Training design through Runachay for high school teachers of UE Teresa de Calcuta. Manta-Ecuador.

Análisis de la Cultura Organizacional como Factor Clave en la Gestión de Ciberseguridad en PYMES.

Autores:

Mgs. Barba-Salazar, Joel Alejandro
UNIVERSIDAD DE GUAYAQUIL
Magister en Ciberseguridad
Guayaquil – Ecuador.
joel.barbas@ug.edu.ec
https://orcid.org/0000-0002-0816-7978

Mgs. Bravo-Duarte, Freddy Lenin
UNIVERSIDAD ESTATAL DE MILAGRO
Magister en Gerencia de Tecnologías
Milagro - Ecuador.
fbravod@unemi.edu.ec
https://orcid.org/0000-0002-7472-6934

MBA. Orellana-Intriago, Maria Fernanda
UNIVERSIDAD DE GUAYAQUIL
Maestra en Administración de Negocios -MBA
Guayaquil - Ecuador.
maria.orellanai@ug.edu.ec
https://orcig.org/0000-0002-9993-0878

MBA. Barzola-López, Luis Humberto
INVESTIGADOR INDEPENDIENTE
Maestro en administracion de negocios - MBA
Ecuador.
luisb_18@hotmail.com
https://orcid.org/0000-0003-4849-7469

Fechas de recepción: 21-JUN-2025 aceptación: 21-JUL-2025 publicación: 30-SEP-2025
https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

La ciberseguridad se ha convertido en un elemento estratégico para las organizaciones, las cuales deben ser capaces de enfrentar los desafíos específicos de la innovación y el crecimiento tecnológico, el propósito principal de esta investigación es indagar acerca del apropiado abordaje de las PYMES ante la implementación de sistemas de ciberseguridad. Enmarcado en una metodología de enfoque cualitativo, y siguiendo cuatro (04) fases de investigación: búsqueda, evaluación, análisis y síntesis, se realizó una revisión sistemática de fuentes referenciales, con la finalidad de consolidar una visión clara de los procedimientos a seguir para mejorar el clima organizacional en las PYMES que enfrentan riesgos de ciberseguridad. En este respecto, las pautas básicas a considerar para que las organizaciones apliquen sistemas se ciberseguridad eficientes, radican en el conocimiento de los riesgos y la disposición de enfrentar los cambios de la era digital, la capacidad de respuesta se centra en la adopción de medidas preventivas, conocimiento de las posibles intrusiones a los sistemas y la protección apropiada de los sistemas informáticos ante los ataques y finalmente los procesos de ciberseguridad, pueden mejorarse con la educación de los empleados, formación permanente, simulacros y auditorías de las posibles debilidades presentes en los sistemas de la empresa.

Palabras Clave: protección de datos; ciberdelincuencia; innovación tecnológica

Abstract

Cybersecurity has become a strategic element for organizations, which must be able to face the specific challenges of innovation and technological growth, the main purpose of this research is to investigate the appropriate approach of SMEs to the implementation of cybersecurity systems. Framed in a qualitative approach methodology, and following four (04) research phases: search, evaluation, analysis and synthesis, a systematic review of reference sources was carried out, with the purpose of consolidating a clear vision of the procedures to follow to improve the organizational climate in SMEs that face cybersecurity risks. In this regard, the basic guidelines to consider for organizations to apply efficient cybersecurity systems are based on knowledge of the risks and the willingness to face the changes of the digital age, the response capacity focuses on the adoption of preventive measures, knowledge of possible intrusions to the systems and the appropriate protection of computer systems against attacks and finally cybersecurity processes can be improved with employee education, ongoing training, drills and audits of possible weaknesses present in the company's systems.

Keywords: data protection; cybercrime; technological innovation

.

Introducción

La transformación digital, se ha presentado como un reto pero a la vez como una oportunidad para las empresas, en lo que se refiere al fortalecimiento de la competitividad, optimizar procesos, elevar eficiencia y mejorar la toma de decisiones. Este fenómeno global ha impactado todos los ámbitos de la vida y por ende revolucionado la manera en que las empresas operan, replanteando la necesidad de realizar innovaciones internas en respuesta al entorno externo del mercado en movimiento. Mateus et al. (2024) explica que, a pesar de la evolución y esfuerzos por la adaptación de las pequeñas y medianas empresas, y de la necesidad imperiosa de la transformación digital, se han observado "riesgos de vulneración de información, afectando negativamente a sus clientes" (pág. 15), lo que significa, un nuevo desafío con posibles impactos económicos.

