CAPITULO 07

Guía de Seguridad Informática para LATAM PC en Santo Domingo de los Tsáchilas: Estrategias de Mitigación de Vulnerabilidades y Capacitación en Ciberseguridad

Guía de Seguridad Informática para LATAM PC en Santo Domingo de los Tsáchilas: Estrategias de Mitigación de Vulnerabilidades y Capacitación en Ciberseguridad.

IT Security Guide for LATAM PC in Santo Domingo de los Tsáchilas: Vulnerability Mitigation Strategies and Cybersecurity Training.

Mendoza-Garcia, Nelson Julian [1]
https://orcid.org/0009-0005-7121-8255
nelson.mendoza.garcia@utelvt.edu.ec
Ecuador, La Concordia, Universidad Técnica Luis Vargas Torres de Esmeraldas

Quel-Martinez, Dilan Alexander [2]
https://orcid.org/0009-0005-2521-3568
dilan.quel.martinez@utelvt.edu.ec
Ecuador, La Concordia, Universidad Técnica Luis Vargas Torres de Esmeraldas

Gongora-Cheme, Roxana Katherine[3]
https://orcid.org/0000-0001-9299-6885
roxana.gongora.cheme@utelvt.edu.ec
Ecuador, La Concordia, Universidad Técnica Luis Vargas Torres de Esmeraldas

DOI / URL: https://doi.org/10.55813/egaea.cl.85

Resumen: Este estudio evalúa las prácticas de seguridad informática de la microempresa LATAM PC y desarrolla una guía adaptada para mitigar sus vulnerabilidades y mejorar la capacitación en ciberseguridad. Mediante un enfoque metodológico mixto, se encuestó a empleados y clientes para evaluar sus percepciones sobre las políticas de seguridad de la empresa. Los resultados revelaron una baja participación de los empleados en programas de capacitación en ciberseguridad, lo que representa un riesgo organizacional. Algunos clientes confiaban en las medidas implementadas, mientras que otros expresaron dudas. En respuesta, se elaboró una guía con recomendaciones y protocolos para mejorar la protección de datos sensibles. La investigación concluye que LATAM PC necesita adoptar políticas de seguridad más efectivas, incluyendo programas de capacitación continua, para reducir los riesgos de ciberataques y fortalecer la confianza del cliente.

Palabras clave: Seguridad, Capacitación, Vulnerabilidades, Protección, Datos.

Abstract:

This study assesses the information security practices of the microenterprise LATAM PC and develops a customized guide to mitigate its vulnerabilities and enhance cybersecurity training. Using a mixed-methods approach, employees and customers were surveyed to understand their perceptions of the company's security policies. Results indicated low employee participation in cybersecurity

training, posing an organizational risk. While some customers trusted the implemented measures, others expressed concerns. In response, a guide with recommendations and protocols was created to improve data protection. The study concludes that LATAM PC should implement more robust security policies, including ongoing training programs, to reduce cyberattack risks and strengthen customer trust.

Keywords: Security, Training, Vulnerabilities, Protection, Data.

7.1. Introducción

En la actualidad, las microempresas desempeñan un papel crucial en la economía global, ofreciendo servicios vitales a diversos sectores. No obstante, con el avance de la tecnología, estas entidades también enfrentan un aumento en los riesgos asociados a la seguridad cibernética. Investigaciones recientes indican que muchas microempresas carecen de planes de seguridad adecuados, lo que las convierte en objetivo fácil para brechas de seguridad, pérdida de información confidencial y ciberataques. La gestión deficiente de la información puede afectar negativamente tanto la reputación de estas empresas como su capacidad para operar de manera continua. Por lo tanto, establecer políticas y directrices de seguridad informática se ha vuelto esencial para garantizar su sostenibilidad.

“A escala global, normativas como la ISO/IEC 27001 han establecido bases sólidas para la gestión de la seguridad de la información. En Ecuador, la Ley Orgánica de Protección de Datos Personales enfatiza la importancia de salvaguardar la información personal en el entorno digital (LOPDP, 2021). Sin embargo, muchas microempresas ecuatorianas aún no han tomado medidas efectivas para proteger sus sistemas y datos. En este marco, "LATAM PC", una microempresa situada en Santo Domingo de los Tsáchilas ha detectado con urgencia la necesidad de fortalecer su seguridad informática. Aunque la empresa gestiona información delicada de sus clientes, incluyendo datos personales y financieros, no dispone de una estrategia integral que aborde todas las áreas de su operación” (LOPDP, 2021) (Abogados, 2021).

