UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA
Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Propuesta de Herramienta de Ciberseguridad fundamentada en un Chatbot basado en la ISO 27001 para la auditoría de buenas prácticas en Servidores Windows y Linux para las Pymes
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo Sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor/a:
Javier Jacinto Navarro Estrella
Tutor/a:
PhD. Renato Toasa PhD. Maryory Urdaneta

Quito – Ecuador

2025

APROBACIÓN DEL TUTOR

Yo, Renato Mauricio Toasa Guachi con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de Herramienta de Ciberseguridad fundamentada en un Chatbot basado en la ISO 27001 para la auditoría de buenas prácticas en Servidores Windows y Linux para las Pymes.

Elaborado por: Javier Jacinto Navarro Estrella, de C.I: 1717635062, estudiante de la Maestría en Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., Septiembre de 2025

Firmado electrónicamente por:
RENATO MAURICIO TOASA GUACHI
Validar únicamente con FirmaEC

_____

Firma

APROBACIÓN DEL TUTOR

Yo, Maryory Urdaneta Herrera con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de Herramienta de Ciberseguridad fundamentada en un Chatbot basado en la ISO 27001 para la auditoría de buenas prácticas en Servidores Windows y Linux para las Pymes.

Elaborado por: Javier Jacinto Navarro Estrella, de C.I: 1717635062, estudiante de la Maestría en Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., Septiembre de 2025

MARYORY URDANETA HERRERA

Firmado digitalmente por MARYORY URDANETA HERRERA
Fecha: 2025.09.19 00:22:26 -05'00'

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Javier Jacinto Navarro Estrella con C.I: 1717635062, autor/a del proyecto de titulación denominado: Desarrollo de una Herramienta de Ciberseguridad basada en un Chatbot para la auditoría de buenas prácticas en Servidores Windows y Linux para las Pymes. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., Septiembre de 2025

Javier Jacinto Navarro Estrella
Time Stamping Security Data

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Las Pymes se caracterizan por ser unidades económicas con una estructura organizativa limitada (tanto en términos de personal como de recursos financieros y tecnológicos) ubicadas a nivel nacional, que entre otras cosas se caracterizan por sus significativas limitaciones al momento de implementar soluciones robustas en áreas críticas como la ciberseguridad lo que las convierte en blancos vulnerables ante amenazas informáticas (Bustillos y Rojas, 2022).

En el Ecuador existen aproximadamente 1.168.688 PYMES, que es conjunto generan 1.582.036 empleos. Dentro de este grupo, las microempresas representan la mayoría con 1.092.126 unidades y 652.622 trabajadores. Les siguen las pequeñas empresas, con 60.113 organizaciones y 447.838 empleados, mientras que las medianas empresas tipo "A" alcanzan 9.806 unidades y 255.287 trabajadores. Finalmente, las medianas tipo "B" suman 6.643 empresas y 226.289 empleados (INEC,2024).

Como parte de la constante transformación digital las Pymes afrontan crecientes desafíos en materia de ciberseguridad ya que a medida que digitalizan sus procesos y almacenan información sensible en servidores con sistemas operativos Windows y Linux, se vuelven blancos cada vez más frecuentes de ciberataques como accesos no autorizados, explotación de vulnerabilidades o robo de datos (Bustillos y Rojas, 2022)

A partir de la pandemia generada en el 2020 se popularizó el desarrollo de chatbots como herramientas que permiten simular conversaciones con usuarios humanos mediante interfaces de texto que con el paso del tiempo y el exponencial desarrollo tecnológico se han integrado con técnicas de inteligencia artificial que les permite comprender el contexto, interpretar intenciones, aprender de las interacciones y ofrecer respuestas más precisas y personalizadas (Wunsch, 2022).

En este escenario, surge la necesidad de desarrollar herramientas accesibles y automatizadas para evaluar el cumplimiento de buenas prácticas en ciberseguridad dentro de los entornos operativos de servidores mediante la implementación de chatbots inteligentes que sean capaces de interactuar con los usuarios mediante lenguaje natural y asistirlos en tareas técnicas como la verificación de configuraciones seguras, la revisión de permisos, el análisis de logs o la identificación de vulnerabilidades.(Peña et al., 2021).

En este sentido, el uso de un chatbot para realizar estas evaluaciones representa una innovación tecnológica aplicable al entorno de las Pymes cuyo enfoque basado en software de

código abierto y diseñado específicamente para entornos empresariales con limitaciones presupuestarias, se vuelve una alternativa eficiente, escalable y de fácil adopción que permitirá automatizar procedimientos repetitivos, reducir errores humanos y facilitar la implementación de medidas correctivas de forma oportuna.

Problema de investigación

La limitada disponibilidad de recursos técnicos y humanos especializados en el que se desenvuelven las PYMES en el Ecuador sumado a la alta complejidad para implementar soluciones de seguridad informática que requieren conocimientos avanzados y altos costos de licenciamiento hace que este tipo de empresas operen sus equipos aplicando las configuraciones por defecto dadas por el fabricante, sin realizar evaluaciones periódicas de seguridad ni aplicar controles adecuados para prevenir accesos no autorizados, explotación de servicios inseguros o fuga de información (Bustillos y Rojas, 2022).

Esta situación las convierte en objetivos atractivos para los ciberdelincuentes, quienes aprovechan precisamente estas debilidades para comprometer sus sistemas, lo que genera la necesidad de desarrollar herramientas innovadoras, automatizadas y de fácil uso, que permitan a las PYMEs evaluar y reforzar sus prácticas de ciberseguridad sin depender exclusivamente de expertos externos.

Objetivo general

Desarrollar una Herramienta de Ciberseguridad fundamentada en un Chatbot basado en la ISO 27001 para la auditoría de buenas prácticas en Servidores Windows y Linux para las Pymes.

Objetivos específicos

- Contextualizar los fundamentos teóricos sobre ciberseguridad, auditoría de sistemas, servidores Windows y Linux, así como el uso de chatbots e inteligencia artificial como herramientas tecnológicas aplicadas a la gestión de seguridad.
- Diagnosticar el nivel de cumplimiento de buenas prácticas de ciberseguridad en servidores Windows y Linux dentro de las PYMEs.
- Desarrollar una herramienta basada en un chatbot inteligente que permita realizar auditorías automatizadas de buenas prácticas en la configuración y mantenimiento de servidores Windows y Linux en PYMEs.
- Validar la efectividad de la herramienta mediante criterio de especialistas en la identificación de vulnerabilidades y el fortalecimiento de la gestión de la seguridad informática.

Vinculación con la sociedad y beneficiarios directos:

La vinculación con la colectividad de este proyecto de titulación se llevó a cabo mediante la implementación y validación de la herramienta de ciberseguridad basada en un chatbot inteligente para las PYMEs. Para ello, se aplicaron encuestas y entrevistas al personal responsable de la gestión de TI, con el fin de conocer su percepción sobre la utilidad y facilidad de uso de la herramienta. Asimismo, se realizó la validación de expertos en ciberseguridad, quienes evaluaron la pertinencia técnica y metodológica de la propuesta. Estos procesos permitieron valorar la efectividad de la herramienta y fortalecer su aplicación práctica en entornos reales. La evidencia de estas actividades se incluye en los anexos del presente documento.

El impacto en la sociedad se la realizará mediante acciones que propicien un ecosistema empresarial más seguro que fomente la confianza en los servicios digitales, estimule el comercio electrónico, minimice las pérdidas económicas por incidentes de seguridad y contribuya a una economía más resiliente frente a delitos informáticos.

Los beneficiarios directos de este proyecto serán:

- Las PYMEs participantes, que recibirán la herramienta y capacitación para mejorar la seguridad de sus servidores Windows y Linux.
- Los administradores de sistemas y personal de TI de las PYMEs, quienes contarán con una herramienta automatizada para realizar auditorías periódicas de seguridad sin requerir conocimientos avanzados en ciberseguridad.
- Los propietarios y gerentes de las PYMEs, que verán reducidos los riesgos operativos y financieros derivados de incidentes de seguridad informática.
- Para la revisión del seminario web se adjunta link de conferencia. https://drive.google.com/file/d/1LQvdzSgjkmoF95KPYjY_0r_8bAbN0fVO/view?usp=drive_link

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

1.1.1 Estado del arte

La investigación de Tejedo (2024) describe el desarrollo de GPT-SOC, un chatbot basado en inteligencia artificial diseñado para asistir a analistas de ciberseguridad en centros de operaciones (SOC), el cual para su funcionamiento integra herramientas de verificación de IPs, dominios y alertas de seguridad, lo que le permite automatizar tareas repetitivas y mejorar la investigación de incidentes ocasionados en servidores tanto Linux como Windows, los resultados alcanzados permiten concluir que GPT-SOC facilita la gestión de alertas, la identificación de amenazas y la toma de decisiones rápidas, reduciendo el tiempo de respuesta y aumentando la precisión en la detección de ataques.

El estudio realizado por Álvarez (2024) se centró en realizar una revisión sistemática (2018–2023) sobre técnicas de IA aplicadas a la ciberseguridad, durante el procesos se identifican 30 estudios relevantes que destacan el uso de IA, aprendizaje profundo, incremental y automático utilizadas para mitigar amenazas como ataques DoS, malware y ransomware, los resultados alcanzados le permitieron al autor demostrar la manera en que los sistemas inteligentes pueden fortalecer la defensa cibernética mediante detección y respuesta automatizada.

La investigación realizada por Moran y Chávez (2021) se centró en realizar una revisión sistemática de 47 estudios sobre IA-chatbots, incluyendo su potencial en gestión de información, automatización de tareas y atención personalizada, durante la exploración se identificaron varios retos éticos, técnicos y de supervisión que deben sr considerados al momento del desarrollo de un chatbots basado en inteligencia artificial, finalmente sus resultados le permitieron al autor proporcionar un marco conceptual útil para desarrollar chatbots aplicados a la ciberseguridad, especialmente en entornos educativos y administrativos.

1.1.2 Ciberseguridad

Es un campo multidisciplinario de las tecnologías de la información enfocado en brindar protección a los sistemas informáticos, redes, programas y datos contra ataques a su integridad, alteraciones o robos con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información (Lores, 2024) como se detalla en la figura 1.

Los descrito en la Figura 1 permiten asegurar que los datos estén resguardados, sean precisos y estén disponibles únicamente para los usuarios autorizados en el momento que se requieran, cuya garantía ha generado que la ciberseguridad se vuelva un componente esencial en todos los

sectores productivos, especialmente en el contexto de la transformación digital, donde el volumen de información sensible gestionada electrónicamente ha aumentado considerablemente.

Figura 1
Pilares fundamentales para la protección.

Nota. El gráfico muestra los conceptos de los 3 pilares para la protección. Tomado de Cano (2022)

A medida que las amenazas cibernéticas se vuelven más complejas y ocurren con mayor frecuencia, la ciberseguridad ha tenido que avanzar más allá de usar solo antivirus o contraseñas. Ahora incluye sistemas para detectar intrusos, firewalls más sofisticados, protección mediante cifrado de datos, análisis del comportamiento de los usuarios y planes para responder rápidamente en caso de un ataque. (Mullo, 2024).

Según el (NIST, 2023), la ciberseguridad no solo consiste en proteger la tecnología, sino también en gestionar los riesgos de manera completa. Esto incluye establecer políticas en la organización, sensibilizar al personal, hacer auditorías constantes y cumplir con normas internacionales como la ISO/IEC 27001, que guía la implementación de sistemas para proteger la información.

En el caso de las PYMES, el reto es mayor porque tienen pocos recursos y no cuentan con personal experto para aplicar medidas de seguridad avanzadas, por eso, suelen ser objetivo frecuente de ataques como el phishing, ransomware y la explotación de fallas en su sistema (Ramirez , 2022). Para estas empresas, usar herramientas que funcionan de forma automática y

son fáciles de usar es una buena opción para mejorar su protección frente a las amenazas digitales que cada día aumentan.

