analizados permiten evidenciar que las vulnerabilidades e incidentes de ciberseguridad en los sistemas de información pueden generar consecuencias operativas, económicas, legales y reputacionales para las organizaciones. Situaciones como ataques de ransomware, accesos no autorizados, pérdida de información y fraudes internos pueden afectar la confidencialidad, integridad y disponibilidad de los datos, además de comprometer la continuidad de los procesos y la confianza de los usuarios en los sistemas de información.

Frente a estos riesgos, la literatura destaca la implementación de medidas preventivas y de control orientadas a fortalecer la seguridad de los sistemas. Entre ellas se encuentran la autenticación multifactor, el cifrado de datos, las auditorías de seguridad, las copias de respaldo, el monitoreo de actividades y la gestión de vulnerabilidades. Asimismo, tecnologías como la inteligencia artificial, el análisis de datos

y blockchain pueden contribuir, según el contexto de aplicación, a mejorar la detección de anomalías, la trazabilidad y la protección de los registros digitales. En conjunto, estas prácticas permiten fortalecer la gestión de riesgos y la capacidad de prevención, respuesta y recuperación ante posibles incidentes de ciberseguridad.

Los controles de ciberseguridad constituyen mecanismos destinados a reducir los riesgos identificados y proteger los activos de información. La **ISO/IEC 27002:2022** proporciona orientación para la selección y aplicación de controles relacionados con diferentes dimensiones de la seguridad de la información, entre ellas el control de acceso, la criptografía, la seguridad de los recursos humanos y la respuesta ante incidentes (ISO, 2022).

A partir de la revisión realizada, los controles pueden organizarse en diferentes categorías:

Tabla 8 Controles desde el desarrollo de conceptos clave y la evolución de la ciberseguridad en los sistemas de información

CATEGORÍA	EJEMPLOS	DE	PROPÓSITO
CONTROLES			
ACCESO	Autenticación, contraseñas robustas, control de privilegios	Evitar accesos no autorizados	
DATOS	Cifrado, copias de seguridad, clasificación de información	Proteger la información	
TECNOLOGÍA	Firewalls, antivirus, actualización de sistemas	Reducir vulnerabilidades	
MONITOREO	Registros, alertas, supervisión de eventos	Detectar actividades anómalas	
INCIDENTES	Protocolos de respuesta, recuperación y comunicación	Reducir impactos	
PERSONAS	Capacitación, concienciación y políticas de seguridad	Disminuir riesgos asociados al factor humano	

CONTINUIDAD	Copias de respaldo, recuperación ante desastres	Mantener o recuperar las operaciones
--------------------	--	---

Fuente: (Elaboración propia, 2024).

El NIST (2024) señala que el marco de ciberseguridad no prescribe una única forma de implementar controles, sino que proporciona resultados de alto nivel y permite que cada organización seleccione las prácticas y controles que mejor respondan a sus necesidades y nivel de riesgo.

Como resultado de esta primera etapa se obtiene una base conceptual estructurada de la ciberseguridad en los sistemas de información, en la cual se integran sus principales conceptos, evolución, amenazas, vulnerabilidades, riesgos, principios de protección y controles.

El principal producto corresponde a una matriz de revisión conceptual, que permitirá organizar los referentes consultados de acuerdo con categorías como concepto, autor o institución, año, aporte teórico, categoría de análisis y aplicabilidad en los sistemas de información.

Adicionalmente, se establece un esquema conceptual de la ciberseguridad, mediante el cual se representa la relación existente entre los sistemas de información, sus activos, las amenazas y vulnerabilidades, la gestión del riesgo, los controles y la capacidad de respuesta y recuperación.

En términos del objetivo específico, esta etapa permite comprender que la ciberseguridad ha evolucionado desde una visión predominantemente técnica hacia un enfoque integral de gestión del riesgo, gobernanza y protección de los activos de información. Los referentes revisados muestran que su aplicación requiere combinar controles tecnológicos, organizacionales y humanos, así como mecanismos de

prevención, detección, respuesta y recuperación. En consecuencia, la ciberseguridad constituye un componente transversal para preservar la seguridad y continuidad de los sistemas de información.

Tabla 9 Base conceptual estructurada de la ciberseguridad en los sistemas de información,

N. °	CATEGORÍA DE ANÁLISIS	CONCEPTO / ASPECTO	PRINCIPAL APOORTE PARA EL OBJETIVO	REFERENTE BIBLIOGRÁFICO APA 7.ª EDICIÓN	LINK
1	Ciberseguridad	Fundamentos y alcance	Permite comprender la ciberseguridad como un enfoque integral para gestionar y reducir los riesgos que afectan a las organizaciones y sus sistemas de información.	National Institute of Standards and Technology. (2024). <i>The NIST Cybersecurity Framework (CSF) 2.0</i> (NIST CSWP 29). (NIST Computer Security Resource Center)	NIST CSF 2.0
2	Ciberseguridad	Estado actual y evolución	Presenta una revisión del estado del arte, desafíos y tendencias de la ciberseguridad,	Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2023). Cyber security: State of the art, challenges and	Artículo científico

F-DC-125

INFORME FINAL DE TRABAJO DE GRADO EN MODALIDAD DE PROYECTO
DE INVESTIGACIÓN, DESARROLLO TECNOLÓGICO, MONOGRAFÍA,
EMPRENDIMIENTO Y SEMINARIO

VERSIÓN: 2.0

				permitiendo identificar su evolución frente a la transformación digital.	future directions. <i>Cyber Security and Applications</i> , 1, 100031. (DOI)	
3	Sistemas de información	Seguridad de sistemas	Permite comprender que la protección debe considerar los sistemas tecnológicos, sus componentes, procesos y entornos de operación.	Shukla, A., Katt, B., Nweke, L. O., Yeng, P. K., & Weldehawaryat, G. K. (2022). System security assurance: A systematic literature review. <i>Computer Science Review</i> , 45, 100496. (DOI)	Artículo científico	
4	Seguridad de la información	Confidencialidad, integridad y disponibilidad	Establece los fundamentos de un sistema de gestión de seguridad de la información y la protección de la información mediante la gestión del riesgo.	International Organization for Standardization. (2022). <i>ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection—Information security management</i>	ISO/IEC 27001:2022	

						systems— Requirements. (ISO)	
5	Controles de seguridad	de protección	Medidas de	Proporcion	International	ISO/IE	
				a controles y buenas prácticas relacionadas con acceso, criptografía, recursos humanos y respuesta a incidentes.	Organization for Standardization. (2022). ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection—Information security controls. (ISO)	C 27002:2022	
6	Gestión del riesgo	Riesgo de ciberseguridad	de	Relaciona	Quinn, S., Pillitteri, V., Barrett, M., Smith, M., & Witte, G. (2024). NIST Cybersecurity Framework 2.0: Enterprise Risk Management Quick-Start Guide (NIST SP 1303). NIST. (NIST)	NIST	SP 1303

7	Amenazas	Panorama de	Permite	European	ENISA
	amenazas		identificar tendencias, tipos de amenazas e incidentes que afectan actualmente los sistemas de información.	Union Agency for Cybersecurity. (2024). <i>ENISA Threat Landscape 2024</i> . (ENISA)	Threat Landscape 2024
8	Riesgo cibernético	Evidencia y disponibilidad de datos	Analiza la literatura sobre riesgo cibernético y muestra la importancia de contar con información para comprender y gestionar estos riesgos.	Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. <i>The Geneva Papers on Risk and Insurance—Issues and Practice</i> , 47, 698–736. (DOI)	Artículo científico
9	Amenazas de ingeniería social	Phishing	Permite comprender el phishing y la ingeniería social como	Adu-Manu, K. S., Ahiable, R. K., Appati, J. K., & Mensah, E. E. (2022). Phishing	Artículo científico

			amenazas que attacks in social aprovechan engineering: A review. vulnerabilidades <i>Journal of Cyber</i> humanas y <i>Security</i> , 4(4), 239–267. tecnológicas. (Tech Science)	
10	Factor humano	Comportamiento y seguridad	Evidencia	Nifakos, S., Artículo científico la importancia del Chandramouli, K., o científico factor humano en la Nikolaou, C. K., seguridad de los Papachristou, P., Koch, sistemas y en la S., Panaousis, E., & exposición a ataques Bonacina, S. (2021). de ingeniería social. Influence of human factors on cyber security within healthcare organisations: A systematic review. <i>Sensors</i> , 21(15), 5119. (PubMed)
11	Computación en la nube	Nuevos entornos tecnológicos	Identificación	Stergiou, C. Artículo científico amenazas, desafíos L., & Psannis, K. E. o científico de seguridad y (2022). A survey of mecanismos de security in cloud, edge, protección en and fog computing.

			entornos cloud, edge y fog.	<i>Sensors</i> , 22(3), 927. (DOI)	
12	Zero Trust	Evolución de los modelos de protección	Presenta el enfoque Zero Trust como evolución de los modelos tradicionales basados en perímetros de seguridad.	Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of Zero Trust security: A brief survey. <i>Entropy</i> , 25(12), 1595. (MDPI)	Artículo científico
13	Inteligencia artificial	IA aplicada a ciberseguridad	Permite comprender la incorporación de inteligencia artificial para detección de amenazas, automatización, respuesta y fortalecimiento de la seguridad.	Kaur, R., Gabrijelčič, D., & T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. <i>Information Fusion</i> , 97, 101804. (DOI)	Artículo científico
14	Inteligencia artificial	Nuevas amenazas	Analiza la utilización de IA y aprendizaje automático tanto para	Ofusoria, L., Bokabab, T., & Mhlongob, S. (2024). Artificial intelligence in	Artículo científico

F-DC-125

INFORME FINAL DE TRABAJO DE GRADO EN MODALIDAD DE PROYECTO
DE INVESTIGACIÓN, DESARROLLO TECNOLÓGICO, MONOGRAFÍA,
EMPRENDIMIENTO Y SEMINARIO

VERSIÓN: 2.0

				fortalecer defensas cybersecurity: A como para desarrollar comprehensive review nuevas modalidades and future direction. de ataques. <i>Applied Artificial Intelligence</i> , 38(1). (DOI)	
15	Machine learning	Amenazas y contramedidas	Examina amenazas contra sistemas de aprendizaje automático y mecanismos para proteger su seguridad y privacidad.	Paracha, A., Arshad, J., Farah, M. B., & Ismail, K. (2024). Machine learning security and privacy: A review of threats and countermeasures. <i>EURASIP Journal on Information Security</i> , 2024, 10. (Springer)	Artículo científico
16	Inteligencia artificial	Evolución de las amenazas	Examina la utilización de IA como herramienta ofensiva y defensiva dentro del contexto de la ciberseguridad.	The Weaponization of Artificial Intelligence in Cybersecurity: A Systematic Review. (2024). <i>Procedia Computer Science</i> ,	Artículo científico

				239,	547–555.	
				(ScienceDirect)		
17	Resiliencia cibernética	Recuperación y adaptación	Permite ampliar la capacidad de preparar, absorber, recuperar y adaptarse frente a incidentes.	Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). A survey on cyber resilience: Key strategies, research challenges, and future directions. <i>ACM Computing Surveys</i> , 56(8), 196. (DOI)	Artículo científico	
18	Respuesta a incidentes	Detección, respuesta y recuperación	Establece la respuesta a incidentes como componente integrado de la gestión del riesgo de ciberseguridad.	Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). <i>Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile</i> (NIST SP 800-61 Rev. 3). NIST. (NIST	NIST SP 800-61 Rev. 3	

					Computer Security Resource Center)	
19	Cadena de suministro	Riesgos tecnológicos de terceros	Incorpora los riesgos derivados de proveedores, productos y servicios tecnológicos dentro de la gestión de ciberseguridad.	Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2024). <i>Cybersecurity supply chain risk management practices for systems and organizations</i> (NIST SP 800-161 Rev. 1, Update 1). NIST. (NIST)	NIST SP 800-161 Rev. 1 Update 1	
20	Gobernanza y madurez	Gestión organizacional	Permite analizar la ciberseguridad desde una perspectiva de gobernanza, gestión del riesgo y desarrollo de capacidades organizacionales.	World Economic Forum. (2024). <i>Global cybersecurity outlook 2024</i> . World Economic Forum. (World Economic Forum)	Global Cybersecurity Outlook 2024	

Fuente: (Elaboración propia, 2026).

Como resultado del desarrollo del primer objetivo específico, se elaborará una matriz de fundamentos conceptuales y evolución de la ciberseguridad en los sistemas de información, integrada por un mínimo de veinte referentes bibliográficos publicados a partir de 2021, entre artículos científicos, normas técnicas, marcos de referencia e informes de organismos especializados.

La matriz permitirá sistematizar los principales conceptos relacionados con la ciberseguridad, los sistemas de información, la seguridad de la información, los activos de información, las amenazas, las vulnerabilidades, los riesgos, los controles de seguridad, la respuesta a incidentes, la resiliencia y la continuidad operativa. Asimismo, permitirá identificar los principales aportes de cada referente y establecer su relación con la aplicabilidad de la ciberseguridad en los sistemas de información.

De manera complementaria, se elaborará un análisis de la evolución conceptual de la ciberseguridad, mediante el cual se evidenciará el tránsito desde enfoques centrados en la protección técnica de equipos, redes y datos hacia modelos integrales fundamentados en la gestión del riesgo, la gobernanza, el factor humano, la inteligencia artificial, la seguridad de la cadena de suministro, la respuesta ante incidentes y la resiliencia cibernética.

FASE II

La segunda etapa se orienta a la identificación de la relación entre la ciberseguridad y el cumplimiento normativo en los sistemas de información, a través del análisis teórico, con la finalidad de determinar su contribución a la integridad y legalidad de los procesos contables y financieros.

La segunda etapa estará orientada a identificar y analizar la relación entre la ciberseguridad y el cumplimiento normativo en los sistemas de información, considerando las disposiciones legales colombianas, los estándares internacionales y los referentes

técnicos relacionados con la protección de la información, la gestión de riesgos, el control de acceso, la respuesta ante incidentes y la continuidad operativa. Este análisis permitirá establecer cómo los mecanismos de ciberseguridad pueden contribuir al cumplimiento de obligaciones relacionadas con la protección, disponibilidad, confidencialidad e integridad de la información.

En el contexto colombiano, esta relación adquiere especial importancia para los sistemas de información contable y financiero, debido a que la información utilizada por las organizaciones debe responder simultáneamente a requerimientos contables, profesionales, legales y de seguridad. La Ley 1314 de 2009 establece el marco para las normas de contabilidad, información financiera y aseguramiento de la información en Colombia y señala que la información financiera debe ser comprensible, transparente, comparable, pertinente y confiable. Por su parte, la Ley 43 de 1990 establece el marco de ejercicio de la profesión contable y reconoce al contador público facultades relacionadas con la fe pública y el dictamen de estados financieros. En consecuencia, la protección de los sistemas y de los datos que soportan la información financiera constituye un elemento relacionado con la confiabilidad y responsabilidad profesional (Congreso de Colombia, 1990, 2009). Ley 43 de 1990 Ley 1314 de 2009

Desde una perspectiva de gestión del riesgo, el NIST Cybersecurity Framework 2.0 (CSF 2.0) plantea que la ciberseguridad debe integrarse a la gestión general del riesgo de la organización. El marco proporciona una estructura para comprender, evaluar, priorizar y comunicar los resultados relacionados con la gestión de los riesgos de ciberseguridad. Su estructura se organiza mediante seis funciones: Govern, Identify, Protect, Detect, Respond y Recover, las cuales permiten relacionar las actividades de seguridad con el gobierno, la gestión del riesgo y la continuidad de las operaciones (Pascoe et al., 2024). NIST Cybersecurity Framework 2.0

De manera complementaria, la ISO/IEC 27001:2022 establece los requisitos para implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. Su enfoque se fundamenta en la gestión de riesgos y busca preservar la confidencialidad, integridad y disponibilidad de la información, considerando de manera articulada las personas, los procesos y la tecnología (International Organization for Standardization [ISO], 2022). ISO/IEC 27001:2022

En consecuencia, la ciberseguridad puede ser entendida como un componente que facilita la gestión del cumplimiento, dado que los controles tecnológicos, administrativos y organizacionales permiten reducir riesgos relacionados con el acceso no autorizado, modificación, pérdida, divulgación, indisponibilidad o destrucción de información. Esta relación adquiere particular relevancia en los sistemas de información contable y financiero, en los cuales la confiabilidad de los datos constituye un elemento fundamental para la preparación, presentación y aseguramiento de la información financiera.