La ciberseguridad se ha convertido en un elemento estratégico, Lagos (2024) señala que, no se trata de innovar y competir, sino de desarrollar las capacidades que generen un entorno digital próspero, dinámico, capaz de abordar desafíos de seguridad que permitan integrar, construir y reconfigurar las competencias cuando sea necesario, no solo internas sino aquellas del entorno que incidan directamente en la postura organizacional en relación a la ciberseguridad.

En este sentido, se presenta una problemática clara en las pequeñas y medianas empresas, y es el nivel de disposición para implementar estos marcos de gestión de seguridad por parte de las PYMES, en este sentido se plantea como propósito principal de esta investigación indagar acerca del apropiado abordaje de las PYMES ante la implementación de sistemas de ciberseguridad, estableciendo en concreto tres interrogantes importantes; 1. ¿Cuáles son las pautas básicas a considerar por la organización al momento de la implementación de sistemas de ciberseguridad, 2. ¿Cuál es la reacción o respuesta de la organización ante situaciones que afectan el apropiado desempeño de los sistemas digitales? Y finalmente 3. ¿De qué manera se pueden mejorar los procesos de ciberseguridad en las PYMES?.

Metodología

La presente investigación, se realiza bajo un enfoque cualitativo, de revisión sistemática de referencias actualizadas del tema de estudio, comparación de casos y otras investigaciones relacionadas con el comportamiento organizacional ante los problemas de ciberseguridad, permitiendo así identificar tendencias y sintetizar la información para consolidar una visión clara de los procedimientos a seguir para mejorar el clima organizacional en las PYMES y mejorar sus prácticas en beneficio de su crecimiento tecnológico, todo esto siguiendo cuatro (04) fases establecidas por Tunqui (2024); búsqueda, evaluación, análisis y síntesis de la información.

Resultado

Cultura organizacional en las PYMES en relación a las nuevas tendencias tecnológicas

Para Alarcon (2024) la micro y pequeña empresa son "una entidad económica formada por una persona física o jurídica, con cualquier tipo de estructura organizacional empresarial permitida por la ley" (pág. 13), las PYMES representan según Villarreal (2024) "una porción significativa del tejido productivo, generadoras de empleo, dinamizando economías locales y aportando crecimiento nacional" (pág. 187), pero para este tipo de empresas muchas veces se presentan problemáticas relacionadas con falta de enfoque en clima y cultura organizacional, y adaptación a nuevas tendencias tecnológicas, por lo que este autor describe algunos factores que influyen en este respecto a continuación en la tabla 1.

Tabla 1

Factores que influyen en la falta de enfoque organizacional en relación a las tendencias tecnológicas.

- Falta de estrategias para la retención de personal, lo que influye en comportamientos como desmotivación, ausencias, renuncias, clima hostil y por ende baja rentabilidad.
- Falta de visión por parte de la empresa de valor o capital humano, centralización de objetivos globales sin importar el clima o insatisfacción laboral, lo que presenta altos índices de rotación, baja productividad, estrés laboral y baja reputación corporativa.
- Liderazgo ineficiente, gestión inadecuada y por ende mal clima laboral.
- Ausencia de áreas definidas para la gestión correcta de aspectos internos y externos.
- Falta de capacidad y muchas veces disposición de adoptar tecnologías digitales y procesos de innovación.
- Falta o pocas habilidades tecnológicas.

Fuente. Villarreal (2024)

Sin embargo, la creciente necesidad de integrar tecnologías de información en los procesos productivos, gestión y comercialización en este tipo de empresas, hace que las PYMES se orienten hacia la innovación, no solo en el uso de equipos y sistemas sino en la transformación de la cultura organizacional completa, es decir, surge una dimensión crítica de mejora permanente donde "la empresa aprende a aprender" Villarreal (2024, pág. 189), y se debe concentrar en un enfoque proactivo de transformación enfocado en talento humano, inversión estratégica y resiliencia frente a los cambios.

