TECNOLOGÍAS DE SEGURIDAD PARA EMPRESAS EN GUAYAQUIL

SECURITY TECHNOLOGIES FOR COMPANIES IN GUAYAQUIL

Fernando Paul Sánchez Ramírez [1*]

[1] Instituto Superior Tecnológico Portoviejo. Ecuador. ORCID: https://orcid.org/0000-0002-5621-8338. Correo: fernando.sanchez@itsup.edu.ec

Lenin Mauricio Andaluz Granda [2]

[2] Instituto Superior Tecnológico Portoviejo. Ecuador. ORCID: https://orcid.org/0000-0003-1207-5600. Correo: lenin.andaluz@itsup.edu.ec

*** Autor para correspondencia: fernando.sanchez@itsup.edu.ec**

Resumen

En un mundo cada vez más informatizado, globalizado, y competitivo resulta imprescindible proteger los bienes y recursos personales, empresariales y gubernamentales. La seguridad se ha convertido en una preocupación fundamental. Las tecnologías de seguridad desempeñan un papel crucial en la protección de datos, sistemas, redes y activos empresariales. La ciudad de Guayaquil enfrenta una realidad desafiante en términos de seguridad empresarial, afectando la estabilidad y prosperidad de las empresas locales. En este sentido la investigación tiene como objetivo proponer estrategias tecnológicas para incrementar la seguridad en las empresas de Guayaquil. Se utilizó el paradigma de investigación mixto, con un enfoque de vinculación de métodos teóricos y empíricos. Se emplearon entrevistas semiestructuradas y encuestas y se consultaron documentos oficiales para obtener información pertinente. La muestra fue seleccionada con muestreo probabilístico y no probabilístico. Se obtuvieron como resultados las principales limitaciones en el uso de tecnologías de seguridad. Se propuso una estrategia tecnológica para incrementar la seguridad de las empresas en Guayaquil. La estrategia integral combina la selección de tecnologías avanzadas de seguridad física, cibernética, y de seguridad informática, además de educación en ciberseguridad, y medidas específicas adaptadas a las necesidades locales de las empresas para incrementar la seguridad empresarial en la ciudad de Guayaquil.

Palabras clave: seguridad; tecnología; estrategia tecnológica

Abstract

In an increasingly computerized, globalized and competitive world, it is essential to protect personal, corporate and governmental assets and resources. Security has become a fundamental concern. Security

technologies play a crucial role in protecting data, systems, networks and business assets. The city of Guayaquil faces a challenging reality in terms of business security, affecting the stability and prosperity of local businesses. In this sense, the objective of this research is to propose technological strategies to increase security in Guayaquil companies. A mixed research paradigm was used, with a focus on linking theoretical and empirical methods. Semi-structured interviews and surveys were used and official documents were consulted to obtain relevant information. The sample was selected with probability and non-probability sampling. The main limitations in the use of security technologies were obtained as results. A technological strategy was proposed to increase the security of companies in Guayaquil. The comprehensive strategy combines the selection of advanced physical, cyber and computer security technologies, cybersecurity education, and specific measures adapted to the local needs of companies to increase business security in the city of Guayaquil.

Keywords: *security; technology; technology strategy*

Fecha de recibido: 12/01/2024
Fecha de aceptado: 22/03/2024
Fecha de publicado: 28/03/2024

Introducción

En un mundo cada vez más informatizado, globalizado, y competitivo resulta imprescindible proteger los bienes y recursos personales, empresariales y gubernamentales. La seguridad se ha convertido en una preocupación fundamental. Las tecnologías de seguridad se refieren a los componentes y políticas utilizados para proteger información, lugares y recursos en sentido general (López 2020).

Las tecnologías de seguridad desempeñan un papel crucial en la protección de datos, sistemas, redes y activos empresariales. Desde la prevención de ciberataques hasta la gestión de riesgos, estas tecnologías abarcan una amplia gama de soluciones diseñadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información (Sánchez 2023). Su objetivo es mitigar el riesgo al prevenir el acceso no autorizado, identificar posibles incidentes, permitir respuestas rápidas, disuadir conductas delictivas y capturar pruebas cruciales en caso de brechas de seguridad (Seminario 2023). Estas tecnologías avanzadas pueden proteger tanto activos físicos como datos electrónicos, tanto in situ como a distancia.

En este artículo, se muestran las principales tecnologías de seguridad utilizadas en el ámbito empresarial, sus desafíos y cómo contribuyen a la resiliencia de las organizaciones. Desde firewalls y sistemas de detección de intrusiones hasta cifrado y autenticación biométrica, descubriremos cómo estas herramientas se combinan para formar una barrera efectiva contra las amenazas cibernéticas. El estudio de las tecnologías de seguridad es de gran importancia en el mundo actual. En la protección de datos y privacidad, las tecnologías de seguridad ayudan a proteger los datos personales y empresariales. Esto es fundamental para evitar el robo de información confidencial, como contraseñas, datos financieros y registros médicos. La privacidad es un derecho

fundamental, y comprender cómo las tecnologías de seguridad protegen la información es esencial para salvaguardarla (Pantoja and Donado 2020).