Ciberseguridad y cumplimiento normativo

El cumplimiento normativo en materia de información implica que las organizaciones identifiquen y atiendan las obligaciones legales, regulatorias, contractuales, profesionales y técnicas que resulten aplicables a sus actividades. En este contexto, la ciberseguridad proporciona mecanismos que permiten reducir los riesgos relacionados con el tratamiento, almacenamiento, procesamiento, transmisión y protección de la información.

En Colombia, la Ley 1314 de 2009 establece los principios y normas de contabilidad, información financiera y aseguramiento de la información, mientras que el Decreto 2420 de 2015 compila el marco reglamentario correspondiente. Este último incorpora, entre otros componentes, los marcos técnicos de información financiera y las

Normas de Aseguramiento de la Información, dentro de las cuales se encuentran las Normas Internacionales de Auditoría (NIA), las Normas Internacionales de Control de Calidad, las Normas Internacionales de Trabajos de Revisión, las ISAE, las NISR y el Código de Ética para profesionales de la contaduría. El Decreto 2420 ha sido objeto de modificaciones posteriores y su texto registra actualizaciones hasta 2026, por lo que debe consultarse junto con las disposiciones que lo modifican, adicionan o sustituyen (Congreso de Colombia, 2009; Presidencia de la República de Colombia, 2015). Decreto 2420 de 2015 – Gestor Normativo

El NIST CSF 2.0 establece que la gestión de la ciberseguridad debe integrarse con la gestión de riesgos de la organización y que los resultados de seguridad pueden utilizarse para orientar decisiones, priorizar acciones y comunicar el estado de los riesgos a las partes interesadas (Pascoe et al., 2024). NIST CSF 2.0

Por otra parte, la ISO/IEC 27001:2022 establece un enfoque sistemático para gestionar los riesgos asociados con los activos de información y determinar controles apropiados para su tratamiento. De esta manera, la seguridad de la información se integra en los procesos de gestión de la organización y no se limita exclusivamente a la implementación de herramientas tecnológicas (ISO, 2022). ISO/IEC 27001:2022

A partir de estos referentes, la relación conceptual entre ciberseguridad y cumplimiento normativo puede representarse de la siguiente manera:

Requerimiento normativo → identificación del riesgo → diseño del control → implementación → monitoreo → generación de evidencia → evaluación del cumplimiento → mejora continua.

Por tanto, el cumplimiento normativo no debe limitarse a la existencia de políticas o documentos, sino que debe estar acompañado de controles implementados,

procedimientos verificables y evidencias que permitan demostrar la gestión de los riesgos.

Protección de datos personales

En Colombia, la protección de datos personales constituye uno de los principales componentes normativos relacionados con la seguridad de la información. La Ley 1581 de 2012 establece disposiciones generales para la protección de datos personales, desarrolla los derechos de los titulares y establece principios y obligaciones relacionados con el tratamiento de información personal. Entre sus principios se encuentran la legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso restringido, seguridad y confidencialidad (Congreso de Colombia, 2012). Ley 1581 de 2012 – Gestor Normativo

Particularmente, el principio de seguridad establecido en la Ley 1581 de 2012 exige la adopción de medidas técnicas, humanas y administrativas necesarias para evitar la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información. Este requerimiento guarda una relación directa con la ciberseguridad, debido a que mecanismos como la autenticación, autorización, cifrado, monitoreo, copias de seguridad y gestión de incidentes contribuyen a reducir este tipo de riesgos (Congreso de Colombia, 2012). Ley 1581 de 2012

De esta manera, para los sistemas de información que procesan datos personales, la ciberseguridad puede contribuir al cumplimiento de las obligaciones de protección mediante controles destinados a preservar la confidencialidad, integridad y disponibilidad de los datos. Esta relación también resulta relevante para los sistemas contables, dado que en ellos pueden procesarse datos de trabajadores, clientes, proveedores, asociados y demás titulares de información.

Protección de la información financiera y crediticia

La Ley 1266 de 2008 regula el hábeas data y establece disposiciones relacionadas con el manejo de información contenida en bases de datos personales, especialmente aquella de naturaleza financiera, crediticia, comercial, de servicios y proveniente de terceros países. Esta regulación resulta relevante para los sistemas de información financieros debido a que establece un marco jurídico para la recolección, tratamiento y circulación de este tipo de información (Congreso de Colombia, 2008). Ley 1266 de 2008 – Gestor Normativo

Posteriormente, la Ley 2157 de 2021 modificó y adicionó la Ley 1266 de 2008, fortaleciendo el derecho al hábeas data respecto de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países (Congreso de Colombia, 2021). Ley 2157 de 2021 – Gestor Normativo

Desde la perspectiva de la ciberseguridad, estas disposiciones pueden relacionarse con controles de acceso, administración de usuarios, protección de bases de datos, actualización de información, mecanismos de autenticación y medidas destinadas a prevenir modificaciones o usos no autorizados. En los sistemas contables y financieros, dichos controles contribuyen a preservar la confiabilidad de los datos empleados en procesos como cartera, cuentas por cobrar, obligaciones financieras y análisis de información económica.

Integridad de los mensajes de datos y registros electrónicos

La Ley 527 de 1999 regula el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales. La norma reconoce efectos jurídicos a los mensajes de datos y establece disposiciones relacionadas con su integridad,

conservación y valor probatorio (Congreso de Colombia, 1999). Ley 527 de 1999 – Gestor Normativo

La legislación establece que, cuando una norma requiera que determinada información sea presentada o conservada en su forma original, este requisito puede satisfacerse mediante un mensaje de datos cuando exista una garantía confiable de que la información ha permanecido íntegra. Asimismo, la norma considera íntegra aquella información que ha permanecido completa e inalterada, salvo modificaciones inherentes a los procesos de comunicación, archivo o presentación (Congreso de Colombia, 1999). Ley 527 de 1999

Este aspecto resulta especialmente relevante para los sistemas de información contable y financiero, debido a que numerosas operaciones, documentos y registros se generan, procesan y conservan actualmente en medios electrónicos. Por ello, los controles de ciberseguridad relacionados con trazabilidad, control de cambios, autenticación, registros de auditoría y copias de seguridad pueden contribuir a preservar la integridad y disponibilidad de dichos registros.

Protección frente a delitos informáticos

La Ley 1273 de 2009 modificó el Código Penal colombiano y creó un bien jurídico denominado “de la protección de la información y de los datos”, incorporando disposiciones dirigidas a preservar los sistemas que utilizan tecnologías de la información y las comunicaciones (Congreso de Colombia, 2009). Ley 1273 de 2009 – SUIN-Juriscol

La norma contempla conductas relacionadas con afectaciones a la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, incluyendo, entre otras, el acceso abusivo a sistemas, la obstaculización ilegítima, la interceptación de datos y el daño informático. Esta disposición permite establecer una

relación jurídica entre determinadas amenazas de ciberseguridad y las consecuencias previstas por el ordenamiento penal colombiano (Congreso de Colombia, 2009). Ley 1273 de 2009

Desde esta perspectiva, la implementación de controles preventivos y detectivos puede contribuir a reducir la exposición de las organizaciones frente a incidentes que afecten sistemas, información y datos. La relación puede representarse de la siguiente manera:

Amenaza, vulnerabilidad, incidente, afectación del sistema o información, impacto organizacional y jurídico.

Gestión del riesgo tecnológico

La gestión del riesgo tecnológico constituye un elemento transversal de la ciberseguridad y del cumplimiento normativo. Esta gestión requiere identificar los activos de información, amenazas, vulnerabilidades, posibles impactos y controles existentes, con el propósito de determinar las acciones necesarias para el tratamiento de los riesgos.

El NIST CSF 2.0 incorpora una perspectiva de gobierno que permite integrar la ciberseguridad con la gestión empresarial del riesgo. Su estructura facilita que las organizaciones establezcan resultados esperados, prioricen acciones y comuniquen sus riesgos de ciberseguridad (Pascoe et al., 2024). NIST Cybersecurity Framework 2.0

De manera complementaria, Quinn et al. (2024) explican que el NIST SP 1303 proporciona orientaciones para integrar la información relacionada con el riesgo de ciberseguridad dentro de la gestión empresarial del riesgo, favoreciendo procesos de monitoreo, evaluación y ajuste entre diferentes unidades y programas organizacionales.

NIST SP 1303 – Enterprise Risk Management Quick-Start Guide

Por consiguiente, la gestión de riesgos tecnológicos debe constituir un proceso continuo y documentado que permita identificar cambios en los sistemas, nuevas amenazas, modificaciones regulatorias y necesidades de control. En el ámbito contable y financiero, este enfoque permite relacionar los riesgos tecnológicos con aquellos que podrían afectar la confiabilidad, integridad, disponibilidad y trazabilidad de la información financiera.

Controles de acceso y protección

Los controles de acceso constituyen mecanismos fundamentales para restringir la utilización de los sistemas de información a usuarios autorizados. Estos controles permiten establecer quién puede acceder a determinada información, bajo qué condiciones y con qué nivel de privilegios.

La ISO/IEC 27001:2022 establece un enfoque sistemático para gestionar los riesgos relacionados con la seguridad de la información y contempla la necesidad de establecer controles apropiados para preservar la confidencialidad, integridad y disponibilidad de los activos de información (ISO, 2022). ISO/IEC 27001:2022

En los sistemas de información contable y financiero, estos controles pueden comprender la identificación individual de usuarios, autenticación segura, autenticación multifactor, autorización por perfiles, gestión de privilegios, segregación de funciones, revisión periódica de usuarios, eliminación de cuentas inactivas, control de accesos privilegiados y registro de actividades.

Estos mecanismos permiten reducir el riesgo de acceso indebido y favorecen la trazabilidad de las operaciones realizadas dentro de los sistemas, aspecto especialmente

relevante cuando los sistemas procesan información financiera utilizada para la elaboración de estados financieros o para procedimientos de auditoría.

Monitoreo y gestión de incidentes

La ciberseguridad requiere mecanismos que permitan identificar oportunamente eventos que puedan comprometer la información o los sistemas. En este sentido, el monitoreo permite detectar actividades anómalas, accesos no autorizados, modificaciones de información, fallas y otros eventos relevantes para la seguridad.

El NIST CSF 2.0 establece las funciones Detect, Respond y Recover, evidenciando que la ciberseguridad no se limita a prevenir incidentes, sino que también requiere capacidad para detectarlos, responder a ellos y recuperar las operaciones afectadas (Pascoe et al., 2024). NIST CSF 2.0

Asimismo, Nelson et al. (2025) señalan que la respuesta ante incidentes debe incorporarse dentro de las actividades de gestión del riesgo de ciberseguridad y plantean recomendaciones para fortalecer la preparación, detección, respuesta, recuperación y mejora derivada de los incidentes. NIST SP 800-61 Rev. 3

Para los sistemas contables y financieros, estos mecanismos resultan relevantes debido a que un incidente puede comprometer registros, bases de datos, aplicaciones, documentos electrónicos o procesos relacionados con la generación de información financiera. En consecuencia, el monitoreo y la respuesta permiten reducir el tiempo de exposición y facilitar la recuperación de la información afectada.

Continuidad y recuperación de los sistemas de información

La ciberseguridad también debe contemplar la capacidad de una organización para mantener o recuperar sus procesos después de una interrupción. La disponibilidad de la información resulta particularmente importante cuando los procesos financieros y contables dependen de sistemas tecnológicos.

La ISO/IEC 27001:2022 considera la disponibilidad como uno de los atributos fundamentales de la seguridad de la información y plantea un proceso de gestión de riesgos orientado a proteger los activos de información frente a diferentes amenazas (ISO, 2022). ISO/IEC 27001:2022

Asimismo, el NIST CSF 2.0 incorpora la función Recover, orientada a restablecer los activos y operaciones afectados por incidentes de ciberseguridad y a desarrollar mecanismos de recuperación apropiados (Pascoe et al., 2024). NIST CSF 2.0

En este sentido, los mecanismos de continuidad pueden incluir copias de seguridad, recuperación de información, procedimientos de contingencia, sistemas alternos, pruebas de restauración, identificación de procesos críticos, asignación de responsabilidades y documentación de procedimientos de recuperación.

La implementación de estos mecanismos permite disminuir los efectos de interrupciones sobre procesos como facturación, recaudo, pagos, registros contables, conciliaciones y generación de informes financieros.

Relación entre ciberseguridad e información contable y financiera

Los sistemas de información contable y financiero procesan datos que sirven como soporte para la generación de información utilizada en la toma de decisiones. En consecuencia, la protección de estos sistemas requiere preservar características como integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad.

La Ley 1314 de 2009 establece que las normas de contabilidad e información financiera tienen como finalidad contribuir a que los informes contables y, particularmente, los estados financieros, proporcionen información comprensible, transparente, comparable, pertinente y confiable. Esta exigencia establece una relación conceptual con la protección de los sistemas que generan, procesan y almacenan dicha información (Congreso de Colombia, 2009). Ley 1314 de 2009

De manera complementaria, la ISO/IEC 27001:2022 plantea que la seguridad de la información debe preservar su confidencialidad, integridad y disponibilidad mediante un proceso sistemático de gestión del riesgo (ISO, 2022). ISO/IEC 27001:2022

Además, la Ley 527 de 1999 establece condiciones relacionadas con la integridad, conservación, accesibilidad y valor probatorio de los mensajes de datos, aspecto relevante cuando los registros y documentos asociados con las operaciones contables y financieras se encuentran en formato electrónico (Congreso de Colombia, 1999). Ley 527 de 1999

Por tanto, la ciberseguridad contribuye a proteger los elementos tecnológicos que soportan la información contable y financiera, mientras que el cumplimiento normativo establece las condiciones jurídicas, profesionales y técnicas que deben observarse en su tratamiento.

Ciberseguridad y control interno

La relación entre ciberseguridad y control interno se establece mediante la identificación y tratamiento de los riesgos que pueden afectar los objetivos organizacionales y la confiabilidad de la información.

En el ámbito profesional contable, la Ley 43 de 1990 establece responsabilidades relacionadas con el ejercicio de la profesión y la fe pública, mientras que el marco de aseguramiento incorporado en el Decreto 2420 de 2015 incluye las Normas Internacionales de Auditoría y demás normas de aseguramiento aplicables en Colombia. En este contexto, los sistemas de información y los controles que inciden sobre la información financiera adquieren importancia para la evaluación de riesgos y la obtención de evidencia de auditoría (Congreso de Colombia, 1990; Presidencia de la República de Colombia, 2015). Ley 43 de 1990 Decreto 2420 de 2015

Desde la perspectiva de la ciberseguridad, los controles tecnológicos pueden complementar los controles administrativos y operativos mediante mecanismos de autenticación, autorización, segregación de funciones, monitoreo, gestión de cambios, respaldo y recuperación. El NIST CSF 2.0 permite vincular la ciberseguridad con el gobierno y la gestión del riesgo organizacional, mientras que ISO/IEC 27001:2022 plantea un sistema de gestión orientado a identificar y tratar los riesgos relacionados con la seguridad de la información (Pascoe et al., 2024; ISO, 2022). NIST CSF 2.0 ISO/IEC 27001:2022

Por tanto, la relación puede representarse de la siguiente manera:

Control interno, identificación de riesgos, controles tecnológicos, monitoreo, evidencia, evaluación, mejora continua.

