DOI: https://doi.org/10.47300/actasidi-unicyt-2024-09

DESAFÍOS EN LA GOBERNANZA DE PYMES MINERAS COLOMBIANAS: GESTIÓN DE TI Y CIBERSEGURIDAD COMO FACTORES CRÍTICOS

Núñez Alvarez, Yenny Stella
Universidad Nacional Abierta y a Distancia – UNAD
Sogamoso, Colombia
yenny.nunez@unad.edu.co
ORCID: https://orcid.org/0000-0002-6868-6278

RESUMEN

Este estudio es una investigación cualitativa documental que analiza la gobernanza de TI, la ciberseguridad y la gestión de riesgos en las Pymes mineras en América Latina, basándose en informes especializados. Se destaca que las empresas mineras de la región en específico de Colombia que han pasado a ser un blanco atractivo para los ciberdelincuentes, enfrentándose a amenazas como el ransomware, ataques dirigidos y el robo de información confidencial, lo que compromete sus operaciones, reputación y finanzas. En este contexto, la gobernanza de TI es fundamental, y estándares como ISO 38500, COBIT 2019 e ISO 27001 proporcionan marcos sólidos para gestionar riesgos cibernéticos y asegurar la alineación de la tecnología con los objetivos empresariales, asegurando la confidencialidad, integridad y disponibilidad de los datos. Asimismo, se enfatiza la relevancia de la cooperación entre las empresas del sector y las entidades gubernamentales para intercambiar información y reforzar la defensa conjunta. Las tendencias futuras apuntan a ciberataques más sofisticados, incluyendo el uso de inteligencia artificial, ataques a la cadena de suministro y la proliferación de dispositivos IoT como amenazas emergentes.

Palabras clave: Ciberseguridad, Gestión de riesgos, Gobernanza de TI, Pymes mineras

ABSTRACT

This study is qualitative documentary research that analyzes IT governance, cybersecurity, and risk management in mining SMEs in Latin America, based on specialized reports. It highlights that mining companies in the region, particularly in Colombia, have become attractive targets for cybercriminals, facing threats such as ransomware, targeted attacks, and the theft of confidential information, which jeopardizes their operations, reputation, and finances. In this context, IT governance is essential, and standards such as ISO 38500, COBIT 2019, and ISO 27001 provide robust frameworks for managing cyber risks and ensuring the alignment of technology with business objectives, safeguarding confidentiality, integrity, and availability of data. Furthermore, the report emphasizes the importance of cooperation between sector companies and government entities to exchange information and strengthen joint defenses. Future trends point to increasingly sophisticated cyberattacks, including the use of artificial intelligence, supply chain attacks, and the proliferation of IoT devices as emerging threats.

Keywords: Cybersecurity, Risk Management, IT Governance, Mining SMEs

1. INTRODUCCIÓN

Dado que las organizaciones dependen de un amplio equipo de colaboradores que operan en diversas áreas funcionales, es fundamental que adopten políticas de seguridad, controles y mecanismos de defensa que estén alineados con la gobernanza TI, la continuidad del negocio y

la ciberseguridad. Cada área, desde operaciones hasta servicios, se apoya en tecnologías de información y productos que, aunque adaptados a sus necesidades específicas, generan información crítica y confidencial que debe protegerse.

La creciente amenaza de ciberataques, como lo revela el Norton Cyber Safety Insights Report de 2023, subraya la urgencia de estas medidas: se estima que 463 millones de personas fueron víctimas de delitos cibernéticos en el último año, con consecuencias económicas y de tiempo significativas. La desarticulación entre gobierno corporativo, gobernanza TI y gestión de ciberseguridad, sumada a la falta de capacitación adecuada del personal, amplifica estos riesgos. Por ello, la organización debe priorizar la creación de políticas de seguridad robustas que protejan sus activos esenciales y aseguren la integridad de sus procesos frente a las amenazas cibernéticas cada vez más sofisticadas. Según el informe, los ciberdelitos con mayores porcentajes fueron: 41% virus en los dispositivos, 35% estafas a través de mensajes, 30% phishing y 24% extorsión, entre otros ataques experimentados.

Normalmente, cuando las personas o empleados dan clic a un link de un correo electrónico o mensaje de texto, están abriendo la puerta a un posible ataque cibernético, ya que en muchas ocasiones desconocen soluciones específicas de privacidad en línea o software de ciberseguridad para protegerse contra estas amenazas. Por lo tanto, es crucial que las organizaciones inviertan en capacitación y concientización del personal, complementando las medidas técnicas con una cultura de seguridad que permita hacer frente a los riesgos cibernéticos de manera integral.

Es claro que, en la actualidad, un número cada vez más elevado de organizaciones se ve motivado a llevar a cabo transformaciones digitales en sus operaciones. Estas transformaciones incorporan o emplean de manera masiva de tecnologías de la información y la comunicación, que abarcan bases de datos, aplicaciones en línea, plataformas digitales y almacenamiento en la nube. Este entorno tecnológico en constante cambio procesa y examina grandes cantidades de datos e información provenientes de diversas áreas clave del funcionamiento empresarial. Este contexto, por lo tanto, indica la necesidad de establecer mecanismos de protección y prevención para resguardar la integridad, disponibilidad y confidencialidad de los datos, así como asegurar la continuidad del negocio ante riesgos y ataques cibernéticos potenciales que podrían impactar gravemente la infraestructura tecnológica. De acuerdo con el informe oficial de la Policía Nacional, hasta ahora en el año en Colombia se han registrado 54.121 denuncias por ataques cibernéticos, lo que representa un incremento del 79% en comparación con 2021 (MinTIC, 2023).

Un reciente estudio de Kaspersky sobre ciberseguridad en Latinoamérica ha revelado que Colombia se encuentra entre los tres países más atacados de la región durante el año 2023. Los datos, recopilados entre junio de 2022 y julio de 2023, evidencian un aumento significativo en los ciberataques dirigidos a pequeñas y medianas empresas colombianas. Estos ataques representaron una preocupación constante y creciente para el sector empresarial, con un aumento notable en la frecuencia y la sofisticación de los mismos. La vulnerabilidad a estos ataques se vio agravada por diversas razones, incluida la falta de recursos, ausencia de una gestión TI, planes de gestión de riesgos informáticos y carencia de personal cualificado en seguridad informática. Además, la proliferación de ciberataques ha convertido a las Pymes en blancos vulnerables, sufriendo las consecuencias de incidentes como el malware y el phishing. Estos ataques no solo generan pérdidas económicas significativas, sino que también afectan considerablemente la confianza de los clientes y ponen en riesgo la continuidad de las operaciones. Ante esta creciente amenaza, es necesario que las Pymes adopten un enfoque proactivo, invirtiendo en soluciones de seguridad robustas para proteger sus activos digitales, capacitando a sus empleados y fomentando una cultura de ciberseguridad.