En este orden de ideas, Benavides (2024) asegura que “la adopción de tecnologías digitales altera las dinámicas organizacionales y la cultura empresarial” (p.5), donde las organizaciones con una cultura sólida tienden a mejorar su desempeño, calidad y productividad, siempre al cuidado de mantener un balance entre tecnología y talento, crecimiento y efectividad, y finalmente integración y adaptación. Este autor señala además los beneficios de la transformación digital para un negocio en la tabla 2 que se presenta seguidamente.

Tabla 2

Beneficios de la transformación digital para las PYMES

- Digitalización de procesos y modelos de negocio.
- Trasladar el diseño de productos y servicios del ámbito físico al ámbito digital, como un enfoque esencial para la planificación estratégica y el funcionamiento moderno de la organización.
- Adopción de una mentalidad de aprovechamiento de la tecnología como forma de trabajo para establecer valores más elevados.
- Visibilidad de los datos registrados en cada proceso y transparencia de la información hacia los clientes.
- Optimización de costos, eficiencia operativa y sostenibilidad en el tiempo.
- Sistemas de seguimiento avanzado que permiten ver en tiempo real el estado de los productos.
- Gestión de cambio y alineación de toda la alta dirección en torno a nuevos objetivos y metas.
- Mejora la experiencia del cliente, aumento de la lealtad y descubrimiento de nuevas oportunidades de ingresos, esto por el hecho de que, al estar al alcance del cliente por medio de las conexiones digitales, éste puede interactuar en cualquier momento y desde cualquier lugar.

Fuente. Benavides (2024)

A través de las nuevas tecnologías e innovación operativa, se han modificado procesos en las culturas organizacionales, mejorado la eficiencia, facilitado la adaptación y generado valor añadid, en este sentido, Carrillo et al. (2025) explica que, “la transformación digital es un proceso complejo que busca crear valor mediante la innovación tecnológica” (pág. 55), este proceso forma parte de un modelo nuevo perteneciente a la industria 4.0, y viene dando una redefinición de las estructuras económicas y sociales a niveles globalizados. Por ende, estos autores establecen algunas características importantes de cómo las empresas pueden redefinir sus modelos de negocio y se describen con detalle en la tabla 3.

Tabla 3

Características para redefinir los modelos de negocio

Invertir en la capacitación de su personal, de manera que puedan enfrentar los desafíos y aprovechar las oportunidades que se presenten.
Convergencia de herramientas avanzadas como; inteligencia artificial, *blockchain*, análisis de datos, almacenamiento en la nube.
Digitalización en las PYMES con un enfoque integral para su implementación.
Reducción de costos externos y fortalecimiento de controles internos para reforzar la eficiencia operativa.
Toma de decisiones estratégicas que mejoren su oferta comercial.

Fuente. Carrillo et al. (2025)

La transformación digital implica para Benavides (2024) "un proceso de reinvención y ajuste de tecnologías digitales" (pág. 2), esto impulsa a las organizaciones a responder a estas crecientes necesidades y alcanzar nuevas expectativas. Las PYMES han adquirido valor gracias a la digitalización, la automatización de procesos internos, nuevas gestiones de inventario y relación con proveedores se han transformado en reducción de costos operativos y aumento de eficiencia, lo que mejora la capacidad de respuesta ante las demandas del mercado. Estos mismos autores enumeran una serie de desafíos que las pequeñas y medianas empresas enfrentan en estos procesos de transformación digital, los cuales se presentan en la tabla 4.

Tabla 4

Desafíos de las PYMES ante los procesos de transformación digital

- Limitación de recursos financieros.
- Infraestructura tecnológica inadecuada.
- Resistencia interna al cambio y a la implementación de nuevos sistemas digitales por parte de los empleados.
- Culturas organizacionales centradas en prácticas tradicionales de poca efectividad.