Finalmente, la ciberseguridad actual no solo reacciona ante problemas, sino que busca adelantarse a ellos y reforzar la capacidad de recuperación. Esto implica el uso continuo de herramientas para detectar ataques, supervisar todo constantemente y aplicar un modelo de confianza mínima, que ayuda a prever riesgos, disminuir el tiempo en que los sistemas están expuestos y mantener el funcionamiento del negocio sin interrupciones (Puerta y Giraldo, 2021).

1.1.3 Buenas prácticas en servidores

Las buenas prácticas, en un contexto, son un conjunto de normas técnicas y operativas recomendadas que se utilizan para asegurar un funcionamiento seguro, racional y estable de los sistemas informáticos para minimizar los riesgos, los ataques en falta de seguridad, optimizar la eficacia y administrar mejor los recursos tecnológicos disponibles (Rubio, 2022).

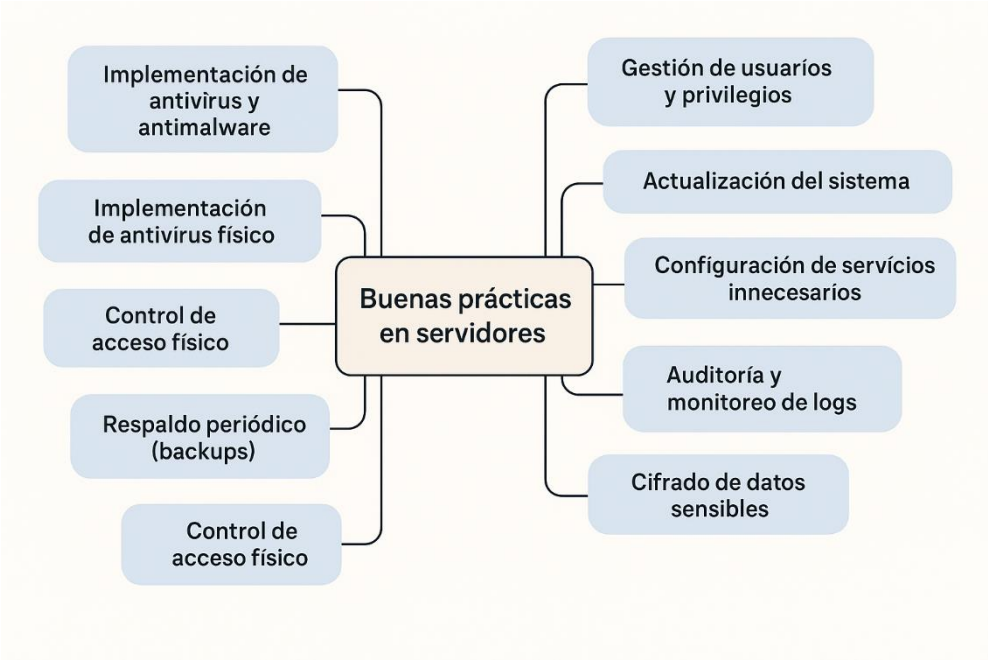
A continuación, se enlistan algunas de las principales buenas prácticas en servidores que deben ser consideradas:

- **Gestión de usuarios y privilegios:** Configurar cuentas con solo los permisos importantes y limitar el uso de cuentas con permisos elevados.
- **Actualización del sistema:** Asegurarse de que el sistema operativo y los servicios estén siempre al día para solucionar fallas de seguridad conocidas.
- **Configuración de firewall:** Implementar y mantener reglas de firewall que restrinjan el tráfico a lo estrictamente necesario.
- **Desactivación de servicios innecesarios:** Identificar y deshabilitar servicios o puertos que no estén en uso para reducir la superficie de ataque.
- **Auditoría y monitoreo de logs:** Revisar periódicamente los registros del sistema para detectar accesos o actividades sospechosas.
- **Cifrado de datos sensibles:** Utilizar protocolos seguros (como HTTPS, SSH y VPN) y cifrado en disco o archivos para proteger la información confidencial.
- **Respaldo periódico (backups):** Implementar mecanismos de respaldos regulares y verificar su integridad.
- **Control de acceso físico:** Asegurar que los equipos sensibles se encuentren en entornos físicos protegidos contra accesos no autorizados.
- **Implementación de antivirus y antimalware:** Utilizar software de protección actualizado que permita detectar y mitigar amenazas conocidas y emergentes.

- **Políticas de contraseñas seguras**: Exigir contraseñas robustas y establecer mecanismos de expiración y bloqueo ante intentos fallidos.

Figura 2

Mapa conceptual de buenas prácticas en servidores



Nota. El mapa conceptual sintetiza las principales prácticas recomendadas para garantizar la seguridad, disponibilidad y eficiencia en servidores Windows y Linux.

La operación práctica y fluida de estas recomendaciones no debe verse como un proceso independiente, sino más bien como un componente de una estrategia global en la gestión de la seguridad de la tecnología de la información, el éxito en este aspecto depende de la formulación de políticas institucionales bien definidas, la capacitación del personal designado para la gestión de servidores y la realización de auditorías periódicas para evaluar el impacto real de los controles instituidos. Según Lores, (2024) la seguridad del servidor debe cumplir con estándares internacionales como ISO/IEC 27001 o los CIS Benchmarks, ya que estos marcos proporcionan un conjunto de estándares que ayudan a las organizaciones a establecer configuraciones uniformes y minimizar el riesgo de explotación de vulnerabilidades.

Por otro lado, la creciente complejidad de las amenazas cibernéticas ha puesto de manifiesto la necesidad de adoptar mecanismos de automatización y monitoreo continuo para aumentar las defensas tradicionales. Herramientas como SIEM (Gestión de Información y Eventos de Seguridad) y sistemas de gestión de parches permiten el monitoreo continuo de eventos críticos, la detección oportuna de anomalías y la iniciación de respuestas efectivas (Chinthala, 2024) así las prácticas de registros de servidor no solo ayudan a defender la infraestructura tecnológica,

sino que también proporcionan continuidad del negocio que, a su vez, mejora la confianza de los clientes y socios estratégicos en la resiliencia digital de la empresa.

1.1.4 Auditoría de sistemas

Un procedimiento sistemático y detallado que evalúa, estudia y examina el funcionamiento, la seguridad, la efectividad y el cumplimiento de los sistemas informáticos de una organización con el propósito de determinar si los activos tecnológicos se están gestionando de manera eficiente y si los controles prescritos están funcionando, y si la infraestructura tecnológica cumple con las políticas y normas internas vigentes y las externas (Gómez y Boumadan, 2025).

Es seguro indicar que esta auditoría abarca no solo un análisis crítico de los sistemas de hardware y software, sino también un examen cruzado igualmente importante de políticas, procedimientos, prácticas operativas, medidas de acceso y seguridad informática suficientes para detectar configuraciones débiles, riesgos operativos y deficiencias, mejorar (Llugsa et al., 2021).

En el contexto de los pasos de ciberseguridad relacionados con la auditoría de sistemas, dichos sistemas de auditoría son críticos para:

- Detectar posibles brechas de seguridad antes de que sean explotadas
- Establecer acciones correctivas o preventivas
- Tener una visión objetiva sobre el estado de su infraestructura tecnológica
- Promover la transparencia y la mejora continua.

La auditoría de sistemas se subdivide en tipos en función de su alcance y objetivos por sí solos, cada tipo de auditoría tiene como objetivo lograr una meta específica; por ejemplo, la auditoría de cuentas busca determinar el grado de cumplimiento de los requisitos de norma internacional como el ISO/IEC 27001 y el NIST SP 800-53, la auditoria ‘operacional’ busca determinar el grado equilibrio de valor y eficiencia de los procesos en los sistemas fundamentales de comercio tecnológico, y la auditoria forense busca en evidencia determinar la causa de una brecha de seguridad lo que se denomina un “successful or unsuccessful security breach” (Cano, 2022). Como enunciado, cada tipo de auditoria añade valor de dentro el sistema de gestión de seguridad de la información.

El avance de la digitalización ha conllevado la formulación de nuevos estratos organizacionales tendientes a maximizar la rentabilidad de las empresas mediante la implementación del e-business. El desarrollo del e-business permite la optimización del control de las relaciones a través de la automatización de la manera mediante la cual los usuarios están

en contacto con la empresa. Esto requiere la gestión de la información a través del internet mediante la gestión de los perfiles para obtener información y la gestión de herramientas que permitan a los usuarios ofrecer servicios a la entidad y mediante servicios propios a las empresas, los cuales requieren procesamiento automatizado. Esto, en todo el flujo, permite agregar valor a los intercambios de documentos y automatizar el procesamiento de cualquier solicitud para ser atendidos. El business presume innovación, integración de tecnologías para maximizar la productividad empresarial, la satisfacción del cliente y la disminución de costos operativos (Martínez, 2022)

En lo siguiente, la Figura 3 muestra los pasos principales en una auditoría de sistemas, subdivididos en tres pasos que deben realizarse en secuencia: planificación y programación, realización de la auditoría y reporte con el plan de acción. Estos pasos corresponden a un conjunto de acciones que, tomadas en conjunto, permiten alcanzar los objetivos de la auditoría, asistiendo en la identificación de riesgos, evaluación del control y la formulación de propuestas destinadas a mejorar la efectividad y eficiencia en las infraestructuras informáticas.

Figura 3
Fases de la Auditoria

Nota. La figura ilustra las fases principales de una auditoría de sistemas: planeación, ejecución e informe con plan de acción, (Sanchez, 2022).

1.1.4.1 Planeación y programación

La fase inicial se centra en definir los objetivos, el alcance, los criterios de evaluación y los enfoques que empleará la auditoría. En esta fase, se seleccionan los sistemas, procesos y/o áreas a evaluar, se definen los recursos necesarios y se elabora un cronograma de actividades. Como señala Beltran (2023), la planificación es importante porque ayuda al auditor a determinar los riesgos potenciales, priorizar los controles a revisar y garantizar que la auditoría se realice de manera eficiente, ordenada y confiable.

1.1.4.2 Ejecución de la auditoría

"Y luego se lleva a cabo la recopilación de información y el análisis de información a través de herramientas como entrevistas, análisis de documentos, pruebas de penetración y la recolección de registros del sistema. El análisis tiene como objetivo asegurarse de que los controles implementados funcionen y que los sistemas tecnológicos funcionen en línea con las políticas de la empresa y los estándares internacionales." Durante la ejecución, se identificarán diversas vulnerabilidades, brechas en la seguridad y mejoras que serán registradas para su futura rectificación forme y plan de acción (Alvarez, 2024)

La última fase es un análisis de un informe de auditoría que captura los resultados y los organiza por nivel de riesgo (alto, medio, bajo). El informe luego proporciona sugerencias para abordar los problemas identificados dentro de la auditoría. El informe continúa incluyendo un plan de acción que detalla las partes responsables, las restricciones de tiempo y el presupuesto asignado a cada acción correctiva. Además, Bustillos y Rojas (2022), mencionan que el énfasis de esta fase no es solo identificar debilidades dentro de la organización, sino fomentar un ambiente en el que la organización prospere con la idea de mejora continua.

Las fases anteriores ayudan a confirmar que la auditoría de sistemas es un proceso ordenado, claro y beneficioso para la entidad, que permite el descubrimiento temprano de vulnerabilidades y el reforzamiento de la seguridad, tanto a nivel informático como operacional.

1.1.5 Chatbot

Un bot es una aplicación que se crea para imitar la conversación de una persona a través de texto o voz y para permitir una respuesta automatizada a los usuarios teniendo conversaciones basadas en reglas predeterminadas, y también utilizando reglas sofisticadas de inteligencia artificial, particularmente en el procesamiento del lenguaje natural (NLP), que permiten a un bot entender las intenciones de los usuarios, derivar lecciones de un conjunto dado de interacciones y ser contextualmente versátil(Bustillos y Rojas, 2022).