La colaboración entre los diferentes departamentos es importante para el éxito de cualquier organización. Cuando todos los actores, desde la alta dirección hasta los empleados de primera línea, trabajan juntos hacia un objetivo común, se maximiza la eficiencia y se obtienen mejores resultados. Esta alineación garantiza que los recursos se utilicen de manera óptima y que se eviten duplicaciones de esfuerzos. Cuando todos los departamentos y niveles de una organización trabajan en sincronía, se logra una gestión más eficiente de los recursos, desde los financieros hasta los tecnológicos. Esta alineación estratégica, que garantiza que todas las acciones estén enfocadas en los objetivos comunes, es clave para el éxito de cualquier empresa. Un marco de gobernanza sólido refuerza esta cohesión, asegurando que las tecnologías de la información estén al servicio de la estrategia empresarial y no al revés. Este modelo se estructura conforme a estándares y marcos de trabajo reconocidos, como COBIT, ISO 38500, ISO 27001, e ISO 27002 que establecen directrices para la gestión y gobierno de TI, evaluación y monitoreo en el control de negocios y seguridad IT, gestión de servicios TI, proporcionando los requisitos técnicos y de gestión necesarios para implementar, mantener y mejorar los sistemas de gestión de seguridad de la información. Al seguir las mejores prácticas y controles de ciberseguridad, garantizamos el cumplimiento de los estándares internacionales y mitigamos los riesgos asociados a la seguridad de la información. Estos elementos proporcionan el fundamento necesario para la formulación de proyectos e indicadores que contribuyen a planificar, gestionar y medir el cumplimiento de objetivos, adaptándose al contexto organizacional en la gestión de recursos tecnológicos e informativos, y estableciendo mecanismos esenciales para el aseguramiento frente a amenazas cibernéticas en la PYMES del sector minero.

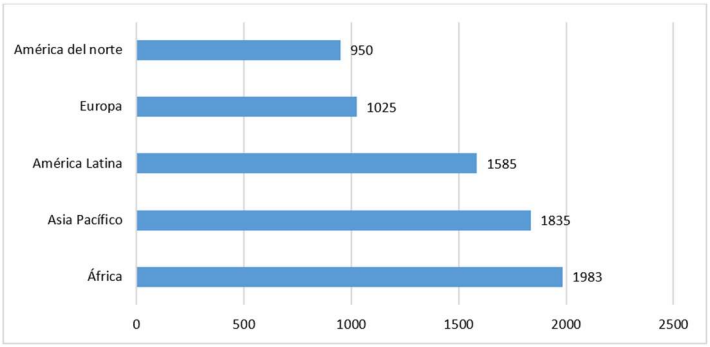
2. MARCO CONCEPTUAL

Ciberseguridad

Según el reporte de ciberseguridad de Check Point Software de 2023, los ciberataques a nivel mundial experimentaron un incremento del 7% en relación con el mismo período del año anterior. En promedio, se registraron 1,248 ataques semanales por organización. El sector educativo fue el más afectado, con un incremento del 15%. La región de Asia-Pacífico experimentó el mayor aumento de ataques (16%). Además, 1 de cada 31 organizaciones sufrió ataques de ransomware cada semana. La sofisticación de los ataques, como el uso de herramientas legítimas para fines maliciosos, resalta la necesidad de que los líderes prioricen la seguridad cibernética preventiva y refuercen estrategias integrales. La aplicación de parches, la capacitación en ciberseguridad y el uso de tecnologías avanzadas de prevención son elementos fundamentales para reducir el creciente riesgo global, como se evidencia en la figura 1.

Figura 1

Promedio de ataques semanales por organización a nivel Mundial



Nota : Informe de ciberseguridad de Check Point Software de 2023, realizado por Check Point (Cyber Security Report 2023 | Check Point Software, 2023)

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.

La gobernanza de TI

En una era caracterizada por altos niveles de interconexión y creciente automatización industrial, las pequeñas y medianas empresas (PYMES) se han convertido en objetivos atractivos para los ciberdelincuentes. Debido a sus recursos limitados y a sistemas de seguridad menos elaborada, estas empresas son especialmente vulnerables a ciberataques que pueden comprometer su información confidencial, dañar su reputación y amenazar su continuidad operativa. Por ello, invertir en ciberseguridad no es solo una necesidad, sino una prioridad para proteger estos activos críticos y asegurar un crecimiento sostenible. La gobernanza de TI, que abarca la implementación de procesos, estructuras organizativas y la adecuada asignación de recursos, asegura que las tecnologías de la información de una empresa respalden y fortalezcan sus estrategias y objetivos (Weill & Ross, 2022). En el ámbito de la ciberseguridad, la gobernanza de TI cobra aún más relevancia, ya que desempeña un papel crucial en la protección de los activos digitales frente a posibles amenazas informáticas. Desarrollar un marco de gobernanza de TI y ciberseguridad específicamente diseñado para las PYMES del sector minero requiere la adopción de estándares y mejores prácticas reconocidas en el campo. Estos marcos proporcionan directrices claras para gestionar de manera efectiva la seguridad informática y proteger los activos clave de la organización.

Madurez de seguridad informática

Los modelos de madurez de seguridad permiten medir lo que se está haciendo bien o las oportunidades de mejora para llegar a un punto de equilibrio, tomando la definición de Alberts, C., & Dorofee, A. (2018). como el modelo de madurez de seguridad de CERT, permiten a las organizaciones evaluar y mejorar su postura de seguridad cibernética a partir del reconocimiento de las oportunidades de mejora y la implementación de controles adecuados, que en un escenario ideal es el de implementar múltiples capas de defensa para proteger los sistemas de información contra amenazas cibernéticas.

Esto se reafirma en el informe denominado III Indicador de madurez en ciberseguridad 2022, realizado por ISMS Forum basado en el marco de trabajo NIST, donde se revela una mejora en la postura de ciberseguridad de las empresas, con un aumento del 43% al 54% en el nivel Maduro. Cabe decir, que el dominio Proteger destaca con un 75% de empresas en niveles Maduros u Optimizados, mientras que Recuperar reporta un crecimiento más lento, alcanzando solo el 58%. Las empresas más grandes, con más de 250 empleados, presentan niveles de madurez más altos (67%), y los sectores de Información y Comunicaciones, Actividades Financieras y Actividades Profesionales lideran en madurez. Sin embargo, persisten áreas de oportunidad, especialmente en el sector de Industria Manufacturera y en el dominio de Recuperar, lo que sugiere la necesidad de seguir fortaleciendo la ciberseguridad en las organizaciones.

Alcanzar la madurez organizacional en ciberseguridad es esencial para las PYMES, ya que fortalece su postura frente a amenazas cibernéticas y asegura la continuidad del negocio. Una

alta madurez implica el despliegue de medidas y procedimientos de seguridad claros y actualizados, que establezcan directrices para la protección de la información y la gestión de incidentes. Además, se requiere desarrollar una conciencia de seguridad entre los empleados, capacitándolos para reconocer y responder a posibles amenazas. La actualización y mantenimiento del software son también indicadores clave, ya que aseguran que la organización esté protegida contra vulnerabilidades conocidas. Lograr alcanzar una madurez organizacional en ciberseguridad, promueve una gestión efectiva de incidentes que permite una respuesta rápida y eficiente ante ataques, minimizando su impacto. Asimismo, actúa como pieza clave en la estrategia integral de gobernanza TI y continuidad de negocio, porque facilita la evaluación y mejora estos aspectos, sino que ayuda a articularse y cumplir con normativas y regulaciones, que posicionan a las PYMES como organizaciones confiables, fortaleciendo su competitividad en el mercado.