Esta articulación permite comprender que la ciberseguridad puede constituir un componente del sistema de control interno cuando los riesgos tecnológicos tienen incidencia sobre los procesos, operaciones y generación de información financiera.

Cumplimiento normativo y protección de la información

El análisis permite establecer que el cumplimiento normativo en materia de ciberseguridad debe entenderse como un proceso continuo, en el cual las organizaciones identifican las disposiciones que les resultan aplicables, determinan los riesgos asociados, implementan controles, monitorean su funcionamiento, conservan evidencias y actualizan sus mecanismos de protección.

Desde el ámbito contable, esta dinámica involucra la articulación de la normativa profesional, las normas de contabilidad e información financiera, las normas de aseguramiento y las disposiciones relacionadas con protección de datos, información electrónica y delitos informáticos. En Colombia, la Ley 43 de 1990, la Ley 1314 de 2009 y el Decreto 2420 de 2015 constituyen referentes fundamentales para el ejercicio profesional y el tratamiento de la información contable y financiera, mientras que las leyes 1581 de 2012, 1266 de 2008, 2157 de 2021, 527 de 1999 y 1273 de 2009 complementan el marco relacionado con la protección y seguridad de la información (Congreso de Colombia, 1990, 1999, 2008, 2009, 2012, 2021; Presidencia de la República de Colombia, 2015). Ley 43 de 1990 Ley 1314 de 2009 Decreto 2420 de 2015 Ley 1581 de 2012 Ley 1266 de 2008 Ley 2157 de 2021 Ley 527 de 1999 Ley 1273 de 2009

El NIST CSF 2.0 permite integrar la gestión de ciberseguridad con la gestión empresarial del riesgo y establecer resultados que pueden ser evaluados y comunicados (Pascoe et al., 2024). NIST CSF 2.0

Por su parte, Quinn et al. (2024), mediante el NIST SP 1303, plantean orientaciones para integrar la información relacionada con el riesgo de ciberseguridad dentro de la gestión empresarial del riesgo, favoreciendo el monitoreo, la evaluación y el ajuste de las acciones de gestión (Quinn et al., 2024). NIST SP 1303

En consecuencia, el cumplimiento normativo puede representarse como un ciclo:

Identificación de obligaciones, identificación de activos, evaluación de riesgos, establecimiento de controles, implementación, monitoreo, evidencia, evaluación del cumplimiento, acciones correctivas, mejora continua.

Esta relación permite establecer que la ciberseguridad no constituye únicamente un componente tecnológico, sino un elemento transversal de la gestión organizacional, el control interno, la protección de la información y el cumplimiento de las obligaciones profesionales y jurídicas relacionadas con los sistemas de información contable y financiero.

Tabla 10 Matriz de relación entre ciberseguridad y cumplimiento normativo en los sistemas de información

NORMA O REFERENTE	REQUERIMIENTO	RIESGO ASOCIADO	CONTROL CIBERSEGURIDAD	DE PROCESO CONTABLE/FINANCIERO	CONTRIBUCIÓN
LEY 1581 DE 2012	Seguridad y de confidencialidad de datos personales	Pérdida, adulteración o no acceso autorizado	Autenticación, autorización, cifrado y monitoreo	Bases de datos de clientes, empleados y proveedores	Protección y confidencialidad
LEY 1266 DE 2008	Seguridad de información financiera y crediticia	Alteración o uso no autorizado	Control de acceso y actualización	Información financiera y crediticia	Integridad y protección
LEY 2157 DE 2021	Fortalecimiento del hábeas data financiero	Tratamiento inadecuado	Gestión de acceso y control de información	Información financiera y crediticia	Cumplimiento normativo
LEY 527 DE 1999	Integridad y conservación de mensajes de datos	Alteración o pérdida	Trazabilidad, respaldo y control de cambios	Documentos y registros electrónicos	Integridad y evidencia
LEY 1273 DE 2009	Protección de la información y los sistemas	Acceso abusivo, daño, interceptación o malware	Autenticación, monitoreo y mecanismos de protección	Sistemas y bases de datos	Prevención y protección

ISO/IEC 27001:2022 | Gestión de la seguridad de la información | Riesgos sobre activos de información | SGSI y controles de seguridad | Procesos organizacionales, contables y financieros | Gestión integral del riesgo

Fuente: (Elaboración propia)

Tabla 11 Matriz de identificación, relación y cumplimiento normativo

CONCEPTO IDENTIFICADO EN LAS FASES I Y II	DEFINICIÓN / IDENTIFICACIÓN	RELACIÓN CON LA CIBERSEGURIDAD	RELACIÓN CON EL CUMPLIMIENTO NORMATIVO	CONTRIBUCIÓN A LA INTEGRIDAD Y LEGALIDAD DE LOS PROCESOS CONTABLES Y FINANCIEROS
CIBERSEGURIDAD	Conjunto de estrategias, controles y prácticas destinadas a proteger sistemas, redes, aplicaciones y datos frente a amenazas digitales.	Constituye el eje central para prevenir, detectar, responder y recuperar los sistemas ante incidentes.	Permite establecer controles alineados con normas de seguridad, protección de datos y gestión de riesgos.	Favorece que la información contable y financiera permanezca protegida, confiable y disponible.
SISTEMAS DE INFORMACIÓN	Conjunto integrado de personas, procesos, datos y tecnologías que permiten capturar, procesar, almacenar y generar información.	Constituyen el entorno donde se aplican los controles de ciberseguridad.	Deben operar bajo políticas y controles que garanticen la protección y tratamiento adecuado de la información.	Permiten mantener procesos contables trazables, verificables y consistentes.
ACTIVOS DE INFORMACIÓN	Datos, bases de datos, aplicaciones, equipos, infraestructura, documentos y demás recursos que tienen valor para la organización.	Su identificación permite determinar qué debe protegerse y frente a qué amenazas.	La gestión de activos permite establecer controles de protección y responsabilidades sobre la información.	Facilita proteger libros contables, comprobantes, estados financieros, bases de datos y registros electrónicos.
CONFIDENCIALIDAD	Garantía de que la información solamente sea	Se protege mediante autenticación, autorización,	Se relaciona con las obligaciones de protección	Reduce el riesgo de divulgación no autorizada de información financiera,

	accesible por personas autorizadas.	cifrado y controles de acceso.	de datos personales y reserva de información.	tributaria, laboral o de terceros.
INTEGRIDAD	Garantía de que la información permanezca completa, exacta y sin modificaciones no autorizadas.	Se fortalece mediante controles de acceso, registros de auditoría, validaciones y mecanismos de detección.	Permite cumplir requisitos relacionados con confiabilidad, conservación y protección de información.	Contribuye directamente a que los registros contables y estados financieros sean confiables y verificables.
DISPONIBILIDAD	Capacidad de acceder a la información y sistemas cuando son requeridos.	Se garantiza mediante respaldos, redundancia, recuperación y continuidad operativa.	Se relaciona con la obligación organizacional de mantener disponibles los sistemas y datos necesarios para la operación.	Permite mantener la continuidad de facturación, nómina, registros contables, pagos y reportes financieros.
AMENAZAS	Eventos o acciones potenciales que pueden afectar los sistemas o activos de información.	Incluyen malware, ransomware, phishing, fraude digital, accesos no autorizados y ataques de denegación de servicio.	El reconocimiento de amenazas permite establecer controles preventivos y de respuesta.	Disminuye la posibilidad de alteración, pérdida, divulgación o indisponibilidad de información financiera.
VULNERABILIDADES	Debilidades existentes en sistemas, procesos, personas o tecnologías que pueden ser aprovechadas por una amenaza.	Su identificación permite corregir debilidades antes de que sean explotadas.	Se vincula con la gestión preventiva de riesgos y la implementación de controles.	Reduce errores, accesos indebidos y manipulaciones que puedan afectar registros contables.
RIESGO DE CIBERSEGURIDAD	Posibilidad de que una amenaza aproveche una vulnerabilidad y genere consecuencias para la organización.	Permite priorizar los activos y controles que requieren mayor protección.	La gestión del riesgo permite demostrar que la organización identifica, evalúa y trata riesgos tecnológicos.	Contribuye a prevenir pérdidas financieras, interrupciones y afectaciones a la confiabilidad de la información.
GESTIÓN DE RIESGOS	Proceso mediante el cual se identifican, analizan, evalúan, tratan y monitorean riesgos.	Integra la ciberseguridad con la gestión empresarial.	Permite articular los controles tecnológicos con políticas y obligaciones legales y organizacionales.	Favorece la prevención de errores, fraudes y eventos que puedan afectar la información financiera.

CONTROLES DE CIBERSEGURIDAD	Medidas técnicas, administrativas y organizacionales destinadas a reducir los riesgos.	Constituyen los mecanismos concretos de protección de los sistemas y activos.	Permiten evidenciar la aplicación de políticas y requisitos de seguridad.	Fortalecen la confiabilidad, trazabilidad y protección de los procesos contables.
CONTROL DE ACCESO	Mecanismos que determinan quién puede ingresar a sistemas, aplicaciones y datos.	Incluye autenticación, autorización, contraseñas, MFA y segregación de privilegios.	Permite restringir el acceso de acuerdo con responsabilidades y necesidades legítimas.	Reduce la posibilidad de modificaciones o consultas no autorizadas en registros financieros.
AUTENTICACIÓN	Procedimiento mediante el cual se verifica la identidad de un usuario.	Constituye una barrera frente al acceso no autorizado.	Apoya el cumplimiento de políticas de seguridad y control de acceso.	Permite establecer responsabilidad sobre las operaciones realizadas en los sistemas contables.
TRAZABILIDAD	Capacidad de identificar y reconstruir las acciones realizadas sobre información o sistemas.	Se fortalece mediante logs, registros de actividad y mecanismos de auditoría.	Facilita demostrar el cumplimiento de procedimientos y controles.	Permite identificar quién creó, modificó o autorizó determinada información contable o financiera.
PROTECCIÓN DE DATOS PERSONALES	Conjunto de principios y mecanismos destinados a garantizar el tratamiento adecuado de datos personales.	Exige controles de seguridad para prevenir pérdida, alteración, acceso o uso no autorizado.	En Colombia se articula especialmente con la Ley 1581 de 2012.	Protege datos de clientes, trabajadores, proveedores y terceros contenidos en sistemas contables.
REGISTROS ELECTRÓNICOS	Información generada, almacenada o transmitida mediante medios electrónicos.	Requiere controles de integridad, autenticidad, conservación y acceso.	La Ley 527 de 1999 reconoce efectos jurídicos a los mensajes de datos y regula aspectos de su integridad y conservación.	Apoya la validez y trazabilidad de facturas, comprobantes, documentos y soportes electrónicos.
DETECCIÓN INCIDENTES	Proceso de identificación oportuna de eventos que pueden comprometer la seguridad.	Corresponde principalmente a la función Detect del NIST CSF 2.0.	Permite responder oportunamente frente a eventos que puedan generar incumplimientos o pérdidas de información.	Reduce el tiempo de exposición de los registros contables frente a alteraciones o accesos indebidos.
RESPUESTA INCIDENTES	Acciones ejecutadas después de identificar un evento de ciberseguridad.	Comprende contención, análisis, comunicación y mitigación del incidente.	Permite establecer procedimientos	Limita los efectos sobre la información financiera y

			documentados para enfrentar incidentes.	facilita la recuperación de registros afectados.
RECUPERACIÓN	Restablecimiento de sistemas, información y operaciones después de un incidente.	Incluye copias de seguridad, recuperación de sistemas y continuidad operativa.	Contribuye al cumplimiento de políticas de continuidad y gestión de riesgos.	Permite recuperar información contable y financiera y mantener la continuidad de las operaciones.
CONTINUIDAD DE LOS SISTEMAS DE INFORMACIÓN	Capacidad de mantener o restablecer las operaciones esenciales después de una interrupción.	Se relaciona directamente con la función Recover del NIST CSF 2.0.	Favorece la gestión de riesgos tecnológicos y operacionales.	Evita interrupciones prolongadas en facturación, contabilidad, tesorería y generación de informes financieros.
GOBERNANZA DE CIBERSEGURIDAD	Estructura mediante la cual se establecen responsabilidades, políticas, objetivos y supervisión de la seguridad.	Corresponde a la función Govern incorporada explícitamente en NIST CSF 2.0.	Permite relacionar las políticas internas con obligaciones legales y regulatorias.	Define responsabilidades sobre la protección y uso adecuado de la información financiera.
MONITOREO	Seguimiento continuo de sistemas, controles, riesgos e incidentes.	Permite identificar anomalías y verificar la eficacia de las medidas de protección.	Facilita demostrar que los controles no solo existen, sino que son supervisados.	Favorece la detección temprana de errores, fraudes y modificaciones indebidas.
CUMPLIMIENTO NORMATIVO	Observancia de leyes, reglamentos, normas técnicas, políticas y procedimientos aplicables.	La ciberseguridad proporciona mecanismos para cumplir requisitos relacionados con información y sistemas.	Integra normas de protección de datos, delitos informáticos, mensajes de datos y seguridad de la información.	Contribuye a que los procesos contables y financieros se desarrollen dentro del marco jurídico aplicable.
LEGALIDAD	Principio según el cual las actuaciones y procesos deben desarrollarse conforme al ordenamiento jurídico.	La ciberseguridad permite controlar el tratamiento, acceso, conservación y protección de la información.	Se relaciona con las obligaciones legales aplicables a datos, sistemas y registros electrónicos.	Disminuye riesgos derivados del tratamiento indebido de información contable y financiera.
INFORMACIÓN CONTABLE FINANCIERA	Y Información utilizada para registrar, controlar, analizar y comunicar las operaciones	Constituye un activo crítico que requiere confidencialidad, integridad, disponibilidad y trazabilidad.	Debe ser gestionada conforme a las normas contables, legales,	La ciberseguridad fortalece su confiabilidad, integridad, disponibilidad y evidencia documental.

económicas de la tributarias y de protección
organización. de información aplicables.

Fuente: (Elaboración propia)

Tabla 12 Matriz integral de conceptos, ciberseguridad y cumplimiento normativo

CONCEPTO DE LAS FASES I Y II	IDENTIFICACIÓN / SIGNIFICADO	RELACIÓN CON CIBERSEGURIDAD	NORMA, LEY O ESTÁNDAR RELACIONADO	APLICACIÓN AL EJERCICIO DEL CONTADOR PÚBLICO	CONTRIBUCIÓN A LA INTEGRIDAD Y LEGALIDAD DE LA INFORMACIÓN CONTABLE Y FINANCIERA
CIBERSEGURIDAD	Protección de sistemas, redes, aplicaciones y datos frente a amenazas digitales.	Constituye el eje de prevención, detección, respuesta y recuperación.	NIST CSF 2.0; ISO/IEC 27001:2022.	Protección de sistemas contables, ERP, información financiera y archivos digitales.	Reduce accesos indebidos, alteraciones, pérdidas y fraudes sobre información financiera.
SISTEMAS DE INFORMACIÓN	Integración de personas, procesos, datos y tecnologías para generar información.	Son el entorno donde se aplican los controles de seguridad.	Decreto 2420 de 2015 y sus modificaciones; NIST CSF 2.0.	Utilización de sistemas contables, financieros, tributarios y de auditoría.	Permite que la información financiera sea procesada y conservada de forma confiable.