Debido a su crecimiento constante y amplia aceptación por proporcionar respuestas rápidas, reducir la carga de trabajo operativa humana, estar disponibles 24/7 y mejorar la experiencia del usuario, este tipo de herramientas ha ganado prominencia en múltiples industrias, incluyendo servicio al cliente, comercio electrónico, educación y atención médica(Aquino, 2023).

Este tipo de herramientas han incursionado en el ámbito empresarial llegando a demostrar que pueden ser utilizados como asistentes virtuales para ejecutar procesos automatizados,

brindar soporte técnico, generar reportes o realizar auditorías en sistemas informáticos; en este sentido, su implementación representa una solución eficiente y escalable, especialmente útil para organizaciones con recursos limitados que buscan mejorar su gestión operativa mediante herramientas digitales inteligentes (Casares, 2023).

1.1.6 Inteligencia Artificial (IA)

La IA es una rama de la informática centrada en el desarrollo de algoritmos capaces de realizar tareas que para su correcta ejecución requieren de la intervención humana como el aprendizaje, el razonamiento, la resolución de problemas y la toma de decisiones con el propósito de dotar a las máquinas la capacidad de emular comportamientos inteligentes que les permitan adaptarse a diferentes entornos y situaciones (Llugsa et al., 2021).

La inteligencia artificial aplica campos como las matemáticas, la biometría, la neurociencia y la lingüística computacional para idear y emplear técnicas como el aprendizaje automático, las redes neuronales NP y las Redes Neuronales Artificiales (ANN), estas técnicas permiten que los modelos procesen e integren datos diversos, aprendan de patrones variados, así como correlacionen respuestas o acciones basadas en esos patrones.

Debido a lo anterior, en el siglo XXI, hay una amplia aceptación y aplicación de la inteligencia artificial en diferentes sectores como la medicina, la robótica, los servicios financieros, la tecnología de la información, y especialmente en la ciberseguridad, donde ayuda en la detección más rápida y precisa de amenazas, la automatización de auditorías, la respuesta a incidentes y la mejora de sistemas de defensa.

Además de las muchas aplicaciones tecnológicas, la inteligencia artificial plantea un escrutinio ético y social que debe abordarse durante su desarrollo y despliegue, algunos problemas fundamentales son garantizar la responsabilidad algorítmica, mitigar los sesgos discriminatorios en los datos de entrenamiento que pueden llevar a decisiones discriminatorias, y abogar por una IA responsable que proteja la privacidad y las libertades civiles de los usuarios. Como dice Alvarez, tales problemas han llevado al desarrollo de marcos regulatorios y pautas de mejores prácticas que intentan equilibrar las tecnologías emergentes y la protección social.

Dentro del ámbito de la seguridad del ciberespacio en relación con pequeñas y medianas empresas, la inteligencia artificial es un activo estratégico en la automatización de procesos críticos como la detección de intrusiones, el análisis de archivos de registro y el escaneo de vulnerabilidades, la IA reduce la necesidad de mano de obra especializada de alto nivel y optimiza los recursos limitados disponibles para estas organizaciones. Al hacerlo, la inteligencia

artificial es más que un motor de transformación digital; también es un socio clave para fortalecer la resiliencia empresarial ante las crecientes amenazas cibernéticas (Chinthala, 2024)

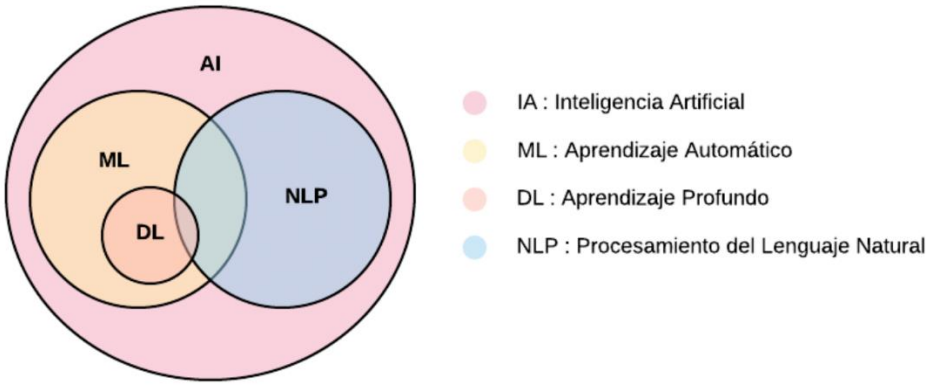
1.1.7 Procesamiento del Lenguaje Natural

Es un campo dedicado a crear métodos para que las máquinas comprendan, analicen, creen y respondan automáticamente al lenguaje que usan las personas, considerando el contexto y la importancia. De esta forma, los sistemas no solo reconocen palabras y frases, sino que también entienden el significado, la intención y la relevancia de las expresiones en cada situación(Garzón et al., 2025)

El procesamiento del lenguaje natural combina la lingüística computacional, la estadística, el aprendizaje automático y el análisis y la semántica linguística para procesar altos volúmenes de texto y voz para proporcionar servicios como traducción automática, asistentes virtuales, chatbots de IA sistemas de respuesta automática, análisis de sentimientos, clasificación de texto y motores de búsqueda avanzados(Gómez y Boumadan, 2025).

A continuación, la Figura 4 muestra la relación entre los principales campos de la inteligencia artificial: IA (Inteligencia Artificial), ML (Aprendizaje Automático), DL (Aprendizaje Profundo) y NLP (Procesamiento del Lenguaje Natural). El diagrama de conjuntos evidencia cómo el PLN se posiciona como un área específica de aplicación de la IA, apoyada en técnicas de aprendizaje automático y profundo para comprender y generar lenguaje humano, lo que resulta fundamental para el desarrollo de chatbots, traductores automáticos y sistemas inteligentes de interacción.

Figura 4
Procesamiento de lenguaje natural



Nota. La figura representa la relación entre inteligencia artificial, aprendizaje automático, aprendizaje profundo y procesamiento del lenguaje natural,(Moran y Chavez, 2021)

1.1.8 Normativas y estándares internacionales

Las normativas y estándares relacionados con la ciberseguridad son marcos regulatorios, guías técnicas y buenas prácticas desarrolladas por organismos internacionales con el propósito de establecer criterios comunes para la gestión segura de la información, la protección de activos tecnológicos y la evaluación de riesgos en los sistemas informáticos, las principales a considerar son:

- ISO/IEC 27001: Establece los requisitos para implementar, mantener y mejorar un SGSI.
- ISO/IEC 27002: Es una norma que complementa a la ISO/IEC 27001 que incorpora controles de seguridad y buenas prácticas para la gestión de la seguridad de la información.
- Criterios de CIS: Los documentos formulados por CIS establecen pautas con configuraciones de seguridad recomendadas que deben ser adoptadas por servidores a nivel empresarial.
- NIST SP 800-53 / SP 800-115: Proporcionan pautas sobre cómo llevar a cabo procedimientos de pruebas de seguridad técnica.

La aceptación de estas regulaciones internacionales permite a las organizaciones alinear sus políticas y prácticas de seguridad con estándares aceptados internacionalmente, lo que aumenta la confianza con clientes, proveedores y socios estratégicos. Además, simplifica el cumplimiento de las obligaciones legales y regulatorias, evitando así multas, mientras mejora la reputación institucional en cuanto a la protección de la información, según (Casares, 2022) el propio proceso de estandarización de la ciberseguridad fomenta no solo medidas de protección, sino también la cultivación de una cultura organizacional orientada a la gestión de riesgos y a la mejora continua.

En contraste, los Benchmarks del CIS y la guía del NIST ofrecen beneficios prácticos al proporcionar configuraciones predeterminadas y metodologías de evaluación prescritas que minimizan las posibilidades de cometer errores de ejecución en la administración del sistema. Si bien estos marcos son ventajosos para casi cualquier organización, pueden ser especialmente beneficiosos para las pequeñas y medianas empresas (PYMES), ya que ofrecen un medio económico y simplificado para mejorar la seguridad de los servidores de Windows y Linux en relación con las limitaciones presupuestarias y de personal especializado existentes (Vega, 2021)

1.2. Proceso investigativo metodológico

1.2.1 Enfoque de la investigación

Se ha elegido el enfoque cualitativo, el cual es flexible, es inductivo, y permite comprender la realidad en el contexto de su propia complejidad. En el caso de esta investigación, la cual es cualitativa, se emplea estratégicamente en el diseño del Chatbot en conjunto con interfaz semiestructurada que permite la recolección de la información que ayuda en la definición de los requerimientos funcionales y en la estipulación de la interacción que guiará el diseño del Chatbot.

El enfoque cualitativo permite profundizar en aspectos de la tecnología innovativa, como el que se presenta en esta investigación, porque facilita el entendimiento de las necesidades y de las vivencias de los sujetos en relación con la gestión de la ciberseguridad en las PYMEs no se recoge solo la información técnica de la configuración de servidores, sino que se incorpora el entendimiento de las cortinas, las esperanzas, y el día a día del personal de TI, diseñando el Chatbot. Esto asegura que el enfoque del diseño sea hacia alternativas que estén fácilmente disponibles, contextualmente apropiadas y suficientemente sustanciales para mejorar la ciberseguridad organizacional.

Asimismo, se incorporó un componente cuantitativo, a través de la aplicación de una encuesta en escala de Likert dirigida a personal de TI, con el fin de medir de manera objetiva el nivel de cumplimiento de buenas prácticas en servidores Windows y Linux. La combinación de ambos enfoques constituye un diseño mixto, que permitió triangular información y aumentar la validez de los resultados

1.2.2 Tipo de investigación

La investigación descriptiva se caracteriza por analizar y detallar de manera precisa las propiedades, características y comportamientos de un fenómeno sin manipularlo, con el objetivo de responder al “qué” y al “cómo” de la situación observada. Para el desarrollo del chatbot, este tipo de investigación permitió identificar con claridad los patrones de comportamiento y las necesidades específicas en materia de ciberseguridad a ser incorporados, complementándose con una aproximación aplicada, orientada a la resolución de un problema concreto en las PYMEs.

1.2.3 Población y muestra del estudio

De acuerdo con lo presentado en la Tabla 1, a nivel nacional existen 16.449 medianas empresas de tipo A y tipo B, las cuales, según su caracterización, han incorporado en sus

procesos productivos y de comercialización infraestructura tecnológica orientada a optimizar su funcionamiento y garantizar un adecuado desenvolvimiento empresarial.

Para la determinación de la muestra, se optó por un muestreo no probabilístico de tipo intencional, seleccionando a un grupo de profesionales en el área de seguridad de la información bajo criterios de afinidad con el objeto de estudio, conocimientos técnicos especializados y experiencia comprobada en la gestión de seguridad informática y en la implementación de buenas prácticas en servidores empresariales. La muestra estuvo conformada por especialistas pertenecientes a diez PYMEs, con el propósito de contar con informantes clave capaces de aportar información relevante, precisa y contextualizada sobre el nivel de cumplimiento de medidas de ciberseguridad en las organizaciones (Ver Anexo 1 – Guía de entrevista; Anexo 2 – Encuesta Likert).

1.3. Análisis de resultados

Como parte de esta investigación, la entrevista consta de un total de 10 preguntas que tienen como objetivo recopilar datos pertinentes sobre el nivel de ciberseguridad dentro de las PYME y las opiniones de los expertos sobre el uso de un chatbot para automatizar la auditoría del servidor.

Pregunta 1: ¿Qué importancia tiene la seguridad de los servidores en el funcionamiento de su empresa?