Gestión de Riesgos

El Informe Global sobre Amenazas 2024 de CrowdStrike revela un entorno cibernético cada vez más complicado y en constante evolución, donde PYMES se han convertido en blancos frecuentes de ciberataques. La creciente habilidad de los cibercriminales, junto con un aumento notable en la frecuencia y gravedad de estos ataques, resalta la necesidad de que las organizaciones establezcan un sistema sólido de gestión de riesgos informáticos. Esta gestión es necesaria a causa de la creciente vulnerabilidad de las infraestructuras tecnológicas y de comunicación a diversas amenazas digitales, como ransomware y robo de datos, que a menudo se ven agravadas por recursos de seguridad limitados. Un ciberataque exitoso puede resultar devastador, causando pérdida de datos, interrupción de operaciones y daños a la reputación. Además, muchas Pymes deben cumplir con regulaciones que exigen la protección de datos, y el incumplimiento puede acarrear sanciones significativas. Implementar una gestión de riesgos informáticos no solo ayuda a mitigar estos riesgos, sino que también otorga una ventaja competitiva al demostrar un compromiso con la seguridad de la información. La gestión de riesgos informáticos contribuye a la gobernanza de TI al alinear las medidas de seguridad con los objetivos estratégicos de la organización, facilitar decisiones informadas sobre inversiones en seguridad y promover un proceso de mejora continua. Al identificar y evaluar riesgos, las empresas pueden adaptar sus estrategias de seguridad y cumplir con normativas aplicables. En conclusión, el informe de CrowdStrike enfatiza la necesidad de que las Pymes adopten una estrategia proactiva en la gestión de riesgos informáticos, lo que les permitirá proteger sus activos digitales, asegurar la continuidad del negocio y mejorar su reputación en un entorno cibernético desafiante.

La administración de riesgos informáticos, la gobernanza de TI y la ciberseguridad son elementos esenciales para las PYMES en un entorno digital cada vez más amenazante, como se destaca en el Global Threat Report 2024 de CrowdStrike. Este informe revela un alarmante aumento del 60% en las campañas de intrusión interactiva, donde los cibercriminales utilizan técnicas manuales para infiltrarse en los sistemas, lo que complica la detección de ataques. Dado que las Pymes son cada vez más blanco de estos ataques sofisticados, es determinante que implementen una gestión de riesgos informáticos efectiva para proteger sus activos y garantizar la continuidad del negocio. Cabe mencionar que el sector tecnológico fue el sector en el que el Chief Analytics Officer (CAO) de CrowdStrike observó actividad de intrusión interactiva con mayor frecuencia en 2023, una tendencia que se mantiene desde 2022.

El control efectivo de riesgos cibernéticos permite a las PYMES identificar, evaluar y priorizar amenazas, lo que les ayuda a gestionar acciones oportunas sobre la asignación de recursos y la inversión en medidas de seguridad. Esto no solo mitiga el impacto de posibles ataques, sino que también asegura el cumplimiento de regulaciones que exigen la protección de datos. Además, una sólida gobernanza de TI alinea las estrategias de seguridad con los objetivos empresariales,

promoviendo una cultura de ciberseguridad que involucra a todos los Stakeholders de la organización. La ciberseguridad, como un elemento fundamental en la gestión de riesgos, se convierte en un factor estratégico clave para la competitividad empresarial. Las organizaciones que demuestran un sólido compromiso con la protección de la información no solo pueden ganar la confianza de sus clientes, sino también mejorar su reputación en el mercado. Normas y marcos como COBIT, ISO 38500 e ISO 27001 ofrecen estructuras, directrices y prácticas que se adaptan a las necesidades particulares de cada empresa. Su diseño flexible integra principios y enfoques actualizados, permitiendo a las organizaciones establecer un sistema de gobernanza alineado con su contexto específico. Al adoptar estos marcos, las empresas pueden identificar y priorizar sus objetivos de TI, asegurando que estén en consonancia con sus metas comerciales generales. Es crucial que las organizaciones evalúen su situación actual en relación con estas características y tomen las medidas necesarias para cerrar la brecha entre su estado actual y el ideal. Las acciones para implementar pueden variar en naturaleza e incluir tecnologías, soluciones y servicios proporcionados por los proveedores de seguridad. Estas opciones permiten una implementación rápida sin requerir una inversión inicial significativa, y su costo se recupera rápidamente al reducir considerablemente los gastos operativos asociados a incidentes y violaciones de datos.

En este contexto, el ciclo de vida de la gestión de riesgos en ciberseguridad incluye las etapas de identificación, evaluación, tratamiento y monitoreo constante de los riesgos cibernéticos. Este enfoque es fundamental para mitigar los posibles impactos en las operaciones de las pequeñas y medianas empresas del sector minero, tal como señalan Stoneburner, G., Goguen, A., y Feringa, A. (2017). Al incorporar estos aspectos en el marco teórico, se crea una base sólida para entender la ciberseguridad y la gestión de TI específicamente en el ámbito de las PYMES mineras. Esto facilita el desarrollo de estrategias efectivas que refuercen la protección de los activos digitales y aseguren la continuidad operativa en un entorno cada vez más digitalizado y lleno de amenazas. En el caso colombiano, el notable aumento de ataques cibernéticos ha suscitado una creciente preocupación en el sector empresarial, particularmente en este sector en específico. La alta dirección de este tipo de organizaciones necesita implementar estrategias que integren eficazmente el gobierno corporativo con la gobernanza de tecnologías de la información (TI) y la ciberseguridad. Esto implica reconocer la interconexión entre los procesos operativos y el uso de tecnologías, lo cual es esencial para enfrentar los desafíos actuales.

Gobernanza Corporativa y de TI

Si bien la gobernanza de TI y la ciberseguridad son conceptos amplios, su aplicación en las PYMES mineras requiere una adaptación específica. Los estándares como ISO 38500, ISO 27001 y COBIT ofrecen un marco sólido, pero deben ajustarse a las particularidades de estas organizaciones, considerando sus recursos limitados, necesidades únicas y el entorno operativo del sector minero. Es fundamental adoptar un enfoque de ciber-resiliencia que priorice la protección de los activos más valiosos, la identificación de amenazas, la preparación ante incidentes y la mejora continua. Al integrar estos elementos en un marco de gobernanza de TI personalizado, las PYMES mineras pueden fortalecer su seguridad, garantizar la continuidad de sus operaciones y afrontar los desafíos del entorno digital con mayor confianza.

La gobernanza de TI, fundamentada en estándares internacionales como ISO 38500, ISO 27001 y COBIT, es un imperativo estratégico para las PYMES mineras en la era digital. Al alinear la tecnología con los objetivos del negocio y establecer un marco de control robusto, estas empresas pueden optimizar sus operaciones, reducir costos y mitigar riesgos significativos. La ciberseguridad, como componente integral de la gobernanza de TI, es esencial para proteger los activos digitales críticos, como datos geológicos, planos de mina y sistemas de control industrial. Un incidente cibernético puede tener consecuencias devastadoras para una PYME minera, incluyendo pérdidas financieras, interrupciones operativas y daños a la reputación. Implementar

un programa de ciberseguridad integral, que incluya la gestión de riesgos, la capacitación del personal y la respuesta a incidentes es una inversión necesaria para garantizar la continuidad del negocio y la sostenibilidad a largo plazo. Al adoptar una postura proactiva en materia de ciberseguridad, las PYMES mineras no solo protegen sus activos, sino que también fortalecen su competitividad y atraen a inversores y clientes que valoran la seguridad de la información.