ACTIVOS DE INFORMACIÓN	Datos, bases de datos, software, equipos, documentos y registros con valor organizacional.	Permiten determinar qué información debe protegerse.	ISO/IEC 27001:2022; NIST CSF 2.0.	Estados financieros, libros, comprobantes, facturas, nómina, declaraciones y bases de datos.	Facilita identificar y proteger información crítica para la toma de decisiones.
CONFIDENCIALIDAD	Acceso a la información únicamente por personas autorizadas.	Se garantiza mediante autenticación, autorización y cifrado.	ISO/IEC 27001:2022; Ley 1581 de 2012.	Protección de información de clientes, empleados, proveedores y empresas.	Evita divulgación indebida de información contable y financiera.
INTEGRIDAD	Información completa, exacta y libre de modificaciones no autorizadas.	Se protege mediante controles, registros de auditoría y validaciones.	ISO/IEC 27001:2022; Ley 527 de 1999; Ley 1273 de 2009.	Preservación de registros y soportes contables.	Contribuye directamente a la confiabilidad de estados financieros y registros contables.
DISPONIBILIDAD	Información accesible cuando sea necesaria.	Respaldos, redundancia, continuidad y recuperación.	ISO/IEC 27001:2022; NIST CSF 2.0.	Acceso oportuno a información necesaria para elaborar estados financieros y auditorías.	Evita interrupciones de los procesos contables y financieros.
AMENAZAS	Eventos potenciales que pueden afectar	Permiten anticipar ataques	NIST CSF 2.0; Ley 1273 de 2009.	Identificación de amenazas sobre	Reduce riesgos de fraude, pérdida y

	sistemas o ransomware, phishing o información. malware.	sistemas contables y financieros.	alteración de información.
VULNERABILIDADES	Debilidades de sistemas, procesos, personas o tecnologías. Pueden ser explotadas por amenazas.	NIST CSF 2.0; ISO/IEC 27001:2022.	Identificación de Disminuye la probabilidad de incidentes que afecten la información financiera.
RIESGO DE CIBERSEGURIDAD	Posibilidad de que una amenaza aproveche una vulnerabilidad y produzca un impacto. Orienta la priorización de controles.	NIST CSF 2.0; ISO/IEC 27001:2022.	Evaluación de riesgos tecnológicos en procesos contables y de auditoría. Permite prevenir pérdidas económicas y afectaciones a la información.
GESTIÓN DEL RIESGO	Identificación, análisis, tratamiento y monitoreo de riesgos. Integra la seguridad con la gestión organizacional.	NIST CSF 2.0; ISO 31000:2018.	Evaluación de riesgos relacionados con información financiera. Fortalece el control preventivo y la toma de decisiones.
CONTROL INTERNO	Políticas y procedimientos destinados a controlar operaciones y riesgos. Incluye controles tecnológicos y de acceso.	Ley 43 de 1990; Decreto 2420 de 2015; NIA 315.	Evaluación de controles internos por el contador y auditor. Favorece la confiabilidad de la información y la prevención del fraude.

GOBERNANZA		Dirección, responsabilidades, políticas y supervisión de la seguridad.	Define quién administra y supervisa los riesgos de ciberseguridad.	NIST CSF 2.0; ISO/IEC 27001:2022.	Definición de responsabilidades sobre información contable y financiera.	Favorece la responsabilidad y cumplimiento institucional.
CONTROL DE ACCESO		Restricción del ingreso a sistemas y datos según autorización.	Evita accesos no autorizados.	ISO/IEC 27001:2022; Ley 1581 de 2012.	Separación de perfiles para contadores, auxiliares, administradores y auditores.	Reduce modificaciones fraudulentas o no autorizadas.
AUTENTICACIÓN		Verificación de la identidad del usuario.	Controla el acceso a sistemas.	ISO/IEC 27001:2022.	Acceso individualizado a plataformas contables y financieras.	Permite atribuir operaciones a usuarios determinados.
SEGREGACIÓN DE FUNCIONES		Distribución de responsabilidades entre diferentes personas.	Disminuye la posibilidad de abuso de privilegios.	NIA 315; COSO; Decreto 2420 de 2015.	Separación entre registro, autorización, custodia y revisión.	Reduce errores y riesgos de fraude financiero.
TRAZABILIDAD		Capacidad de identificar qué ocurrió, cuándo y quién realizó una operación.	Se logra mediante logs y registros de actividad.	Ley 527 de 1999; NIA 500; NIA 530.	Seguimiento de modificaciones y transacciones contables.	Permite verificar y sustentar operaciones financieras.

EVIDENCIA AUDITORÍA	DE	Información utilizada por el auditor para fundamentar sus conclusiones.	Requiere preservar autenticidad, integridad y disponibilidad.	NIA 500; Decreto 2420 de 2015.	Obtención y evaluación de evidencia electrónica y documental.	Fortalece la sustentación de las conclusiones del auditor.
INFORMACIÓN FINANCIERA		Información sobre situación, rendimiento y flujos financieros de una entidad.	Debe protegerse frente a pérdida, alteración y acceso indebido.	NIIF / Decreto 2420 de 2015 y modificaciones vigentes.	Preparación y presentación de estados financieros.	Favorece información confiable para usuarios internos y externos.
NIIF		Normas para reconocimiento, medición, presentación y revelación de información financiera.	Los sistemas deben proteger los datos utilizados para aplicar las NIIF.	Ley 1314 de 2009; Decreto 2420 de 2015; Decreto 701 de 2026.	Preparación de información financiera bajo el marco aplicable al grupo de la entidad.	Contribuye a la comparabilidad, transparencia y confiabilidad de la información.
NIIF PARA PYMES		Marco de información financiera aplicable al Grupo 2.	Requiere protección de los datos que sustentan los estados financieros.	Decreto 2420 de 2015; Decreto 701 de 2026.	Preparación de información financiera de PYMES.	Permite generar información financiera conforme al marco técnico vigente.
GRUPO 3 / MICROEMPRESAS		Marco de contabilidad simplificada para las microempresas que	Requiere controles proporcionales para	Decreto 2420 de 2015, Anexo 3 y	Registro y presentación simplificada de	Protege la confiabilidad de la

	cumplen los proteger registros y modificaciones información información de las requisitos soportes. aplicables. financiera. microempresas. correspondientes.
NIAS	Normas Exigen considerar Decreto 2420 de Planeación, Contribuyen a Internacionales de riesgos, controles y 2015, Anexo 4. evaluación de obtener evidencia Auditoría aplicables a evidencia, incluidos los riesgos, suficiente y trabajos de auditoría riesgos tecnológicos procedimientos y adecuada para según el marco cuando sean evidencia de sustentar el informe. colombiano. relevantes. auditoría.
NIA 200	Objetivos generales Exige una auditoría Decreto 2420 de Orienta la Favorece la del auditor basada en principios 2015, Anexo 4. responsabilidad credibilidad de la independiente. profesionales y general del auditor. información evidencia. auditada.
NIA 300	Planeación de una Permite incorporar Decreto 2420 de Planeación de Favorece una auditoría de estados riesgos tecnológicos en 2015, Anexo 4. procedimientos de auditoría organizada financieros. la planificación cuando auditoría. y orientada a sean relevantes. riesgos.
NIA 315	Identificación y Es especialmente Decreto 2420 de Evaluación del Permite identificar valoración de riesgos relevante cuando los 2015, Anexo 4. sistema de riesgos que podrían de incorrección sistemas de información y afectar la material. información intervienen controles relevantes confiabilidad de en procesos para la auditoría. estados financieros. financieros.

NIA 330	Respuestas del auditor frente a riesgos valorados.	Permite diseñar procedimientos de auditoría frente a riesgos identificados.	Decreto 2420 de 2015, Anexo 4.	Aplicación de pruebas y procedimientos de auditoría.	Fortalece la respuesta frente a riesgos de incorrección material.
NIA 500	Evidencia de auditoría.	Incluye la necesidad de evaluar la confiabilidad de la información utilizada.	Decreto 2420 de 2015, Anexo 4.	Evaluación de documentos, registros y evidencia electrónica.	Fortalece la trazabilidad y sustentación de las conclusiones.
CÓDIGO DE ÉTICA	Principios éticos aplicables al contador público.	Implica manejo responsable y confidencial de información.	Ley 43 de 1990; Decreto 2420 de 2015, Anexo 4.	Actuación profesional del contador.	Contribuye a la confianza, integridad y responsabilidad profesional.
FE PÚBLICA	Facultad legal del contador público para dar fe en asuntos propios de su profesión.	Requiere especial protección de la información sobre la cual se emiten certificaciones o dictámenes.	Ley 43 de 1990.	Certificaciones, dictámenes y actuaciones profesionales.	Refuerza la responsabilidad sobre la veracidad e integridad de la información.
PROTECCIÓN DE DATOS PERSONALES	Protección jurídica de los datos de personas naturales.	Exige controles de seguridad para evitar acceso, pérdida, alteración o uso indebido.	Ley 1581 de 2012; Decreto 1377 de 2013; Decreto 255 de 2022.	Tratamiento de información de clientes, empleados, proveedores y terceros.	Garantiza legalidad, seguridad y confidencialidad en el tratamiento de datos.

HÁBEAS FINANCIERO	DATA	Derecho relacionado con el tratamiento de información financiera, crediticia y comercial.	Exige proteger bases de datos y garantizar calidad y actualización de información.	Ley 1266 de 2008; Ley 2157 de 2021.	Manejo de información financiera y crediticia.	Favorece exactitud, actualización y protección de información financiera.
INFORMACIÓN FINANCIERA, CREDITICIA COMERCIAL	Y	Datos relacionados con obligaciones, comportamiento financiero y relaciones comerciales.	Son activos sensibles que requieren protección.	Ley 1266 de 2008 y Ley 2157 de 2021.	Procesos contables, financieros y de análisis empresarial.	Protege la calidad y seguridad de la información utilizada para decisiones financieras.
DATOS ELECTRÓNICOS		Información generada, enviada, recibida o almacenada mediante sistemas electrónicos.	Requieren integridad, autenticidad y disponibilidad.	Ley 527 de 1999.	Facturación, comprobantes, comunicaciones y documentos electrónicos.	Favorece la validez y conservación de soportes contables.
INTEGRIDAD DOCUMENTOS ELECTRÓNICOS	DE	Conservación completa e inalterada de la información electrónica.	Requiere controles contra modificación o eliminación no autorizada.	Ley 527 de 1999.	Conservación de libros, documentos y soportes electrónicos.	Fortalece el valor probatorio y la trazabilidad.
DELITOS INFORMÁTICOS		Conductas ilícitas contra información,	Comprende acceso abusivo, daño informático,	Ley 1273 de 2009.	Protección de sistemas utilizados para información	Refuerza la protección jurídica de la información.

	datos y sistemas informáticos.	interceptación y otras conductas.		contable y financiera.	
SEGURIDAD DE LA INFORMACIÓN	Protección de información frente a amenazas y riesgos.	Integra controles técnicos, administrativos y organizacionales.	ISO/IEC 27001:2022.	Protección de información profesional, contable y financiera.	Preserva confidencialidad, integridad y disponibilidad.
GESTIÓN DE INCIDENTES	Preparación, detección, respuesta y recuperación ante incidentes.	Permite reducir el impacto de ataques.	NIST CSF 2.0; NIST SP 800-61 Rev. 3.	Respuesta frente a incidentes que afectan sistemas contables.	Reduce pérdida de información y tiempos de interrupción.
CONTINUIDAD	Capacidad de mantener o recuperar procesos después de una interrupción.	Respaldos, recuperación y planes de contingencia.	NIST CSF 2.0; ISO/IEC 27001:2022.	Continuidad de procesos contables y financieros.	Permite mantener la disponibilidad de la información.
MONITOREO	Seguimiento permanente de riesgos, controles y eventos.	Permite detectar comportamientos anómalos.	NIST CSF 2.0; ISO/IEC 27001:2022.	Supervisión de sistemas y controles contables.	Facilita detectar oportunamente errores, fraudes o accesos indebidos.
CUMPLIMIENTO NORMATIVO	Observancia de leyes, decretos, estándares y obligaciones profesionales.	Integra controles de ciberseguridad con obligaciones jurídicas.	Ley 43 de 1990; Ley 1314 de 2009; Decreto 2420 de 2015; legislación de datos y delitos informáticos.	Marco integral de actuación del contador público.	Permite que la información y los procesos se desarrollen conforme al

					ordenamiento aplicable.
LEGALIDAD	Actuación conforme a la legislación vigente.	La seguridad contribuye a garantizar tratamiento lícito de información.	Ley 43 de 1990; Ley 1581 de 2012; Ley 527 de 1999; Ley 1273 de 2009.	Actuación profesional y manejo de información.	Reduce riesgos jurídicos y fortalece la confianza en la información.

Fuente: (Elaboración propia)

FASE III

En la tercera etapa se realizará un análisis bibliográfico orientado a identificar las principales ventajas, limitaciones y desafíos asociados con la implementación de medidas de ciberseguridad en los sistemas de información, con especial atención a aquellos utilizados para gestionar información financiera y contable. Para ello, se considerarán investigaciones académicas, estándares internacionales, informes técnicos y documentos institucionales que permitan analizar los efectos de los controles de ciberseguridad sobre la protección de los activos de información, la gestión del riesgo, la continuidad operativa y el cumplimiento de obligaciones.

El NIST Cybersecurity Framework 2.0 señala que la gestión de la ciberseguridad puede contribuir a que las organizaciones comprendan, evalúen, prioricen y comuniquen sus esfuerzos para gestionar los riesgos de ciberseguridad. El marco puede ser utilizado por organizaciones de diferentes tamaños, sectores y niveles de madurez, lo cual permite adaptar las medidas de protección a las características y necesidades particulares de cada organización (National Institute of Standards and Technology [NIST], 2024). NIST Cybersecurity Framework 2.0

Ventajas en la implementación

Entre las principales ventajas que serán analizadas se encuentran la protección de los activos de información, reducción de la exposición a amenazas, prevención de accesos no autorizados, fortalecimiento de la confidencialidad, integridad y disponibilidad, mejora de la capacidad de respuesta ante incidentes, continuidad operativa, fortalecimiento de la confianza de las partes interesadas y apoyo al cumplimiento de requisitos legales y regulatorios. La ISO/IEC 27001:2022 plantea que un sistema de gestión de seguridad de la información permite gestionar los riesgos relacionados con la información y favorecer la resiliencia frente a incidentes, la protección de la integridad, confidencialidad y disponibilidad de los datos y la integración de la seguridad en los procesos organizacionales (International Organization for Standardization [ISO], 2022). ISO/IEC 27001:2022

En relación con la protección de la información, las medidas de ciberseguridad permiten establecer controles orientados a preservar los activos frente a diferentes amenazas. El ENISA Threat Landscape 2024 identifica amenazas relacionadas con la disponibilidad, ransomware, datos, ataques de ingeniería social y otras modalidades, y analiza medidas de mitigación asociadas con estos riesgos. Estos resultados permiten sustentar la importancia de implementar controles preventivos, detectivos y de respuesta en los sistemas de información (European Union Agency for Cybersecurity [ENISA], 2024). ENISA Threat Landscape 2024

Otra ventaja se relaciona con la gestión y priorización de los riesgos. El NIST CSF 2.0 incorpora una función de gobierno y establece resultados que pueden utilizarse para comprender y priorizar los riesgos de ciberseguridad. De esta manera, la organización puede orientar recursos hacia aquellos activos, procesos y amenazas que presentan mayor relevancia para sus objetivos (NIST, 2024). NIST CSF 2.0

La implementación de controles también puede contribuir a la continuidad operativa. Las medidas relacionadas con copias de seguridad, recuperación, respuesta ante incidentes y disponibilidad permiten reducir las consecuencias de eventos que interrumpan los sistemas de información. En este sentido, el NIST CSF 2.0 incorpora la función Recover, orientada a desarrollar y ejecutar actividades apropiadas para restaurar los activos y operaciones afectados por incidentes de ciberseguridad (NIST, 2024). NIST Cybersecurity Framework 2.0

La ciberseguridad también puede contribuir al cumplimiento regulatorio, debido a que determinados controles permiten demostrar que la organización adopta medidas para proteger la información y gestionar los riesgos asociados con su tratamiento. La ISO/IEC 27001:2022 plantea un sistema de gestión que permite establecer procesos sistemáticos para identificar y tratar riesgos de seguridad de la información, mientras que el NIST CSF 2.0 facilita la organización de resultados y prácticas relacionadas con la gestión del riesgo (ISO, 2022; NIST, 2024). ISO/IEC 27001:2022 NIST CSF 2.0

En el ámbito de los sistemas de información financieros y contables, estas ventajas adquieren particular relevancia debido a que una afectación de la información puede comprometer registros, documentos electrónicos, bases de datos, procesos de facturación, cuentas por cobrar, cuentas por pagar, nómina, conciliaciones y generación de informes financieros. Por ello, la aplicación de controles de seguridad puede contribuir a preservar las características de calidad de la información y reducir riesgos asociados con su pérdida, alteración o indisponibilidad.