Los expertos señalaron que los servidores son el núcleo operativo de sus negocios, ya que allí se alojan sistemas críticos (ERP, bases de datos de clientes, sistemas contables y de facturación) y una falla de seguridad no solo interrumpiría los procesos internos, sino que además afectaría la reputación de la empresa y la confianza de los clientes; por tanto, no se percibe como un gasto opcional, sino como una condición indispensable de sostenibilidad.

Pregunta 2: ¿Con qué frecuencia se realizan auditorías de seguridad en sus servidores Windows y/o Linux?

Se evidenció que la mayoría de las PYMEs no tiene un calendario formal de auditorías, algunas realizan revisiones esporádicas cuando ocurre un incidente o cuando un proveedor externo lo exige; sin embargo, a nivel general no existe una práctica sistemática, lo que significa que las vulnerabilidades permanecen abiertas durante largos períodos, incrementando las posibilidades de ataques exitosos.

Pregunta 3: ¿Qué métodos o herramientas utilizan actualmente para verificar buenas prácticas de configuración?

Aunque algunos conocen las guías de CIS o NIST, no cuentan con herramientas prácticas para aplicarlas, sumado a que este tipo de herramientas comerciales disponibles resultan costosas y poco adaptadas a la realidad de las PYMEs, por lo que la mayoría indicó que se apoyan en métodos manuales (revisar logs, validar configuraciones básicas) o en herramientas parciales como antivirus, firewalls sencillos o scanners gratuitos.

Pregunta 4: ¿Qué dificultades enfrentan al realizar estas auditorías?

Las dificultades identificadas incluyen:

- Falta de tiempo para realizar revisiones exhaustivas
- Escasez de personal capacitado en ciberseguridad
- Costos elevados de herramientas profesionales

Factores como estos en conjunto contribuyen a por qué en lugar de planificar estrategias proactivas, los responsables de TI eligen atender la resolución inmediata de problemas, creando así un ciclo ininterrumpido de vulnerabilidad.

Pregunta 5: ¿Qué consecuencias ha tenido la falta de controles adecuados?

Algunos entrevistados admitieron haber enfrentado incidentes como intentos de intrusión, interrupciones del servicio o accesos no autorizados, mientras que otros expresaron su preocupación por la filtración de información sensible o incidentes que afectarían directamente las ventas junto con las relaciones con los clientes.

Pregunta 6: ¿Considera que una herramienta automatizada podría facilitar la auditoría?

Todos coincidieron en que sí, ya que una solución de este tipo permitiría ahorrar tiempo, reducir errores humanos, aplicar controles de forma más consistente y automatizar procesos repetitivos permitiendo liberar al personal técnico para tareas más estratégicas.

Pregunta 7: ¿Qué características debería tener una herramienta de este tipo para ser útil en una PyME?

Se sugirió que la herramienta debería ser fácil de usar, con una interfaz clara, multiplataforma (Windows y Linux), de bajo costo o libre acceso, y con respuestas comprensibles que incluyan recomendaciones prácticas de remediación paso a paso considerando que la mayoría de PYMES no cuenta con personal técnico especializado.

Pregunta 8: ¿Cree que un chatbot inteligente sería una alternativa práctica?

La percepción fue mayoritariamente positiva ya que los entrevistados destacaron que un chatbot podría interactuar en lenguaje natural, responder dudas específicas y guiar paso a paso en la auditoría, lo que reduciría la dependencia de manuales técnicos extensos y costosos.

Pregunta 9: ¿Qué limitaciones y riesgos percibe en un chatbot de auditoría?

Se destacó la importancia de mantener actualizado el conocimiento del chatbot con nuevas vulnerabilidades del sistema y versiones del sistema operativo; así como el riesgo de que la herramienta pueda ofrecer recomendaciones incompletas o poco claras.

Pregunta 10: ¿Qué impacto tendría una solución de este tipo en la empresa?

Se anticipa que el fortalecimiento de la seguridad digital al reducir el nivel de vulnerabilidades críticas mejorará la confianza de los clientes y socios, al tiempo que garantizará la continuidad operativa.

Con el fin de complementar el análisis cualitativo de las entrevistas a expertos, se aplicó una encuesta estructurada con escala de Likert (1 = Muy en desacuerdo, 5 = Muy de acuerdo) dirigida al personal de TI de las PYMEs. Este instrumento permitió cuantificar la percepción sobre la importancia de la seguridad en servidores, la frecuencia de auditorías y la aceptación de un chatbot como herramienta de apoyo. En la tabla 2 se presentan los principales resultados obtenidos:

Tabla 1

Resultados de la encuesta con escala de Likert

Pregunta	1 Muy en desacuerdo	2 En desacuerdo	3 Neutral	4 De acuerdo	5 Muy de acuerdo	Tendencia
Importancia de la seguridad de servidores	0%	3%	5%	40%	52%	Alta valoración (92% en 4–5)
Frecuencia de auditorías de seguridad	45%	25%	20%	7%	3%	Baja frecuencia (70% en 1–2)
Facilidad de uso esperada en la herramienta	2%	5%	5%	48%	40%	Preferencia por simplicidad (88% en 4–5)

Aceptación de un chatbot inteligente	5%	4%	6%	50%	35%	Alta aceptación (85% en 4–5)
Impacto en la seguridad de la empresa	3%	2%	5%	42%	48%	Impacto positivo esperado (90% en 4–5)

Nota: *Los resultados reflejan que, aunque las PYMEs reconocen la alta importancia de la seguridad de servidores y muestran una buena aceptación hacia el uso de un chatbot, persiste una baja frecuencia en la realización de auditorías sistemáticas, lo que evidencia la necesidad de herramientas accesibles y automatizadas.*

Los resultados presentados en la tabla permiten evidenciar una alta conciencia sobre la importancia de la ciberseguridad en las PYMEs, así como una amplia aceptación hacia soluciones innovadoras como el chatbot inteligente para auditorías. Sin embargo, también se confirma que la frecuencia de auditorías de seguridad es baja, debido a limitaciones de tiempo, recursos y personal especializado. Esta situación refuerza la pertinencia de la propuesta tecnológica, ya que una herramienta automatizada puede cubrir esas brechas y mejorar la gestión de la seguridad digital en este tipo de empresas.

CAPÍTULO II: PROPUESTA

2.1 Fundamentos teóricos aplicados

El diseño de una herramienta de ciberseguridad basada en un chatbot para la auditoría de buenas prácticas en servidores requiere de una base teórica sólida que respalde su pertinencia. En esta sección se abordan los fundamentos directamente relacionados con el problema de investigación, considerando aspectos técnicos, normativos y tecnológicos.

2.1.1 Seguridad de la información en PYMEs

La protección de datos y sistemas se convierte en vital importancia para cualquier empresa. Este problema es de especial importancia y es más agudo para las PYMES ya que se ofrecen su servicio más sensible, limitados. Información como bases de datos de clientes, sistemas de cuentas y contabilidad, e inclusive sistemas de accesos internos, deben protegerse a todo coste. La norma ISO/IEC 27001 establece que para que la seguridad de datos e información se gestione adecuada y eficientemente, énfasis deben hacerse en las políticas y controles orientados a la data (concerniente a la data, datos y sistemas) para proteger la confidencialidad, integridad y disponibilidad, más que protección de los datos (NIST, 2023).

Estudios más recientes señalan que las PYMES muestran un patrón de vulnerabilidades persistentes repetidas al no implementar un conjunto seguro de marcos por lo tanto, se convierten en un blanco fácil para los ataques (Bustillos y Rojas, 2023). Esta base teórica apoya la proposición de la disponibilidad de una herramienta automatizada para la auditoría y verificación más rigurosa de las protecciones de los servidores en su lugar.

2.1.2 Normativas y estándares internacionales de ciberseguridad

Los estándares internacionales sirven como puntos de referencia fundamentales incluso para el ámbito de los controles tecnológicos. Por ejemplo, la ISO/IEC 27001, ISO/IEC 27002, los Benchmarks del CIS e incluso las Guías NIST SP 800-53 definen las configuraciones técnicas particulares para la configuración segura de sistemas (Casares, 2022; Vega, 2021).

Estos marcos de referencia proporcionan métricas de construcción que permiten a las organizaciones automatizar procesos de seguridad y minimizar el error humano en la gestión de servidores, integrar estos estándares en el razonamiento del chatbot asegura que las auditorías realizadas se basen en estándares aceptados a nivel mundial.

2.1.3 Chatbots aplicados a la auditoría informática

Los chatbots han evolucionado desde simples aplicaciones programadas con el uso de reglas hasta sistemas complejos que utilizan el procesamiento de lenguaje natural (PLN) para interactuar y mantener conversaciones fluidas y contextualizadas con los usuarios (Peña et al., 2022) su uso se centra en ayudar en la verificación de configuraciones, el monitoreo de registros y la detección de vulnerabilidades (Ramírez et al., 2023).

Cuando se han integrado con bases de conocimiento actualizadas, los chatbots han mostrado la capacidad de hacer diagnósticos y, en particular, de aconsejar a los administradores de TI sobre qué acciones deben realizar para alinearse a los estándares de buenas prácticas y, por tanto, para disminuir el uso de costosos manuales técnicos.

2.1.4 Procesamiento del Lenguaje Natural como soporte a la seguridad

La capacidad de comprensión e interpretación del lenguaje humano por parte de las máquinas (PLN) es una de las ramas más fundamentales de la inteligencia artificial (IA), que impacta en el diseño de chatbots (Microsoft, 2025). Ahora, los modelos entrenados en grandes conjuntos de datos permiten que un chatbot comprenda preguntas formuladas en lenguaje natural y responda a un nivel técnico apropiado adaptado al usuario.

2.1.5 Automatización y monitoreo en ciberseguridad

La creciente complejidad de las amenazas cibernéticas demanda el uso de herramientas de monitoreo continuo y automatización para respaldar las defensas de perímetro tradicionales, las herramientas SIEM (Gestión de Información y Eventos de Seguridad) centralizan registros, detección de anomalías y respuesta proactiva a incidentes (Chinthala, 2024).

El chatbot propuesto se inspira en este principio al automatizar la auditoría de cumplimiento de las mejores prácticas y asegura revisiones regulares en servidores Windows y Linux para reducir riesgos.

2.1.6 Resiliencia digital y sostenibilidad empresarial

El último aspecto de la resiliencia digital crítica es la capacidad de cualquier organización para predecir, resistir y recuperarse de incidentes cibernéticos y seguir garantizando la continuidad del negocio (Sierra y Magnolia, 2022). Especialmente para las pequeñas y medianas empresas (PYMES), esto es crucial, ya que la interrupción de los sistemas empresariales puede resultar en graves consecuencias económicas y pérdida de confianza por parte de clientes y proveedores.

Esta herramienta está en sintonía con este aspecto, ya que proporciona un mecanismo fácil de usar y automatizado que mejora la seguridad digital de manera rentable, sin necesidad de gastar en licencias o contratar servicios de consultoría externos.

2.1.7 Otros trabajos relacionados

Numerosos estudios han buscado aplicaciones de chatbots e inteligencia artificial en la industria de la seguridad de la información, proporcionando experiencias que servirían como fundamentos para la propuesta de este proyecto.

Tejedo (2024), por ejemplo, desarrolló chatbots gpt que son chatbots impulsados por inteligencia artificial destinados a proporcionar asistencia a los analistas del centro de seguridad operativa. Esta herramienta incorpora funciones de verificación de ip y dominio, realiza automatización de tareas repetitivas, respuesta a incidentes para servidores windows, Linux y mejora los tiempos de respuesta en general. La evidencia de esta investigación concluye que el uso de chatbots acelera la detección y la respuesta a amenazas de seguridad y mejora la precisión general en la detección de amenazas.