3. MATERIALES Y MÉTODOS

El presente estudio se sustenta en una exhaustiva revisión de la literatura relacionada, enfocándose en el estado actual de la gestión de Tecnologías de la Información (TI) y la ciberseguridad en las PYMES de América Latina, con un énfasis especial en la identificación de desafíos y brechas en la gobernanza de TI y la ciberseguridad en este contexto.

La metodología de la investigación adopta un enfoque cuantitativo que facilita la medición y análisis de los datos recolectados. La recolección de información se llevará a cabo mediante una variedad de instrumentos, complementados con el análisis documental.

El estudio se centrará en las PYMES del sector minero y su gobernanza TI, considerando sus infraestructuras tecnológicas, los recursos disponibles y las políticas definidas para la administración de servicios y operaciones. Se analizarán específicamente las infraestructuras TI, la gobernanza de TI, la ciberseguridad y la continuidad del negocio dentro de estas empresas, dado que el entorno altamente competitivo y la relevancia económica del sector minero requieren sistemas tecnológicos robustos y bien gestionados.

Las PYMES mineras enfrentan importantes desafíos en cuanto a la seguridad de la información y la resiliencia operativa, especialmente en un contexto en el que la minería es una pieza clave de la economía regional. La selección de esta población permite explorar cómo estas empresas gestionan sus infraestructuras TI, implementan medidas de ciberseguridad y aseguran la continuidad de sus operaciones ante posibles incidentes. Dado que la mayoría de estas empresas son pequeñas y medianas, enfrentan limitaciones de recursos y capacidades, lo que hace aún más crucial comprender sus prácticas y necesidades en materia de TI para garantizar su sostenibilidad y competitividad en el sector.

El estudio culmina con recomendaciones prácticas y acciones correctivas basadas en principios de gobernanza, orientadas a mejorar la gestión de TI y la ciberseguridad en las PYMES mineras de la región.

4. RESULTADOS Y DISCUSIÓN

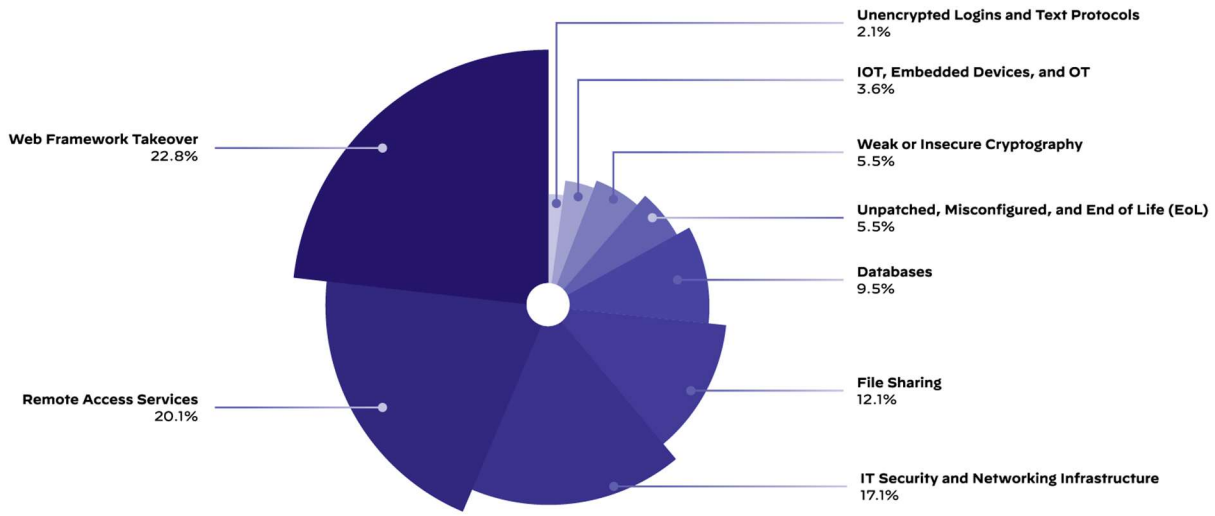
Necesidades y desafíos para adoptar la gestión de TI y la ciberseguridad en Pymes del sector minero.

Las organizaciones adoptan tecnologías de información y comunicación para agilizar y optimizar sus procesos productivos, comerciales, cadenas de suministro y servicios. Sin embargo, la ciberseguridad a menudo se implementa de manera inadecuada, lo que incrementa significativamente la vulnerabilidad a ataques cibernéticos e incidentes que comprometen activos críticos, servicios e infraestructuras TI. Esta situación es particularmente crítica en las Pymes, que suelen destinar menos recursos a la ciberseguridad, exponiéndolas a mayores riesgos.

La dependencia creciente de sistemas digitales en los procesos operacionales esenciales para la continuidad del negocio subraya la necesidad de alinear las estrategias de gobernanza TI con los recursos disponibles para mitigar los riesgos y amenazas. Sin embargo, la falta de un inventario completo y actualizado de los activos, tanto locales como en la nube, compromete la aplicación efectiva de políticas de gobernanza, generando una brecha que no es adecuadamente

valorada por la alta gerencia. Esta desconexión entre las estrategias de ciberseguridad y las operaciones corporativas es un talón de Aquiles que los atacantes cibernéticos explotan activamente.

Figura 2
Distribución de las categorías de exposición a la superficie de ataque



Nota: Informe de amenazas a la superficie de ataque 2023 . Distribución de las categorías de exposición observadas en las 250 organizaciones en los últimos 12 meses. Por Palo Alto Networks, 2023.

Según el Attack Surface Threat Report de Palo Alto Networks (2023), y como se puede observar en la figura 2 los ciberatacantes buscan y atacan activamente sitios web que ejecutan software vulnerable, como versiones inseguras de servidores web Apache, PHP, y jQuery, así como servicios de acceso remoto como RDP (Remote Desktop Protocol), SSH (Secure Shell), y VNC (Virtual Network Computing) son protocolos utilizados para acceder y administrar sistemas de manera remota. RDP permite controlar una computadora remota con una interfaz gráfica, comúnmente usado en entornos Windows. SSH, principalmente en sistemas Unix/Linux, proporciona acceso seguro mediante línea de comandos, mientras que VNC permite compartir y controlar la pantalla de otra computadora de manera multiplataforma. Aunque son herramientas esenciales para la administración remota, si no se configuran o protegen adecuadamente, pueden ser explotadas por atacantes para obtener acceso no autorizado a sistemas críticos.

Estos ataques de ransomware, que representan el 20 % de las exposiciones observadas, pueden resultar en pérdidas financieras significativas, daño reputacional y otras graves consecuencias para las Pymes. Además, servicios comprometidos como RDP han demostrado ser vectores clave en la interrupción de negocios a través del ransomware. El informe también destaca que el 17% de las exposiciones observadas se relacionan con la infraestructura de TI y redes, incluyendo protocolos de capa de aplicación y páginas de inicio de sesión administrativas expuestas a través de Internet. Estas vulnerabilidades, que afectan dispositivos como enrutadores, cortafuegos y VPN, pueden comprometer funciones comerciales críticas y datos sensibles.