De igual manera, se estudiarán las posibles desventajas, limitaciones y desafíos derivados de la implementación de estas medidas. Entre ellos se encuentran los costos de implementación y mantenimiento, requerimientos de capacitación, disponibilidad de personal especializado, complejidad tecnológica, necesidad de actualización

permanente, integración con sistemas existentes, gestión de terceros y posibles dificultades relacionadas con las capacidades organizacionales.

El World Economic Forum (2024) señala que las organizaciones enfrentan diferencias importantes en sus capacidades de ciberseguridad y que la escasez de talento especializado constituye uno de los desafíos del entorno. El informe también evidencia diferencias entre organizaciones de distinto tamaño en materia de resiliencia cibernética, aspecto que resulta relevante al analizar las condiciones necesarias para implementar medidas de seguridad de manera sostenible (World Economic Forum, 2024). Global Cybersecurity Outlook 2024

La disponibilidad de recursos humanos y financieros constituye, por tanto, una condición que debe considerarse en el análisis. La implementación de medidas de ciberseguridad requiere inversiones en infraestructura, software, capacitación, monitoreo, mantenimiento y actualización. ENISA (2024) señala la necesidad de fortalecer las capacidades y recursos destinados a la ciberseguridad para responder a un entorno de amenazas en evolución. 2024 Report on the State of Cybersecurity in the Union

Otra limitación corresponde a la complejidad tecnológica y organizacional. La implementación de controles no depende exclusivamente de adquirir herramientas tecnológicas, sino de integrarlas con procesos, políticas, personas y responsabilidades. ISO (2022) plantea precisamente un enfoque integral de seguridad de la información que considera personas, políticas y tecnología, lo cual implica que las organizaciones deben desarrollar capacidades organizacionales además de implementar soluciones técnicas. ISO/IEC 27001:2022

También puede presentarse una dependencia de personal especializado, especialmente cuando las organizaciones requieren administrar sistemas de monitoreo, respuesta ante incidentes, análisis de vulnerabilidades, gestión de identidades y otros

controles especializados. El World Economic Forum (2024) identifica la escasez de competencias y talento en ciberseguridad como uno de los desafíos que afectan la capacidad de las organizaciones para desarrollar y mantener sus capacidades de protección. Global Cybersecurity Outlook 2024

La actualización permanente de los controles constituye otro desafío. Las amenazas evolucionan y aparecen nuevas técnicas de ataque, vulnerabilidades y modalidades de afectación. ENISA (2024) muestra que el panorama de amenazas cambia continuamente y que las organizaciones deben ajustar sus estrategias de mitigación de acuerdo con los riesgos identificados. Por consiguiente, la implementación de ciberseguridad debe entenderse como un proceso dinámico y no como una actividad realizada una única vez. ENISA Threat Landscape 2024

Asimismo, la integración entre sistemas puede representar una dificultad cuando las organizaciones poseen aplicaciones desarrolladas en diferentes momentos, plataformas de distintos proveedores o sistemas que no utilizan estructuras homogéneas. Esta situación puede requerir procesos adicionales de configuración, migración, interoperabilidad y gestión de riesgos, particularmente cuando los sistemas de información financieros se encuentran conectados con plataformas bancarias, tributarias, comerciales, de nómina o de facturación electrónica.

En consecuencia, el análisis de esta etapa no buscará establecer una valoración general sobre la implementación de medidas de ciberseguridad, sino identificar, a partir de la literatura revisada, las diferentes perspectivas relacionadas con sus beneficios, limitaciones y condiciones de implementación. De esta manera, se podrá comprender que las medidas de ciberseguridad pueden fortalecer la protección de los sistemas de información, pero su implementación también requiere recursos, capacidades, actualización, planificación y gestión organizacional.

Ventajas de la implementación de medidas de ciberseguridad

Las ventajas identificadas en la literatura pueden organizarse en tres dimensiones principales: protección de la información, eficiencia operativa y cumplimiento regulatorio.

a. Protección de la información

La implementación de controles de ciberseguridad contribuye a proteger la confidencialidad, integridad y disponibilidad de los activos de información. ISO/IEC 27001:2022 establece un enfoque basado en riesgos que permite identificar vulnerabilidades y aplicar medidas para proteger la información frente a diferentes amenazas (ISO, 2022). ISO/IEC 27001:2022

Entre las principales ventajas se encuentran:

- Reducción de accesos no autorizados;
- Protección de datos personales y financieros;
- Reducción del riesgo de modificación no autorizada;
- Protección frente a pérdida o destrucción de información;
- Fortalecimiento de la autenticación;
- Mayor trazabilidad de las operaciones;
- Fortalecimiento de las copias de seguridad;
- Detección temprana de incidentes;
- Recuperación de información después de una interrupción.

Estas ventajas son especialmente relevantes para los sistemas contables y financieros, debido a que la información procesada en ellos constituye un activo necesario para la operación y para la generación de informes financieros.

b. Eficiencia operativa

Las medidas de ciberseguridad también pueden contribuir a organizar y formalizar los procesos de gestión de riesgos y controles. El NIST CSF 2.0 permite estructurar las actividades de ciberseguridad mediante funciones y resultados que facilitan la identificación, priorización y comunicación de los riesgos (NIST, 2024). NIST CSF 2.0

En consecuencia, pueden generarse beneficios relacionados con:

- Mayor organización de los controles;
- Identificación de procesos críticos;
- Reducción de interrupciones;
- Establecimiento de responsabilidades;
- Mejor respuesta ante incidentes;
- Fortalecimiento de procesos de respaldo;
- Mejora de la continuidad operativa;
- Apoyo a la toma de decisiones sobre riesgos tecnológicos.

c. Cumplimiento regulatorio

La implementación de controles puede facilitar el cumplimiento de obligaciones relacionadas con la protección y tratamiento de la información. ISO/IEC 27001:2022 permite establecer un sistema de gestión documentado y basado en riesgos, mientras que los marcos como NIST CSF 2.0 permiten organizar resultados de seguridad y relacionarlos con las necesidades de la organización (ISO, 2022; NIST, 2024). ISO/IEC 27001:2022 NIST CSF 2.0

Para los sistemas de información contable y financiero, esto puede contribuir a demostrar la existencia de políticas, controles, procedimientos y evidencias relacionadas con la protección de la información.

Desventajas, limitaciones y desafíos

Las desventajas y limitaciones deben analizarse como condiciones que pueden dificultar la implementación o sostenibilidad de las medidas de ciberseguridad.

a. Costos de implementación y mantenimiento

La implementación de controles puede requerir recursos para adquisición de tecnologías, configuración, mantenimiento, monitoreo, actualización y capacitación. Por esta razón, las organizaciones deben establecer prioridades de acuerdo con sus riesgos, objetivos y capacidades financieras.

El NIST CSF 2.0 plantea que las organizaciones pueden utilizar el marco para comprender y priorizar sus esfuerzos de ciberseguridad, lo que permite relacionar las acciones de seguridad con las necesidades y capacidades particulares de cada organización (NIST, 2024). NIST CSF 2.0

b. Necesidad de capacitación

Las medidas de ciberseguridad requieren conocimientos y competencias por parte de los responsables de los sistemas y de los usuarios. El World Economic Forum (2024) identifica la disponibilidad de talento y competencias como uno de los desafíos del entorno mundial de ciberseguridad. Global Cybersecurity Outlook 2024

En los sistemas contables, esta necesidad incluye tanto al personal encargado de administrar los sistemas como a los usuarios que manejan información financiera, debido a que comportamientos inadecuados pueden incrementar la exposición a amenazas como phishing, ingeniería social o uso indebido de credenciales.

c. Complejidad tecnológica

La diversidad de aplicaciones, plataformas, dispositivos, servicios en la nube y sistemas heredados puede aumentar la complejidad de la gestión de seguridad. En consecuencia, las organizaciones requieren mecanismos de integración, monitoreo y actualización que permitan mantener un nivel de protección coherente.

d. Actualización permanente

Las amenazas evolucionan continuamente. ENISA (2024) documenta la evolución de las amenazas y técnicas utilizadas contra organizaciones, lo que evidencia la necesidad de revisar periódicamente las medidas de protección y adaptar los controles a las nuevas condiciones del entorno. ENISA Threat Landscape 2024

e. Dependencia de personal especializado

La administración de determinadas soluciones de seguridad puede requerir competencias técnicas específicas. Esta situación puede representar una limitación para organizaciones con recursos humanos reducidos o con dificultades para acceder a profesionales especializados. El World Economic Forum (2024) identifica precisamente la brecha de capacidades como uno de los retos del ecosistema de ciberseguridad. Global Cybersecurity Outlook 2024

f. Integración con sistemas existentes

La incorporación de nuevos controles puede requerir ajustes en aplicaciones, bases de datos, procesos y procedimientos existentes. En sistemas financieros, estos cambios deben gestionarse cuidadosamente para evitar interrupciones de los procesos contables y garantizar que las medidas de seguridad sean compatibles con las necesidades operativas.

Impacto sobre la protección de la información

La implementación de medidas de ciberseguridad tiene como uno de sus principales propósitos reducir los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información. ISO/IEC 27001:2022 identifica estos tres atributos como componentes fundamentales de la seguridad de la información y propone un enfoque basado en la gestión del riesgo (ISO, 2022). ISO/IEC 27001:2022

Para los sistemas de información financieros, la protección de estos atributos resulta relevante porque una alteración, pérdida, divulgación o indisponibilidad de los datos puede afectar procesos como registros contables, conciliaciones, facturación, cartera, pagos y elaboración de informes financieros.

Por ello, las medidas de ciberseguridad pueden relacionarse con la protección de los siguientes elementos:

Activos de información, confidencialidad, integridad, disponibilidad, trazabilidad, recuperación.

Impacto sobre la eficiencia operativa

La eficiencia operativa se relaciona con la capacidad de desarrollar los procesos de manera organizada, continua y con un uso adecuado de los recursos. En este contexto, la ciberseguridad puede contribuir a establecer procedimientos de identificación de riesgos, asignación de responsabilidades, monitoreo, respuesta y recuperación.

El NIST CSF 2.0 proporciona una estructura que permite organizar las actividades de ciberseguridad y adaptarlas a las necesidades de la organización, independientemente de su tamaño o sector (NIST, 2024). NIST CSF 2.0

Sin embargo, la eficiencia no debe interpretarse exclusivamente como reducción de costos. La implementación de controles puede inicialmente incrementar actividades de supervisión, capacitación, documentación y monitoreo. Por esta razón, el análisis bibliográfico deberá considerar tanto los beneficios operativos como los recursos necesarios para alcanzarlos.

Impacto sobre el cumplimiento regulatorio

Las medidas de ciberseguridad pueden apoyar el cumplimiento regulatorio mediante la implementación de controles, políticas, procedimientos y mecanismos de evidencia. En el contexto colombiano, esta relación adquiere importancia frente a disposiciones relacionadas con la protección de datos personales, información financiera, registros electrónicos y protección de los sistemas informáticos.

La Ley 1581 de 2012 establece el principio de seguridad para el tratamiento de datos personales y exige medidas técnicas, humanas y administrativas destinadas a evitar adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento a la información. Por tanto, los controles de ciberseguridad pueden constituir mecanismos de apoyo para atender estas obligaciones (Congreso de Colombia, 2012). Ley 1581 de 2012

De igual manera, la Ley 527 de 1999 establece disposiciones relacionadas con los mensajes de datos y su integridad y conservación, aspecto que adquiere relevancia en los procesos contables y financieros que utilizan documentos y registros electrónicos (Congreso de Colombia, 1999). Ley 527 de 1999

Por consiguiente, la ciberseguridad puede contribuir al cumplimiento regulatorio cuando los controles implementados permiten proteger la información, conservar evidencias, restringir accesos y demostrar la existencia de procedimientos de gestión y protección.

Matriz comparativa de ventajas y desventajas

Tabla 13 Matriz comparativa de ventajas y desventajas

DIMENSIÓN	MEDIDA DE CIBERSEGURIDAD	VENTAJAS IDENTIFICADAS	DESVENTAJAS, LIMITACIONES O DESAFÍOS	IMPACTO EN SISTEMAS FINANCIEROS Y CONTABLES
PROTECCIÓN DE INFORMACIÓN	Control de acceso	Reduce accesos no autorizados.	los no administración permanente de usuarios y privilegios.	Requiere la información financiera y contable. Protege la
PROTECCIÓN DE INFORMACIÓN	Autenticación multifactor	Incrementa seguridad acceso.	la del costos y adaptación de los usuarios.	Puede generar requerir de los de credenciales. Reduce el riesgo de uso indebido
PROTECCIÓN DE INFORMACIÓN	Cifrado	Protege información durante almacenamiento y la transmisión.	la el gestión adecuada de claves.	Requiere infraestructura y información financiera sensible. Protege la información

F-DC-125

INFORME FINAL DE TRABAJO DE GRADO EN MODALIDAD DE PROYECTO
DE INVESTIGACIÓN, DESARROLLO TECNOLÓGICO, MONOGRAFÍA,
EMPREDIMIENTO Y SEMINARIO

VERSIÓN: 2.0

PROTECCIÓN DE INFORMACIÓN	Copias de seguridad	Permiten recuperar información ante pérdidas o incidentes.	Requieren almacenamiento, pruebas y mantenimiento.	Facilitan la recuperación de registros contables.
PROTECCIÓN DE INFORMACIÓN	Monitoreo	Facilita la detección de actividades anómalas.	Requiere herramientas y personal capacitado.	Permite identificar modificaciones o accesos inusuales.
PROTECCIÓN DE INFORMACIÓN	Gestión de vulnerabilidades	Permite identificar y corregir debilidades.	Requiere evaluaciones periódicas y actualización.	Reduce riesgos sobre los sistemas contables.
EFICIENCIA OPERATIVA	Automatización de controles	Reduce tareas manuales y mejora la consistencia.	Requiere configuración, integración y mantenimiento.	Facilita los controles sobre operaciones financieras.
EFICIENCIA OPERATIVA	Gestión de incidentes	Permite responder de manera estructurada.	Requiere procedimientos, responsables y capacitación.	Reduce el impacto de incidentes sobre procesos contables.
EFICIENCIA OPERATIVA	Continuidad y recuperación	Reduce interrupciones y facilita la restauración.	Requiere inversión y pruebas periódicas.	Mantiene procesos de facturación, pagos y contabilidad.
EFICIENCIA OPERATIVA	Gestión centralizada de seguridad	Facilita la supervisión de los controles.	Puede incrementar la complejidad inicial.	Facilita la supervisión de sistemas financieros.

CUMPLIMIENTO REGULATORIO	Políticas de seguridad	Formalizan responsabilidades y procedimientos.	Deben actualizarse y comunicarse permanentemente.	Apoyan el cumplimiento de obligaciones de protección.
CUMPLIMIENTO REGULATORIO	Registro de actividades	Genera evidencia y trazabilidad.	Requiere almacenamiento y protección de registros.	Facilita la auditoría de operaciones financieras.
CUMPLIMIENTO REGULATORIO	Protección de datos	Apoya el cumplimiento de obligaciones sobre datos personales.	Requiere identificar los datos y aplicar controles adecuados.	Protege datos de clientes, trabajadores y proveedores.
CUMPLIMIENTO REGULATORIO	Gestión de riesgos	Permite identificar y tratar riesgos de manera documentada.	Requiere recursos y seguimiento continuo.	Fortalece el control de riesgos financieros y tecnológicos.
CUMPLIMIENTO REGULATORIO	Evidencia de controles	Permite demostrar las acciones de cumplimiento.	Requiere documentación y conservación de evidencias.	Facilita procesos de auditoría y revisión.