En la prevención de amenazas cibernéticas, el ciberespacio está lleno de amenazas, como *malware*, *ransomware*, *phishing* y ataques de denegación de servicio (DDoS). Estudiar las tecnologías de seguridad permite comprender cómo detectar, prevenir y mitigar estas amenazas. Las organizaciones y los individuos deben estar preparados para enfrentar ataques cibernéticos y proteger sus activos digitales. En el cumplimiento legal y regulatorio, muchas leyes y regulaciones exigen que las organizaciones implementen medidas de seguridad para proteger los datos de los usuarios y clientes. Estudiar estas tecnologías ayuda a garantizar el cumplimiento normativo y evita sanciones legales (Preciado Oquendo 2021).

Además, para la seguridad en la nube y transformación digital. La adopción de la nube y la transformación digital requieren una comprensión sólida de las tecnologías de seguridad. Esto incluye la autenticación, el cifrado, la gestión de identidad y acceso, y la seguridad de la infraestructura en la nube. Las empresas modernas deben estar al tanto de las últimas tendencias y mejores prácticas para proteger sus operaciones digitales (Campos Merchán 2018). Es importante también la protección de la reputación y continuidad del negocio. Las brechas de seguridad pueden dañar la reputación de una empresa y afectar su confianza con los clientes. Estudiar las tecnologías de seguridad ayuda a prevenir interrupciones en las operaciones comerciales y a mantener la confianza del público.

Tipos de tecnologías de seguridad

Seguridad de TI (Tecnología de la Información): la seguridad de TI protege la integridad de las tecnologías de la información, como sistemas informáticos, redes y datos, contra ataques, daños o acceso no autorizado. Conserva la confidencialidad de la información y bloquea el acceso a hackers. Las tecnologías de seguridad de TI incluyen soluciones como firewalls, antivirus, detección y respuesta de *Endpoints* (EDR), y agentes de seguridad de acceso a la nube (CASB).

Seguridad de Datos y Ciberseguridad:

La seguridad de datos y la seguridad informática son tipos de prácticas y sistemas de ciberseguridad que protegen la información y las redes de accesos no autorizados o interrupciones. La ciberseguridad también abarca la protección de dispositivos *Endpoint*s, redes y la nube.

Tendencias Emergentes:

A medida que aumentan los dispositivos conectados, inteligencia artificial y tecnologías IoT en la seguridad, proteger los datos en tránsito y en reposo se convierte en un objetivo clave teniendo como meta el desarrollo evolutivo de ciudades inteligentes (Verjel-Clavijo and Guerrero-Bayona 2023).

Las empresas deben considerar una combinación de seguridad física, ciberseguridad y seguridad informática para enfrentar las amenazas tanto físicas como cibernéticas. En la actualidad, la ciudad de Guayaquil enfrenta serios desafíos en materia de seguridad (Allan 2008), lo que hace imperativo la implementación de medidas concretas para resguardar la integridad de los negocios. Estos constituyen el pilar fundamental del comercio local y una fuente vital de empleo en la ciudad. En este contexto, resulta indispensable contar con el equipamiento adecuado y adquirir ciertos conocimientos que contribuyan a fortalecer la seguridad de los

establecimientos. Todo ello con el objetivo de satisfacer la necesidad imperante de protección y posibilitar la toma rápida de medidas ante cualquier amenaza que se perciba en el entorno comercial (Pruna, Jeada, and Jumbo 2020).

En el contexto específico de Guayaquil, se explorará la aplicación de tecnologías de punta, como la inteligencia artificial y la analítica de datos, para desarrollar un sistema integral de seguridad empresarial. Esto incluirá la implementación de cámaras inteligentes en puntos estratégicos, la elaboración de algoritmos predictivos adaptados a los patrones delictivos locales y la promoción de colaboración entre empresas y las autoridades pertinentes (Campos Merchán 2018; Preciado Oquendo 2021).

La investigación se propone no sólo como un ejercicio académico, sino como una respuesta práctica a los desafíos diarios que enfrentan los negocios en la ciudad. Se buscará proporcionar a los empresarios de Guayaquil herramientas concretas para fortalecer sus defensas ante la delincuencia, al tiempo que se promueve la colaboración activa con las instituciones locales para garantizar la seguridad de la comunidad empresarial y, por ende, la prosperidad sostenible de la ciudad.

Antecedentes

En Guayaquil, Ecuador, se han realizado investigaciones relevantes en el ámbito de la seguridad y la tecnología.

