Ciberseguridad organizacional y gobernanza: Evaluación normativa, cultura y estrategias de ciberresiliencia en el contexto de la transformación digital

Organizational cybersecurity and governance: regulatory assessment, culture, and cyber resilience strategies in the context of digital transformation

https://doi.org/10.5281/zenodo.21341667

AUTORES:

Andy Guilbert Bayas Huilcapi *
https://orcid.org/0000-0003-1334-6089
abayas@utb.edu.ec
Universidad Técnica de Babahoyo
Facultad de Administración, Finanzas e Informática

Gabriela Madelley Cabezas Goyes
https://orcid.org/0000-0002-5397-7750
gcabezas@utb.edu.ec
Universidad Técnica de Babahoyo
Facultad de Administración, Finanzas e Informática

Tatiana Yessenia Bohórquez Nivela
tatyloven@yahoo.com
Escuela de Educación Básica Francisco Robles

Nora Úrsula Huilcapi Mazacón
nuhuilcapi@utb.edu.ec
Universidad Técnica de Babahoyo
Facultad de Administración, Finanzas e Informática

DIRECCIÓN PARA CORRESPONDENCIA: **abayas@utb.edu.ec**

Fecha de recepción: 03 /12 / 2025

Fecha de aceptación: 10 / 12 / 2025

RESUMEN

La investigación analiza la relación entre ciberseguridad organizacional y gobernanza digital, destacando la importancia de integrar normativas, cultura de seguridad y estrategias de ciberresiliencia para proteger los activos digitales. Se evidencia que las organizaciones enfrentan una brecha entre el cumplimiento normativo y su aplicación práctica, por lo que es

necesario fortalecer la capacitación, la gestión de riesgos y la adopción de marcos como ISO 27001, NIST, COBIT e ITIL. En este contexto, la ciberseguridad requiere un enfoque integral que combine tecnología, personas y gobernanza para garantizar la continuidad operativa y la resiliencia empresarial.

Palabras clave: *Ciberseguridad, Ciberresiliencia, Transformación digital*

ABSTRACT

The research analyzes the relationship between organizational cybersecurity and digital governance, highlighting the importance of integrating regulations, security culture, and cyber-resilience strategies to protect digital assets. It shows that organizations face a gap between regulatory compliance and practical implementation, making it necessary to strengthen training, risk management, and the adoption of frameworks such as ISO 27001, NIST, COBIT, and ITIL. In this context, cybersecurity requires a comprehensive approach that combines technology, people, and governance to ensure operational continuity and business resilience.

Keywords: *Cybersecurity, Cyberresilience, Digital Transformation*

INTRODUCCIÓN

La investigación analiza la convergencia de la Ciberseguridad Organizacional y Gobernanza dentro del marco evaluativo de la normativa **,** cultura y estrategias de ciberresiliencia en el contexto de la transformación digital, basándonos en el estudio realizado por (Cruz Tunqui, 2024) damos a conocer que la ciberseguridad se ha convertido en prioridad para las empresas en la era digital, donde la protección de los sistemas informáticos es vital en la continuidad del negocio y la confianza del cliente. En este contexto, la adopción de medidas preventivas de ciberseguridad se vuelve crucial en el marco de la investigación de mercados digitales.

En este escenario, el presente estudio busca analizar cómo las normativas internacionales, la cultura organizacional y la gestión de riesgos inciden en el fortalecimiento de la ciberseguridad y la resiliencia digital de las PYMES, aportando un marco de referencia para su protección en la era digital.

1.1. Contexto global de la ciberseguridad y aumento de incidentes cibernéticos

En la era digital contemporánea, la ciberseguridad se ha consolidado como un pilar esencial para la protección de los sistemas empresariales. La creciente dependencia de las tecnologías de la información y la comunicación (TIC) ha expuesto a las organizaciones a una variedad de amenazas cibernéticas que evolucionan constantemente, poniendo en riesgo la integridad, confidencialidad y disponibilidad de sus datos y servicios.

De acuerdo con (Bone Andrade, 2023) la creciente frecuencia y sofisticación de los ciberataques subraya la necesidad urgente de fortalecer las medidas de ciberseguridad en las empresas. Implementar estrategias de seguridad robustas no solo protege los activos digitales, sino que también garantiza la continuidad operativa y la confianza de los clientes y socios comerciales, Las tecnologías emergentes han revolucionado la ciberseguridad empresarial, permitiendo una defensa más proactiva y adaptativa frente a las amenazas. La inteligencia artificial se posiciona como una herramienta clave para analizar grandes volúmenes de datos en tiempo real y detectar patrones sospechosos que podrían indicar un ataque en curso, aquí las respuestas organizacionales han recurrido a los programas de capacitación en ciberseguridad, ya que estos han disminuido hasta en un 50 % los casos de phishing en empresas que invierten en educación para sus empleados. Estas iniciativas incluyen simulaciones de ataques, cursos interactivos y campañas de concienciación que permiten a los empleados identificar y responder adecuadamente a intentos de ataque. Además, el cumplimiento de normativas internacionales, como la Directiva NIS 2 y el GDPR, obliga a las organizaciones a establecer políticas y procedimientos más sólidos, las políticas internas de ciberseguridad se erigen como un componente esencial para mitigar el impacto del factor humano en la ocurrencia de incidentes. El fortalecimiento de programas de capacitación continua ha demostrado su eficacia al reducir el impacto de amenazas como el phishing, gracias a la concienciación de los empleados sobre los riesgos digitales, la ciberseguridad empresarial se encuentra en una fase de transición hacia enfoques más integrales, que combinan soluciones tecnológicas avanzadas con una sólida gobernanza organizacional y cumplimiento normativo. Las empresas deben priorizar la inversión en tecnologías

disruptivas como la IA y el blockchain, mientras refuerzan su cultura interna mediante programas de formación y la adopción de marcos normativos que fomenten la resiliencia y la colaboración.