Fuente: (Elaboración propia 2026)

El análisis bibliográfico realizado permitió establecer que la implementación de medidas de ciberseguridad en los sistemas de información financieros constituye un componente relevante para la protección de los activos de información, la gestión de los riesgos tecnológicos, la continuidad de las operaciones y el cumplimiento de las obligaciones relacionadas con el tratamiento y protección de la información. Los referentes analizados coinciden en que la ciberseguridad debe abordarse mediante una combinación de controles tecnológicos, procedimientos organizacionales, gestión del riesgo, capacitación de los usuarios y mecanismos de seguimiento y mejora continua

(National Institute of Standards and Technology [NIST], 2024; International Organization for Standardization [ISO], 2022).

En la dimensión de protección de la información, se identificó que las principales ventajas están relacionadas con el fortalecimiento de la confidencialidad, integridad y disponibilidad de los datos. La aplicación de controles de acceso, autenticación, copias de seguridad, monitoreo, detección de incidentes y mecanismos de recuperación permite reducir la exposición de los activos de información frente a accesos no autorizados, alteraciones, pérdidas, destrucción o indisponibilidad. Esta situación adquiere especial importancia en los sistemas financieros y contables, debido a que estos procesan información necesaria para registros contables, facturación, cartera, pagos, nómina, conciliaciones y generación de informes financieros (ISO, 2022; ENISA, 2024).

El análisis también permitió establecer que la ciberseguridad contribuye a fortalecer la gestión y priorización de los riesgos. El NIST Cybersecurity Framework 2.0 propone un enfoque que permite a las organizaciones identificar, comprender, priorizar y comunicar sus esfuerzos de gestión del riesgo de ciberseguridad. En consecuencia, las organizaciones pueden orientar sus recursos hacia los activos, procesos y amenazas que requieren mayor atención, considerando sus características, objetivos y capacidades particulares (NIST, 2024).

Respecto de la eficiencia operativa, se identificó que las medidas de ciberseguridad pueden favorecer una mayor organización de los controles, definición de responsabilidades, identificación de procesos críticos, establecimiento de mecanismos de respaldo y fortalecimiento de las capacidades de respuesta y recuperación. El NIST CSF 2.0 estructura la gestión de la ciberseguridad mediante las funciones Govern, Identify, Protect, Detect, Respond y Recover, proporcionando una estructura para organizar las actividades relacionadas con la gestión del riesgo y la protección de los sistemas de información (NIST, 2024).

Sin embargo, el análisis evidenció que la implementación de controles de ciberseguridad también implica limitaciones y desafíos. Entre los principales se encuentran los costos de adquisición, implementación y mantenimiento de tecnologías, la necesidad de capacitación permanente, la disponibilidad de personal especializado, la complejidad de integrar diferentes plataformas y sistemas, la actualización continua de los controles y la necesidad de adaptar las medidas de protección a un entorno de amenazas en constante transformación. El World Economic Forum (2024) identifica, entre otros aspectos, las diferencias de capacidades entre organizaciones y las dificultades asociadas con la disponibilidad de talento especializado como factores relevantes para la resiliencia cibernética.

En este sentido, la implementación de ciberseguridad no debe entenderse como una acción única basada exclusivamente en la adquisición de herramientas tecnológicas. La ISO/IEC 27001:2022 plantea un enfoque de gestión basado en riesgos que involucra personas, políticas, procesos y tecnología. Por consiguiente, una organización requiere desarrollar capacidades institucionales que permitan administrar, supervisar, actualizar y evaluar permanentemente los controles implementados (ISO, 2022).

En relación con el cumplimiento regulatorio, se estableció que las medidas de ciberseguridad pueden contribuir a la protección de la información y al establecimiento de evidencias sobre los procedimientos implementados. En el contexto colombiano, la Ley 1581 de 2012 establece obligaciones relacionadas con la seguridad de los datos personales, mientras que la Ley 527 de 1999 regula aspectos relacionados con los mensajes de datos, el comercio electrónico y las firmas digitales. Estas disposiciones adquieren importancia para los sistemas de información financieros y contables que utilizan documentos, registros y datos electrónicos en el desarrollo de sus operaciones (Congreso de Colombia, 1999, 2012).

Asimismo, la protección de la información financiera debe analizarse en articulación con el marco normativo de la contabilidad y el aseguramiento de la información. La Ley 1314 de 2009 y el Decreto 2420 de 2015 establecen el marco colombiano relacionado con las normas de contabilidad, información financiera y aseguramiento. En consecuencia, la ciberseguridad puede relacionarse con la confiabilidad de los sistemas que soportan la generación, procesamiento, conservación y presentación de información financiera, especialmente cuando existen riesgos de modificación, pérdida, acceso no autorizado o indisponibilidad de los datos.

A partir de la revisión realizada, se consolidó la siguiente síntesis:

Tabla 14 Síntesis de las ventajas y desventajas de la implementación de medidas de ciberseguridad en los sistemas de información financieros

DIMENSIÓN	PRINCIPALES IDENTIFICADAS	VENTAJAS	PRINCIPALES LIMITACIONES O DESAFÍOS	APLICACIÓN EN SISTEMAS FINANCIEROS Y CONTABLES
PROTECCIÓN DE LA INFORMACIÓN	Fortalece la confidencialidad, integridad y disponibilidad de la información; permite controlar los accesos, realizar respaldos, recuperar información y detectar oportunamente incidentes de seguridad.		Implica costos de implementación y mantenimiento, actualización permanente de tecnologías, aparición de nuevas vulnerabilidades y necesidad de contar con personal capacitado en seguridad de la información.	Protege registros contables, bases de datos, facturación electrónica, cartera, nómina, información tributaria, estados financieros y documentos electrónicos frente a pérdida, alteración, divulgación o acceso no autorizado.
EFICIENCIA OPERATIVA	Permite organizar los controles de seguridad, identificar procesos críticos, establecer responsabilidades, automatizar actividades, fortalecer la		Puede generar complejidad tecnológica, dificultades de integración entre sistemas, necesidades adicionales de capacitación y un incremento	Contribuye al fortalecimiento de los procesos contables, financieros y administrativos; facilita la automatización de controles, la continuidad de facturación y pagos, la gestión documental y la

CUMPLIMIENTO REGULATORIO	continuidad operativa y estructurar la respuesta ante incidentes.	inicial de las actividades de supervisión y control.	generación oportuna de información financiera.
	Facilita la protección de datos, la conservación de evidencias, la trazabilidad de operaciones, el control de accesos y la documentación de políticas y procedimientos de seguridad.	Exige mantener actualizados los controles, procedimientos y evidencias frente a cambios normativos, tecnológicos y organizacionales; además, requiere seguimiento y evaluación periódica.	Apoya el cumplimiento de disposiciones relacionadas con protección de datos personales, información financiera, registros electrónicos, conservación documental, auditoría, control interno y aseguramiento de la información.

Fuente: (Elaboración propia 2026)

En términos generales, el resultado de la etapa demuestra que las medidas de ciberseguridad presentan beneficios relacionados con la protección de la información, la continuidad y organización de las operaciones y el apoyo al cumplimiento regulatorio, pero su implementación exige considerar condiciones económicas, tecnológicas y organizacionales. Por ello, la efectividad de las medidas depende no solamente de las herramientas utilizadas, sino también de la capacidad de la organización para gestionar los riesgos, capacitar a sus usuarios, supervisar los controles y mantenerlos actualizados.

Finalmente, el resultado de esta etapa se concreta en una matriz de ventajas y desventajas de las medidas de ciberseguridad en los sistemas de información financieros, estructurada en las dimensiones de protección de la información, eficiencia operativa y cumplimiento regulatorio. Esta matriz permite relacionar los beneficios identificados en la literatura con las principales limitaciones y condiciones de implementación, proporcionando un referente para comprender integralmente el papel de la ciberseguridad en la protección de los sistemas de información financieros y contables.

Evaluación del impacto de las medidas de ciberseguridad

A partir del análisis bibliográfico desarrollado en la Fase III, se evaluó el impacto de las medidas de ciberseguridad en tres dimensiones: protección de la información, eficiencia operativa y cumplimiento regulatorio. Los resultados permiten establecer que dichas medidas tienen una incidencia transversal sobre los sistemas de información financieros y contables, debido a que no solamente buscan prevenir incidentes de seguridad, sino también preservar la disponibilidad de los sistemas, fortalecer los procesos organizacionales y apoyar el cumplimiento de las obligaciones relacionadas con el tratamiento y protección de la información.

Impacto en la protección de la información

En la dimensión de protección de la información, el impacto se relaciona principalmente con la preservación de la confidencialidad, integridad y disponibilidad de los datos. La implementación de controles de acceso, mecanismos de autenticación, copias de seguridad, monitoreo, detección de incidentes y procedimientos de recuperación permite establecer barreras frente a accesos no autorizados, modificaciones indebidas, pérdida de información y afectaciones sobre la disponibilidad de los sistemas. Este enfoque coincide con ISO/IEC 27001:2022 y con el NIST Cybersecurity Framework 2.0, que plantean la gestión de los riesgos de seguridad de la información mediante controles y procesos organizados (International Organization for Standardization [ISO], 2022; National Institute of Standards and Technology [NIST], 2024).

En los sistemas de información financieros y contables, este impacto adquiere especial importancia porque una alteración o pérdida de información puede afectar registros contables, facturación, cuentas por cobrar, cuentas por pagar, nómina, conciliaciones y generación de informes financieros. Por tanto, la ciberseguridad

contribuye a disminuir la exposición de estos activos y a fortalecer las condiciones necesarias para conservar información confiable y disponible para los procesos organizacionales.

El análisis de ENISA (2024) permite complementar esta evaluación, debido a que identifica amenazas relacionadas con la disponibilidad, ransomware, datos e ingeniería social, entre otras. En consecuencia, las medidas de protección no deben concentrarse exclusivamente en la prevención, sino incorporar mecanismos de detección, respuesta y recuperación frente a posibles incidentes (European Union Agency for Cybersecurity [ENISA], 2024).

Evaluación: el impacto sobre la protección de la información se evidencia en el fortalecimiento de los controles destinados a preservar los activos de información y reducir los riesgos de pérdida, alteración, divulgación o indisponibilidad. No obstante, este impacto depende de que los controles sean actualizados, supervisados y adaptados a la evolución de las amenazas.

Impacto en la eficiencia operativa

En cuanto a la eficiencia operativa, las medidas de ciberseguridad generan un impacto relacionado con la organización de los procesos, la definición de responsabilidades, la identificación de activos críticos, la gestión de riesgos, el respaldo de información y la capacidad de responder y recuperarse ante incidentes. El NIST CSF 2.0 proporciona una estructura que permite organizar las actividades de ciberseguridad mediante las funciones Govern, Identify, Protect, Detect, Respond y Recover, facilitando su incorporación a los procesos de gestión organizacional (NIST, 2024).

En los sistemas financieros y contables, esta organización puede contribuir a disminuir las interrupciones de los procesos y fortalecer la continuidad de actividades

como facturación, procesamiento de transacciones, gestión de cartera, pagos y generación de información financiera. De igual manera, la definición de procedimientos de respaldo y recuperación permite establecer mecanismos para restablecer las operaciones cuando se presentan incidentes que afectan los sistemas.

Sin embargo, la evaluación también permite identificar que la ciberseguridad puede generar inicialmente mayores requerimientos de tiempo y recursos asociados con capacitación, documentación, monitoreo, supervisión, actualización e integración de controles. Por esta razón, la eficiencia operativa no debe entenderse únicamente como reducción inmediata de costos, sino como la capacidad de mantener procesos organizados, controlados y disponibles frente a eventos que puedan afectar su funcionamiento.

El World Economic Forum (2024) identifica, además, diferencias en las capacidades de ciberseguridad entre organizaciones y dificultades relacionadas con la disponibilidad de talento especializado. Esto implica que el impacto operativo está condicionado por las capacidades humanas, tecnológicas y financieras disponibles para implementar y mantener los controles.

Evaluación: el impacto sobre la eficiencia operativa se manifiesta principalmente en la organización de los controles, la continuidad de los procesos y la capacidad de respuesta y recuperación. Sin embargo, requiere inversiones, capacitación y adaptación tecnológica para que los controles puedan integrarse adecuadamente a los procesos existentes.

Impacto en el cumplimiento regulatorio

En la dimensión de cumplimiento regulatorio, las medidas de ciberseguridad pueden contribuir mediante la implementación de políticas, procedimientos, controles y

evidencias orientadas a proteger la información y demostrar la existencia de mecanismos de gestión y seguridad.

En Colombia, la Ley 1581 de 2012 establece disposiciones relacionadas con la protección de datos personales y contempla el principio de seguridad para evitar, entre otros riesgos, la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento a la información. Por esta razón, los controles de ciberseguridad constituyen mecanismos que pueden apoyar el cumplimiento de las obligaciones relacionadas con la protección de los datos personales (Congreso de Colombia, 2012).

De igual manera, la Ley 527 de 1999 establece disposiciones relacionadas con los mensajes de datos y su utilización en actividades electrónicas. Esta regulación resulta relevante para los sistemas financieros y contables que utilizan documentos y registros electrónicos, debido a la necesidad de preservar condiciones de integridad, conservación y disponibilidad de la información utilizada en los procesos organizacionales (Congreso de Colombia, 1999).

La relación con el ámbito contable también se establece mediante la Ley 1314 de 2009 y el Decreto 2420 de 2015 y sus modificaciones, que conforman parte del marco colombiano relacionado con la contabilidad, la información financiera y el aseguramiento de la información. En este contexto, la ciberseguridad puede apoyar la protección de los sistemas que intervienen en la generación, procesamiento, almacenamiento y transmisión de información financiera.

Evaluación: el impacto sobre el cumplimiento regulatorio se relaciona con la capacidad de la organización para establecer controles, procedimientos y evidencias que permitan proteger la información y atender las obligaciones aplicables. Sin embargo, el cumplimiento requiere actualización permanente de los controles y revisión de los cambios normativos, tecnológicos y organizacionales.

Síntesis de la evaluación

Dimensión Impacto identificado Principales aportes Condiciones o limitaciones
Protección de la información Fortalecimiento de la confidencialidad, integridad y disponibilidad. Control de accesos, respaldo, detección, respuesta y recuperación. Actualización permanente y adaptación a nuevas amenazas.

Eficiencia operativa Mayor organización, continuidad y capacidad de respuesta de los procesos. Identificación de procesos críticos, responsabilidades, respaldos y recuperación. Costos, capacitación, personal especializado e integración tecnológica.

Cumplimiento regulatorio Fortalecimiento de los mecanismos para proteger y gestionar la información. Políticas, controles, procedimientos y evidencias de cumplimiento. Necesidad de mantener los controles y documentación actualizados.

En síntesis, la evaluación realizada permite establecer que el impacto de las medidas de ciberseguridad es transversal a los sistemas de información financieros y contables. En materia de protección, contribuyen a preservar la confidencialidad, integridad y disponibilidad de la información; en materia operativa, favorecen la continuidad, organización y recuperación de los procesos; y en materia regulatoria, apoyan la implementación de controles y procedimientos relacionados con la protección de la información y el cumplimiento de las disposiciones aplicables.

No obstante, el impacto identificado no depende únicamente de la existencia de herramientas tecnológicas. Su efectividad está condicionada por la disponibilidad de recursos, la capacitación del personal, la gestión del riesgo, la integración de los controles con los procesos organizacionales, la supervisión y la actualización permanente frente a la evolución de las amenazas y del marco regulatorio. En consecuencia, la ciberseguridad debe comprenderse como un proceso continuo de gestión y mejora, integrado a los sistemas de información y a los procesos financieros y contables.