De manera similar, Alvarez (2024) llevó a cabo una revisión sistemática sobre el uso de técnicas de inteligencia artificial en la ciberdefensa y encontró 30 estudios que utilizan aprendizaje automático y profundo para frustrar ataques DoS, malware y ransomware. Esta investigación demuestra que la inteligencia artificial es una herramienta significativa en los sistemas de ciberdefensa debido a su capacidad de detección temprana de amenazas y automatización de respuestas rápidas.

Su trabajo complementario realizado por López, Gómez y Boumadan (2025) sobre las aplicaciones y desafíos de los chatbots inteligentes en entornos enfocados en organizaciones documenta el énfasis puesto en la gestión de la información, la automatización de tareas y el soporte técnico. El estudio señala la necesidad de abordar cuestiones éticas, técnicas y de supervisión dentro de su ciclo de vida ‘diseñar-desarrollar-desplegar’, que puede aplicarse fácilmente a la creación de un chatbot para auditorías de servidores en pymes.

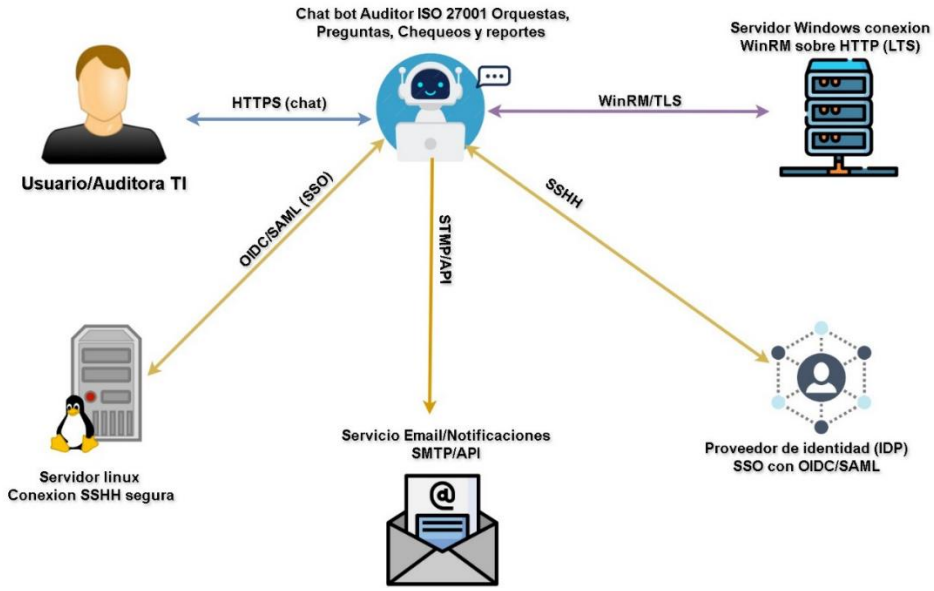
En última instancia, el trabajo de Peña, Giraldo, Arango y Bucheli (2022) sobre un chatbot diseñado específicamente para atender las necesidades de solicitudes de información durante la pandemia de COVID apunta a la versatilidad de los chatbots para responder a necesidades contextuales urgentes, mejorando así la agilidad de la información y minimizando las dependencias de las personas.

2.2 Descripción de la Propuesta

La propuesta es crear una herramienta de ciberseguridad sofisticada basada en un chatbot inteligente que se centra en auditar las mejores prácticas de seguridad en servidores Windows y Linux en pequeñas y medianas empresas en Ecuador. Su construcción integra fundamentos de seguridad de la información, auditoría informática, procesamiento del lenguaje natural e inteligencia artificial, con el fin de brindar un producto tecnológico accesible, automatizado y basado en estándares internacionales.

La propuesta del Chatbot Auditor ISO 27001 se apoya en una arquitectura que integra distintos componentes y protocolos de comunicación orientados a garantizar conexiones seguras con servidores y servicios de correo electrónico y sistemas de gestión de identidad. Esta estructura permite la interacción del usuario a través de un canal de comunicación cifrado, mientras que el Chatbot se conecta con servidores Linux mediante SSH seguro y con servidores Windows a través de WinRM/TLS. izado y basado en estándares internacionales. Asimismo, se contempla la integración con servicios de notificación mediante SMTP/API y con proveedores de identidad bajo estándares como OIDC/SAML. Lo que asegura la autenticación y autorización confiables. En la Figura 5 se presenta la descripción de esta propuesta, donde se ilustra la relación entre los diferentes elementos de la arquitectura y lo mecanismos de seguridad que los soportan.

Figura 5
Descripción de la propuesta



Nota: *Arquitectura del Chatbot Auditor ISO 27001 con conexiones seguras a servidores, correo e identidad.*

a. Estructura general

La estructura de la herramienta propuesta se organiza en cuatro componentes principales:

1. **Interfaz de interacción en lenguaje natural**
    - Permite la comunicación entre el usuario y el chatbot.
    - Procesa preguntas y comandos en lenguaje natural.
    - Presenta resultados y recomendaciones en formato claro y comprensible.
2. **Módulo de procesamiento del lenguaje natural (PLN)**
    - Interpreta la intención de la consulta del usuario.
    - Transforma la entrada de texto en comandos técnicos aplicables.
    - Está basado en técnicas de IA y modelos de análisis semántico.
3. **Módulo de auditoría de servidores**
    - Ejecuta verificaciones en servidores Windows y Linux.
    - Valida parámetros de seguridad como gestión de usuarios, permisos, estado de actualizaciones, configuración de firewalls, cifrado y logs.
    - Se apoya en lineamientos de ISO/IEC 27001, CIS Benchmarks y NIST.
4. **Base de conocimiento y repositorio de buenas prácticas**
    - Almacena estándares internacionales, políticas y reglas de seguridad.
    - Se actualiza periódicamente con nuevas vulnerabilidades y controles.
    - Proporciona al chatbot la información necesaria para emitir recomendaciones.

b. Explicación del aporte

Cada componente aporta al funcionamiento integral de la herramienta:

- **Interfaz de interacción**: facilita el acceso a procesos complejos de auditoría mediante un lenguaje sencillo y natural, reduciendo la barrera técnica para usuarios con conocimientos limitados.
- **Módulo de PLN**: transforma el lenguaje humano en comandos técnicos precisos, lo que permite que el sistema sea intuitivo y flexible.

- **Módulo de auditoría**: constituye el núcleo del sistema, al ejecutar la verificación de parámetros críticos en servidores Windows y Linux detectando configuraciones inseguras y emitiendo alertas oportunas.
- **Base de conocimiento**: garantiza que las recomendaciones emitidas estén fundamentadas en normas reconocidas a nivel internacional incrementando la confiabilidad del chatbot.

El aporte general de la propuesta radica en ofrecer a las PYMEs un asistente virtual de ciberseguridad, capaz de automatizar auditorías, reducir riesgos, optimizar recursos humanos y económicos y fortalecer la resiliencia digital.

c. Estrategias y/o técnicas

Para la construcción de la herramienta se aplicaron diversas estrategias y técnicas que garantizaron tanto la rigurosidad académica como la factibilidad práctica del producto. En primer lugar, se llevó a cabo una investigación bibliográfica y documental, que permitió recopilar marcos normativos internacionales como la ISO 27001, los CIS Benchmarks y las guías del NIST, además de fundamentos teóricos relacionados con ciberseguridad, auditoría y chatbots. Esta etapa resultó esencial para alinear el desarrollo de la propuesta con estándares reconocidos y con experiencias previas documentadas en la literatura científica.

Luego, se utilizó un diseño sustractivo, por el cual la herramienta fue diseñada como un conjunto de bloques autónomos (interfaz de usuario, módulo de procesamiento de lenguaje natural, módulo de auditoría, base de conocimiento), el enfoque retuvo la escalabilidad del sistema y la facilidad de mantenimiento, en la que los componentes pueden actualizarse sin perjudicar el funcionamiento general de la solución.

Además, se utilizó un enfoque de prototipado incremental, que implicaba crear versiones iniciales del chatbot y validarlas progresivamente con especialistas en TI de las PYME, esto ayudó a adaptar el producto a los puntos de dolor reales del ecosistema empresarial.

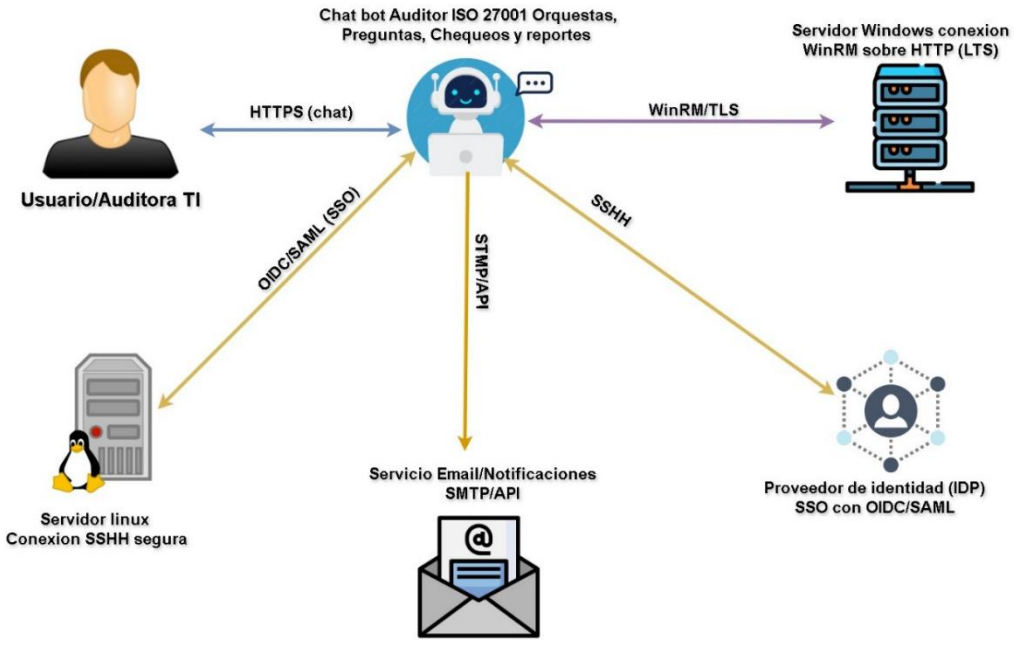
Los enteros utilizados validaron la investigación experta a través de entrevistas y pruebas funcionales con especialistas en ciberseguridad, logrando la relevancia y utilidad de la herramienta y asegurando la fiabilidad de los resultados.

Otra técnica descrita fue la automatización de procesos empresariales, lograda a través de la programación de guiones y la programación rutinaria de verificaciones de configuración automatizadas establecidas para servidores Windows y Linux. Esto redujo el trabajo manual y el riesgo de errores humanos durante la auditoría.

d. Arquitectura propuesta (según el diagrama C4–L1)

La Figura 6 presenta el diagrama de contexto de la solución. En él se observan los actores, sistemas externos y los flujos de comunicación seguros que habilitan la auditoría automática de servidores Windows y Linux por medio del chatbot.