De igual manera (Díaz, 2023) expresa que los incidentes cibernéticos deben tratarse como eventos sistémicos, que requieren una gobernanza colaborativa, multiactor y transnacional, En este sentido, se reconoce que la cultura organizacional, la educación de los usuarios y la preparación para incidentes son tan importantes como las herramientas tecnológicas en la defensa del entorno digital.

Podemos concluir que, en la era digital actual, la ciberseguridad se ha convertido en un pilar esencial para proteger los sistemas empresariales ante amenazas cada vez más sofisticadas, las empresas deben fortalecer sus estrategias mediante tecnologías emergentes como la inteligencia artificial y programas de capacitación que reduzcan riesgos como el phishing. Además, el cumplimiento de normativas internacionales como la NIS 2 y el GDPR refuerza la gobernanza y la protección de datos, señalando que los incidentes cibernéticos deben abordarse con una gobernanza colaborativa y una sólida cultura organizacional.

1.2. Brecha entre normativas internacionales y prácticas organizacionales

El análisis de la implementación de medidas de seguridad de datos en el país revela una notable discrepancia entre la creación de normativas y su aplicación efectiva, según (Avila Coello, 2024). Esta situación subraya la urgencia de reforzar los recursos tecnológicos y la capacitación, sobre la necesidad de formación especializada y recursos suficientes para adoptar tecnologías de seguridad avanzadas. La importancia de una cultura de seguridad cibernética para la fortaleza organizativa ante amenazas digitales sugiere la necesidad de una transformación cultural que eleve la seguridad de la información a una prioridad colectiva., de igual manera (Tupia, 2025) indica que Los organismos reguladores han reconocido la importancia de la evaluación de riesgos cibernéticos en el sector público. Normativas como la ISO/IEC 27005:2022, que proporciona directrices para la gestión del riesgo de seguridad de la información, y el NIST Cybersecurity Framework (CSF) 2.0, que establece un enfoque basado en cinco

funciones clave (Identificar, Proteger, Detectar, Responder y Recuperar), han servido como referencia para muchas organizaciones. Adicionalmente, marcos de gobernanza y gestión de riesgos de TI como RISK-IT 2.0 de ISACA e ITIL 4 ofrecen un enfoque estructurado para la alineación de la ciberseguridad con los objetivos estratégicos institucionales.

Podemos concluir que la seguridad de datos en las organizaciones evidencia una brecha entre la creación de normativas y su aplicación efectiva, lo que exige fortalecer los recursos tecnológicos y la capacitación especializada. Esta situación resalta la necesidad de una cultura organizacional orientada a la seguridad de la información como prioridad colectiva. Y que la relevancia de marcos internacionales como la ISO/IEC 27005:2022 y el NIST CSF 2.0, que guían la gestión de riesgos cibernéticos mediante funciones clave como identificar, proteger y responder.

Justificación del estudio: importancia de integrar gobernanza, cultura y resiliencia

La ciberseguridad organizacional y la gobernanza son componentes interdependientes que determinan la capacidad de una institución para proteger sus activos digitales y mantener su continuidad operativa. Integrar la gobernanza, la cultura organizacional y la resiliencia resulta esencial, ya que la seguridad no depende únicamente de la tecnología, sino también de la conciencia, compromiso y comportamiento de las personas dentro de la organización. Una buena gobernanza establece políticas, responsabilidades y controles claros; una cultura de seguridad fomenta la participación activa y la prevención; y la resiliencia permite responder y recuperarse eficazmente ante incidentes cibernéticos.

De acuerdo con (Nuñes Alvares, 2024) En el contexto latinoamericano, es fundamental que las organizaciones, especialmente las Pymes del sector minero, incrementen la inversión en ciberseguridad y gestionen de manera más eficiente sus infraestructuras tecnológicas y de comunicaciones. El creciente número de ciberataques, como se evidenció en el primer trimestre de 2023, determina la necesidad de adoptar marcos de gobernanza sólidos como la ISO 38500, la ISO 27001 y COBIT. Estos estándares no solo permiten mejorar las estrategias de defensa ante amenazas cibernéticas, sino que también optimizan la gestión del riesgo y potencian el talento humano en las áreas de TI. Implementar estas buenas prácticas

fortalecerá la resiliencia digital y protegerá a las organizaciones de los riesgos que amenazan su sostenibilidad operativa.

Objetivos generales y específicos de la investigación

1.4.1 Objetivo General

Analizar la ciberseguridad organizacional y la gobernanza desde una perspectiva integral, evaluando el marco normativo, la cultura de seguridad y las estrategias de ciberresiliencia en el contexto de la transformación digital, con el fin de proponer lineamientos que fortalezcan la protección de los activos digitales y la continuidad operativa de las organizaciones.

1.4.2 Objetivos Específicos

Examinar el cumplimiento y la aplicabilidad de las principales normativas y marcos de referencia internacionales en materia de ciberseguridad dentro de las organizaciones en proceso de transformación digital.

Evaluar el impacto de la cultura organizacional y las prácticas de concienciación en la consolidación de una gobernanza efectiva de la ciberseguridad.

Identificar y proponer estrategias de ciberresiliencia que integren tecnología, gestión de riesgos y gobernanza para fortalecer la respuesta y recuperación ante incidentes cibernéticos.

MARCO TEÓRICO

2.1. Ciberseguridad organizacional: definiciones y componentes clave

- **2.1.1. Protección de activos digitales**

  De acuerdo con (Dante & Lafuente, 2022) en materia de ciberseguridad y protección de datos las empresas están bajo la presión de adaptarse a las crecientes expectativas de los consumidores en un entorno digital que exige rapidez y personalización en el servicio. Esta realidad exige un enfoque empresarial ágil, capaz de gestionar la complejidad del mercado actual y responder de manera efectiva a las amenazas, se debe de entender la importancia de la ciberseguridad puesto que la falta de comprensión por parte de la dirección y de los individuos en las empresas sobre la

importancia de la ciberseguridad es uno de los desafíos para esta. La falta de conciencia de los gerentes acerca de la importancia de la ciberseguridad conduce a la falta de apoyo para sus sistemas de protección y a la actualización continua de los mismos, creando brechas, así como la falta de conciencia de los individuos sobre la importancia de la ciberseguridad, lo que conlleva a errores graves que provocan violaciones de seguridad, la ciberseguridad engloba a cualquier tecnología, acción o práctica que se pone en uso para la prevención de los distintos ciberataques y la mitigación de sus impactos. Esta presenta como objetivo la protección de aspectos como los sistemas, las aplicaciones, los dispositivos de orden informático, los datos de carácter confidencial, los activos financieros y digitales de personas y empresas u organizaciones contra condiciones como los virus informáticos, los ataques provenientes de ransomware de alta tecnología, entre otros.