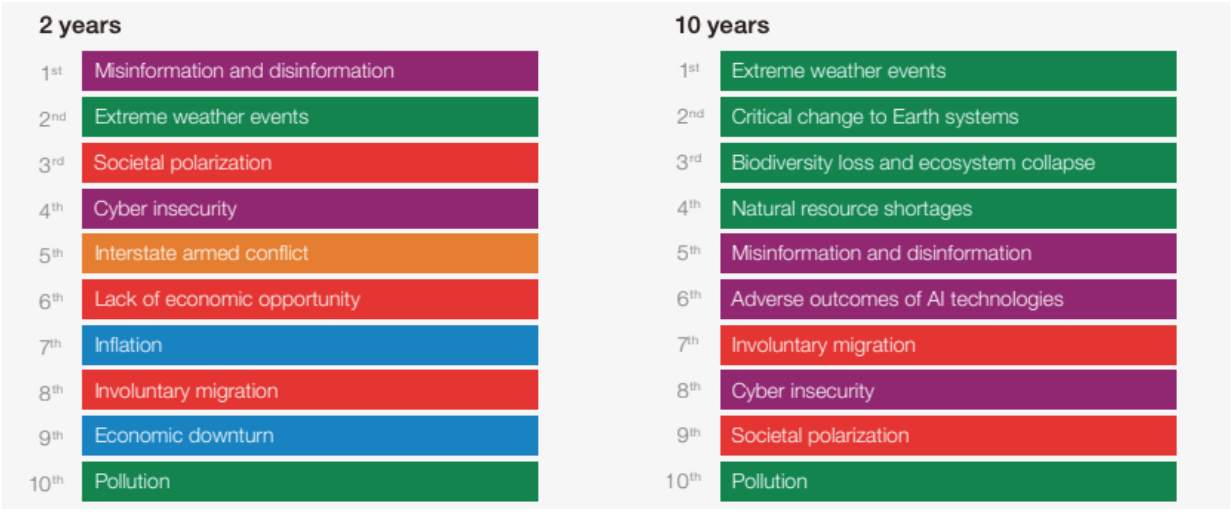
Fuente. Carrillo et al. (2025)

Las empresas, a consideración de Mateus et al. (2024) se han ajustado a estas realidades cambiantes, han alcanzado la madurez digital requerida por el mercado y ajustado sus procesos, modelos de negocio y cultura empresarial con la implementación de tecnologías digitales, enfrentando cada una sus dificultades particulares, pero actualmente existe una elevada exposición

de información que impacta negativamente su desempeño, y es donde entra en juego la llamada ciberseguridad. “A nivel mundial, la ciberseguridad es también un desafío crucial” (p. 17), en los últimos diez (10) años los riesgos cibernéticos se encuentran entre las diez primeras amenazas del mundo en aspectos relacionados con economía, medio ambiente, geopolítica, sociedad y tecnología, así lo publica Zahidi, The Global Risks Report (2024) y se muestra a continuación en la figura 1.

Figura 1

Riesgos globales clasificados por gravedad a corto y largo plazo



Fuente. Zahidi, The Global Risks Report (2024)

En virtud de esta información Mateus et al. (2024) enumera a los países latinoamericanos con mayor índice de ciberataques sobre todo en cuestiones de finanzas y hurto de identidad, colocando en primer lugar a Brasil, México, Colombia y Perú en esta última una alarmante cifra de “18 ataques por minuto” (pág. 18) y un total de “9.6 millones de intentos registrados en 2023” (pág. 19). Ante este panorama es necesario destacar a Iglesias y Pecker (2024) que enumeraron ocho (08) pasos para atravesar estos cambios organizacionales y adentrarse en aspectos de ciberseguridad, los cuales se muestran a continuación en la tabla 5.

Tabla 5

Pasos para atravesar cambios organizacionales relacionados con tecnología

1. Establecer un sentido de urgencia, como iniciativa al proceso de transformación.	5. Empoderar a los colaboradores, enlaces entre áreas para eliminar barreras y una estructura organizacional rígida.

2. Crear una coalición entre los líderes y personal técnico especializado.	6. Generar victorias a corto plazo, establecer objetivos que motiven y demuestren mejoras rápidas, tangibles y avances hacia la transformación.
3. Desarrollar una visión y estrategia, establecer una hoja de ruta clara para asegurar avances positivos.	7. Consolidar cambios a través de la transformación digital segura.
4. Comunicar visión de cambio, comunicación uniforme para evitar la resistencia al cambio.	8. Anclar los nuevos enfoques a la cultura organizacional, como nuevas herramientas y procesos prácticos cotidianos, de manera que aseguren sostenibilidad a largo plazo.