Figura 6
Arquitectura propuesta



Nota: *Esquema de integración del Chatbot Auditor ISO 27001 con servidores, servicios de correo e identidad mediante conexiones seguras.*

a. Actores y sistemas

1. **Usuario/Auditor TI /Chatbot Auditor (HTTPS):** canal de interacción en lenguaje natural, cifrado de extremo a extremo.
2. **Servidores Windows (WinRM/TLS):** destino de las verificaciones mediante PowerShell Remoting.
3. **Servidores Linux (SSH endurecido):** destino de chequeos remotos sin agente.
4. Proveedor de Identidad (IdP) con SSO OIDC/SAML: autenticación centralizada y autorización basada en roles (RBAC).
5. **Servicio de notificaciones (SMTP/HTTPS):** envío de reportes y alertas a responsables.

b. Flujos clave (flechas del diagrama)

1. **Autenticación SSO (OIDC/SAML):** El usuario inicia sesión ante el IdP; el chatbot

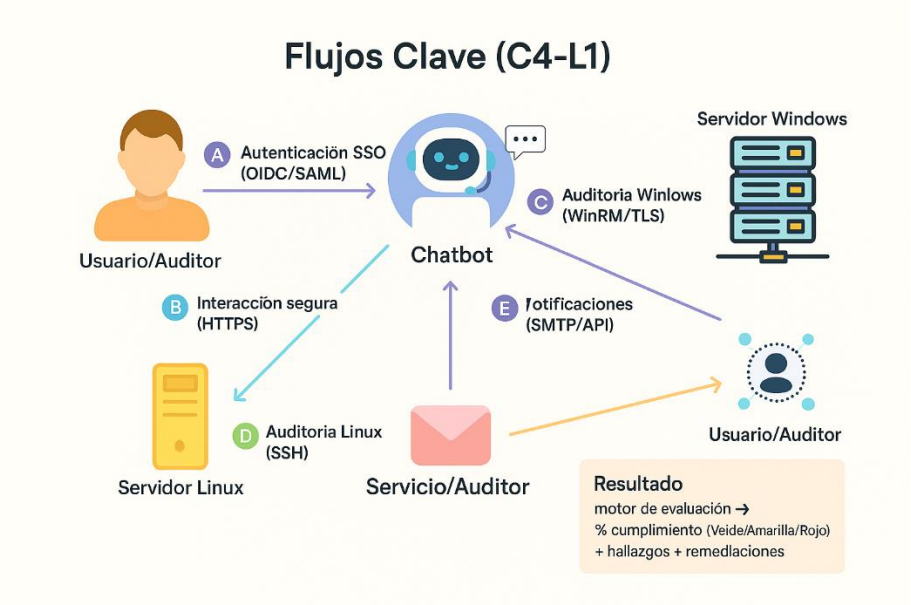
valida el token y aplica RBAC para limitar acciones y alcance.

2. **Interacción segura (HTTPS):** El usuario converso con el chatbot; las peticiones y respuestas viajan cifradas.
3. **Auditoría en Windows (WinRM/TLS):** El orquestador ejecuta comandos/PowerShell para consultar políticas, parches, firewall, auditoría, antivirus y otros controles.
4. **Auditoría en Linux (SSH):** Se ejecutan verificaciones de acceso (root/login), autenticación por contraseña/clave, firewall, actualizaciones, logrotate, integridad y sincronización de tiempo (NTP).
5. **Notificaciones (SMTP/API):** El sistema remite reportes y alertas al correo o sistemas de gestión

c. Resultado del proceso

Con las evidencias recolectadas, el motor de evaluación calcula un porcentaje de cumplimiento ponderado y lo presenta en un semáforo (Verde/Amarillo/Rojo). Además, explica los hallazgos y propone acciones de remediación, sustentadas en la base de conocimiento alineada con ISO/IEC 27001, CIS y NIST, la Figura 7 presenta los flujos claves de autenticación y auditoria.

Figura 7
Flujos Claves



Nota: *El diagrama muestra los flujos clave de autenticación, auditoría y notificación en el sistema con chatbot.*

d. Tecnologías y herramientas

La Tabla 3 resume las principales herramientas utilizadas en el desarrollo de la solución propuesta, organizadas por capas tecnológicas y su respectivo rol dentro del sistemas. Para la interfaz inicial (MVP) se empleó Streamlit (Python), mientras que en producción se integró React/Next.js con Tailwind para ofrecer un frontend moderno y en tiempo real. La capa auditorias y control de accesos. El procesamiento de tareas en paralelo se gestionó mediante Redis y Celery, garantizando ejecución eficiente y tolerancia a fallos. La recolección de evidencias se realizó en servidores Linux a través de SSH y Bash, y en entornos Windows con WinRM/TLS y estructuro en YAML, mientras que para almacenamiento se utilizaron SQLite y PostgreSQL, junto con MinIO/S3 para reportes. Finalmente, la capa reportaría se generó en HTML/PDF mediante librerías como wkhtmltopdf y WeasyPrint, permitiendo la descarga de informes completos con evidencias.

Tabla 2

Herramientas utilizadas

Capa	Tecnología propuesta	Rol en la solución
Interfaz (MVP)	**Streamlit (Python)**	UI tipo messenger, chat seguro y descarga de reportes.
Interfaz (Producción)	**React/Next.js + Tailwind**	Frontend moderno, en tiempo real (WebSockets).
Orquestador/API	**Python + FastAPI**	Endpoints del chat, orquestación de auditorías, RBAC.
Jobs/colas	**Redis + RQ/Celery**	Ejecución paralela de auditorías y reintentos.
Colector Linux	**SSH (Paramiko) + Bash**	Verificaciones remotas sin agente.
Colector Windows	**WinRM/TLS (pywinrm) + PowerShell**	Chequeos de políticas, parches y auditoría.
Base de conocimiento	**YAML**	Reglas de controles, pesos, umbrales y descripciones.
Almacenamiento estructurado	**SQLite (MVP) / PostgreSQL (prod.)**	Runs, hallazgos, usuarios, catálogo KB.
Almacenamiento de reportes	**MinIO/S3**	HTML/PDF y evidencias JSON.
Reportería	**HTML** (+ **wkhtmltopdf/WeasyPrint** para PDF)	Reportes descargables con evidencias.
Autenticación	**OIDC/SAML (Keycloak/Auth0)**	SSO, emisión/validación de tokens, perfiles.

Seguridad	**TLS 1.2+**, **Vault/Secrets**	Cifrado en tránsito y gestión de secretos.
Observabilidad	**Prometheus + Grafana**, **Loki/ELK**	Métricas, logs y alertas.
Despliegue	**Docker/Compose** (MVP) / **Kubernetes** (prod.)	Empaquetado, escalabilidad, alta disponibilidad.

i. Visión general

La solución es un Chatbot Auditor de Ciberseguridad para PYMEs, basado en la norma ISO/IEC 27001, el sistema revisa servidores Windows y Linux (sin necesidad de instalar software o con un programa ligero), recoge información técnica como configuraciones, parches y políticas, evalúa y califica el nivel de cumplimiento según una lista de controles, explica los resultados con un lenguaje sencillo y da recomendaciones para corregir problemas. Además, genera reportes en HTML o PDF y guarda un registro de cada verificación.

ii. Casos de uso principales

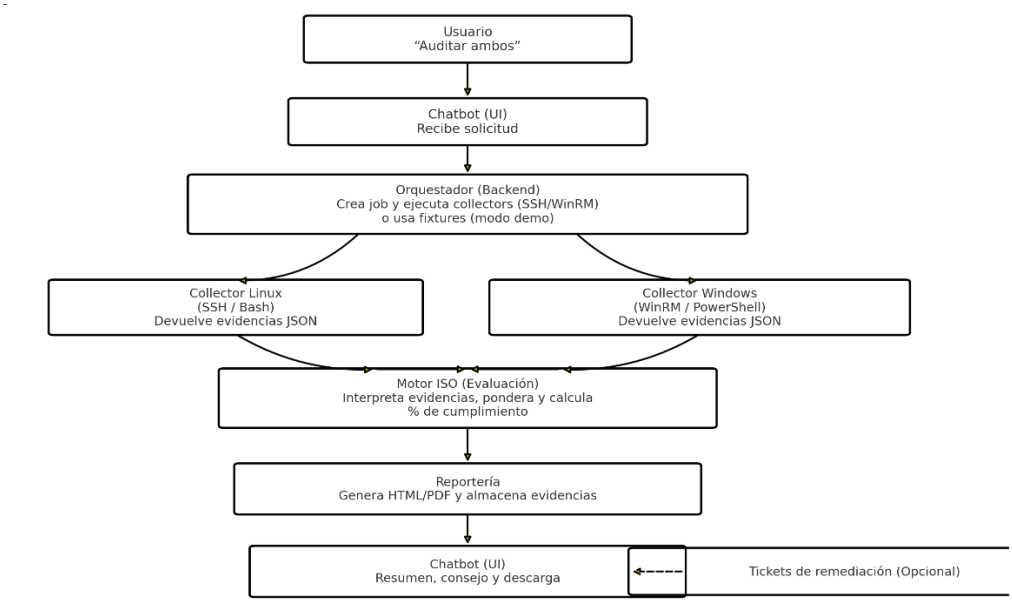
1. Auditoría bajo demanda. El usuario invoca “auditar linux/windows/ambos”; el sistema ejecuta los chequeos, calcula el porcentaje de cumplimiento y presenta un semáforo (Verde/Amarillo/Rojo) con recomendaciones.
2. Auditoría programada. Corridas periódicas (semanal/mensual) con histórico de tendencias y comparación entre ejecuciones.
3. Asistente de remediación. El bot indica qué comando/política cambiar, cómo validarlo y dónde queda la evidencia.
4. Gestión de evidencias. Almacena los JSON de resultados y anexa evidencias a los reportes para auditoría posterior.
5. Panel de cumplimiento (fase 2). Consolida el porcentaje global, por servidor y por dominio ISO.

iii. Arquitectura de la solución

- **Capa de interacción (Chat Web):** Es una ventana de chat parecida a Messenger, donde puedes escribir o usar botones rápidos. Los resultados salen en el mismo chat, con una explicación fácil y un botón para descargar el informe.

- **Orquestador del chatbot (Backend):** Reconoce lo que quieres hacer (auditar Linux, Windows, ambos o pedir el reporte), organiza la búsqueda de datos, llama al sistema que evalúa y te da un resumen basado en la norma ISO/IEC 27001.
- **Motor de evaluación ISO:** Usa una lista de controles con información como nombre, peso, y qué se espera. Examina los datos, calcula la puntuación, pone un color según el resultado (verde, amarillo o rojo) y da recomendaciones automáticas.

Figura 8
Flujo Chatbot Auditor



Nota: *El diagrama resume el flujo E2E desde la solicitud "Auditar ambos" hasta la generación del reporte y la creación de tickets.*

e. Demostración del MVP y trazabilidad de evidencias

La versión básica del Chatbot Auditor ISO 27001 permite hacer auditorías cuando se necesiten, tanto para Linux como para Windows. En la misma conversación, muestra el porcentaje de cumplimiento, un semáforo de colores y un botón para descargar el reporte en HTML o PDF. La interfaz ayuda al usuario con acciones rápidas como "Auditar Linux", "Auditar Windows" o "Auditar Ambos", y además guarda un registro: cada hallazgo tiene su evidencia técnica en formato JSON con detalles como id, nombre de la revisión, resultado y evidencia.