Otras exposiciones incluyen el intercambio de archivos inseguro, que representa el 12 % de las vulnerabilidades, y las bases de datos con información confidencial expuestas directamente a Internet, que representan el 9 % de las amenazas. La vulneración de estos sistemas no solo permite el acceso a los datos actuales, sino también a todos los futuros datos transmitidos a través de ellos, aumentando considerablemente el riesgo de filtraciones.
Adicionalmente, se observan riesgos significativos en sistemas sin parches, mal configurados o al final de su vida útil, criptografía débil, dispositivos IoT, tecnologías operativas (OT), y aplicaciones comerciales críticas. Estas vulnerabilidades, si no son abordadas de manera proactiva, pueden tener consecuencias devastadoras para la seguridad y continuidad operativa de las Pymes, subrayando la urgencia de una gobernanza TI robusta y una gestión de riesgos alineada con las realidades actuales del ciberespacio.

Estado de la gobernanza de TI y ciberseguridad.
Según Incident Response Report 2022de Palo Alto Networks (2022), las Pymes, al igual que otras organizaciones, están cada vez más expuestas a riesgos significativos debido a la proliferación de ataques cibernéticos como el ransomware y el compromiso de correo electrónico empresarial (BEC). Estos tipos de ataques representaron aproximadamente el 70 % de los incidentes cibernéticos, afectando gravemente la continuidad del negocio. El ransomware, un tipo de malware que cifra archivos esenciales obliga a las organizaciones a pagar un rescate a cambio de la promesa de restaurar el acceso y no divulgar datos sensibles. Por otro lado, el BEC se basa en estafas sofisticadas que comprometen cuentas de correo electrónico legítimas para desviar fondos empresariales. Además, los ciberdelincuentes están combinando extorsión con cifrado y, en algunos casos, recurren a la extorsión pura, amenazando con liberar datos si no se paga. Estas tácticas no solo representan una amenaza financiera, sino que también pueden causar un daño reputacional significativo.

Para mitigar estas amenazas, es importante que las Pymes implementen una gobernanza TI robusta, alineada con el gobierno corporativo. Esto incluye establecer políticas claras, mantener una supervisión constante y asegurarse de que las medidas de seguridad estén en consonancia con los riesgos actuales. La falta de un enfoque integral en la gobernanza expone a las organizaciones a brechas en la seguridad de la información, amplía la superficie de ataque y deja las infraestructuras TI vulnerables. Por lo tanto, es esencial que la alta dirección comprenda el valor estratégico de invertir en ciberseguridad y en la implementación de controles adecuados, garantizando así la protección de la información crítica y la continuidad del negocio.

Los medios sospechosos de acceso inicial a los sistemas e infraestructuras de las Pymes reflejan las tácticas, técnicas y procedimientos más comunes utilizados por los atacantes para infiltrarse y sacar provecho. Los tres principales vectores de ataque identificados son el phishing, la explotación de vulnerabilidades de software conocidas y los ataques de fuerza bruta dirigidos a obtener credenciales, particularmente a través del Protocolo de Escritorio Remoto (RDP). Según Incident Response Report 2022 de Palo Alto Networks (2022), Estos métodos representaron más del 77% de las causas raíz sospechosas de intrusiones. Adicionalmente, el uso de credenciales previamente comprometidas se destaca como otro medio comúnmente empleado por los atacantes para obtener acceso inicial.

Las organizaciones suelen descubrir que han sido comprometidas a través de alertas de seguridad o al encontrar software instalado de manera sospechosa en sus sistemas, lo que sugiere actividad anómala en la red. En algunos casos, los atacantes revelan su presencia con una nota de rescate o mediante métodos inusuales. El gobierno TI juega un rol crucial en mitigar estos riesgos, estableciendo políticas de seguridad efectivas, promoviendo la actualización constante de software para evitar la explotación de vulnerabilidades conocidas, y asegurando

que las prácticas de autenticación sean robustas para prevenir ataques de fuerza bruta. Además, la implementación de mecanismos de detección temprana y respuesta rápida es vital para identificar y neutralizar amenazas antes de que causen un daño significativo. La alineación entre la gobernanza TI y las estrategias corporativas es esencial para garantizar que las Pymes no solo reaccionen ante incidentes, sino que también fortalezcan proactivamente su postura de seguridad frente a estas amenazas comunes.

La gestión de TI y la ciberseguridad en Pymes del sector minero es fundamental para entender las necesidades y desafíos específicos de estas organizaciones es necesaria la revisión bibliográfica que abarca los últimos años y se centra en la gestión de TI y la ciberseguridad en PYMES, especialmente en el contexto de la estrategia organizacional y operacional. Marco de Gobernanza La gobernanza es un tema clave en la gestión de TI y la ciberseguridad. Los estándares ISO 38500, ISO 27001 y COBIT son fundamentales para establecer un marco de gobernanza efectivo.

Estos estándares proporcionan directrices para la gestión y gobierno de TI, evaluación y monitoreo en el control de negocios y seguridad IT, gestión de servicios TI, requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI), así como buenas prácticas y controles de ciberseguridad. Gestión de TI y Ciberseguridad en PYMES Las PYMES del sector minero enfrentan desafíos específicos en la gestión de TI y la ciberseguridad. La falta de recursos, ausencia de una gestión TI, planes de gestión de riesgos informáticos y carencia de personal cualificado en seguridad informática son algunos de los obstáculos que enfrentan estas organizaciones. Es importante implementar un marco de gobernanza que aborde estos desafíos y brinde soluciones efectivas. Estrategia Organizacional y Operacional.

La estrategia organizacional y operacional de las PYMES del sector minero debe ser integral y considerar la gestión de TI y la ciberseguridad como parte fundamental de su planificación y ejecución. Un marco de gobernanza efectivo puede ayudar a las PYMES a mejorar su capacidad para responder a los desafíos de la ciberseguridad y a fortalecer su estrategia organizacional y operacional.

En resumen, el estado del arte sobre la gestión de TI y la ciberseguridad en PYMES del sector minero es fundamental para entender las necesidades y desafíos específicos de estas organizaciones. Un marco de gobernanza efectivo, basado en estándares como ISO 38500, ISO 27001 y COBIT, puede ayudar a las PYMES a mejorar su capacidad para responder a los desafíos de la ciberseguridad y a fortalecer su estrategia organizacional y operacional.

Gestión de TI y Ciberseguridad en PYMES colombianas

Estado Actual de la Gestión de TI y Ciberseguridad en PYMES colombianas teniendo en cuenta diferentes trabajos de investigación como la realizada por Giraldo, B., & Rocha, Á. (2018) analizan las prácticas y desafíos en la implementación de sistemas de gestión de seguridad de la información en PYMES colombianas, proporcionando una visión general de las deficiencias y necesidades en este ámbito. Asimismo, se deduce las brechas en la Gobernanza de TI y Ciberseguridad en PYMES del Sector Minero de acuerdo con el estudio efectuado por Molina, J., & Sánchez, A. (2020) el cual identifica desafíos específicos relacionados con la protección de datos, la gestión de riesgos y la falta de recursos especializados.

Varios estudios sobre el Diseño de Marcos de Gobernanza Adaptados a PYMES del Sector Minero han propuesto marcos de gobernanza adaptados a las necesidades de las PYMES en diferentes sectores. Por ejemplo, el trabajo de Arbeláez, M., & Gómez, C. (2019) desarrolló un

marco de gobernanza de TI para PYMES colombianas, ofreciendo recomendaciones específicas para la implementación efectiva en entornos empresariales de menor escala.