Fuente. Iglesias y Pecker (2024)

Desde estas perspectivas y procesos de cambio tecnológico, se deben adoptar estrategias de ciberseguridad eficaces y adaptables tomando en consideración limitaciones técnicas, presupuestales, organizacionales y prácticas, así lo menciona Cachaya et al. (2025).

Gestión de ciberseguridad

Con todos los cambios digitales que han surgido últimamente, las empresas se encuentran "más expuestas a vulnerabilidad de seguridad" Carrillo et al. (2025, pág. 69), y estas amenazas cibernéticas pueden establecer brechas de datos, desconfianza de clientes y proveedores generando mala reputación para las empresas. Estos desafíos y ataques pueden darse por varios factores a consideración de Morera et al. (2024) y Mateus et al. (2024), los cuales se presentan en la siguiente tabla.

Tabla 6

Factores que pueden desencadenar ataques cibernéticos

- Interconexión creciente, con la expansión del internet y sistemas cada vez más interconectados existe una potencial vulnerabilidad de los datos.
- Complejidad de los sistemas, con tantas capas y protocolos de hardware y software se hace más difícil la protección en los puntos de acceso.
- Dependencia de datos en los sistemas informáticos lo que puede ocasionar interrupción en las operaciones comerciales, pérdida de confidencialidad de datos y manipulación de información confidencial.
- Acceso a malware avanzado, técnicas de ingeniería social a manos de los ciber delincuentes.

- Escases de habilidades de protección en cuanto a ciberseguridad, poco personal preparado en este ámbito.
- Robo de información bancaria, hurto de identidad e información privada,

Fuente. Morera et al. (2024) y Mateus et al. (2024)

La ciberseguridad, es clave para asegurar altos niveles de competitividad, buena reputación, innovación y amplia permanencia en el mercado, "la información es el activo más valioso de las PYMES y su pérdida de compromiso puede tener consecuencias graves para su negocio" Morera et al. (2024, pág. 5), así mismo, es importante la adopción de políticas de seguridad, controles y mecanismos para la defensa muy alineados también con las ordenanzas gubernamentales de cada país.

El entorno tecnológico está en constante cambio, a través de diversas plataformas digitales se procesan y examinan grandes cantidades de datos e información que incluyen bases de datos, aplicaciones en línea, almacenamiento en la nube, entre otros; en el ámbito empresarial se deben establecer mecanismos de prevención, protección, resguardo, integridad y disponibilidad de los datos que permita asegurar la continuidad del negocio y por supuesto los potenciales ataques cibernéticos que puedan atacar la infraestructura digital, Núñez (2024). La gestión para los riesgos que involucra la ciberseguridad, enfrenta desafíos que las organizaciones necesitan abordar con estrategias adecuadas que eliminen amenazas de liberación de datos, amenazas financieras o daño reputacional significativo. Algunas de las principales funciones que se deben tomar en cuenta, al momento de evaluar riesgos comprenden a consideración de Mateus et al. (2024) las siguientes descritas en la tabla 7.