Tabla 15 Evaluación del impacto de las medidas de ciberseguridad en los sistemas financieros y contables

DIMENSIÓN EVALUADA	ASPECTOS ANALIZADOS	MEDIDAS CIBERSEGURIDAD RELACIONADAS	DE IMPACTO EN LOS SISTEMAS FINANCIEROS Y CONTABLES	BENEFICIOS IDENTIFICADOS	LIMITACIONES O DESAFÍOS
PROTECCIÓN DE LA INFORMACIÓN	Confidencialidad, integridad y disponibilidad de la información.	Control de accesos, autenticación, copias de seguridad, cifrado, monitoreo, detección de incidentes y recuperación.	Reduce la exposición de registros contables, facturación, cartera, nómina, cuentas por cobrar y pagar e informes financieros frente a pérdida, alteración, divulgación o acceso no autorizado.	Mayor confiabilidad y disponibilidad de la información; reducción de riesgos asociados con pérdida o modificación de datos; fortalecimiento de la protección de activos de información.	Evolución permanente de las amenazas, vulnerabilidades tecnológicas, necesidad de actualización de controles y personal especializado.
EFICIENCIA OPERATIVA	Organización de procesos, continuidad operativa, gestión de riesgos y capacidad de respuesta.	Identificación de activos críticos, gestión de riesgos, respaldos, planes de respuesta, recuperación y continuidad.	Contribuye a mantener la continuidad de procesos como facturación, procesamiento de transacciones, pagos, cartera, conciliaciones y generación de información financiera.	Mayor organización de responsabilidades, reducción de interrupciones, recuperación de operaciones y fortalecimiento de la continuidad de los procesos.	Costos de implementación, capacitación, monitoreo, actualización tecnológica e integración de los controles con los procesos existentes.
CUMPLIMIENTO REGULATORIO	Protección de datos, gestión documental, controles y generación de evidencias.	Políticas de seguridad, procedimientos, controles de acceso, gestión documental, registros, monitoreo y	Apoya el cumplimiento de obligaciones relacionadas con la protección y gestión de información	Mayor capacidad para demostrar la aplicación de controles, fortalecer la gestión de información y atender	Cambios normativos, necesidad de actualización documental, seguimiento

		mecanismos de protección de datos.	utilizada en procesos financieros y contables.	requerimientos regulatorios.	permanente y adaptación de los controles a nuevas obligaciones.
GESTIÓN DEL RIESGO	Identificación, valoración, tratamiento y seguimiento de riesgos de ciberseguridad.	Evaluaciones de riesgo, identificación de activos, análisis de vulnerabilidades, monitoreo y planes de tratamiento.	Permite identificar amenazas que pueden afectar la información y los procesos financieros y establecer mecanismos de tratamiento.	Mayor capacidad preventiva y mejor toma de decisiones sobre recursos destinados a seguridad.	Requiere información actualizada, metodología definida, seguimiento continuo y participación de diferentes áreas.
RESPUESTA Y RECUPERACIÓN	Capacidad institucional para detectar, responder y recuperar operaciones ante incidentes.	Planes de respuesta, copias de seguridad, recuperación ante desastres, monitoreo y protocolos de actuación.	Reduce el tiempo de interrupción de los sistemas y facilita la recuperación de información y procesos financieros después de un incidente.	Mayor resiliencia operativa y capacidad de restablecer servicios críticos.	Dependencia de infraestructura tecnológica, pruebas periódicas, disponibilidad de recursos y preparación del personal.
GESTIÓN ORGANIZACIONAL	Gobernanza, responsabilidades, capacitación y cultura de seguridad.	Políticas institucionales, asignación de responsabilidades, capacitación, procedimientos y supervisión.	Favorece la incorporación de la ciberseguridad dentro de la gestión de los sistemas de información financieros y contables.	Mayor conciencia del riesgo, definición de responsabilidades y fortalecimiento de la cultura de seguridad.	Resistencia al cambio, falta de capacitación, disponibilidad limitada de talento especializado y recursos financieros.

Fuente: (Elaboración propia 2026)

Tabla 16 Sin tesis de los resultados

Dimensión	Resultado de la evaluación	Nivel de incidencia identificado
Protección de la información	Fortalece la confidencialidad, integridad y disponibilidad de los datos financieros y contables.	Directa y transversal
Eficiencia operativa	Favorece la continuidad, organización y recuperación de los procesos críticos.	Directa, condicionada por recursos y capacidades
Cumplimiento regulatorio	Apoya la implementación de controles, procedimientos y evidencias para la gestión y protección de la información.	Directa, condicionada por la actualización normativa
Gestión del riesgo	Permite anticipar, identificar y tratar amenazas que pueden afectar los activos de información.	Transversal
Respuesta y recuperación	Fortalece la capacidad de restablecer procesos y sistemas después de incidentes.	Crítica para la
Gestión organizacional	Integra la seguridad con las responsabilidades, políticas y procesos institucionales.	Transversal permanente y

Fuente: (Elaboración propia 2026)

6 CONCLUSIONES

Teniendo en cuenta los resultados obtenidos, se concluye que los fundamentos teóricos de la ciberseguridad en los sistemas de información: una revisión conceptual.

La revisión de la literatura permitió comprender que la ciberseguridad constituye un componente fundamental de los sistemas de información, debido a su función en la protección de la confidencialidad, integridad y disponibilidad de los datos. Asimismo, se evidenció que su evolución ha estado relacionada con la transformación digital de las organizaciones, pasando de enfoques centrados principalmente en la protección de equipos y redes hacia modelos integrales que incorporan gestión de riesgos, protección de datos, prevención de incidentes, monitoreo continuo y capacidad de respuesta. En este contexto, la ciberseguridad resulta especialmente relevante para los sistemas de información financieros y contables, donde la confiabilidad de los datos constituye un elemento esencial para la generación de información útil para la toma de decisiones.

Igualmente, el análisis teórico permitió identificar una relación directa entre la ciberseguridad y el cumplimiento normativo, puesto que las medidas de protección tecnológica contribuyen a preservar la integridad, disponibilidad, confidencialidad y trazabilidad de la información que soporta los procesos contables y financieros. Se estableció que el cumplimiento de disposiciones relacionadas con seguridad de la información, protección de datos, controles internos y gestión de riesgos requiere que las organizaciones implementen mecanismos orientados a prevenir accesos no autorizados, alteraciones, pérdidas y divulgaciones indebidas de información. Por tanto, la ciberseguridad no debe considerarse únicamente como una herramienta tecnológica, sino como un elemento de apoyo al control organizacional y al cumplimiento de las obligaciones legales y regulatorias aplicables a los sistemas de información.

Y el estudio bibliográfico permitió describir que la implementación de medidas de ciberseguridad en los sistemas de información financieros genera beneficios relacionados con una mayor protección de los datos, reducción de riesgos asociados a incidentes, fortalecimiento de los controles, continuidad de las operaciones y mayor confiabilidad de la información financiera. No obstante, también se identificaron posibles limitaciones, entre ellas los costos de implementación y mantenimiento, la necesidad de infraestructura tecnológica, la capacitación permanente del personal, la complejidad de integrar nuevas herramientas y la posibilidad de generar cargas adicionales sobre determinados procesos operativos. En consecuencia, el impacto de la ciberseguridad debe analizarse de manera integral, considerando simultáneamente la protección de la información, la eficiencia operativa y el cumplimiento regulatorio, de manera que las medidas adoptadas respondan a los riesgos y necesidades específicas de cada organización.

7 RECOMENDACIONES

Se recomienda que las organizaciones fortalezcan el conocimiento sobre los conceptos, principios y evolución de la ciberseguridad mediante procesos de capacitación y actualización permanente dirigidos al personal que participa en la administración y utilización de los sistemas de información. Esta formación debe abordar aspectos relacionados con la protección de la información, gestión de riesgos, control de accesos, prevención de incidentes y buenas prácticas de seguridad, de manera que la ciberseguridad sea comprendida como un componente transversal de los procesos organizacionales y no únicamente como una responsabilidad del área tecnológica.

Se recomienda integrar las medidas de ciberseguridad con los mecanismos de control interno y las políticas de cumplimiento normativo de las organizaciones. Para ello, es conveniente establecer procedimientos documentados para la gestión de accesos, protección de datos, respaldo de información, trazabilidad de las operaciones, gestión de incidentes y conservación de los registros contables y financieros. Asimismo, se recomienda realizar revisiones periódicas de los controles implementados frente a los requerimientos legales y regulatorios aplicables, con el propósito de identificar oportunamente posibles brechas y establecer acciones de mejora.

Se recomienda que la implementación de medidas de ciberseguridad en los sistemas de información financieros se realice a partir de un análisis previo de riesgos, necesidades y recursos disponibles, considerando tanto los beneficios como las posibles limitaciones de las soluciones adoptadas. Las organizaciones deberían priorizar controles que contribuyan a proteger la información financiera sin afectar innecesariamente la eficiencia de los procesos. De igual manera, se recomienda establecer mecanismos de seguimiento y evaluación que permitan verificar periódicamente aspectos como la protección de la información, continuidad operativa, efectividad de los controles, cumplimiento regulatorio y respuesta ante incidentes de seguridad.

Por último, se recomienda adoptar un enfoque de mejora continua de la ciberseguridad, en el cual las medidas tecnológicas, los procedimientos organizacionales y la capacitación del talento humano se desarrollen de manera articulada. La protección de los sistemas de información financieros requiere considerar que las amenazas y las tecnologías evolucionan constantemente; por ello, los controles no deben permanecer estáticos, sino ser revisados, actualizados y ajustados de acuerdo con los nuevos riesgos, cambios normativos y necesidades de la organización.

8 REFERENCIAS BIBLIOGRÁFICAS

- Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2023). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 1*, 100031. <https://doi.org/10.1016/j.csa.2023.100031>
- Almeida-Blacio, J. H., Naranjo-Armijo, F. G., Maldonado-Pazmiño, H. O., & Rodríguez-Lara, A. D. (2024). Inteligencia artificial como mecanismo eficiente de la contabilidad. *Código Científico Revista de Investigación*, 5*(E3), 334–364. <https://revistacodigocientifico.itslosandes.net/index.php/1/article/view/320>
- Almeida, E. N. A. de. (2024). **The integration of blockchain technology in accounting and auditing** [Tesis de maestría, University of Saint Joseph]. University of Saint Joseph.
- Almario, J. (2022). **Análisis de las amenazas y riesgos cibernéticos que afrontan los usuarios y las organizaciones en la consulta y/o adquisición de servicios turísticos con medios electrónicos** [Trabajo de grado, Universidad Nacional Abierta y a Distancia].
- Alvarado, D. (2022). **Diplomado en contabilidad, auditoría y aseguramiento bajo estándares internacionales, énfasis en medianas y pequeñas empresas-Pymes** [Diplomado, Universidad Santo Tomás].
- Álvarez, D. (2019). Algunos aspectos jurídicos del cifrado de comunicaciones. *Derecho PUCP*, 83*, 241–262. <https://doi.org/10.18800/derechopucp.201902.008>
- Arias, J., & Covinos, M. (2021). **Diseño y metodología de la investigación**. Enfoques Consulting EIRL.
- Azcona, N. (2024). **¿Cuáles son las ventajas y desventajas de la ciberseguridad?** Universidad de México.
- Barrera, J. (2020). Control interno, su vínculo con la eficiencia operativa y la rentabilidad. *Vinculatégica EFAN*, 6*(1), 734–741. <https://doi.org/10.29105/vtga6.1-626>
- Bermúdez, M. (2020). **Introducción a las bases de datos**. Universidad San Marcos.
- Brown, P., & Lee, C. (2021). Financial fraud and cybersecurity. *Journal of Financial Security**, 87–101.

F-DC-125

INFORME FINAL DE TRABAJO DE GRADO EN MODALIDAD DE PROYECTO
DE INVESTIGACIÓN, DESARROLLO TECNOLÓGICO, MONOGRAFÍA,
EMPRENDIMIENTO Y SEMINARIO

VERSIÓN: 2.0

- Bushman, I. (2021). The development of the intellectual economy of the future: Trends, challenges of the future. **Futurity Economics & Law*, 1*(3), 33–42. <https://doi.org/10.57125/FEL.2021.09.25.04>
- Caamaño Fernández, E. E., & Gil Herrera, R. J. (2020). Prevención de riesgos por ciberseguridad desde la auditoría forense: Conjugando el talento humano organizacional. **NOVUM, Revista de Ciencias Sociales Aplicadas*, 1*(10), 61–80. <https://revistas.unal.edu.co/index.php/novum/article/view/84210>
- Caldentey, J. M., Urquijo, B. S., & Almazor, M. G. (2022). Competency-based cybersecurity training and awareness: A systematic literature review. **Pixel-Bit. Revista de Medios y Educación*, 63*, 197–225.
- Calle-Tenesaca, M. E., & Andrade-Amoroso, R. P. (2024). Ciberseguridad en contabilidad: Protegiendo la integridad de los datos financieros en empresas comerciales. **Revista Metropolitana de Ciencias Aplicadas*, 7*(S2), 87–98. <https://doi.org/10.62452/bdc3pg66>
- Cardenas, L., Peña, H., & Cardenas, N. (2024). **Guía para la gestión y clasificación de un incidente de ciberseguridad**. Universidad Nacional Abierta y a Distancia. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf
- Castellanos, E. (2020). **Importancia de las organizaciones Fintech “tecnología financiera” para el sistema financiero tradicional** [Trabajo de grado, Universidad Militar Nueva Granada].
- Chai, K. Y., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. **Journal of ICT in Education*, 8*(2), 34–42. <https://doi.org/10.37134/jictie.vol8.2.4.2021>
- Changmarín, C. (2021). Big data y su impacto en el ejercicio de la contaduría pública, las empresas y los sistemas de información: Una mirada a la ética. **Actualidad Contable Faces*, 24*(42), 9–35. <https://doi.org/10.53766/ACCON/2021.42.01>
- Cibersafety. (2025, 10 de noviembre). **Ingeniería social: Fraude humano y ciberseguridad**. <https://cibersafety.com/ingenieria-social-fraude-humano-ciberseguridad/>

Congreso de Colombia. (1990, 13 de diciembre). *Ley 43 de 1990, por la cual se adiciona la Ley 145 de 1960, reglamentaria de la profesión de contador público y se dictan otras disposiciones*. Departamento Administrativo de la Función Pública. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=66148>

Congreso de Colombia. (1999, 18 de agosto). *Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación*. Departamento Administrativo de la Función Pública. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276>

Congreso de Colombia. (2008, 31 de diciembre). *Ley 1266 de 2008, por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales*. Departamento Administrativo de la Función Pública. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488>

Congreso de Colombia. (2009, 13 de julio). *Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones*. SUIN-Juriscol. <https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes%2F1676699>

Congreso de Colombia. (2009, 13 de julio). *Ley 1314 de 2009, por la cual se regulan los principios y normas de contabilidad e información financiera y de aseguramiento de información aceptados en Colombia*. Departamento Administrativo de la Función Pública. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36833>

Congreso de Colombia. (2012, 17 de octubre). *Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales*. Departamento Administrativo de la Función Pública. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

Congreso de Colombia. (2012, 22 de noviembre). *Decreto 2364 de 2012, por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999 sobre la firma electrónica*. Alcaldía Mayor de Bogotá. <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=50583>

- Congreso de Colombia. (2021, 29 de octubre). *Ley 2157 de 2021, por medio de la cual se modifica y adiciona la Ley Estatutaria 1266 de 2008*. Departamento Administrativo de la Función Pública. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=173246>
- Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance—Issues and Practice, 47*, 698–736. <https://doi.org/10.1057/s41288-022-00266-6>
- Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal, 33*(7), 76–105. <https://doi.org/10.1108/TQM-09-2020-0202>
- Deloitte. (2023). *AI in accounting: Cybersecurity challenges*. <https://www2.deloitte.com>
- Díazgranados, H. (2021). *Ciberataques en América Latina crecen un 24% durante primeros ocho meses de 2021*. Kaspersky Daily. <https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-losprimeros-ocho-meses-de-2021/22718/>
- Entrust. (2026). *What is identity and access management?*. <https://www.entrust.com/es/resources/learn/what-is-identity-and-access-management>
- Europa Press. (2018, 9 de febrero). *La danesa Maersk pierde 983 millones en 2017, lastrada por el ciberataque de junio*. <https://www.europapress.es/economia/noticia-danese-maersk-pierde-983-millones-2017-lastrada-ciberataque-junio-20180209122406.html>
- European Union Agency for Cybersecurity. (2024a). *2024 report on the state of cybersecurity in the Union*. <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-cybersecurity-in-the-union>
- European Union Agency for Cybersecurity. (2024b). *ENISA threat landscape 2024*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
- European Commission. (2025). *El Reglamento general de protección de datos (RGPD)*. Dirección General de la Comunicación.