Tomando cada uno de los referentes se puede establecer que la gobernanza de TI no solo implica la creación de normas, protocolos y pautas, sino que también abarca la integración de estos elementos en la estrategia corporativa, la cultura organizacional y las rutinas diarias. En este sentido, la gobernanza de la ciberseguridad es esencial para garantizar la continuidad del negocio y la gestión eficaz de la cadena de suministro, especialmente en sectores críticos como el minero, donde la estabilidad y seguridad de las operaciones son vitales.

En el caso específico de las Pymes del sector minero, la implementación de una sólida gobernanza de TI es necesaria. Estas empresas, aunque de menor tamaño, manejan infraestructuras y datos críticos que, en caso de ser comprometidos, podrían afectar no solo sus operaciones, sino también la seguridad y estabilidad económica de la región. Además, la interconexión de sus sistemas con otras infraestructuras críticas a nivel nacional requiere un enfoque integral de la ciberseguridad que trascienda la simple estandarización y promueva la cohesión entre todos los elementos del ecosistema cibernético.

Los retos relacionados con la gobernanza de la ciberseguridad en las PYMES incluyen la necesidad de una colaboración estrecha entre los actores de seguridad pública y las empresas, para crear un entorno donde las estrategias de seguridad sean coherentes y efectivas. Esta colaboración es esencial para mejorar la gestión de incidentes, la recopilación de datos y la automatización de procesos basadas en las nuevas tecnologías, lo que puede resultar en ahorros significativos y escalabilidad para las PYMES. En otras palabras, la implementación de una gobernanza de TI efectiva no solo refuerza la seguridad cibernética, sino que también permite participar de manera más activa en las políticas públicas que pueden aportar al entorno empresarial.

Validación de Marcos de Gobernanza

El panorama de los riesgos cibernéticos es cada vez más crítico a nivel global, afectando a empresas de todos los tamaños, gobiernos y organizaciones de diversos sectores. Las amenazas como el robo de datos, la extorsión y las interrupciones operativas están en aumento, lo que genera repercusiones financieras, legales y de reputación. En respuesta, ha habido una creciente regulación en áreas como la privacidad y la infraestructura crítica. El Informe de Riesgo Global 2024 del Foro Económico Mundial sitúa la "inseguridad cibernética" entre los cinco principales riesgos, con el costo de los delitos cibernéticos proyectado a alcanzar 23 billones de dólares en 2027. La adopción de nuevas tecnologías ha ampliado la superficie de ataque de las organizaciones, lo que hace imprescindible que los líderes comprendan y gestionen estos riesgos de manera efectiva. Es fundamental que la alta dirección de las pequeñas y medianas empresas (Pymes) colombianas, especialmente en el sector minero, adopte prácticas de gobernanza de TI adecuadas que se alineen con su contexto empresarial y el nivel de infraestructura tecnológica disponible.

La implementación de estándares como ISO 38500, ISO 27001 y COBIT es requerida para establecer un marco robusto que permita a estas organizaciones tomar decisiones estratégicas informadas y supervisar efectivamente sus marcos de ciberseguridad. Estas normas ofrecen directrices claras sobre la responsabilidad, la evaluación y el monitoreo de las prácticas de TI, lo que ayuda a gestionar los riesgos cibernéticos de manera integral. En un contexto latinoamericano, donde las Pymes enfrentan desafíos específicos como la falta de recursos y capacitación, es esencial que se incorporen políticas efectivas de control de acceso a la red (NAC) y se fomente la apropiación de soluciones de software libre. Esto no solo mejorará la

seguridad informática al identificar vulnerabilidades y amenazas, sino que también protegerá la privacidad de los datos sensibles. Además, es necesario abordar las limitaciones actuales en las técnicas de correlación basadas en reglas dentro de los sistemas de Gestión de Información y Eventos de Seguridad (SIEM), que afectan la capacidad de detección y respuesta ante incidentes. Al adoptar un enfoque proactivo y alineado con estos estándares internacionales, las Pymes del sector minero pueden fortalecer su resiliencia cibernética y asegurar un manejo más efectivo de sus activos tecnológicos.

En este sentido se puede nombrar la validación de marcos de gobernanza a través de estudios de caso es una práctica común. Investigaciones como la de García, R., & Durán, M. (2021) utilizaron estudios de caso en PYMES colombianas para validar la efectividad de marcos de gobernanza de TI y ciberseguridad, proporcionando insights prácticos para su implementación. Esto se asocia de igual manera con las Buenas Prácticas y Mecanismos para Mejorar la Gestión de TI y Ciberseguridad que se evidencian en el trabajo de Pérez, J., & Ríos, L. (2020) donde proporciona recomendaciones específicas para fortalecer la ciberseguridad en PYMES colombianas, incluyendo la capacitación del personal, la implementación de controles de acceso y la adopción de tecnologías de seguridad avanzadas. (Latorre Gómez et al., 2024) de la Universidad EAN en el Diseño de un Modelo de Gobierno para la Gestión de TI en la Corporación se centra en crear un marco adaptado a las necesidades específicas de la organización para optimizar la gestión de tecnologías de la información. En este se realiza una revisión de mejores prácticas y un análisis del estado actual de TI en una organización específica, en donde se llevó a cabo un análisis interno y externo mediante herramientas como el análisis PESTEL y un diagnóstico organizacional, lo que facilitó la comprensión del contexto en el que opera la organización. Además, se aplicaron técnicas de recolección de datos, como encuestas y entrevistas, para obtener información relevante sobre la situación actual de TI en la corporación. Estas metodologías integradas permitieron diseñar un modelo de gobernanza adaptado a las necesidades específicas de la organización, alineando sus objetivos estratégicos con las mejores prácticas del sector. identificando desafíos como la falta de estructura en los procesos y la dependencia del conocimiento del personal. En donde se elige el marco de trabajo COBIT 2019 como base para el diseño, proponiendo un plan de implementación que incluye un cronograma de actividades para mejorar la eficiencia en la gestión de recursos y garantizar la seguridad de datos. Las expectativas incluyen una mejor alineación estratégica entre TI y los objetivos del negocio, así como un enfoque en la mejora continua y gestión proactiva del riesgo, contribuyendo a la competitividad y sostenibilidad de la Corporación.

Interpretación de los Resultados y Comparación con Estudios Previos

Se ha registrado un aumento alarmante en la sofisticación y complejidad de los ciberataques, destacando amenazas emergentes como el ransomware y ataques dirigidos. Este fenómeno se alinea con estudios previos que indican un uso creciente de inteligencia artificial para desarrollar ataques más elaborados. Informes como el de Kaspersky, que sitúan a Colombia entre los países más atacados en Latinoamérica, indicando la urgencia de abordar las vulnerabilidades en la gestión de riesgos informáticos de las PYMES mineras. Es esencial que estas empresas implementen medidas efectivas para fortalecer su ciberseguridad y proteger sus activos críticos ante un panorama de amenazas en constante evolución.

Al revisar el panorama actual de los Modelos de Gobernanza en las Pymes del sector minero, se evidencia la necesidad de implementar, fortalecer o actualizar los existentes para enfrentar las crecientes amenazas cibernéticas. Esto resulta crucial para este tipo de empresas, que con frecuencia operan con recursos limitados y estructuras organizativas simplificadas. La implementación de un modelo de gobernanza enfocado en la ciberseguridad permitirá a estas

organizaciones gestionar de manera más efectiva sus activos tecnológicos, alineándolos con sus objetivos estratégicos.