Tabla 7

Funciones para evaluar riesgos de ciberseguridad

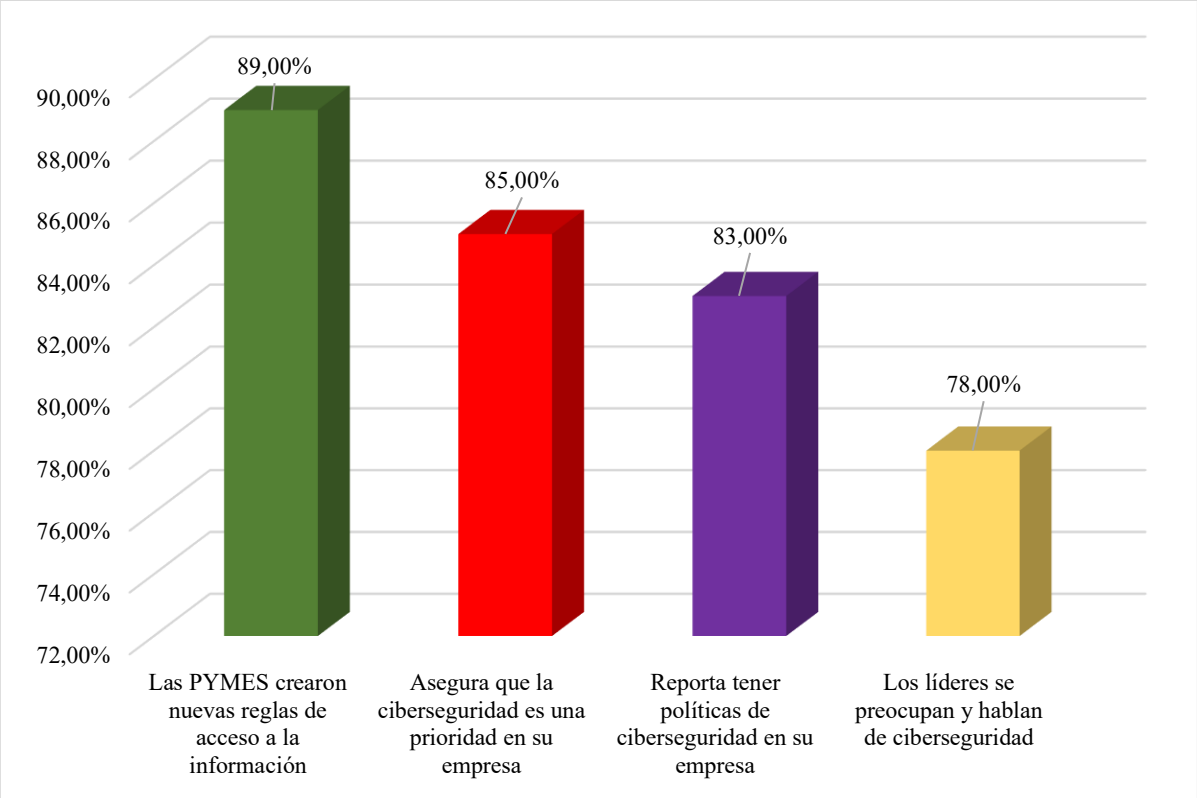
Identificar, los principales activos de la organización.
Proteger, activar y desarrollar controles que permitan cuidar los activos identificados.
Detectar, los potenciales eventos maliciosos que impacten a la compañía y esclarecer la capacidad de respuesta.
Responder, organizar la capacidad de contención y erradicación las amenazas de ciberseguridad en progreso.
Recuperar, acciones para volver a la normalidad en el menor tiempo posible, después de una amenaza materializada tomando en consideración el impacto que se haya generado.

Fuente: Mateus et al. (2024)

La ciberseguridad ha evolucionado, no solo se considera un componente técnico sino un elemento estratégico fundamental para el resguardo y éxito de las iniciativas digitales implementadas en las organizaciones, desde las PYMES hasta las de mayor envergadura Lagos (2024), en este sentido, Mateus et al. (2024) muestra un panorama interesante que viene sucediendo con las PYMES desde el año 2020, y se describe a continuación en el siguiente gráfico.

Gráfico 1

PYMES y ciberseguridad



Fuente. Mateus et al. (2024)

La ciberdelincuencia puede afectar a empresas de cualquier tipología, Valero (2024) explica que cualquiera que almacene información, maneje transacciones financieras o tenga presencia en línea puede ser objeto de ataque, en la tabla 8 este autor enumera las más sensibles, entendiendo que la seguridad no es un concepto universal, sino que es particular a cada sector de producción y dependiendo de las características distintivas de cada una tendrá abordajes diferentes.

Tabla 8

Tipos de empresas que con frecuencia son objetivo de ciberdelincuentes

- Financieras, bancos y plataformas de pago.
- De Tecnología y desarrollo de software.
- De Salud, centros con información médica sensible.
- Energía e infraestructura, agua, servicios públicos, con implicaciones potenciales para la seguridad nacional.
- Comercio electrónico, aquellas que manejan gran cantidad de información, clientes y transacciones financieras.
- De defensa, aeroespaciales, con información altamente calificada con intereses políticos.
- De Investigación y desarrollo, tecnologías innovadoras, y uso de propiedad intelectual.
- Medios de comunicación, con información que pueda comprometer la integridad de la misma.
- Cadenas de suministro.
- Servicios gubernamentales con datos sensibles.