El objetivo de este estudio es crear una guía de seguridad informática adaptada a LATAM PC, que permita abordar las vulnerabilidades de sus sistemas y mejorar la protección de los datos sensibles. La investigación se basa en teorías relacionadas con la ciberseguridad, la gestión de riesgos y mejores prácticas internacionales, respondiendo a la necesidad local de reforzar la protección de los activos digitales en microempresas. La revisión de estudios anteriores revela que la falta de políticas claras y un escaso nivel de capacitación del personal son factores que incrementan la exposición a riesgos cibernéticos, haciendo aún más urgente la implementación de soluciones de seguridad en estas organizaciones.

Para enfrentar estos desafíos, se propone un enfoque mixto que incluirá encuestas al personal para examinar el estado actual de la seguridad en la empresa, además de un análisis de vulnerabilidades que servirá para diseñar una guía de políticas de seguridad informática apropiadas. Este estudio tiene como finalidad no solo mejorar la infraestructura tecnológica de LATAM PC, sino también establecer un marco de referencia que pueda ser útil para otras microempresas ecuatorianas que se encuentren en situaciones similares.

El principal propósito de esta investigación es desarrollar una guía de seguridad informática que ayude a LATAM PC a optimizar la protección de su información sensible, reducir las vulnerabilidades de sus sistemas y garantizar la continuidad de sus operaciones.

Tras la implementación de la guía de seguridad informática en LATAMPC, se logró una reducción significativa de las vulnerabilidades, en particular frente a amenazas como el phishing. El personal adoptó las nuevas políticas de seguridad de manera positiva, y gracias a las capacitaciones recibidas, se incrementó su conciencia sobre prácticas seguras. La aplicación de la guía permitió mejorar la protección de los datos sensibles, así como optimizar la eficiencia operativa de la microempresa.

Los principales beneficiarios fueron los empleados y los clientes de LATAM PC. Para los empleados, la guía proporcionó un entorno de trabajo más seguro y mejoró sus conocimientos sobre ciberseguridad, lo cual es esencial para prevenir ciberataques, ya que, como señalan (Hadar & Shapira, 2021), “la formación de los empleados juega un rol crucial en la creación de una cultura de ciberseguridad”. Los clientes, por su parte, ganaron mayor confianza en los servicios de la empresa, al asegurarse una mejor protección de su información personal y financiera.

7.1. Materiales y métodos

La investigación se planteó como un estudio descriptivo y aplicado, empleando un enfoque mixto que combina métodos cualitativos y cuantitativos. El objetivo fue evaluar el estado de la seguridad informática en LATAM PC y crear una guía de seguridad adaptada a sus necesidades.

En cuanto a la población estudiada, se trabajó con el personal de LATAMPC, que consta de alrededor de 4 empleados de diferentes áreas. Además, se incluyó a 20 clientes de la microempresa para obtener una perspectiva más amplia sobre las prácticas de seguridad.

Para recopilar información, se aplicaron varias técnicas:

Encuestas: Se creó un cuestionario estructurado que se distribuyó entre los empleados y los clientes para evaluar su conocimiento sobre seguridad informática y sus prácticas actuales. Las encuestas se realizaron tanto de manera presencial como por correo electrónico, lo que garantizó una alta tasa de respuesta. Se utilizaron escalas de Likert para medir las respuestas.

Desarrollo de la guía de seguridad: Con los resultados de las encuestas y el análisis de vulnerabilidades, se elaboró una guía de seguridad informática. Esta guía incluye políticas y procedimientos claros, protocolos de capacitación para el personal y recomendaciones para proteger los datos sensibles.