En base a esto podemos concluir que destaca la creciente presión que enfrentan las empresas para adaptarse a un entorno digital dinámico, donde los consumidores demandan rapidez, personalización y seguridad. En este contexto, la ciberseguridad se presenta como un elemento estratégico fundamental, no solo técnico, sino también cultural y organizacional. Los autores señalan que uno de los principales desafíos radica en la falta de conciencia y compromiso tanto de la alta dirección como del personal, lo que genera vulnerabilidades y brechas de seguridad. La ausencia de apoyo y actualización en los sistemas de protección compromete la integridad de los datos y activos digitales. Por ello, la ciberseguridad debe entenderse como un proceso integral y preventivo, orientado a proteger sistemas, dispositivos y recursos frente a amenazas como virus o ransomware, garantizando la confianza, continuidad y resiliencia empresarial en la era digital.

- **2.1.2. Gestión del riesgo cibernético**

La gestión del riesgo cibernético constituye un componente esencial dentro de la estrategia de seguridad organizacional, ya que permite identificar, evaluar y mitigar las amenazas digitales que pueden afectar la continuidad del negocio. Según el NIST (2023), este proceso implica una comprensión integral de los activos críticos, las vulnerabilidades y el impacto potencial de los incidentes cibernéticos, con el fin de establecer controles proporcionales al nivel de riesgo.

De acuerdo con Tupia (2025), los marcos de referencia como la ISO/IEC 27005:2022 y el NIST Cybersecurity Framework (CSF) 2.0 proporcionan metodologías estructuradas para la gestión del riesgo de seguridad de la información, al integrar funciones clave como Identificar, Proteger, Detectar, Responder y Recuperar. Estos modelos permiten a las organizaciones alinear la ciberseguridad con los objetivos estratégicos y garantizar la continuidad de los servicios críticos frente a posibles incidentes. Además, fomentan una visión holística que abarca tanto los aspectos técnicos como los humanos y organizacionales, consolidando una cultura de seguridad basada en la prevención y la mejora continua.

Asimismo, Ávila Coello (2024) sostiene que la eficacia en la gestión del riesgo cibernético depende de la madurez tecnológica y cultural de las organizaciones. La falta de recursos, capacitación o gobernanza adecuada puede incrementar la exposición a amenazas y dificultar la respuesta ante incidentes. Por ello, se requiere una combinación equilibrada entre tecnología, políticas y formación del personal, respaldada por una gobernanza sólida que asegure la implementación y revisión constante de los controles. En síntesis, la gestión del riesgo cibernético no solo es una medida defensiva, sino una estrategia integral de sostenibilidad y confianza digital en el marco de la transformación tecnológica global.

- **2.1.3. Políticas y controles técnicos y administrativos**

Las políticas y controles técnicos y administrativos son elementos fundamentales dentro del marco de la gobernanza de la ciberseguridad, ya que establecen las directrices, responsabilidades y mecanismos necesarios para proteger los activos digitales de una organización. Según Bone Andrade (2023), las políticas de seguridad definen las normas y procedimientos que orientan el comportamiento del personal y el uso adecuado de los recursos tecnológicos, garantizando la confidencialidad, integridad y disponibilidad de la información. Estas políticas deben estar alineadas con los objetivos estratégicos institucionales y ser revisadas periódicamente para adaptarse a la evolución de las amenazas y del entorno digital.

Por su parte, los controles técnicos comprenden las herramientas y mecanismos tecnológicos destinados a prevenir, detectar y mitigar incidentes de seguridad, tales como cortafuegos, sistemas de detección de intrusos, autenticación multifactor, cifrado de datos y gestión de vulnerabilidades. De acuerdo con Díaz (2023), estos controles permiten fortalecer la infraestructura tecnológica y responder de manera oportuna ante posibles ataques, contribuyendo a la resiliencia operativa.

En complemento, los controles administrativos abarcan las acciones de gestión, auditoría y capacitación orientadas a fomentar una cultura organizacional de seguridad. Ávila Coello (2024) señala que la formación continua del personal y la existencia de procesos de monitoreo y evaluación son esenciales para minimizar el riesgo asociado al factor humano, responsable de gran parte de los incidentes cibernéticos. En conjunto, las políticas y los controles técnicos y administrativos conforman un sistema integral que permite a las organizaciones anticiparse a las amenazas, cumplir con las normativas vigentes y fortalecer la gobernanza de la ciberseguridad en el contexto de la transformación digital.

2.2. Gobernanza de la ciberseguridad

- **2.2.1. Rol de la alta dirección y alineación con objetivos estratégicos**

El rol de la alta dirección es determinante en la consolidación de una estrategia de ciberseguridad organizacional efectiva, ya que desde este nivel se definen las políticas, prioridades y recursos necesarios para garantizar la protección de la información y la continuidad operativa. Según Dante y Lafuente (2022), la falta de comprensión o apoyo por parte de los directivos es uno de los principales factores que debilita la seguridad digital en las empresas, generando brechas y vulnerabilidades críticas. Por ello, la dirección debe asumir un liderazgo activo, promoviendo una cultura de seguridad que involucre a toda la organización y asegure la integración de la ciberseguridad en la gestión estratégica y operativa.