Fuente. Valero (2024)

Los riesgos asociados a la ciberseguridad y protección de datos, afectan directamente el clima organizacional, no solo en las PYMES, sino en cualquier tipo de empresa, lo cual implica a consideración de Segura (2024) desafíos en el manejo de grandes volúmenes de datos, "muchas empresas no cuentan con las medidas adecuadas para proteger la información, lo que puede generar vulnerabilidad en el sistema" (pág. 11). Para este respecto López y Ordóñez (2024) señalan que se deben realizar auditorías informáticas y prácticas especializadas en detectar, prevenir y mitigar esos riesgos relacionados con el denominado "phishing, ransomware y malware" (pág. 16), términos en inglés utilizados para denominar a las técnicas de suplantación de identidad, programas maliciosos de restricción a archivos o sistemas y programas para dañar o comprometer sistemas, redes o dispositivos; y describen en qué consiste este tipo de auditorías en la tabla 9.

Tabla 9

Aspectos a evaluar en auditorías informáticas

Evaluación de la seguridad de res y sistemas, análisis y evaluaciones de vulnerabilidad y configuración de seguridad.
Concienciación y capacitación del personal, educación continua del personal en relación a las amenazas de seguridad informática, simulacros, sesiones de capacitación que le ayuden a los empleados a reconocer y evitar ataques.

Implementación de controles de seguridad, instalación de sistemas de detección, filtros de correos electrónicos, antivirus actualizados.
Monitorización y detección temprana de actividades sospechosas, descargas o comportamientos anómalos del sistema.
Respuesta y recuperación ante incidentes, puesta en marcha de planes de respuesta, restaurar sistemas, copias de seguridad, comunicación oportuna.
Actualización de sistemas, esto ayuda a reducir las brechas de seguridad y la superficie de ataques maliciosos.

Fuente. López y Ordóñez (2024)

Finalmente, es importante destacar que la ciberseguridad es prioridad para todo tipo de empresas en la era digital, así lo destaca Tunqui (2024), cuando menciona que si se estudian las amenazas de ciberseguridad es posible preparar adecuadamente a la organización y su capacidad de respuesta, al entender el entorno y las amenazas se puede reaccionar más eficientemente para tener una salida victoriosa ante las adversidades digitales.

Conclusión

En virtud de las interrogantes planteadas y en base al propósito principal de esta investigación, se puede concluir que:

1. Las pautas básicas a considerar para que las organizaciones apliquen sistemas se ciberseguridad eficientes, radican en el conocimiento de los riesgos y la disposición de enfrentar los cambios de la era digital.
2. La capacidad de respuesta en organizaciones como las PYMES, se centra en la adopción de medidas preventivas, conocimiento de las posibles intrusiones a los sistemas y la protección apropiada de los sistemas informáticos ante los ataques, mientras más datos se manejen mayores deben ser los niveles de protección.
3. Los procesos de ciberseguridad en las PYMES, pueden mejorarse con la educación de los empleados, formación permanente, puesta en práctica, simulacros y auditorías de las posibles debilidades presentes en los sistemas de la empresa.

La innovación no solo se refiere a la actualización de equipos, influye más profundamente a procesos, sistemas y comportamientos humanos.

Referencias bibliográficas

Alarcon, J. (2024). Proyecto de innovación para mejorar el clima y cultura organizacional de empresas PYMES. Proyecto de Innovación para optar al Grado Académico de Bachiller en Planificación de procesos estratégicos de recursos humanos, Escuela de Educación Superior Tecnológica Privada "Zegel", Programa de estudios en Planificación de Recursos HUmanos. Obtenido de https://repositorio.zegel.edu.pe/handle/20.500.13065/691

Benavides, C. (2024). Analizar la incidencia de la transformación digital en el contexto de la cultura organizacional del sector logístico explorador de la ciudad de Bogotá D.C. Universidad La Gran Colombia, Especialización en gerencia. Obtenido de https://repository.ugc.edu.co/items/67879d91-c040-4456-9fff-c27d413c5441

Cachaya, H., Castañeda, H., Torres, L., & Pérez, J. (2025). Sandbox virtual con herramientas open sourse para pentesting: Una propuesta tecnológica aplicada a la seguridad cibernética de las pymes. Sapiens in Artificial Intelligence, 2(2), 1-14. Obtenido de https://revistasapiensec.com/index.php/Sapiens_in_Artificial_Intelligen/article/view/216