Es fundamental fortalecer la toma de decisiones por parte de la alta gerencia, involucrando a los líderes de TI y ciberseguridad, quienes desempeñan un papel clave en el nivel ejecutivo. En el caso de las PYMES, esto puede implicar la creación de roles específicos o comités que integren la ciberseguridad en la planificación estratégica, garantizando que las inversiones tecnológicas estén alineadas con la protección de los activos críticos.

Es esencial establecer un monitoreo constante para identificar vulnerabilidades antes de que sean explotadas. Esto implica que, dentro de la gobernanza de TI en las Pymes Colombianas del sector minero, se deben integrar medidas, mecanismos y procesos adecuados, así como implementar herramientas accesibles y apropiadas para su tamaño. De esta manera, las empresas podrán mantenerse informadas sobre el estado de su infraestructura tecnológica y responder de manera efectiva a posibles amenazas cibernéticas.

5. CONCLUSIONES

Se observa la falta de recursos y concientización, las Pymes mineras colombianas, en general, destinan menos recursos a la ciberseguridad en comparación con empresas más grandes, lo que incrementa su exposición a riesgos. Esto se debe a la percepción de que la inversión en ciberseguridad no es prioritaria o estratégica, especialmente en aquellas que no cuentan con una infraestructura robusta de TI.

Se establece el aumento de la superficie de ataque, la dependencia creciente de las tecnologías digitales en procesos críticos, como la automatización de operaciones, gestión de inventarios y sistemas remotos, ha aumentado significativamente la superficie de ataque. Los atacantes explotan vulnerabilidades en software obsoleto y configuraciones débiles, afectando la continuidad operativa de las Pymes.

Es evidente la Gobernanza de TI deficiente, la ausencia de un marco sólido de gobernanza de TI, como la implementación adecuada de estándares (ISO 27001, ISO 38500, COBIT), compromete la aplicación efectiva de políticas de ciberseguridad. Esta desconexión entre las operaciones diarias y la gestión de seguridad permite brechas que los atacantes explotan.

Se identifica la explotación de vulnerabilidades comunes, los Protocolos como RDP y SSH, si no son configurados de manera segura, son objetivos frecuentes de ataques de fuerza bruta, lo que aumenta la probabilidad de incidentes como ransomware o compromisos de acceso remoto, afectando la infraestructura crítica y la continuidad de negocio.

Se reafirma la necesidad de estrategias proactivas, debido a que se observa la urgencia de que las Pymes implementen medidas de detección y respuesta ante incidentes, alineando las políticas de ciberseguridad con la estrategia corporativa. Es fundamental que la alta gerencia entienda la importancia de la ciberseguridad y destine los recursos necesarios para mitigar riesgos.

Un gobierno de TI colaborativo es esencial para construir una ciberseguridad adaptable y en constante evolución. Al combinar tecnologías de vanguardia con procesos de evaluación de riesgos dinámicos, las organizaciones pueden anticiparse a las amenazas emergentes y responder de manera efectiva a los incidentes. Además, al fomentar una cultura de mejora

continua, se garantiza que las medidas de seguridad se ajusten a las necesidades cambiantes del entorno empresarial

Es esencial que un gobierno de TI sólido promueve la colaboración efectiva entre los equipos de tecnología, las áreas de negocio y los empleados. Esta interacción facilita la detección temprana de amenazas, permite una respuesta ágil ante incidentes y propicia una mejora continua en las medidas de seguridad. Todo esto no solo asegura la continuidad del negocio, sino que también refuerza la confianza de clientes y socios comerciales, estableciendo así una base robusta para el crecimiento sostenible y la resiliencia organizacional.

En conclusión, la metodología que se desarrolló fue a través de un análisis crítico y reflexivo de los hallazgos, evaluando estudios previos, casos de éxito y la revisión de la literatura en el contexto del sector minero, la gobernanza de TI y el panorama de la ciberseguridad. Este análisis profundiza en los factores críticos asociados y su influencia en la gestión efectiva de riesgos e incidentes informáticos.

REFERENCIAS

Agbodoh-Falschau, K. R., & Ravaonorohanta, B. H. (2023). Investigating the influence of governance determinants on reporting cybersecurity incidents to police: Evidence from Canadian organizations' perspectives. Technology in Society, 74, 102309. https://doi.org/10.1016/j.techsoc.2023.102309

Anagnostakis, D. (2022). The External Face of the EU's Cybersecurity Policies: Promoting Good Cybersecurity Governance Abroad? En D. Soyaltin-Colella (Ed.), EU Good Governance Promotion in the Age of Democratic Decline (pp. 237-257). Springer International Publishing. https://doi.org/10.1007/978-3-031-05781-6_11

Andersen, T., Aryee, J., Acheampong, G., & Hansen, A. S. (2023). The continuous search for new port governance models: Experiences from a developing country. Journal of Shipping and Trade, 8(1), 10. https://doi.org/10.1186/s41072-023-00139-8

Anu, V. (2022). Information security governance metrics: a survey and taxonomy. Information Security Journal: A Global Perspective, 31(4), 466–478. https://doi-org.bibliotecavirtual.unad.edu.co/10.1080/19393555.2021.1922786

Anvar kyzy, S., Dunn, G. J., & Sweeney, J. A. (2022). Chain and silk: Alternative futures of blockchain governance in Kyrgyzstan. European Journal of Futures Research, 10(1), 5. https://doi.org/10.1186/s40309-022-00192-9

Anvar kyzy, S., Dunn, G. J., & Sweeney, J. A. (2022). Chain and silk: Alternative futures of blockchain governance in Kyrgyzstan. European Journal of Futures Research, 10(1), 5. https://doi.org/10.1186/s40309-022-00192-9

Azinheira, B., Antunes, M., Maximiano, M., & Gomes, R. (2023). A methodology for mapping cybersecurity standards into governance guidelines for SME in Portugal. CENTERIS – International Conference on ENTERprise Information Systems / ProjMAN – International Conference on Project MANagement / HCist – International Conference on Health and Social Care Information Systems and Technologies 2022, 219, 121-128. https://doi.org/10.1016/j.procs.2023.01.272

Azinheira, B., Antunes, M., Maximiano, M., & Gomes, R. (2023). A methodology for mapping cybersecurity standards into governance guidelines for SME in Portugal. CENTERIS – International Conference on ENTERprise Information Systems / ProjMAN – International Conference on Project MANagement / HCist – International Conference on Health and Social Care Information Systems and Technologies 2022, 219, 121-128. https://doi.org/10.1016/j.procs.2023.01.272

Cabrera, X. E. O., & Galarza, M. D. Á. (2022). Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019. Polo del Conocimiento: Revista científico-profesional, 7(3), 16.https://dialnet.unirioja.es/servlet/articulo?codigo=8399852

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Computer Science Review, 50, 100592. https://doi.org/10.1016/j.cosrev.2023.100592

D. A. Saputra, I. Alif, R. A. Wijaya, Y. G. Sucahyo and M. K. Hammi, "Role of IT in IT Governance Practices Maturity Perspective," 2019 International Conference on Advanced Computer Science and information Systems (ICACSIS), Bali, Indonesia, 2019, pp. 325-330, doi: 10.1109/ICACSIS47736.2019.8979844.