En cuanto a los aspectos éticos, antes de comenzar la investigación, se obtuvo la autorización de la administración de LATAMPC, asegurando así el cumplimiento de los principios éticos. Además, se cumplió con las normativas éticas relacionadas con el manejo de datos, conforme a la Ley Orgánica de Protección de Datos Personales de Ecuador. Según el análisis sobre aspectos éticos en la investigación, es fundamental que se respete el derecho a la privacidad y se obtenga el consentimiento informado de los participantes, garantizando así una adecuada protección de sus datos personales (Sierra, 2021)

7.2. Resultados

7.2.1. Comunicaciones sobre amenazas de seguridad

En las encuestas realizadas, se preguntó a los empleados y clientes si recibían comunicaciones regulares de la empresa sobre posibles amenazas a la seguridad. Los resultados indicaron que el 60% de los encuestados afirmó que sí recibían este tipo de comunicaciones de forma periódica. Sin embargo, el 40% indicó que no recibía ninguna notificación sobre riesgos o amenazas de seguridad informática.

Tabla 1

¿Recibe comunicaciones regulares de la empresa sobre posibles amenazas a la seguridad?

N°	Alternativas	F	%
1	Si	12	60%
2	No	8	40%
Total		**20**	**100%**

Nota: Resultados de la encuesta sobre la recepción de comunicaciones regulares por parte de la empresa acerca de posibles amenazas a la seguridad informática

Este resultado refleja que, aunque una mayoría está informada sobre posibles amenazas, aún existe un porcentaje considerable que no recibe comunicaciones

regulares, lo que podría representar un riesgo en la falta de conocimiento y preparación frente a posibles ciberataques.

7.2.2. Participación en capacitaciones sobre seguridad informática

Tabla 2

¿Asisten a las capacitaciones sobre seguridad informática que ofrece la empresa?

N°	Alternativas	F	%
1	Si	4	20%
2	No	16	80%
Total		**20**	**100%**

Nota: Resultados de la ficha de observación sobre la asistencia de los empleados a las capacitaciones en seguridad informática ofrecidas por la empresa.

Se observó que el 80% de los empleados de la microempresa no asiste a las capacitaciones sobre seguridad informática, lo que representa un riesgo significativo para la organización. Esta falta de preparación podría hacer que el personal sea más vulnerable ante amenazas, como el phishing y otros ataques cibernéticos.

Además, solo el 20% del equipo recibe la formación necesaria, lo que resulta insuficiente para garantizar una protección adecuada en todas las áreas operativas. Esta situación subraya la necesidad urgente de implementar políticas de capacitación más efectivas para mitigar los riesgos asociados con la seguridad informática.

7.2.3. Percepción sobre las medidas de prevención de ciberataques

Tabla 3

¿Cree que la empresa toma medidas suficientes para prevenir ciberataques?

N°	Alternativas	F	%
1	Si	14	70%
2	No	6	30%
Total		**20**	**100%**

Nota: Resultados de la encuesta sobre la percepción de los clientes respecto a las medidas de prevención de ciberataques implementadas por la empresa.

Los resultados de la encuesta reflejan que el 70% de los clientes respondió afirmativamente, lo que indica que una mayoría considera que la empresa tiene implementadas medidas adecuadas de seguridad. Sin embargo, el 30% de los clientes no percibe las acciones de la empresa como suficientes, lo que revela que una parte significativa de la clientela tiene dudas o no se siente completamente segura con las políticas de ciberseguridad actuales.

Los resultados de la encuesta reflejan que a pesar de que la mayoría de los clientes confía en las medidas de seguridad de la empresa, el hecho de que un

30% considere que no son suficientes resalta la necesidad de reforzar o mejorar las prácticas de seguridad cibernética. Este grupo podría estar buscando mayor transparencia en las medidas implementadas o protocolos de seguridad más visibles. Para aumentar la confianza en toda su base de clientes, la empresa podría considerar revisar sus políticas de seguridad o mejorar la comunicación sobre las acciones que ya está tomando para proteger sus sistemas y datos.

7.2.4. Capacitación del personal técnico en seguridad informática

Tabla 4

¿Cree que el personal técnico de la empresa está debidamente capacitado en temas de seguridad informática?

N°	Alternativas	F	%
1	Si	15	75%
2	No	5	25%
Total		**20**	**100%**

Nota: Resultados de la encuesta sobre la percepción de la capacitación del personal técnico en temas de seguridad informática

En relación con la pregunta sobre si los clientes creen que el personal técnico de la empresa está debidamente capacitado en temas de seguridad informática, el 75% respondió que sí, mientras que el 25% indicó que no. Este resultado muestra que una mayoría de los encuestados confía en la competencia del personal en materia de seguridad, pero también revela que una parte significativa de la clientela tiene reservas sobre la capacitación del equipo.