Carrillo, Á., Michel, L., Lizcano, M., & Carrillo, E. (2025). La transformación digital y su impulso en la creación de valor para las PYMES. Piensa Diferente. Revista Pensamiento Transformacional, 4(12), 53-72. Obtenido de https://revistapensamientotransformacional.editorialpiensadiferente.com/index.php/pensamiento_transformacional/article/view/97

Iglesias, L., & Pecker, I. (2024). Análisis del cambio organizacional y su impacto en el capital humano ante la implementación de tecnologías 4.0. Trabajo final de la carrera Ingeniería Industrial, Universidad Nacional de Mar de Plata, Facultad de Ingeniería. Obtenido de https://rinfi.fi.mdp.edu.ar/handle/123456789/988

Lagos, J. (2024). Transformación digital y ciberseguridad. Economía y Negocios. Universidad de Chile. Obtenido de https://repositorio.uchile.cl/bitstream/handle/2250/205366/Tesis%20-%20JOSE%20ANTONIO%20LAGOS%20MELO.docx.pdf?sequence=1

López, K., & Ordóñez, Y. (2024). Auditoría y ciberseguridad en el sector comercial: evaluación de resiliencia ante amenazas digitales. Revista Multidisciplinaria Perspectivas Investigativas, 4, 14-27. Obtenido de http://www.rperspectivasinvestigativas.org/index.php/multidiscipinaria/article/view/154

Mateus, D., Cigaran, G., & Rodríguez, B. (2024). Modelo ProLab: PYMESHIELD, propuesta de modelo de negocio sostenible de ciberseguridad para Pymes. Tesis para obtener el grado

académico de maestro en administración estratégica de empresas, Centrum. PUPC. Escuela para los buenos negocios. Obtenido de https://tesis.pucp.edu.pe/bitstreams/df9f89dc-ad71-4bcc-978c-9c180087b3b8/download

Morera, O., Ochoa, A., Farfán, J., & Herrera, H. (2024). La importancia de la ciberresilencia en las empresas PYMES en Colombia. Los Libertadores, 1-19. Obtenido de https://repository.libertadores.edu.co/items/52b041af-5152-451b-9842-5911a07162c1

Núñez, Y. (2024). Desafíos en la gobernanza de Pymes mineras colombianas: gestión de TI y Ciberseguridad como factores críticos. UNICYT. Actas del IX Congreso de Investigación, Desarrollo e Innovación de la Universidad Internacional de Ciencia y Tecnología, 82-495. Obtenido de http://revistas.unicyt.org/index.php/actasidi-unicyt/article/view/221

Segura, N. (2024). Transformación digital con Inteligencia Artificial: Impacto en el posicionamiento de marca y rendimiento financiero en empresas colombianas. Marketing y transformación digital, 1-10. Obtenido de https://repositorio.unbosque.edu.co/items/03cfb702-a8ed-45ad-a613-f89f3d2b41b9

Tunqui, C. (2024). Ciberseguridad: Protección de la empresa en la era digital. Revista MAYA. Administración y Turismo, 6(2), 14-26. Obtenido de https://revistamaya.org/index.php/maya/article/view/1166

Valero, J. (2024). Marco y taxonomía de ciberseguridad para la pequeña y mediana empresa. Trabajo final de grado presentado en la Escola Técnica Superior d`Enginyeria de Telecomunicació de Barcelona de la Universitat Politécnica de Catalunya, Universitat Politécnica de Catalunya BARCELONATECH. Obtenido de https://upcommons.upc.edu/handle/2117/410928

Villarreal, G. (2024). Del saber al hacer: transformación de las PYMES ecuatorianas a través de la Educación Tecnológica. SAPIENS. Sapiens Internacional Multidisciplinary Journal, 1(3), 185-197. Obtenido de https://revistasapiensec.com/index.php/sapiens/article/view/57

Zahidi, S. (2024). The global risks reporto 2024. World Economic Forum(19th Edition), 1-124. Obtenido de https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Agradecimiento:

N/A

Nota:

El artículo no es producto de una publicación anterior.