De acuerdo con Tupia (2025), la alineación de la ciberseguridad con los objetivos estratégicos implica reconocerla como un pilar transversal del negocio, no solo como una función técnica. Esto requiere integrar la gestión de riesgos cibernéticos dentro

de los procesos de planificación, inversión y toma de decisiones corporativas. Una dirección comprometida establece una gobernanza clara, asigna responsabilidades y fomenta la comunicación entre las áreas de tecnología, cumplimiento y gestión de riesgos, asegurando que las iniciativas de seguridad aporten valor y sostenibilidad al negocio.

Asimismo, Ávila Coello (2024) enfatiza que el compromiso de la alta dirección fortalece la resiliencia organizacional y la capacidad de respuesta ante incidentes cibernéticos. Cuando los líderes reconocen la ciberseguridad como una ventaja competitiva y un componente esencial de la reputación corporativa, promueven inversiones continuas en tecnología, formación y cumplimiento normativo. En este sentido, el rol directivo no se limita a supervisar, sino a dirigir estratégicamente la seguridad digital, asegurando su alineación con la misión, visión y metas institucionales, y garantizando así un entorno organizacional seguro, confiable y preparado para los retos de la transformación digital.

- **2.2.2. Marcos de referencia: ISO/IEC 27001, ISO 38500, NIST, COBIT**

Los marcos de referencia en ciberseguridad y gobernanza de TI como ISO/IEC 27001, ISO 38500, NIST y COBIT proporcionan estructuras metodológicas que permiten a las organizaciones gestionar de forma sistemática la seguridad de la información y la alineación tecnológica con los objetivos estratégicos. La ISO/IEC 27001 es uno de los estándares internacionales más reconocidos para el establecimiento, implementación y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI). Según (Tupia, 2025), este marco ayuda a las instituciones a identificar riesgos, aplicar controles de seguridad y garantizar la confidencialidad, integridad y disponibilidad de los datos, lo que fortalece la confianza y la resiliencia organizacional frente a amenazas digitales.

Por su parte, la ISO 38500 se centra en la gobernanza corporativa de las tecnologías de la información, orientando a la alta dirección en la toma de decisiones estratégicas sobre el uso responsable, ético y eficaz de las TI. De acuerdo con (Avila Coello, 2024), este marco promueve principios de responsabilidad, transparencia y

cumplimiento, asegurando que la tecnología se utilice para generar valor y apoyar los objetivos empresariales. Complementariamente, el NIST Cybersecurity Framework (CSF), desarrollado por el Instituto Nacional de Estándares y Tecnología de EE. UU., establece cinco funciones clave Identificar, Proteger, Detectar, Responder y Recuperar que guían a las organizaciones en la gestión integral de riesgos cibernéticos, permitiendo una respuesta estructurada ante incidentes.

Finalmente, el marco COBIT (Control Objectives for Information and Related Technologies) proporciona un modelo de gobernanza y gestión de TI que integra procesos, indicadores y buenas prácticas para garantizar que los recursos tecnológicos se administren de manera eficiente y alineada con la estrategia organizacional. Según (Bone Andrade, 2023), COBIT facilita la comunicación entre las áreas técnicas y la alta dirección, permitiendo una visión unificada de la seguridad, el cumplimiento y el valor empresarial. En conjunto, estos marcos de referencia conforman una base sólida de gobernanza, control y mejora continua, indispensable para afrontar los desafíos de la transformación digital con una gestión responsable, segura y estratégica de la tecnología.

- **2.2.3. Métricas y mecanismos de control de la gobernanza TI**

  Las métricas y mecanismos de control en la gobernanza de TI son instrumentos esenciales para evaluar el desempeño, la eficacia y el grado de alineación de las tecnologías de la información con los objetivos estratégicos de la organización. Según ISO 38500, la gobernanza de TI requiere un enfoque basado en la medición y la supervisión continua, a fin de asegurar que las decisiones tecnológicas generen valor y mitiguen los riesgos asociados.

  De acuerdo con (Tupia, 2025), los mecanismos de control abarcan tanto herramientas técnicas como procedimientos administrativos que garantizan la correcta implementación de políticas, normas y marcos de referencia. Entre ellos se incluyen auditorías de TI, evaluaciones de madurez, revisiones de cumplimiento, controles de acceso y análisis de vulnerabilidades, los cuales contribuyen a mantener la integridad y confiabilidad de los sistemas. Estos mecanismos también facilitan la identificación

temprana de desviaciones o fallas en los procesos de seguridad, permitiendo una respuesta ágil y la adopción de medidas correctivas oportunas.

Asimismo, (Bone Andrade, 2023) resalta que la eficacia de la gobernanza TI depende de la integración entre métricas, monitoreo continuo y retroalimentación estratégica. Esto implica establecer un ciclo de mejora continua donde los resultados de las evaluaciones se traduzcan en acciones concretas de optimización tecnológica, capacitación del personal y fortalecimiento de políticas de seguridad. En conjunto, las métricas y los mecanismos de control permiten transformar la gobernanza TI en un proceso dinámico, transparente y orientado a resultados, asegurando que la tecnología aporte valor sostenible, cumplimiento normativo y resiliencia organizacional en el contexto de la transformación digital.

2.3. Cultura de ciberseguridad en las organizaciones

- **2.3.1. Concienciación, capacitación y cambio de comportamiento**

La concienciación, la capacitación y el cambio de comportamiento constituyen pilares fundamentales en la construcción de una cultura sólida de ciberseguridad organizacional**.** Según (Dante & Lafuente, 2022)**,** la falta de comprensión y compromiso por parte de directivos y empleados es uno de los mayores factores de riesgo, pues las brechas de seguridad suelen originarse en errores humanos o en la falta de atención a las políticas de protección. La concienciación busca generar una actitud proactiva frente a las amenazas digitales, sensibilizando al personal sobre la importancia de la seguridad de la información como responsabilidad compartida dentro de la organización.