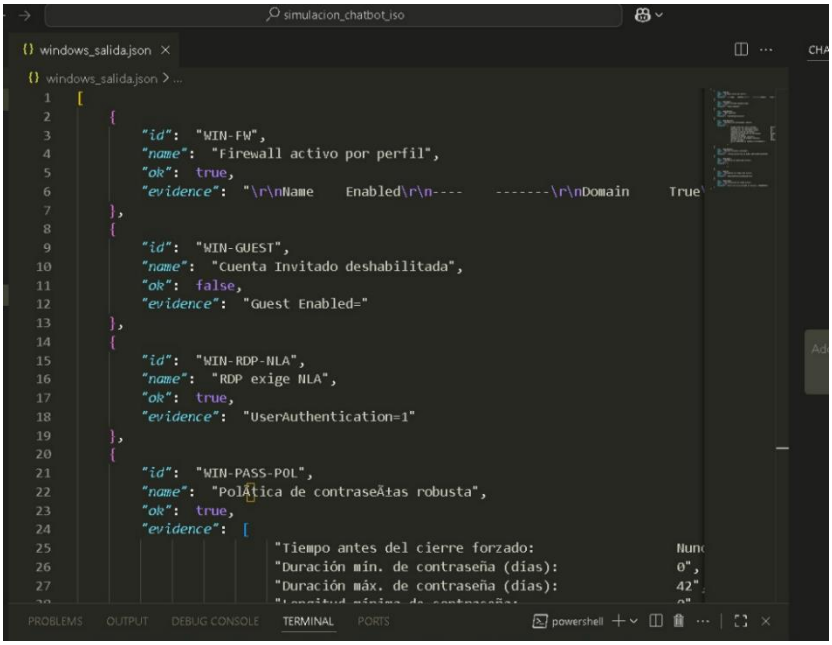
Durante la ejecución, los colectores (SSH/Paramiko en Linux y WinRM/PowerShell en Windows) devuelven evidencias estructuradas que el motor de evaluación interpreta contra el catálogo de controles (con pesos y umbrales). El resultado puede verse de dos formas:

1. Tarjeta de resumen en la propia UI (consejo de remediación incluido)

2. Reporte detallado con tabla de chequeos (ID, Chequeo, Control ISO, Estado, Evidencia) y el resultado global.

La solución también registra condiciones operativas, por ejemplo, errores de privilegios en comandos de Windows como parte de la evidencia; esto permite justificar por qué un control no se pudo verificar y qué acción correctiva tomar (ejecutar PowerShell con privilegios elevados, agregar el usuario al grupo Remote Management Users, habilitar PSRemoting/WinRM, etc.).

Figura 9
Errores de privilegios

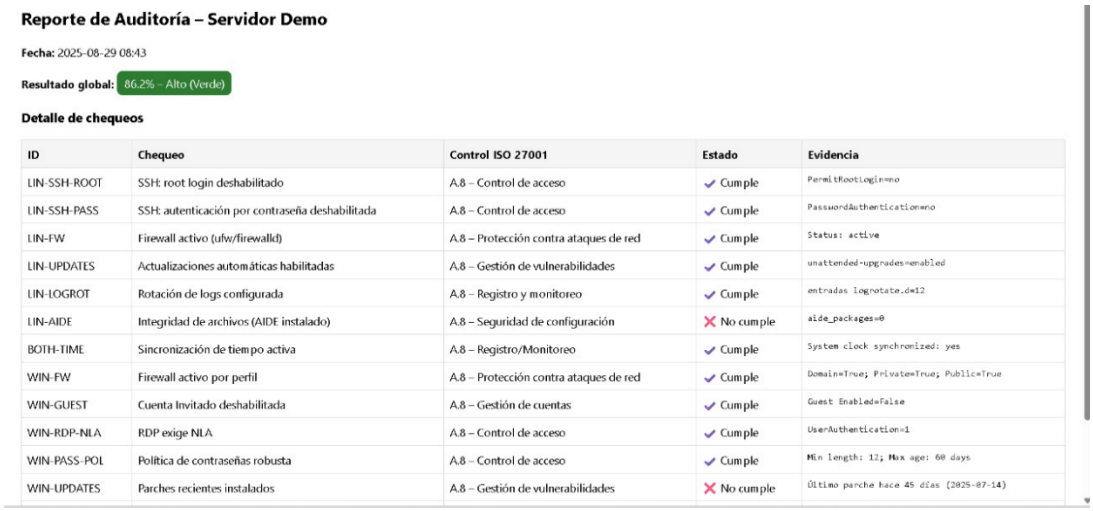


Nota: *Archivo JSON con resultados de auditoría en Windows, que muestra configuraciones evaluadas (firewall, cuentas, RDP y políticas de contraseñas) junto con su evidencia.*

En la Figura 9 se ve el reporte de auditoría que generó el MVP. Allí aparece el porcentaje total de cumplimiento (86,2% – Alto, Verde) y el detalle de los controles según la norma ISO/IEC 27001 (A.8). Cada fila muestra el ID del control, qué se revisó, si cumple o no, y la evidencia técnica usada para llegar a esa conclusión, lo que permite hacer seguimiento y definir prioridades. En el ejemplo, la mayoría de los controles en Linux (SSH, firewall, actualizaciones, registros, NTP) y en Windows (firewall por perfil, usuario Invitado, NLA, contraseñas) están cumplidos. Pero se encontraron puntos importantes por mejorar: integridad de archivos en Linux (porque no está instalado AIDE) y gestión de vulnerabilidades en Windows (con parches que tienen 45 días), los cuales se deben incluir en el plan de corrección.

Figura 10

Reporte de Auditoria



Reporte de Auditoría – Servidor Demo

Fecha: 2025-08-29 08:43

Resultado global: 86.2% – Alto (Verde)

Detalle de chequeos

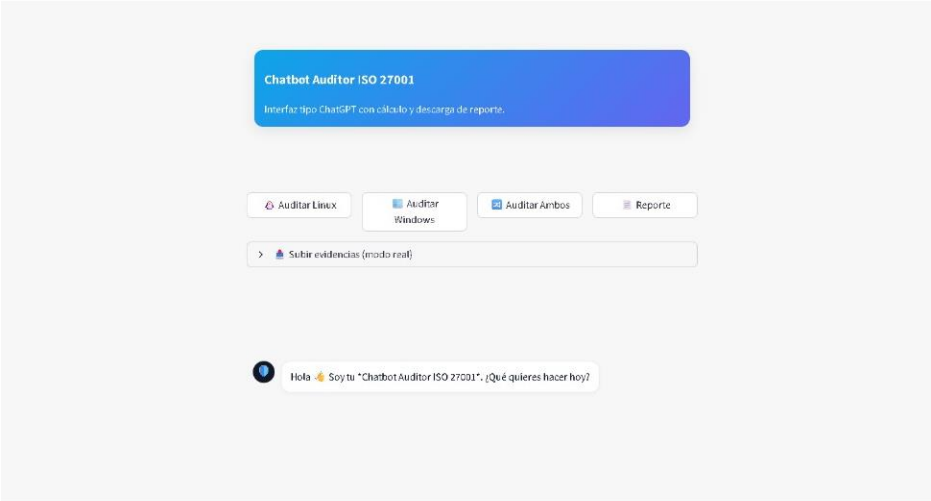
ID	Chequeo	Control ISO 27001	Estado	Evidencia
LIN-SSH-ROOT	SSH: root login deshabilitado	A.8 – Control de acceso	✓ Cumple	PermitRootLogin=no
LIN-SSH-PASS	SSH: autenticación por contraseña deshabilitada	A.8 – Control de acceso	✓ Cumple	PasswordAuthentication=no
LIN-FW	Firewall activo (ufw/firewalld)	A.8 – Protección contra ataques de red	✓ Cumple	Status: active
LIN-UPDATES	Actualizaciones automáticas habilitadas	A.8 – Gestión de vulnerabilidades	✓ Cumple	unattended-upgrades=enabled
LIN-LOGROT	Rotación de logs configurada	A.8 – Registro y monitoreo	✓ Cumple	entradas logrotate.d=12
LIN-AIDE	Integridad de archivos (AIDE instalado)	A.8 – Seguridad de configuración	✗ No cumple	aide_packages=0
BOTH-TIME	Sincronización de tiempo activa	A.8 – Registro/Monitoreo	✓ Cumple	System clock synchronized: yes
WIN-FW	Firewall activo por perfil	A.8 – Protección contra ataques de red	✓ Cumple	Domain=True; Private=True; Public=True
WIN-GUEST	Cuenta Invitado deshabilitada	A.8 – Gestión de cuentas	✓ Cumple	Guest Enabled=False
WIN-RDP-NLA	RDP exige NLA	A.8 – Control de acceso	✓ Cumple	UserAuthentication=1
WIN-PASS-POL	Política de contraseñas robusta	A.8 – Control de acceso	✓ Cumple	Min length: 12; Max age: 60 days
WIN-UPDATES	Parches recientes instalados	A.8 – Gestión de vulnerabilidades	✗ No cumple	Último parche hace 45 días (2025-07-14)

Nota: *Reporte de auditoría de un servidor demo, con un cumplimiento global del 86.2%, detallando controles ISO 27001, estados de verificación y evidencias asociadas.*

En la Figura 10 se muestra la pantalla principal del Chatbot Auditor ISO 27001 (MVP), con un diseño parecido a Messenger y botones rápidos para empezar la auditoría: auditar Linux, Windows o ambos. También está el acceso para ver el reporte y para subir evidencias (modo real). Desde esta pantalla, el usuario inicia todo el proceso: el chatbot recibe la solicitud, corre las herramientas que recogen los datos y, al terminar, muestra el resultado en el mismo chat junto con la opción para descargar el reporte.

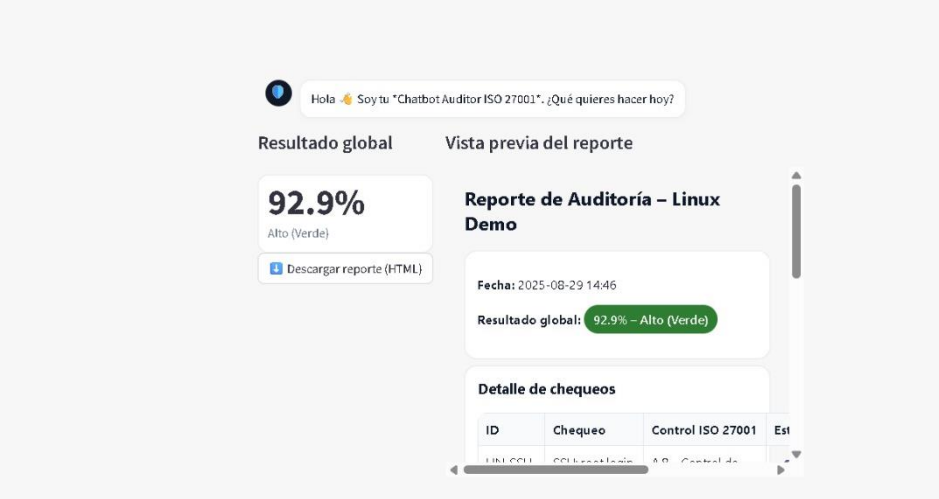
Figura 11

Pantalla principal del Chatbot Auditor



En la Figura 11 se muestra la respuesta en la propia interfaz del chatbot tras ejecutar la auditoría: a la izquierda, el resultado global (92,9 % – *Alto, Verde*) y el botón de descarga del reporte (HTML); a la derecha, la vista previa embebida del reporte, que permite revisar de inmediato la fecha de ejecución, el semáforo de cumplimiento y el detalle de chequeos sin salir del hilo de conversación. Esta disposición facilita la toma rápida de decisiones y garantiza la trazabilidad entre el resumen y la evidencia detallada.