La percepción positiva sobre la capacitación del personal técnico es un buen indicador de la confianza que los clientes tienen en la capacidad del equipo para manejar cuestiones de seguridad informática. Sin embargo, el 25% que no comparte esta opinión señala que hay margen para mejorar en la formación y actualización del personal. La empresa podría beneficiarse al invertir en más capacitación y certificaciones en seguridad.

7.2.5. Seguimiento posterior a las reparaciones

Tabla 5

¿Considera que la empresa realiza un seguimiento adecuado después de la reparación para asegurarse de que todo funciona correctamente?

N°	Alternativas	F	%
1	Si	15	75%
2	No	5	25%
Total		20	100%

Nota: Resultados de la encuesta sobre la percepción de la capacitación del personal técnico en temas de seguridad informática

En la pregunta sobre el seguimiento posterior a las reparaciones, el 65% de los clientes afirmó que la empresa realiza un seguimiento adecuado, mientras que el 35% consideró que no es suficiente. Esto indica que, aunque la mayoría está satisfecha, una porción significativa no lo está.

La percepción de un seguimiento adecuado después de la reparación es esencial para garantizar la satisfacción del cliente y la confianza en la calidad del servicio. Aunque el 65% de los encuestados se siente satisfecho, el 35% que no lo está indica que hay oportunidades para mejorar este aspecto. La empresa podría considerar implementar procedimientos más estructurados para el seguimiento post-reparación, asegurando que todos los clientes reciban atención continua y se sientan apoyados después del servicio.

7.3. Conclusiones

La presente investigación ha revelado que un alarmante 80 % de los empleados no asiste a la capacitación sobre seguridad informática en la microempresa LATAMPC. Esta situación pone de manifiesto un riesgo significativo para la empresa porque la falta de conocimiento y capacitación adecuada en seguridad informática puede hacer que el personal sea más susceptible a amenazas cibernéticas, como el phishing y otros ataques. Los hallazgos demuestran que la educación en ciberseguridad es crucial para proteger los datos confidenciales y mantener la integridad de las operaciones de la microempresa.

Además, el hecho de que solo un 20% del personal esté recibiendo la capacitación necesaria muestra que las iniciativas de la formación actual son insuficientes. Esta situación puede afectar la seguridad de la empresa y la confianza de los clientes, así como la reputación de LATAMPC en el mercado. Por lo tanto, es fundamental que la empresa adopte un enfoque proactivo en la implementación de políticas de seguridad más sólidas que incluyan un programa de capacitación regular y accesible para todos los empleados.

La investigación también ayudó a crear una guía de seguridad informática para microempresas. Este documento no solo proporcionará herramientas de referencia para el personal, sino que también establecerá un marco de políticas y procedimientos claros para garantizar la protección de datos y disminuir las vulnerabilidades detectadas. Al llevar a cabo estas acciones, LATAMPC mejorará su capacidad para enfrentar amenazas cibernéticas y aumentará la confianza de los clientes en su capacidad para proteger datos confidenciales.

Además, los resultados reflejan las percepciones de los empleados sobre el seguimiento realizado por la empresa después de las reparaciones, donde el 65% de ellos pensó que se hicieron correctamente. Sin embargo, el 35% restante expresó preocupaciones, lo que indica que los procesos de seguimiento aún

necesitan mejorar. Esto demuestra la importancia de evaluar continuamente las prácticas de la empresa y hacer cambios para asegurarse de que cumplan con los estándares de calidad y seguridad esperados.

Este estudio muestra que LATAM PC enfrenta desafíos significativos en cuanto a ciberseguridad debido a la baja participación de su personal en capacitaciones. Se recomienda la implementación de un programa de capacitación continua en seguridad informática para todos los empleados, dado que el conocimiento en ciberseguridad es esencial para reducir los riesgos asociados a ciberataques y fortalecer la protección de datos sensibles. La guía de seguridad informática desarrollada proporciona políticas y protocolos claros, y representa una herramienta útil no solo para LATAM PC, sino también para otras microempresas ecuatorianas que buscan mejorar sus prácticas de seguridad. Esta guía ayudará a LATAM PC a adoptar un enfoque preventivo y a construir un entorno digital seguro, lo que aumentará la confianza de los clientes y protegerá sus operaciones frente a las amenazas emergentes de ciberseguridad.