La capacitación continua permite desarrollar las competencias técnicas y conductuales necesarias para prevenir, detectar y responder ante incidentes cibernéticos. De acuerdo con (Bone Andrade, 2023), los programas de formación deben incluir simulaciones de ataques, cursos interactivos y prácticas reales que fortalezcan la respuesta del personal ante situaciones críticas, reduciendo significativamente el impacto de amenazas como el **phishing** o el **ransomware**. Estas iniciativas no solo mejoran la preparación técnica, sino que también promueven la adopción de hábitos seguros en el uso cotidiano de la tecnología.

Finalmente, el cambio de comportamiento representa el resultado tangible de una gestión eficaz de concienciación y formación. (Avila Coello, 2024) sostiene que el verdadero éxito de la ciberseguridad radica en transformar la conducta del personal, integrando la seguridad digital en la cultura organizacional y en las rutinas laborales. Este cambio implica pasar de una actitud reactiva a una mentalidad preventiva y colaborativa, donde cada individuo asume un rol activo en la protección de los recursos informáticos. En conjunto, la concienciación, la capacitación y el cambio de comportamiento fortalecen la resiliencia cibernética y aseguran una defensa integral frente a las crecientes amenazas del entorno digital.

- **2.3.2. Factores humanos y resistencia al cambio digital**

  Los factores humanos y la resistencia al cambio representan uno de los mayores desafíos en la implementación efectiva de estrategias de ciberseguridad y gobernanza tecnológica. Según (Dante & Lafuente, 2022)**,** la falta de comprensión sobre la importancia de la ciberseguridad por parte de directivos y empleados genera vulnerabilidades críticas en los sistemas organizacionales. El comportamiento humano, influido por hábitos, desconocimiento o desinterés, puede conducir a errores que comprometen la integridad de la información. Por ello, el factor humano no debe verse únicamente como un riesgo, sino como un componente esencial que, bien gestionado, puede convertirse en el principal aliado de la seguridad digital.

  La resistencia al cambio suele manifestarse cuando las organizaciones introducen nuevas políticas, herramientas o procesos relacionados con la ciberseguridad. De acuerdo con Ávila (Avila Coello, 2024), esta resistencia surge por la falta de comunicación, la escasa participación de los empleados en el proceso de transformación y la percepción de que los nuevos sistemas limitan su autonomía o aumentan su carga laboral. Superar esta barrera requiere una estrategia de gestión del cambio organizacional basada en la empatía, la transparencia y la participación, donde los colaboradores comprendan los beneficios y el propósito de las medidas adoptadas.

  Por su parte, (Bone Andrade, 2023) sostiene que la clave para reducir la resistencia y fortalecer la cultura de seguridad está en la formación continua y la motivación interna**.** Invertir en programas de concienciación y comunicación que promuevan la

confianza y el sentido de responsabilidad colectiva ayuda a transformar la actitud del personal frente a la seguridad. En este sentido, abordar los factores humanos y la resistencia al cambio no solo mejora la aceptación de las políticas tecnológicas, sino que impulsa una cultura organizacional resiliente, capaz de adaptarse a los retos de la transformación digital con compromiso y sostenibilidad.

- **2.3.3. Indicadores de madurez cultural en seguridad**

  Los indicadores de madurez cultural en seguridad permiten evaluar el grado en que una organización ha integrado la ciberseguridad en su cultura corporativa, comportamientos y procesos internos. Según la *ENISA (2023)*, estos indicadores miden aspectos como la concienciación del personal, la adherencia a políticas de seguridad, la participación activa en programas de formación y la capacidad de respuesta ante incidentes. A medida que la madurez aumenta

  De acuerdo con *PwC (2022)*, los niveles de madurez cultural pueden clasificarse desde una etapa reactiva, en la que los empleados solo cumplen normas por obligación, hasta una etapa proactiva, en la que todos los miembros comprenden su papel en la protección de los activos digitales y contribuyen activamente a la mejora continua. Esta evolución refleja una gobernanza de TI sólida y una gestión de riesgos integral.

  Finalmente, los indicadores más relevantes incluyen el índice de cumplimiento de políticas de seguridad**,** la tasa de participación en capacitaciones, el número de incidentes reportados internamente, y el nivel de confianza digital entre empleados y dirección.

2.4. Ciberresiliencia organizacional

- **2.4.1. Concepto y evolución del término**
- La ciberresiliencia organizacional se define como la capacidad de una entidad para anticipar, resistir, recuperarse y adaptarse frente a incidentes cibernéticos que puedan afectar su funcionamiento, reputación o continuidad operativa (*ENISA, 2022*). A diferencia de la ciberseguridad tradicional, que se centra principalmente en la protección técnica, la ciberresiliencia abarca una visión más integral que incluye la gestión del riesgo, la continuidad del negocio y la cultura organizacional.

- El término ha evolucionado notablemente desde su origen en la década de 2000. Inicialmente, la resiliencia se aplicaba a contextos psicológicos y de ingeniería, refiriéndose a la capacidad de recuperación ante la adversidad. Con el aumento de los ciberataques y la dependencia digital, el concepto fue adaptado al ámbito tecnológico, dando origen al término ciberresiliencia (*World Economic Forum, 2018*).

3. Estrategias de Ciberresiliencia en la Era Digital

Objetivo: Proponer estrategias que integren gobernanza, tecnología y cultura hacia la resiliencia organizacional, la ciberresiliencia se ha convertido en un componente esencial de la sostenibilidad digital y la competitividad organizacional. En un entorno caracterizado por la hiperconectividad, la automatización y el uso intensivo de datos, las organizaciones requieren estrategias integradas que combinen la gobernanza corporativa, las tecnologías avanzadas y la cultura de seguridad para anticiparse, resistir y recuperarse de los incidentes cibernéticos. De acuerdo con el World Economic Forum (2023), la resiliencia digital no depende únicamente de la inversión tecnológica, sino del alineamiento estratégico entre las decisiones empresariales y la gestión del riesgo para adaptarse al cambio.