EY. (2021). *Lessons from cybersecurity incidents*. <https://security.intuit.com>

EY. (2022). *Data security in the accounting sector*. https://www.ey.com/en_gl

Fortinet. (2026a). *CIA triad*. <https://www.fortinet.com/lat/resources/cyberglossary/cia-triad>

Fortinet. (2026b). *What is cloud security?*. <https://www.fortinet.com/lat/resources/cyberglossary/what-is-cloud-security>

Fortinet. (2026c). *Defense in depth*. <https://www.fortinet.com/lat/resources/cyberglossary/defense-in-depth>

García, B., Sánchez, M. A., & Abadía, J. (2021). Herramienta web con tecnología de cadena de bloques para un sistema de facturación electrónica en Colombia. *Información Tecnológica, 32*(3), 15–24. <https://doi.org/10.4067/S0718-07642021000300015>

García, C. (2021). *Ciberseguridad en el sector financiero*. Universidad Pontificia Comillas.

Gómez, A. (2024, 25 de abril). *Cybersecurity ethics*. Our Lady of the Lake University. <https://www.ollusa.edu/blog/cybersecurity-ethics.html>

Gómez, P. N. (2021). *[Trabajo de grado sobre ciberseguridad y finanzas]*. Universitat de Barcelona. https://diposit.ub.edu/dspace/bitstream/2445/179365/1/TFM-CiF_Gomez.pdf

Gomero, R., & Sánchez, D. (2024). Ciberseguridad en servicios de apoyo al médico ocupacional de la ciudad de Lima. *Revista Médica Herediana, 35*(1), 38–43. <https://doi.org/10.20453/rmh.v35i1.5298>

González, J. (2025). *De la seguridad informática a la resiliencia cibernética*. ResearchGate. https://www.researchgate.net/publication/393025048_De_la_seguridad_informatica_a_la_resiliencia_cibernetica

Grupo Concepto. (2026). *Sistema de información*. Concepto. <https://concepto.de/sistema-de-informacion/>

- Hernández, et al. (2022). Normas Internacionales de Contabilidad (NIC 11) y sus protocolos para contratos en empresas del Cantón Santo Domingo: Un análisis de factibilidad. *Revista Dilemas Contemporáneos: Educación, Política y Valores*.
- Hopkins, N. (2017, 10 de octubre). *Deloitte hack hit server containing emails from across US government*. *The Guardian*. <https://www.theguardian.com/business/2017/oct/10/deloitte-hack-hit-server-containing-emails-from-across-us-government>
- Huanca, H. (2021). *Impacto de la Ley Sarbanes-Oxley en las organizaciones y empresas peruanas* [Trabajo de grado, Universidad Nacional del Callao].
- Information Systems Audit and Control Association. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA.
- International Auditing and Assurance Standards Board. (2022a). *2021 handbook of international quality control, auditing, review, other assurance, and related services pronouncements*. <https://www.iaasb.org/publications/2021-handbook-international-quality-control-auditing-review-other-assurance-and-related-services>
- International Auditing and Assurance Standards Board. (2022b). *Norma Internacional de Auditoría 315 (Revisada 2019): Identificación y valoración de los riesgos de incorrección material*. <https://www.iaasb.org/publications/norma-internacional-de-auditoria-315-revisada-2019-y-modificaciones-de-concordancia-y-en>
- International Organization for Standardization. (2022a). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. <https://www.iso.org/standard/27001.html>
- International Organization for Standardization. (2022b). *ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection—Information security controls*. <https://www.iso.org/standard/75652.html>

- International Organization for Standardization. (2022c). *ISO/IEC 27005:2022: Information security, cybersecurity and privacy protection—Guidance on managing information security risks*. <https://www.iso.org/standard/80585.html>
- International Telecommunication Union. (2024). *Global cybersecurity index 2024* (5th ed.). <https://www.itu.int/itu-d/reports/statistics/global-cybersecurity-index-2024/>
- Jiménez, J. (2022). *Ciberdelincuencia: Evolución y relación con la actual situación de pandemia. Nuevas modalidades y problemáticas* [Trabajo de grado, Universidad de Salamanca].
- Johnson, et al. (2022). Digitalization and cybersecurity in accounting. *International Journal of Finance & Technology*, 112–130.
- Joseph, L. (2024, 11 de marzo). *COBIT: Gobernanza de TI*. Lemon Learning. <https://lemonlearning.com/es/blog/cobit-gobernanza-de-ti>
- Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of Zero Trust security: A brief survey. *Entropy*, 25*(12), 1595. <https://doi.org/10.3390/e25121595>
- Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97*, 101804. <https://doi.org/10.1016/j.inffus.2023.101804>
- Kosinski, M. (2026). *Threat intelligence*. IBM. <https://www.ibm.com/mx-es/think/topics/threat-intelligence>
- KPMG. (2022). *Cyber risk in financial services*. <https://home.kpmg/xx/en/home/insights.html>
- Kumar, R., & Bhatia, M. (2020). Review of security in cloud computing: Integrity, confidentiality and availability of data. En *2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON)* (pp. 334–337). IEEE. <https://doi.org/10.1109/GUCON48875.2020.9231255>

F-DC-125

INFORME FINAL DE TRABAJO DE GRADO EN MODALIDAD DE PROYECTO
DE INVESTIGACIÓN, DESARROLLO TECNOLÓGICO, MONOGRAFÍA,
EMPRENDIMIENTO Y SEMINARIO

VERSIÓN: 2.0

- Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management, 34*(6), 1597–1629. <https://doi.org/10.1108/JEIM-06-2020-0240>
- Kurose, J. F., & Ross, K. W. (2023). *Computer networking: A top-down approach* (8th ed.). Pearson.
- La Nación. (2020, 1 de septiembre). *Un ciberataque a la empresa Deloitte reveló información confidencial de sus clientes*. <https://www.lanacion.com.ar/tecnologia/un-ciberataque-a-la-empresa-deloitte-revelo-informacion-confidencial-de-sus-clientes-nid2066257/>
- Mari, S. M. (2021). *[Documento académico]*. Universidad Autónoma de Nuevo León. <http://eprints.uanl.mx/26139/>
- Mejía, I. (2022). *Control interno como herramienta para la gestión financiera y contable en instituciones del sector público* [Trabajo de grado, Pontificia Universidad Católica del Ecuador].
- Meneses, C. (2024). *Blockchain: La seguridad de los datos*. Universidad Sergio Arboleda. <https://www.usergioarboleda.edu.co/noticias/blockchain-la-seguridad-datos/>
- Milenio. (2021, 25 de septiembre). *Deloitte admite hackeo; información no corre riesgo*. <https://www.milenio.com/estilo/deloitte-admite-hackeo-informacion-corre-riesgo>
- Montes, & Marín. (2020). *[Trabajo académico]*. Tecnológico de Antioquia. <https://dspace.tdea.edu.co/handle/tdea/612>
- MOONFLOW. (2025, 25 de julio). *Ciberseguridad en fintech*. <https://www.moonflow.ai/es-mx/blog/ciberseguridad-en-fintech>
- Motañez, M. (2019). *¿La Ley SOX permite a través del diseño de un modelo de auditoría mejorar el sistema de control interno en la empresa ABC?* [Trabajo de grado, Universidad Militar Nueva Granada].
- Muñoz Hernández, H., Zapata Cantero, L. G., Requena Vidal, D. M., & Ricardo Villadiego, L. (2020). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en

F-DC-125

INFORME FINAL DE TRABAJO DE GRADO EN MODALIDAD DE PROYECTO
DE INVESTIGACIÓN, DESARROLLO TECNOLÓGICO, MONOGRAFÍA,
EMPRENDIMIENTO Y SEMINARIO

VERSIÓN: 2.0

Colombia. *Revista Venezolana de Gerencia, 24*(2), 528–541.
<https://doi.org/10.37960/revista.v24i2.31508>

National Institute of Standards and Technology. (2024a). *The NIST cybersecurity framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). U.S. Department of Commerce.
<https://doi.org/10.6028/NIST.CSWP.29>

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors, 21*(15), 5119. <https://doi.org/10.3390/s21155119>

Ofusori, L., Bokaba, T., & Mhlongo, S. (2024). Artificial intelligence in cybersecurity: A comprehensive review and future direction. *Applied Artificial Intelligence, 38*(1), Article 2439609. <https://doi.org/10.1080/08839514.2024.2439609>

Oliveira, C. (2020). *Sistema de control de acceso para entidades* [Trabajo académico, Universidad de las Ciencias Informáticas].

Oliveira, E., & Freitas, A. (2020). Os porquês da tecnologia blockchain ainda não ter sido popularizada: Um ensaio teórico. *Revista Gestão & Tecnologia, 20*(1), 284–295. <https://doi.org/10.20397/2177-6652/2020.v20i1.1706>

Organización de las Naciones Unidas. (2022). *[Documento sobre ciberseguridad y seguridad de la información]*.

Ortega, J. (2024). *Ciberseguridad: Manual práctico*. Ecoe Ediciones.

OSTEC GROUP. (2021, 11 de mayo). *Diferencias entre análisis de vulnerabilidad y pentest*. <https://ostec.blog/es/seguridad/diferencias-entre-analisis-de-vulnerabilidad-y-pentest/>

Otonne, et al. (2023). Adoption of financial technology and performance of deposit money banks in Nigeria. *Futurity Economics & Law, 3*(2), 95–114. <https://doi.org/10.57125/FEL.2023.06.25.07>

F-DC-125

INFORME FINAL DE TRABAJO DE GRADO EN MODALIDAD DE PROYECTO
DE INVESTIGACIÓN, DESARROLLO TECNOLÓGICO, MONOGRAFÍA,
EMPREDIMIENTO Y SEMINARIO

VERSIÓN: 2.0

- Paracha, A., Arshad, J., Farah, M. B., & Ismail, K. (2024). Machine learning security and privacy: A review of threats and countermeasures. *EURASIP Journal on Information Security, 2024*, 10. <https://doi.org/10.1186/s13635-024-00158-3>
- Pérez, A. (2022). *Influencia del control interno en la contabilidad de la empresa “Sierra Andina” SAC en el distrito de Independencia, Huaraz-2018* [Trabajo de grado, Universidad Católica Los Ángeles de Chimbote].
- Petroff, A. (2017, 27 de junio). *Hackers lanzan ciberataque masivo contra empresas y agencias en Europa*. CNN en Español. <https://cnnespanol.cnn.com/2017/06/27/hackers-lanzan-ciberataque-masivo-contra-empresas-y-agencias-en-europa/>
- Pihel, J. (2025, 22 de diciembre). *Cybersecurity for accountants*. UKU. <https://getuku.com/articles/cybersecurity-for-accountants>
- PIRANI.(2026). *Ciberseguridad: Qué es, cómo funciona y su importancia*. <https://www.piranirisk.com/es/academia/especiales/ciberseguridad-que-es-como-funciona-y-su-importancia>
- PwC. (2023). *Global economic crime and fraud survey 2023*. <https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html>
- Quiñonez, et al. (2021). Normas Internacionales de Información Financiera (NIIF 9), medición y clasificación de los instrumentos financieros. *Revista Publicando, 8*(31), 194–206. <https://doi.org/10.51528/rp.vol8.id2244>
- Rigopoulos, K., Quinn, S., Pascoe, C., Marron, J., Mahn, A., & Topper, D. (2024). *NIST cybersecurity framework 2.0: Resource & overview guide* (NIST Special Publication 1299). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.1299>
- Ribas, et al. (2021). *[Documento académico]*. Universidad Nacional de La Plata. <https://sedici.unlp.edu.ar/handle/10915/132395>

Rivera, J. C. (2019, 22 de agosto). *Los marcos normativos contables en Colombia y la presentación de la información financiera en taxonomías*. Comunidad Contable. <http://www.comunidadcontable.com/BancoConocimiento/los-marcos-normativos-contables-en-colombia-y-la-presentacion-de-la-informacion-financiera-en-taxono.asp>

Robles, D. (2024). *Análisis de la importancia de delitos informáticos en Latinoamérica* [Trabajo de grado, Universidad Santo Tomás].

Rodríguez, I. (2022). *La auditoría de cumplimiento y los riesgos cibernéticos*. Auditool. <https://www.auditool.org/blog/auditoria-de-ti/la-auditoria-de-cumplimiento-y-los-riesgos-ciberneticos>

Rodríguez, I. (2024, 26 de junio). *De la vulnerabilidad a la seguridad: La importancia de la auditoría de sistemas de información*. Auditool. <https://www.auditool.org/blog/auditoria-de-ti/de-la-vulnerabilidad-a-la-seguridad-la-importancia-de-la-auditoria-de-sistemas-de-informacion>

Runtuwene, et al. (2024). Face identification using image processing with the National Institute of Standards and Technology (NIST) method. *Jurnal Teknik Informatika (JUTIF)*, 4*(5), 375–384. <https://jutif.if.unsoed.ac.id/index.php/jurnal/article/view/2350>

Salazar Cruz, A. P., & Rodríguez Polo, S. (2020). *Impacto del software en la contabilidad colombiana* [Trabajo de grado, Universidad Piloto de Colombia]. <http://repository.unipiloto.edu.co/handle/20.500.12277/9359>

SapConcur. (2024). *¿Cuáles son las ventajas de digitalizar la contabilidad financiera en las empresas?* SAP Concur.

Sadradin, et al. (2024). *Educación del siglo XXI: Investigación e innovación para el liderazgo educativo*. Dykinson.

Sedano, W. K., & Salman, M. (2021). Auditing Linux operating system with Center for Internet Security (CIS) standard. En *2021 International Conference on Information Technology (ICIT)* (pp. 466–471). IEEE. <https://doi.org/10.1109/ICIT52682.2021.9491663>

- Sikdar, B. (2021). *[Documento IEEE]*. IEEE Xplore. <https://ieeexplore.ieee.org/document/9251914>
- Smith, J., & White, L. (2021). Cybersecurity risks in accounting firms. *Journal of Accounting and Cybersecurity, 18*(2), 45–60.
- Spilnyk, I., & Palukh, M. (2019). Accounting in the digital economy conditions. *The Institute of Accounting, Control and Analysis in the Globalization Circumstances, 1*(2), 83–93. <https://doi.org/10.35774/ibo2019.01.083>
- Stallings, W. (2021). *Cryptography and network security: Principles and practice* (6th ed.). Pearson.
- Stergiou, C. L., & Psannis, K. E. (2022). A survey of security in cloud, edge, and fog computing. *Sensors, 22*(3), 927. <https://doi.org/10.3390/s22030927>
- Suberg, W. (2020). *Deloitte lidia con hack colosal, su brecha de seguridad hace eco del caso de Equifax*. Cointelegraph. <https://es.cointelegraph.com/news/deloitte-grapples-with-major-hack-security-lapse-echoes-equifax>
- Superintendencia de Industria y Comercio. (2026). *Sobre la protección de datos personales*. <https://www.sic.gov.co/content/sobre-la-protecci%C3%B3n-de-datos-personales>
- Torres, O. (2023, 11 de julio). *Gestión de riesgos basado en COSO ERM*. Pirani

9. APÉNDICES

TURNITIN