1. En el análisis expuesto en (Planv 2022) se destaca la importancia de la tecnología y la cooperación internacional para abordar los desafíos de seguridad en Guayaquil. Se menciona la visita del presidente Lasso a la UPC de La Prosperina, blanco de ataques de las llamadas mafias narco delictivas. El pragmatismo y acciones concretas son necesarias para que los ciudadanos se sientan más seguros en Ecuador.
2. Desde el Laboratorio de Investigación de ESET, se han analizado tendencias en ciberseguridad que tendrán impacto en la región en 2024. Estas incluyen el impacto de la Inteligencia Artificial (IA), el cibercrimen en aplicaciones de mensajería y campañas de espionaje (Noticias 2023).
3. El análisis de la seguridad turística en la ciudad de Guayaquil se enfoca en la seguridad turística en Guayaquil, la capital económica de Ecuador. A pesar de la convivencia con la inseguridad, se ha experimentado un año particularmente violento.
4. “La cooperación entre Ecuador y China en tecnologías de seguridad: el caso del ECU 911”: Este estudio examina la cooperación entre Ecuador y China en tecnologías de seguridad, específicamente en el contexto del sistema ECU 911. Se analiza el uso de sistemas de vigilancia y su impacto en la privacidad y las libertades individuales (Morena-Alvarez and Vila-Seoane 2023).

Estas investigaciones contribuyen al entendimiento y la mejora de la seguridad en Guayaquil, combinando tecnología y enfoques colaborativos.

Tecnologías en la seguridad de la información

La seguridad de la información es crucial para proteger activos digitales y garantizar la privacidad y confidencialidad de los datos. Algunos de los enfoques para la protección de activos digitales son:

- Agentes de seguridad de acceso a la nube (CASB): Estos proporcionan un punto de control crítico para la utilización segura y compatible de los servicios en la nube a través de múltiples proveedores. Ayudan a proteger los datos y aplicaciones en la nube.
- Detección y Respuesta de Endpoints (EDR): Estas tecnologías están diseñadas para proteger los dispositivos finales (como computadoras y dispositivos móviles) y detectar posibles infracciones. Permiten una respuesta más rápida ante amenazas.
- Enfoques sin firma para la Prevención de Endpoints: Dado que los enfoques basados en firmas son ineficaces contra ataques avanzados, se están desarrollando técnicas alternativas. Estas incluyen la protección de memoria, la prevención de exploits y el uso de aprendizaje automático para identificar y bloquear malware.
- Análisis del comportamiento del usuario y de las Entidades (UEBA): Estas tecnologías se centran en el análisis de comportamientos de usuarios y otras entidades (como *Endpoints* y aplicaciones). Proporcionan resultados más precisos para la detección de amenazas.

La ciudad de Guayaquil enfrenta una realidad desafiante en términos de seguridad empresarial, afectando la estabilidad y prosperidad de las empresas locales (Allan 2008). Este fenómeno se manifiesta en diversas problemáticas, donde la delincuencia y la inseguridad impactan directamente en la operatividad y sostenibilidad económica de los negocios. Entre las causas identificadas, se destaca el incremento de actividades delictivas, como robos y vandalismo, que amenazan la seguridad física de los establecimientos. La falta de una infraestructura de seguridad efectiva y la limitada aplicación de tecnologías avanzadas contribuyen a la vulnerabilidad de los negocios ante estas amenazas. Además, la proliferación de ciberataques y fraudes electrónicos agrega un componente significativo a este panorama, exponiendo a las empresas a riesgos financieros y pérdida de datos sensibles.

Los efectos de esta problemática son diversos y perjudiciales para la comunidad empresarial. La pérdida de inventario debido a robos y daños materiales afecta directamente la rentabilidad y la capacidad de reinversión de las empresas. La inseguridad también desanima la inversión extranjera y local, limitando el crecimiento económico y la generación de empleo. Adicionalmente, la falta de confianza en las transacciones comerciales, exacerbada por la inseguridad cibernética, obstaculiza el desarrollo de un entorno empresarial robusto (Verjel-Clavijo and Guerrero-Bayona 2023).

Esta investigación contribuye a fortalecer la seguridad comercial en la ciudad de Guayaquil mediante la implementación de tecnologías adaptadas localmente, como sistemas de vigilancia avanzados y medidas cibernéticas. Se destaca la importancia de la educación en ciberseguridad y la adopción de pagos electrónicos para reducir riesgos físicos y financieros en los negocios locales, contribuyendo así a la seguridad general de la ciudad.

En este contexto, esta investigación se propone identificar a fondo las causas subyacentes de la inseguridad empresarial en Guayaquil, considerando tanto amenazas físicas como digitales. Se busca comprender la intersección entre la falta de medidas preventivas y la necesidad urgente de fortalecer la infraestructura de seguridad mediante la aplicación de tecnologías específicas. Al abordar estas causas y comprender sus efectos,

se pretende proponer estrategias concretas y adaptadas que no solo mitiguen los riesgos, sino que también fomenten un entorno empresarial seguro y próspero en la ciudad.

Materiales y métodos

Este estudio utiliza el paradigma de investigación Mixto, permite utilizar métodos y técnicas cualitativos y cuantitativos con el objetivo de obtener, analizar y procesar los datos adecuadamente. El estudio de las tecnologías de seguridad para los negocios en Guayaquil requiere la vinculación de datos e información provenientes de expertos en seguridad, dueños y usuarios de empresas en Guayaquil y además información recopilada de fuentes teóricas, literatura especializada y actualizada en el tema.

Se utilizó el siguiente diseño teórico-metodológico:

Problema de investigación: ¿Cómo incrementar la seguridad de las empresas en la ciudad de Guayaquil?