3.1. Diseño de estrategias de prevención y mitigación

El diseño de estrategias efectivas de prevención y mitigación debe basarse en un enfoqueproactivo de gestión del riesgo cibernético, integrando políticas de seguridad, controles técnicos, monitoreo continuo y cultura organizacional. Según la norma ISO/IEC 27005 (2022), la prevención debe sustentarse en la identificación de vulnerabilidades críticas, la evaluación de riesgos emergentes y la implementación de medidas de mitigación como segmentación de redes, autenticación multifactor y cifrado de datos. La mitigación, por su parte, implica contar con protocolos de contención y respuesta rápida ante incidentes para reducir los impactos operativos, financieros y reputacionales.

3.2. Integración de inteligencia artificial y analítica predictiva en la detección temprana de amenazas

La aplicación de inteligencia artificial (IA) y analítica predictiva está transformando la manera en que las organizaciones detectan y gestionan amenazas. Los sistemas basados en machine learning permiten identificar patrones anómalos en tiempo real, anticipando posibles ciberataques antes de que ocurran (IBM Security, 2023). Estas herramientas analizan grandes volúmenes de datos provenientes de redes, endpoints y registros de

actividad, fortaleciendo las capacidades de los Security Operations Centers (SOC). La IA no reemplaza la intervención humana, sino que potencia la toma de decisiones informadas, facilitando la priorización de riesgos y la asignación eficiente de recursos.

3.3. Planes de continuidad de negocio y recuperación ante desastres (BCP/DRP)

Los planes de continuidad de negocio (BCP) y recuperación ante desastres (DRP) son pilares fundamentales para mantener la estabilidad operativa en situaciones de crisis cibernética. Según el National Institute of Standards and Technology (NIST SP 800-34 Rev. 1, 2020), un plan de continuidad eficaz debe incluir la identificación de procesos críticos, la definición de niveles aceptables de interrupción, copias de respaldo seguras y estrategias de comunicación durante emergencias. Los DRP, por su parte, deben garantizar la restauración rápida de servicios esenciales mediante la automatización de procesos, replicación de datos y validación de sistemas. Estas prácticas consolidan la resiliencia operativa, asegurando la continuidad de los servicios esenciales incluso bajo condiciones adversas.

3.4. Resiliencia basada en datos e innovación tecnológica

La resiliencia basada en datos se fundamenta en la capacidad de utilizar la información como recurso estratégico para mejorar la seguridad, la adaptabilidad y la toma de decisiones. El uso de tecnologías emergentes como la computación en la nube, el blockchain y el edge computing contribuye a la descentralización del riesgo y la mejora de la trazabilidad de los incidentes (Navarrete, 2025). Estas innovaciones permiten crear ecosistemas digitales más seguros, donde la información no solo se protege, sino que se convierte en una fuente de aprendizaje y mejora continua. La innovación tecnológica, alineada con la gobernanza, potencia la creación de entornos resilientes, capaces de evolucionar junto con las amenazas digitales.

3.5. Evaluación de capacidades de respuesta y adaptación

La evaluación de la capacidad de respuesta y adaptación es un proceso clave para determinar el nivel de madurez cibernética de una organización. Esta evaluación debe realizarse mediante auditorías, pruebas de penetración, ejercicios de simulación (*cyber drills*) y análisis post-incidente (*ISO 22301*, 2019). Asimismo, los indicadores de desempeño (KPIs) y madurez (KMMs) permiten medir la efectividad de las políticas y estrategias implementadas. Las organizaciones resilientes no solo se enfocan en recuperarse tras un ataque, sino en aprender y mejorar continuamente su capacidad de anticipación y respuesta, promoviendo

una cultura de mejora continua y aprendizaje organizacional, de acuerdo con (Muñoz, 2025) se puede decir que la adopción de tecnologías como la robótica avanzada y la inteligencia artificial también abre nuevas oportunidades laborales en áreas como el desarrollo de software, análisis de datos y mantenimiento de sistemas complejos (Industriall Global Union, 2020).

En síntesis, las estrategias de ciberresiliencia en la era digital deben concebirse como un ecosistema integral que vincule gobernanza, tecnología y cultura organizacional. Solo mediante un enfoque sistémico y adaptativo es posible fortalecer la capacidad de las organizaciones para resistir los ciberataques, recuperarse rápidamente y evolucionar frente a un entorno digital en constante transformación.

- **6. Metodología de la Investigación**

La investigación se desarrollará bajo un enfoque mixto (cualitativo–cuantitativo), ya que busca tanto analizar marcos normativos y modelos conceptuales como recoger evidencia empírica en PYMES.

- **6.1. Enfoque y tipo de investigación**

Este enfoque busca describir, analizar y proponer estrategias integradas que vinculen la gobernanza de TI, la innovación tecnológica y la cultura organizacional, evaluando su contribución al fortalecimiento de la resiliencia ante incidentes cibernéticos. Desde una perspectiva cuantitativa, se pueden emplear métricas de desempeño y madurez en seguridad.

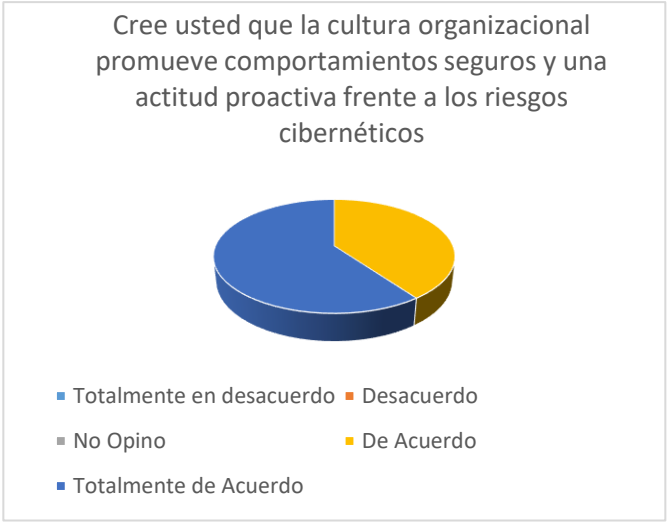
- **6.2. Técnicas de recolección de datos**

  Se procedieron a realizar encuestas, conformadas por cinco preguntas de opción múltiple, valoradas en la escala de Likert, las mismas que se desarrollaron a través de un formulario de Google para obtener los datos necesarios para su posterior análisis.