Referencias Bibliográficas

Abogados, F. P. (2021). Ecuador: Overview of the data protection law. Quito: Falconi Puig Abogados.

Asamblea Nacional de la República del Ecuador. (2021). LOPDP. Ecuador: Asamblea Nacional de la República del Ecuador.

Boné-Andrade, M. F. (2023). Inclusión Digital y Acceso a Tecnologías de la Información en Zonas Rurales de Ecuador. Revista Científica Zambos, 2(2), 1-16. https://doi.org/10.69484/rcz/v2/n2/40

Celi-Párraga, R. J., Boné-Andrade, M. F., Mora-Olivero, A. P., & Sarmiento-Saavedra, J. C. (2023). Ingeniería del Software I: Requerimientos y Modelado del Software. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.21

Colina-Vargas, A. M., & Espinoza-Mina, M. A. (2024). Perspectiva del desarrollo y uso del software en Ecuador: Un recorrido desde la bibliometría y el análisis de contenido. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.91

Erazo-Luzuriaga, A. F., Ramos-Secaira, F. M., Galarza-Sánchez, P. C., & Boné-Andrade, M. F. (2023). La inteligencia artificial aplicada a la optimización de programas informáticos. Journal of Economic and Social Science Research, 3(1), 48–63. https://doi.org/10.55813/gaea/jessr/v3/n1/61

Galarza-Sánchez, P. C. (2023). Adopción de Tecnologías de la Información en las PYMEs Ecuatorianas: Factores y Desafíos. Revista Científica Zambos, 2(1), 21-40. https://doi.org/10.69484/rcz/v2/n1/36

Galarza-Sánchez, P. C., Agualongo-Yazuma, J. C., & Jumbo-Martínez, M. N. (2022). Innovación tecnológica en la industria de restaurantes del Cantón Pedro Vicente Maldonado. Journal of Economic and Social Science Research, 2(1), 31–43. https://doi.org/10.55813/gaea/jessr/v2/n1/45

García-Peña, V. R. (2023). Desarrollo y Uso de Aplicaciones Móviles en el Contexto Ecuatoriano. Revista Científica Zambos, 2(3), 1-15. https://doi.org/10.69484/rcz/v2/n3/46

Hadar, I., & Shapira, B. (2021). Building a cybersecurity culture in organizations. Springer.

Montalván-Vélez, C. L., Mogrovejo-Zambrano, J. N., Romero-Vitte, I. J., & Pinargote-Carrera, M. L. D. C. (2024). Introducción a la Inteligencia Artificial: Conceptos Básicos y Aplicaciones Cotidianas . Journal of Economic and Social Science Research, 4(1), 173–183. https://doi.org/10.55813/gaea/jessr/v4/n1/93

Picoy-Gonzales, J. A., Huarcaya-Taype, R., Contreras-Canto, O. H., & Omonte-Vilca, A. (2023). Fortalecimiento Metodológico de la Seguridad Informática en Posgrados: Análisis y Estrategias de Mejora. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.56

Ramos-Secaira, F. M. (2023). Seguridad Cibernética en Empresas Ecuatorianas: Prácticas y Retos Actuales. Revista Científica Zambos, 2(3), 16-28. https://doi.org/10.69484/rcz/v2/n3/47

Sánchez-Caguana, D. F., Philco-Reinozo, M. A., Salinas-Arroba, J. M., & Pico-Lescano, J. C. (2024). Impacto de la Inteligencia Artificial en la Precisión y Eficiencia de los Sistemas Contables Modernos. Journal of Economic and Social Science Research, 4(3), 1–12. https://doi.org/10.55813/gaea/jessr/v4/n3/117

Sierra, C. (2021). Aspectos éticos en la investigación y protección de datos personales en Ecuador. Quito: Universidad Central del Ecuador.

Solano-Gutiérrez, G. A. (2024). La Tecnología en la Educación a Distancia: Revisión de Progresos y Obstáculos a Superar. Revista Científica Zambos, 3(2), 48-73. https://doi.org/10.69484/rcz/v3/n2/17