El objeto de estudio centrado en las tecnologías de seguridad, mientras que c**ampo de acción** está relacionado con las estrategias tecnológicas para incrementar la seguridad de las empresas en la ciudad de Guayaquil. **El objetivo general** permitió investigar en los estudios que existe sobre el tema para proponer una estrategia tecnológica para incrementar la seguridad de las empresas en la ciudad de Guayaquil.

Los objetivos específicos permitieron **i**dentificar las causas de la inseguridad empresarial percibidas como amenazas físicas y cibernéticas en Guayaquil **y** seleccionar las herramientas tecnológicas de seguridad disponibles para las empresas ecuatorianas.

La hipótesis fue el camino que permitió enriquecer la investigación para sistematizar y analizar la utilización de estrategias integrales que combinen la selección de tecnologías avanzadas de seguridad física, cibernética, y de seguridad informática además de educación en ciberseguridad, y medidas específicas adaptadas a las necesidades locales de las empresas, incrementan la seguridad empresarial en la ciudad de Guayaquil en el panorama internacional y nacional.

Para la selección de los métodos se utilizó un enfoque de análisis teórico-práctico, donde se combina la revisión bibliográfica con la aplicación práctica (Yébenes 2000). Se investigan las teorías y conceptos relacionados con la seguridad y las tecnologías de seguridad, mediante el método teórico de análisis y síntesis, pero también se realizan pruebas, mediciones y se obtienen datos en entornos empresariales reales. Se utilizaron además métodos empíricos, entrevistas semi estructuradas a expertos en seguridad, líderes empresariales y profesionales del sector. También se diseñaron encuestas para recopilar datos sobre prácticas de seguridad en empresas locales.

Se utilizó además la revisión de documentos oficiales como:

1. Estadísticas locales sobre incidentes de seguridad.
2. Políticas de seguridad empresarial aplicables en Ecuador.
3. Tecnologías emergentes utilizadas por las empresas locales

La selección de la muestra fue mediante técnicas de muestreo probabilístico y no probabilístico. Se utilizó el muestreo intencional para obtener información precisa a través de expertos en seguridad (10 expertos) y se

utilizó una muestra de 75 personas entre dueños de empresas, usuarios y clientes de empresas en Guayaquil con el objetivo de obtener información referente a:

1. Datos de empresas en Guayaquil que han experimentado incidentes de seguridad.
2. Prácticas de seguridad implementadas por empresas locales.
3. Opiniones de expertos en seguridad empresarial en la región

Las figuras 1 y 2 muestran la composición de la muestra de acuerdo a las características de las empresas de los encuestados. Mostrándose una equilibrada composición en cuanto a tamaño (micro, pequeña y mediana) y en cuanto a sector (comercio, servicios, manufactura, otros).

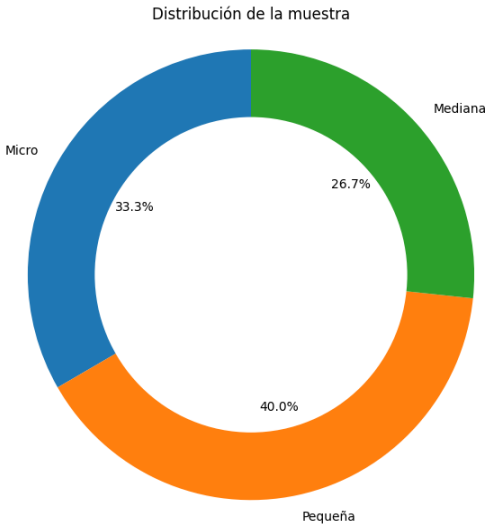

Figura 1. Distribución de la muestra según tamaño de la empresa.

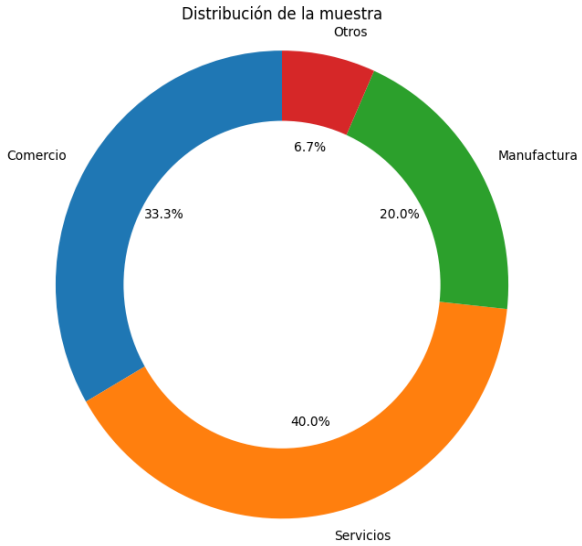

Figura 2. Distribución de la muestra según sector de la empresa.