1) Cree usted que la cultura organizacional promueve comportamientos seguros y una actitud proactiva frente a los riesgos cibernéticos

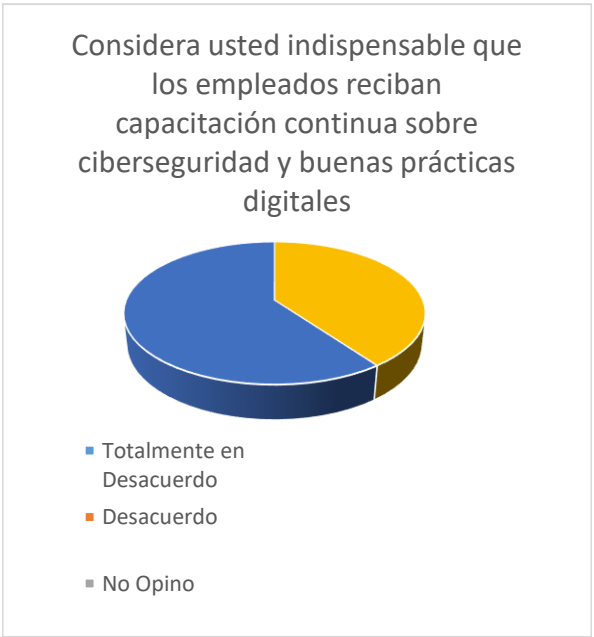
Descripción	fi	%
Totalmente en Desacuerdo	0	0
Desacuerdo	0	0
No Opino	0	0%
De Acuerdo	8	40%
Totalmente de Acuerdo	12	60%
Total	**20**	**100%**

Tabla 1



2) Considera usted indispensable que los empleados reciban capacitación continua sobre ciberseguridad y buenas prácticas digitales.

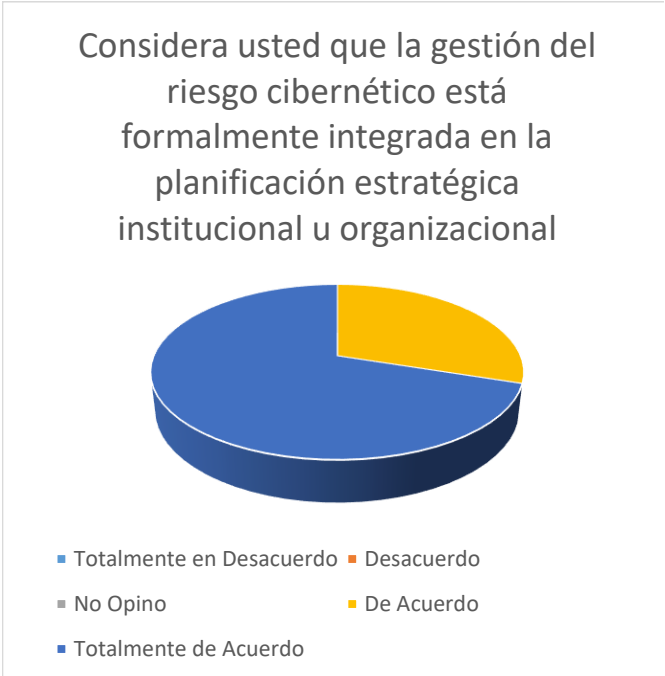
Descripción	fi	%
Totalmente en Desacuerdo	0	0
Desacuerdo	0	0
No Opino	0	0%
De Acuerdo	8	40%
Totalmente de Acuerdo	12	60%
Total	**20**	**100%**



3) Considera usted que la gestión del riesgo cibernético está formalmente integrada en la planificación estratégica institucional u organizacional

Descripción	fi	%
Totalmente en Desacuerdo	0	0
Desacuerdo	0	0
No Opino	0	0%
De Acuerdo	6	30%
Totalmente de Acuerdo	14	70%
Total	**20**	**0%**

Tabla 3



4) Considera usted que los procesos de transformación digital incluyen evaluaciones previas de riesgos cibernéticos antes de implementar nuevas tecnologías.

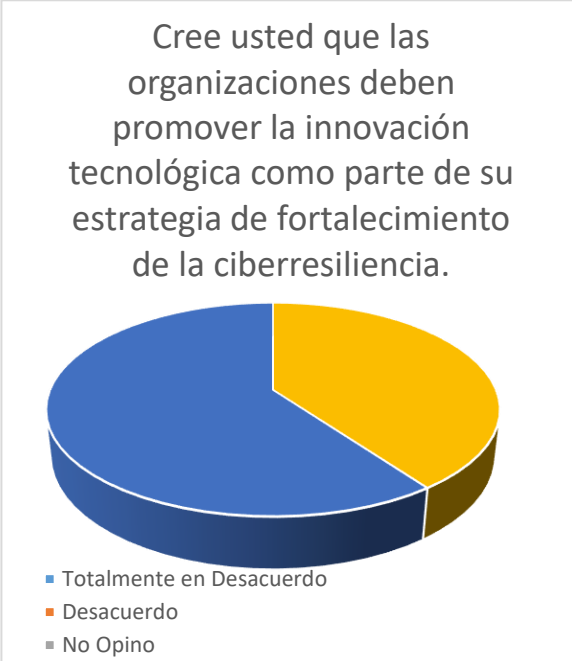
Descripción	fi	%
Totalmente en Desacuerdo	0	0
Desacuerdo	0	0
No Opino	0	0%
De Acuerdo	6	30%
Totalmente de Acuerdo	14	70%
Total	**20**	**100%**

Tabla 4

5) Cree usted que las organizaciones deben promover la innovación tecnológica como parte de su estrategia de fortalecimiento de la ciberresiliencia.