Del-Real, C., & van Steen, T. (2023). Researching Cybersecurity Governance: Insights from Fieldwork with Cybersecurity Experts and End-Users. En A. M. Díaz Fernández, C. Del-Real, & L. Molnar (Eds.), Fieldwork Experiences in Criminology and Security Studies: Methods, Ethics, and Emotions (pp. 485-509). Springer International Publishing. https://doi.org/10.1007/978-3-031-41574-6_26

Donta, P. K., Sedlak, B., Casamayor Pujol, V., & Dustdar, S. (2023). Governance and sustainability of distributed continuum systems: A big data approach. Journal of Big Data, 10(1), 53. https://doi.org/10.1186/s40537-023-00737-0

Donta, P. K., Sedlak, B., Casamayor Pujol, V., & Dustdar, S. (2023). Governance and sustainability of distributed continuum systems: A big data approach. Journal of Big Data, 10(1), 53. https://doi.org/10.1186/s40537-023-00737-0

Famularo, J. (2023). Corporate social responsibility communication in the ICT sector: Digital issues, greenwashing, and materiality. International Journal of Corporate Social Responsibility, 8(1), 8. https://doi.org/10.1186/s40991-023-00082-8

Famularo, J. (2023). Corporate social responsibility communication in the ICT sector: Digital issues, greenwashing, and materiality. International Journal of Corporate Social Responsibility, 8(1), 8. https://doi.org/10.1186/s40991-023-00082-8

Fontão, A., Ábia, B., Wiese, I., Estácio, B., Quinta, M., Santos, R. P. dos, & Dias-Neto, A. C. (2018). Supporting governance of mobile application developers from mining and analyzing technical questions in stack overflow. Journal of Software Engineering Research and Development, 6(1), 8. https://doi.org/10.1186/s40411-018-0052-6

Genov, N. (2015). The future of individualization in Europe: Changing configurations in employment and governance. European Journal of Futures Research, 2(1), 46. https://doi.org/10.1007/s40309-014-0046-5

Gudowsky, N., & Peissl, W. (2016). Human centred science and technology—Transdisciplinary foresight and co-creation as tools for active needs-based innovation governance. European Journal of Futures Research, 4(1), 8. https://doi.org/10.1007/s40309-016-0090-4

Hao, Y., Qiu, Z., Xu, Q., He, Q., Fang, X., & Wang, C. (2023). Innovation strategy design of public sports service governance based on cloud computing. Journal of Cloud Computing, 12(1), 69. https://doi.org/10.1186/s13677-023-00448-0

Heo, K., & Seo, Y. (2021). Anticipatory governance for newcomers: Lessons learned from the UK, the Netherlands, Finland, and Korea. European Journal of Futures Research, 9(1), 9. https://doi.org/10.1186/s40309-021-00179-y

Heo, K., & Seo, Y. (2021). Anticipatory governance for newcomers: Lessons learned from the UK, the Netherlands, Finland, and Korea. European Journal of Futures Research, 9(1), 9. https://doi.org/10.1186/s40309-021-00179-y

Hinrichs, M. M., & Johnston, E. W. (2020). The creation of inclusive governance infrastructures through participatory agenda-setting. European Journal of Futures Research, 8(1), 10. https://doi.org/10.1186/s40309-020-00169-6

Hinrichs, M. M., & Johnston, E. W. (2020). The creation of inclusive governance infrastructures through participatory agenda-setting. European Journal of Futures Research, 8(1), 10. https://doi.org/10.1186/s40309-020-00169-6

Liu, C.-W., Huang, P., & Lucas, H. C. (2020). Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. Journal of Management Information Systems, 37(3), 758–787. https://doi-org.bibliotecavirtual.unad.edu.co/10.1080/07421222.2020.1790190

Lu, P., Zhou, L., & Fan, X. (2023). Platform governance and sociological participation. The Journal of Chinese Sociology, 10(1), 3. https://doi.org/10.1186/s40711-023-00181-w

Ma, L., Chen, D., & Gao, L. (2008). Overseas listing, voluntary corporate governance and performance. Frontiers of Business Research in China, 2(3), 440-457. https://doi.org/10.1007/s11782-008-0026-3

Mueller, R., & Roger Yin. (2023). Sentry insurance and california consumer privacy act: a business case on IT governance, data security, and compliance. Issues in Information Systems, 24(3), 174–180. https://doi-org.bibliotecavirtual.unad.edu.co/10.48009/3_iis_2023_115

Naguib, H. M., Kassem, H. M., & Naem, A. E.-H. M. A. (2024). The impact of IT governance and data governance on financial and non-financial performance. Future Business Journal, 10(1), 15. https://doi.org/10.1186/s43093-024-00300-0

Naguib, H. M., Kassem, H. M., & Naem, A. E.-H. M. A. (2024). The impact of IT governance and data governance on financial and non-financial performance. Future Business Journal, 10(1), 15. https://doi.org/10.1186/s43093-024-00300-0

Nuñez, M., Palmer, X.-L., Potter, L., Aliac, C. J., & Velasco, L. C. (2023). ICT Security Tools and Techniques among Higher Education Institutions: A Critical Review. International Journal of Emerging Technologies in Learning, 18(15), 4–22. https://doi-org.bibliotecavirtual.unad.edu.co/10.3991/ijet.v18i15.40673

Nyasha, G., Nwosu, L. I., Bereng, M. C., Mahlaule, C., & Segotso, T. (2024). A Systematic Literature Review on the Impact of Cybersecurity Threats on Corporate Governance During the Covid-19 Era. En T. Moloi & B. George (Eds.), Towards Digitally Transforming Accounting and Business Processes (pp. 157-174). Springer Nature Switzerland.

Orellana-Cabrera, X. E., & Álvarez-Galarza, M. D. (2022). Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019. Polo del Conocimiento, 7(3), 706-726.https://www.polodelconocimiento.com/ojs/index.php/es/article/view/3758

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2023). Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. International Journal of Information Management Data Insights, 3(2), 100191. https://doi.org/10.1016/j.jjimei.2023.100191

Savaş, S., & Karataş, S. (2022a). Cyber governance studies in ensuring cybersecurity: An

Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. International Journal of Accounting Information Systems, 51, 100642. https://doi.org/10.1016/j.accinf.2023.100642

Y. Durachman, Y. Chairunnisa, D. Soetarno, A. Setiawan and F. Mintarsih, "IT security governance evaluation with use of COBIT 5 framework: A case study on UIN Syarif Hidayatullah library information system," 2017 5th International Conference on Cyber and IT Service Management (CITSM), Denpasar, Indonesia, 2017, pp. 1-5, doi: 10.1109/CITSM.2017.8089302.

Yulianto, F. L. Gaol, S. H. Supangkat and B. Ranti, "A Comprehensive Model for Enhancing Cybersecurity Resilience and IT Governance Through Red Teaming Exercises," 2023 29th International Conference on Telecommunications (ICT), Toba, Indonesia, 2023, pp. 1-7, doi: 10.1109/ICT60153.2023.10374068.

Simola, J., Takala, A., Lehkonen, R., Frantti, T., & Savola, R. (2024, June). The Importance of Cybersecurity Governance Model in Operational Technology Environments. In European Conference on Cyber Warfare and Security (Vol. 23, No. 1, pp. 506-515).