En la propuesta de la estrategia tecnológica para incrementar la seguridad en los negocios de Guayaquil se tuvieron en cuenta los siguientes indicadores:

1. Tasas de incidentes de seguridad: permite examinar la frecuencia y el tipo de incidentes de seguridad que afectan a las empresas en Guayaquil. Esto podría incluir ataques cibernéticos, brechas de datos, malware, etc.
2. Nivel de cumplimiento normativo: permite evaluar si las empresas cumplen con las regulaciones y estándares de seguridad aplicables en Ecuador. Por ejemplo, la Ley Orgánica de Protección de Datos Personales (LOPD) y otras normativas relacionadas.
3. Inversión en tecnologías de seguridad: permite analizar el presupuesto y los recursos destinados a la implementación y mantenimiento de tecnologías de seguridad.
4. Efectividad de las soluciones de seguridad: mide la eficacia de las soluciones de seguridad utilizadas.
5. Tiempo de Detección y Respuesta a Incidentes: calcula el tiempo que lleva detectar y responder a incidentes de seguridad. Un tiempo más corto es indicativo de una mejor postura de seguridad.
6. Nivel de Conciencia y Capacitación del Personal: evalúa si los empleados están capacitados en prácticas seguras de TI.
7. Evaluación de Vulnerabilidades: realiza análisis de vulnerabilidades en sistemas, aplicaciones y redes, identificar si Existen brechas de seguridad que necesitan ser abordadas
8. Índice de Riesgo: calcula un índice de riesgo específico para cada empresa. Considera factores como la exposición a amenazas, la criticidad de los activos y la madurez de las políticas de seguridad.
9. Adopción de Tecnologías Emergentes: investiga si las empresas están adoptando tecnologías emergentes como inteligencia artificial, *blockchai*n o soluciones de seguridad en la nube.
10. Evaluación de Incidentes Pasados: analiza incidentes de seguridad anteriores y qué se puede aprender de ellos para mejorar la seguridad futura.

Resultados y discusión

El análisis y procesamiento de los datos arrojaron como resultado que Ecuador se encuentra en la séptima posición en América Latina en términos de ciberseguridad. Sin embargo, solo el 3% de las empresas ecuatorianas cuentan con herramientas que mitigan los riesgos cibernéticos en la nube. A pesar de esto, muchas grandes empresas han invertido en personal capacitado para el área de seguridad de la información y ciberseguridad. La figura 3 muestra los resultados de las encuestas acerca de los mayores desafíos o limitaciones en la implementación de tecnologías de seguridad delincuencial en las empresas de Guayaquil.

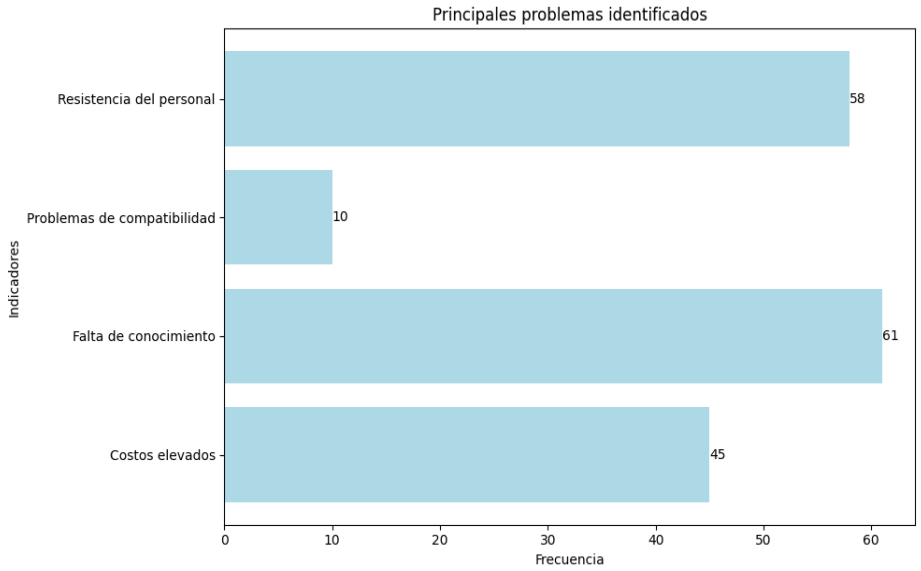

Figura 3. Desafíos en la implementación de tecnologías de seguridad delincuencial en las empresas de Guayaquil

Algunas empresas destacadas en el campo de la ciberseguridad en Ecuador incluyen:

Sertechma Cia. Ltda: ofrece soluciones de seguridad industrial, tecnología y mantenimiento locativo para empresas y edificios.
Grupo Business IT: especializado en servicios informáticos de alta tecnología y soluciones "Green IT" sostenibles.
Ecuador VirtualIT: representante de empresas como VMware y Veeam, expertos en virtualización y seguridad de la información.
Procesos IQ: ofrece servicios de transformación digital, desarrollo de software, seguridad informática y sistemas ERP.
Los datos encontrados confirman que las empresas en Guayaquil**,** utilizan diversas tecnologías de seguridad, algunas de las más utilizadas son:

1. Agentes de seguridad de acceso a la nube (CASB): proporcionan un punto de control crítico para la utilización segura y compatible de servicios en la nube a través de múltiples proveedores. Ayudan a gestionar los riesgos asociados con el uso de aplicaciones en la nube.