Descripción	fi	%
Totalmente en Desacuerdo	0	0
Desacuerdo	0	0
No Opino	0	0%
De Acuerdo	2	10%
Totalmente de Acuerdo	18	90%
Total	**20**	**100%**

Tabla 5



DISCUSIÓN DE RESULTADOS

PREGUNTAS	ANÁLISIS
¿Cree usted que la cultura organizacional promueve comportamientos seguros y una actitud proactiva frente a los riesgos cibernéticos?	El 40% está de acuerdo y el 60% totalmente de acuerdo, en tanto la organización muestra un entorno cultural sólido y comprometido con la seguridad informática, aunque sería recomendable continuar fortaleciendo las estrategias de sensibilización y capacitación para mantener y ampliar esta cultura de prevención y responsabilidad digital.
¿Considera usted indispensable que los empleados reciban capacitación continua sobre ciberseguridad y buenas prácticas digitales?	El 40% está de acuerdo y el 60% totalmente de acuerdo, podemos evidenciar una fuerte percepción positiva sobre la relevancia de la capacitación continua en ciberseguridad. Esto indica que los empleados valoran el aprendizaje constante como una herramienta fundamental para proteger los activos digitales de la

	organización y promover una cultura de prevención y responsabilidad tecnológica.
¿Considera usted que la gestión del riesgo cibernético está formalmente integrada en la planificación estratégica institucional u organizacional?	El 70% que se muestra totalmente de acuerdo refleja que la mayoría percibe la ciberseguridad como una prioridad estratégica, El 30% restante, que está "de acuerdo", sugiere que, aunque la gestión del riesgo está presente, podría fortalecerse su implementación práctica, su seguimiento o su alineación con los objetivos de negocio, la encuesta demuestra que la gestión del riesgo cibernético está consolidada como parte integral de la planificación estratégica, lo cual es un signo de madurez digital y compromiso institucional con la protección de los activos de información.
¿Considera usted que los procesos de transformación digital incluyen evaluaciones previas de riesgos cibernéticos antes de implementar nuevas tecnologías?	El 70% que está totalmente de acuerdo indica que la mayoría percibe que la institución posee procedimientos estructurados para analizar amenazas y vulnerabilidades antes de la implementación tecnológica. El 30% restante, aunque también valora la existencia de dichas evaluaciones, podría reflejar que aún existen áreas por fortalecer, como la sistematización de los procesos, la documentación o la participación del personal en dichas evaluaciones, los resultados muestran que la organización mantiene una visión estratégica y preventiva en materia de ciberseguridad dentro de la transformación digital.
¿Cree usted que las organizaciones deben promover la innovación tecnológica como parte de su estrategia de fortalecimiento de la ciberresiliencia?	La encuesta demuestra que existe una percepción ampliamente favorable hacia la promoción de la innovación tecnológica como pilar de la ciberresiliencia. Esto indica que la organización reconoce que la resiliencia digital no depende únicamente de políticas reactivas, sino de una evolución tecnológica constante que permita responder de forma eficiente y segura a los desafíos del entorno digital.

CONCLUSIONES

A pesar de la existencia de estándares internacionales (ISO 27001, ISO 38500, NIST CSF 2.0, COBIT), su implementación efectiva sigue siendo baja en las PYMES. Es necesario fortalecer las capacidades institucionales mediante auditorías y liderazgo.

La ciberseguridad no se ha interiorizado como valor cultural. La falta de capacitación y concienciación mantiene al factor humano como el principal vector de riesgo. Se recomienda institucionalizar programas de formación continua y simulaciones de ciberataques.

Las empresas han avanzado en infraestructura y monitoreo técnico, pero aún carecen de planes integrales de recuperación ante incidentes. La adopción de IA y analítica de datos representa una oportunidad estratégica para anticipar amenazas y mejorar la respuesta.

La ciberseguridad debe abordarse como un componente estratégico de la gobernanza organizacional: Implementar un Modelo de Gobernanza Cibernética Integrada (MGCI) basado en ISO 38500, NIST CSF y COBIT.

- Fomentar una Cultura de Ciberconciencia con indicadores de madurez medibles.
- Establecer centros de monitoreo y respuesta (SOC) en colaboración con entidades regulatorias y académicas.
- Desarrollar políticas nacionales de apoyo a PYMES en formación, financiamiento y cumplimiento normativo.

REFERENCIAS BIBLIOGRÁFICAS

Avila Coello, A. (2024). Seguridad de la información en instituciones públicas : desafíos y buenas prácticas en el contexto. 4, 140–156.

Bone Andrade, F. (2023). Evaluación de la evolución de la ciberseguridad en sistemas empresariales modernos Evaluation of the evolution of cybersecurity in modern enterprise systems . 01, 25–38.

Cruz Tunqui, R. C. (2024). Ciberseguridad: Protección de la empresa en la era digital. Maya-Revista de Administración y Turismo, 6(2), 14–26.

Dante, R., & Lafuente, P. (2022). Ciberseguridad en empresas : Revisión sistemática sobre desafíos y estrategias para proteger activos digitales assets. 6, 1–15.

Díaz, J. J. G. (2023). De la seguridad informática a la resiliencia cibernética. https://doi.org/10.29236/sistemas.n175a6

Muñoz, D. (2025). Optimización de la cadena de suministro a través de tecnologías emergentes. 1–77.

Navarrete, L. (2025). Aplicación de tecnologías de Edge Computing en la Industria 4.0. 3, 1–16.

Nuñes Alvares, Y. (2024). DESAFÍOS EN LA GOBERNANZA DE PYMES MINERAS COLOMBIANAS : GESTIÓN DE TI Y CIBERSEGURIDAD COMO FACTORES CRÍTICOS. 82–98.

Tupia, M. (2025). Un Modelo de Componentes para la Evaluación de Riesgos de Ciberseguridad en Instituciones Públicas. 11–28.