2. Detección y respuesta en los *Endpoints* (EDR): estas soluciones protegen los dispositivos finales (como computadoras y dispositivos móviles) y permiten detectar posibles infracciones y reaccionar de manera más rápida ante amenazas.
3. Enfoques sin firma para la prevención de Endpoints: considerando que los enfoques basados en firmas son ineficaces contra ataques avanzados, se están utilizando técnicas como la protección de memoria, la prevención de *exploits* y el aprendizaje automático para identificar y bloquear malware.
4. Análisis del comportamiento del usuario y de las entidades (UEBA): estas tecnologías proporcionan análisis centrados en el comportamiento de los usuarios y otras entidades (como *Endpoints* y aplicaciones). Esto mejora la precisión en la detección de amenazas.
5. Seguridad en la Nube: las empresas están adoptando soluciones de seguridad basadas en la nube para proteger sus datos y aplicaciones. Esto incluye cifrado, autenticación multifactor y control de acceso.
6. Reconocimiento automático de matrículas (ANPR): aunque no es exclusivo de Guayaquil, esta tecnología se utiliza para la seguridad en estacionamientos y accesos a edificios comerciales.
7. Cámaras de seguridad y sistemas de alarma: Aunque comunes en todo el mundo, estas tecnologías siguen siendo esenciales para la seguridad en negocios locales.

La tabla 1 resume las respuestas a algunas de las preguntas realizadas a los encuestados, evidenciando la predominancia de acuerdo entre los encuestados sobre la influencia que podría tener el planteamiento de incentivos o políticas desde el gobierno local, las necesidades de formación y el impacto positivo que puede tener en el crecimiento de las empresas.

Tabla 1. Resumen de los resultados de las respuestas de la muestra encuestada.

Pregunta	Respuestas posibles	Respuesta dominante
¿Consideras que el gobierno local debería ofrecer algún tipo de incentivo o apoyo para que las empresas implementen tecnologías de seguridad delincuencial?	a) Sí, b) No, c) No estoy seguro/a	b) Sí (83%)
¿Te gustaría recibir asesoramiento o información adicional sobre las tecnologías de seguridad delincuencial disponibles en el mercado?	a) Sí, b) No, c) Tal vez	b) Sí (94%)
¿En qué medida crees que la implementación de tecnologías de seguridad delincuencial puede impactar positivamente en el crecimiento y la estabilidad de tu empresa?	a) Muy positivamente, b) Positivamente, c) Neutro, d) Negativamente, e) Muy negativamente	a) Muy positivamente (89%)

Estrategia tecnológica para incrementar la seguridad de las empresas en Guayaquil

Objetivo: Incrementar la seguridad de los negocios o empresas en Guayaquil mediante la adopción de diferentes tecnologías de seguridad combinadas de manera que permita abordar los riesgos y proteger tanto física como digitalmente los bienes y recursos.

Acciones que pueden ejecutarse en las empresas.

1. Configuración de servicios y altas de usuarios de manera segura e implementación de mejores prácticas para garantizar operaciones seguras.

2. Evaluación de los riesgos específicos para los negocios y priorización de la seguridad de los activos clave.
3. Aprovechamiento de la arquitectura segura de la nube y disminución de la exposición al riesgo mediante proveedores confiables.
4. Capacitación al personal de las empresas en cuestiones de seguridad, haciendo énfasis en las tecnologías más actuales.
5. Educación sobre la necesidad de la seguridad y protección de los datos, tanto en los dispositivos como en la red.
6. Instalación de equipos de seguridad física como vallas, puertas con cerradura, circuitos cerrados de televisión y detectores de movimiento.
7. Implementación de soluciones tecnológicas como sistemas de vigilancia y alarmas conectadas con entidades de seguridad competentes.
8. Implementación de un sistema eficiente para gestionar llamadas de emergencia y coordinar respuestas rápidas ante situaciones críticas.
9. Utilización de tecnología de reconocimiento facial para identificar personas y prevenir el acceso no autorizado a instalaciones o áreas sensibles.
10. Instalación de megáfonos y cámaras de seguridad en lugares estratégicos para monitorear y disuadir actividades delictivas.
11. Proporcionar a los empleados y clientes una forma rápida de solicitar ayuda en caso de emergencia.
12. Reclutamiento de receptores de llamadas, psicólogos y médicos para manejar situaciones de crisis de manera efectiva.
13. Utilización de drones equipados con inteligencia artificial para realizar recorridos perimetrales y detectar intrusos en las instalaciones. Estos dispositivos pueden ser programados para patrullar áreas críticas y proporcionar una vista aérea en tiempo real.
14. Implementación de sistemas de acceso basados en aplicativos móviles. Estos candados electrónicos permiten activar y desactivar cerraduras sin necesidad de contacto físico, mejorando la seguridad en edificios y oficinas.
15. Actualización de los sistemas de videovigilancia con algoritmos de inteligencia artificial. Estos algoritmos pueden detectar patrones anómalos, reconocer rostros y alertar sobre posibles amenazas.
16. Implementación de sistemas de reconocimiento biométrico para el acceso a áreas restringidas. Huellas dactilares, reconocimiento facial o escaneo de retina son opciones seguras y eficientes.
17. Utilización de cámaras de seguridad conectadas a la red para monitoreo remoto. Almacenamiento de las grabaciones en la nube para evitar pérdida de datos y acceder a ellos desde cualquier ubicación.
18. Capacitación regular sobre ciberseguridad y buenas prácticas a tus empleados. La concienciación es clave para prevenir ataques y proteger la información sensible.
19. Realización de auditorías periódicas para evaluar la efectividad de las medidas de seguridad implementadas. Identifica vulnerabilidades y toma acciones correctivas.

20. Colaboración con el Clúster de Transformación Digital de Guayaquil, que busca impulsar cambios tecnológicos en beneficio de las empresas. La colaboración y el intercambio de conocimientos son esenciales.

Recursos

1. Drones de Vigilancia
2. Candados Electrónicos y duros
3. Medios de protección física
4. Infraestructura robusta
5. Diseño de una infraestructura sólida que incluya servidores, computadoras, cámaras, redes y componentes de comunicación seguros.
6. Considera la arquitectura general de la solución y la protección de datos.

Evaluación de la estrategia

1. Establecimiento de Métricas y reportes de seguridad para evaluar la efectividad de la estrategia.
2. Generación de reportes para monitorear el estado de la seguridad.

Esta estrategia tecnológica debe adaptarse continuamente a las amenazas cambiantes y estar alineada con los objetivos comerciales específicos de cada empresa. La inversión en tecnología y la formación constante son inversiones clave para proteger los activos empresariales y garantizar la continuidad del negocio.

Desafíos que las tecnologías de seguridad enfrentan en Ecuador y en el mundo actual

- Rápida evolución tecnológica: el constante avance tecnológico presenta oportunidades, pero también desafíos. Las soluciones de seguridad deben adaptarse rápidamente a las nuevas amenazas y vulnerabilidades.
- Ciberataques y amenazas persistentes: los ciberdelincuentes emplean tácticas cada vez más sofisticadas. La seguridad debe estar un paso adelante para proteger datos, redes y sistemas.
- Privacidad y protección de datos: la creciente cantidad de datos personales y su manejo plantean desafíos en términos de privacidad y cumplimiento normativo (como el RGPD en Europa).
- Inteligencia artificial y automatización: si bien estas tecnologías mejoran la seguridad, también pueden ser utilizadas por atacantes. La detección de amenazas debe evolucionar para enfrentar esta realidad.
- Conectividad y dispositivos IoT: la proliferación de dispositivos interconectados aumenta la superficie de ataque. La seguridad debe abordar la diversidad de dispositivos y sus vulnerabilidades.
- Escasez de talento en ciberseguridad: la demanda de expertos en ciberseguridad supera la oferta. Capacitar y retener profesionales competentes es un desafío constante.
- Ataques a infraestructuras críticas: las infraestructuras esenciales (energía, transporte, salud) son objetivos atractivos para ciberataques. Protegerlas es crucial.
- Desafíos geopolíticos y ciberespionaje: las tensiones entre países pueden manifestarse en ciberataques. La seguridad debe considerar estos aspectos.
- Educación y concienciación: usuarios y empleados deben comprender las buenas prácticas de seguridad. La concienciación es vital para prevenir ataques.
- Balance entre seguridad y usabilidad: implementar medidas de seguridad sin afectar la experiencia del usuario es un desafío constante.

De manera general, las tecnologías de seguridad deben adaptarse, innovar y colaborar para enfrentar estos desafíos y proteger nuestros sistemas y datos.

Conclusiones

El diseño teórico-metodológico propuesto permitió desarrollar la investigación con éxito y la selección de los métodos y técnicas permitió obtener la información oportuna en cada caso.

Se identificaron las causas de la inseguridad empresarial percibidas como amenazas físicas y cibernéticas en Guayaquil. Entre las causas identificadas, se destaca el incremento de actividades delictivas, como robos y vandalismo, que amenazan la seguridad física de los establecimientos. La falta de una infraestructura de seguridad efectiva y la limitada aplicación de tecnologías avanzadas contribuyen a la vulnerabilidad de los negocios ante estas amenazas. Además, la proliferación de ciberataques y fraudes electrónicos agrega un componente significativo a este panorama, exponiendo a las empresas a riesgos financieros y pérdida de datos sensibles.

Se seleccionaron las herramientas tecnológicas de seguridad disponibles para las empresas ecuatorianas de acuerdo a la disponibilidad, los conocimientos y las necesidades de cada empresa. Se propuso una estrategia tecnológica para incrementar la seguridad de las empresas en Guayaquil. La estrategia integral combina la selección de tecnologías avanzadas de seguridad física, cibernética, y de seguridad informática, además de educación en ciberseguridad, y medidas específicas adaptadas a las necesidades locales de las empresas para incrementar la seguridad empresarial en la ciudad de Guayaquil.

La estrategia tecnológica para incrementar la seguridad de las empresas en Guayaquil fue diseñada teniendo la estructura: Objetivo, Actividades, Recursos y Evaluación de la estrategia. La estrategia propuesta se sustentó en:

- Un enfoque integral, la seguridad no debe limitarse a una sola área. La colaboración entre expertos en seguridad informática, profesionales de la seguridad física y abogados especializados es esencial.
- Tecnología adaptativa: las soluciones tecnológicas deben adaptarse a las necesidades específicas de cada empresa. No existe una solución única para todos los casos.
- Educación continua: capacitación constante del personal es crucial. La concienciación sobre ciberseguridad y el uso adecuado de las herramientas tecnológicas son fundamentales.
- Evaluación periódica: las auditorías de seguridad tecnológica deben realizarse regularmente para identificar vulnerabilidades y aplicar mejoras.
- Colaboración externa: la cooperación con organizaciones como el Clúster de Transformación Digital de Guayaquil puede proporcionar conocimientos valiosos y oportunidades de crecimiento.
- La inversión en tecnología y la implementación de estrategias sólidas son esenciales para proteger los negocios y garantizar la confianza de los clientes en el entorno empresarial de Guayaquil.

Referencias

Allan, Henry. 2008. “Reordenamiento Urbano, Seguridad Ciudadana Y Centros de Tolerancia En Quito Y Guayaquil,” June. https://repositorio.flacsoandes.edu.ec/handle/10469/2306.

Campos Merchán, L. X. 2018. “Cloud Computing Como Estrategia Tecnológica Para Las Pymes Caso Práctico: Empresa Noviatat SA de La Ciudad de Guayaquil.”

https://dspace.uniandes.edu.ec/handle/123456789/8518.

López, L. C. J. 2020. "Seguridad Ciudadana Y Tecnología: Uso, Planeación Y Regulación de La Videovigilancia En Latinoamérica." *Dikê, Revista de Investigación En Derecho*. http://portal.amelica.org/ameli/journal/48/481820001/html/.

Morena-Alvarez, Carla, and Maximiliano Vila-Seoane. 2023. "La Cooperación Entre Ecuador Y China En Tecnologías de Seguridad: El Caso Del ECU 911." *URVIO. Revista Latinoamericana de Estudios de Seguridad*, June. https://doi.org/10.17141/urvio.36.2023.5847.

Noticias, Ecuador. 2023. "Tendencias en Seguridad Informática para 2024." Ecuador Noticias. December 9, 2023. https://ecuadornoticias.com/tendencias-en-seguridad-informatica-para-2024/.

Pantoja, N. D., and S. A. Donado. 2020. "Selección de Indicadores Para La Implementación de Un IDS En PYMES." *Revista Ibérica de*. search.proquest.com. https://search.proquest.com/openview/ddddee94d23b4c4a6d43646933893d01/1?pq-origsite=gscholar&cbl=1006393.

Planv. 2022. "2023: el año de la tecnología y cooperación internacional en materia de seguridad." Plan V. December 27, 2022. https://www.planv.com.ec/historias/analisis/2023-el-ano-la-tecnologia-y-cooperacion-internacional-materia-seguridad.

Preciado Oquendo, K. L. 2021. "Importancia de La ISO 27001 En Las Pymes de Guayaquil: Caso de Estudio Transnave." https://dspace.ups.edu.ec/handle/123456789/20935.

Pruna, Francisco Xavier Jurado, Pamela Valeria Yarad Jeada, and Joe Luis Carrión Jumbo. 2020. "Análisis de las características del sector microempresarial en latinoamérica y sus limitantes en la adopción de tecnologías para la seguridad de la información." *REVISTA CIENTÍFICA ECOCIENCIA* 7 (1): 1–26.

Sánchez, R. D. 2023. "Marco Mínimo de Ciberseguridad Para PYMEs En El Contexto de La Industria 4.0." https://ciateq.repositorioinstitucional.mx/jspui/handle/1020/659.

Seminario, L. S. 2023. "Inseguridad Ciudadana: Problema Social, Latente Que Afecta a Nivel de Latinoamérica." *Revista de Climatologıa Edición Especial Ciencias*. https://rclimatol.eu/wp-content/uploads/2023/12/Articulo-CS23-Laura-S-1.pdf.

Verjel-Clavijo, G. A., and A. M. Guerrero-Bayona. 2023. "Ciudad Inteligente: Mejoramiento de La Seguridad Ciudadana a Través Del Uso de Nuevas Tecnologías." *Revista Ingenio*. https://revistas.ufps.edu.co/index.php/ingenio/article/view/3510.

Yébenes, Juan Antonio Valor. 2000. "Metodología de La Investigación Científica." https://books.google.com/books?hl=es&lr=&id=SmdxEAAAQBAJ&oi=fnd&pg=PT45&dq=enfoque+te%C3%B3rico-pr%C3%A1ctico+%2B+metodo+investigacion&ots=O02xsBG9k3&sig=VoWC877HIBaXDNXnBMMikTCjj2A.