Figura 12
Respuesta de la interfaz

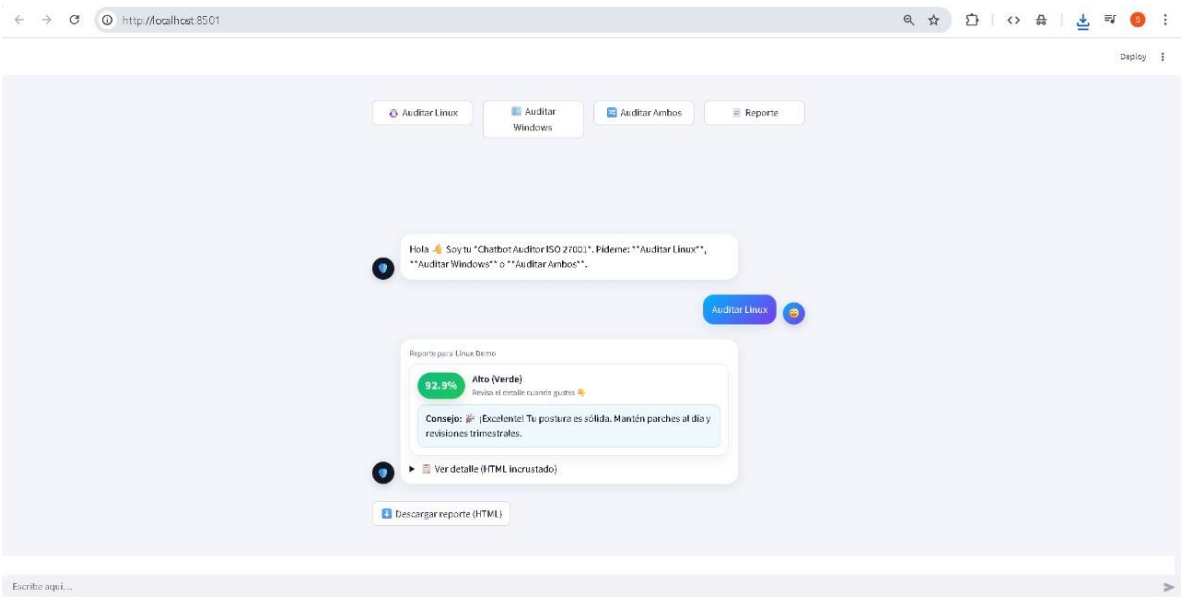


Nota: Elaboración propia.

En la Figura 12 se observa la respuesta interactiva del chatbot tras ejecutar *Auditar Linux*: el sistema inserta en el mismo hilo una tarjeta de resultado con el porcentaje de cumplimiento (92,9 % – Alto, Verde), un mensaje de orientación (Consejo) y un control para expandir el detalle del reporte en HTML incrustado; además, habilita la descarga en un clic del informe completo. Este diseño reduce el cambio de contexto, acelera la toma de decisiones y mantiene la trazabilidad entre el resumen, la evidencia y la acción de remediación sugerida.

Figura 13

Respuesta interactiva del chatbot



Nota: Elaboración propia.

El MVP del Chatbot Auditor ISO/IEC 27001 mostró que funciona completamente para PYMEs: desde que el usuario pide auditar en la interfaz tipo Messenger, pasando por la recolección de datos sin necesidad de agentes (por SSH o WinRM), la evaluación según los controles A.8 y la creación de reportes (HTML/PDF) con evidencia guardada en formato JSON. La interfaz muestra el resultado general con un semáforo, explica los hallazgos con palabras claras y da recomendaciones específicas, lo que ayuda a tomar decisiones rápido sin perder tiempo.

f. Resultados destacados

1. Linux (demo): 92,9% (Alto – Verde), con consejos para mejorar y detalles incluidos.
2. Consolidado (ejemplo): 86,2% (Alto – Verde), con una tabla que muestra los controles según la norma ISO/IEC 27001 A.8.
3. Windows: se revisaron el firewall por perfil, el usuario Invitado, RDP-NLA y la política de contraseñas; además, se comprobó que se manejan bien los errores de privilegios (0x00000522), lo que sirve como evidencia para corregir problemas.
4. Brechas encontradas: en Linux, falta instalar AIDE para la integridad de archivos; en Windows, hay parches con más de 45 días sin actualizar. Estos puntos deben incluirse en el plan de mejora.

2.3 Validación de la propuesta

La validación de la propuesta se llevó a cabo mediante el método de criterios de especialistas, con el fin de garantizar que la herramienta diseñada cumpliera con los objetivos planteados y respondiera a las necesidades reales del entorno empresarial (Ver anexo 3)

Para ello, se seleccionó un grupo de expertos en seguridad informática y administración de servidores Windows y Linux, quienes contaban con experiencia comprobada en la implementación de buenas prácticas de ciberseguridad en PYMEs. Los especialistas evaluaron la propuesta en función de los siguientes criterios:

- **Pertinencia**: grado en que la herramienta responde a las necesidades de las PYMEs en la gestión de la seguridad.
- **Validez técnica**: cumplimiento de los lineamientos establecidos en normativas internacionales como ISO/IEC 27001, CIS Benchmarks y NIST.
- **Funcionalidad**: capacidad del chatbot para realizar auditorías automatizadas de configuraciones críticas en servidores.
- **Usabilidad**: facilidad de uso e interacción en lenguaje natural, accesible para usuarios con distintos niveles de conocimiento técnico.
- **Viabilidad**: posibilidad de implementación práctica en entornos reales, considerando recursos humanos, técnicos y económicos.

El uso de este método dio la posibilidad de retroalimentación directa de los expertos y todos coincidieron en que la herramienta es una adición innovadora y útil para reforzar la seguridad de la información en las PYMEs. También señalaron la capacidad de la herramienta para reducir la necesidad de consultoría externa y para permitir auditorías de manera continua sin la necesidad de una experiencia técnica altamente especializada.

En resumen, la validación por parte de los criterios de los especialistas confirma que la propuesta es técnica y económicamente válida, metodológicamente compatible y funcionalmente relevante, lo que justifica su necesidad de implementación práctica para mejorar la ciberseguridad de las pequeñas y medianas empresas.

2.4 Matriz de articulación de la propuesta

El marco para la construcción de la herramienta de ciberseguridad basada en un chatbot no se concibe en aislamiento, sino que es el resultado de una síntesis de las dimensiones teóricas, metodológicas, técnicas y de resultados de la investigación. En este sentido, la matriz de articulación de la propuesta permite apreciar cómo cada uno de los ejes principales del proyecto se apoya en teorías previas aisladas, se opera con metodologías específicas, se aborda con

técnicas y estrategias adecuadas, y se fundamenta en última instancia utilizando instrumentos fiables para garantizar la veracidad de los hallazgos.

La matriz de articulación de la propuesta se presenta a continuación, en la que se resume la relación entre los ejes principales del proyecto y sus correspondientes instrumentos teóricos, metodológicos, técnicos y de validación. El formato de esta tabla permite apreciar cómo cada aspecto del trabajo está organizado estructuralmente para asegurar que haya un flujo lógico y un fundamento racional en el desarrollo del chatbot propuesto.

Tabla 3

Matriz de articulación

	Ejes o partes principales del proyecto	Sustento teórico	Sustento metodológico	Estrategias/técnicas	Descripción de resultados	Instrumentos aplicados
1	Seguridad de la Información	Basada en la triada de la seguridad (confidencialidad, integridad y disponibilidad) y en normas ISO/IEC 27001 y NIST (Lores, 2024; NIST, 2023).	La metodología de investigación fue bibliografía que permitió tener los conceptos detallados	Revisión de marcos normativos y literatura científica.	Identificación de principios fundamentales de la ciberseguridad aplicables a PYMEs.	Textos, figuras, referencias bibliográficas.
2	Buenas prácticas en servidores (Windows/Linux)	Lineamientos técnicos para gestión de usuarios, privilegios, firewall, cifrado y respaldos (Rubio, 2022; Vega, 2021).	Revisión comparativa de estándares (ISO, CIS, NIST).	Diseño modular de la propuesta incorporando parámetros de seguridad.	Definición de controles críticos que serán auditados por el chatbot.	Guías técnicas, CIS Benchmarks, documentación normativa.
3	Auditoría de sistemas	Concepto y fases de la auditoría informática (planeación, ejecución, informe) (Aquino et al., 2023; Cano, 2022).	Aplicación de metodología descriptiva y entrevistas a expertos.	Automatización de procesos de verificación en servidores.	Elaboración de un proceso automatizado de auditoría basado en estándares.	Guías de auditoría, entrevistas semiestructuradas, listas de verificación.
4	Chatbot con IA y PLN	Chatbots inteligentes para asistencia en seguridad y auditoría (Peña et al., 2022; Ramírez et al., 2023). Procesamiento del lenguaje natural (Mullo et al., 2024).	Prototipado incremental y validación cualitativa.	Construcción de módulos: interfaz, PLN, auditoría y base de conocimiento.	Desarrollo del prototipo funcional del chatbot para auditoría de buenas prácticas.	Scripts de prueba, simulaciones, entrevistas con expertos.
5	Validación de la propuesta	Teoría del juicio de expertos y usabilidad de herramientas tecnológicas (Álvarez, 2024; López et al., 2025).	Método de validación cualitativa y descriptiva.	Encuestas, pruebas funcionales, retroalimentación de especialistas.	Verificación de la utilidad, pertinencia y confiabilidad del producto en PYMEs	Encuestas, entrevistas, matrices de evaluación.

Nota. *La matriz resume la articulación entre los componentes principales de la propuesta y los fundamentos teóricos, metodológicos y técnicos que la sustentan. Elaboración propia a partir de la investigación realizada.*

La matriz ilustra que la propuesta no es puramente teórica. También se relaciona con aspectos metodológicos y técnicos que aseguran su practicidad. Esto también ilustra que los componentes propuestos del chatbot no son solo académicos, sino también prácticos, lo que refuerza la coherencia interna y la relevancia para el contexto de las PYMEs. Por lo tanto, la matriz sirve como un elemento importante para validar la solidez del proyecto y la practicidad del proyecto como una ayuda para la gestión de la seguridad informática.

CONCLUSIONES

Relacionándonos con el primer objetivo, diseñamos la arquitectura de un Auditor de Chatbots conforme a la norma ISO/IEC 27001. Tiene una interfaz de chat para la interacción del usuario, un subsistema de programación de tareas, agentes recolectores que se pueden desplegar mediante SSH y WinRM sin necesidad de instalación, un evaluador de control para la evaluación ponderada de controles, y un módulo de informes que asegura la trazabilidad procedimental. Estos componentes están asociadamente lógicos y funcionalmente al dominio A.8 de acceso, protección de red, vulnerabilidades y controles de monitoreo, lo que proporciona una solución técnica sólida adaptada para pymes.

Para el segundo objetivo, implementamos y probamos un prototipo funcional que realiza auditorías tanto en Linux como en Windows. Durante la prueba se generaron evidencias en formato JSON, se calculó el nivel de cumplimiento y se generaron reportes en HTML y PDF con señales visuales de estatus, los resultados mostraron un cumplimiento alto: 92,9% en Linux y 86,2% en el consolidado total. Se verificaron controles importantes como SSH, firewall, Network Level Authentication y gestión de contraseñas. Además, se detectaron dos brechas concretas: ausencia de AIDE en Linux y un tiempo prolongado para aplicar parches en Windows, lo que orienta a tomar acciones rápidas para mejorar la seguridad.

En cuanto al tercer objetivo, expertos evaluaron la propuesta y asignaron un promedio de 72,9% destacaron la innovación y la base tecnológica empleada. Sin embargo, señalaron que algunos aspectos como la aplicabilidad, factibilidad, enfoque pedagógico y las indicaciones para su uso podrían mejorarse, estos puntos no requieren cambios importantes y se pueden resolver con materiales adicionales, como una guía rápida, ejemplos prácticos y una pequeña sección de preguntas frecuentes. Esto confirma que la propuesta es pertinente y puede aplicarse en el contexto de las PYMEs.

El cuarto y último objetivo formuló una línea solución y un plan de mejora para llevar esta a producción. Sus recomendaciones incluían la instalación y configuración de AIDE en Linux, la reducción a 30 días o menos de la Ventana Permisible de Implantación de Parche en Windows, y la implementación de auditorías y mantenedores de resultados para el historial de auditorías y post resultados funciones. Para la implementación final se recomendó el uso de FastAPI, PostgreSQL, SSO, control de acceso basado en roles, gestión de colas de Redis, y un panel web de React con operación sin agentes y trazabilidad de procesos así la herramienta se auditará, puntuará y reportará con evidencias el cumplimiento de buenas prácticas en servidores Linux y Windows, estableciendo una sólida base para la adopción institucional.

RECOMENDACIONES

Con respecto a la primera deducción acerca de la elaboración del diseño de la solución, se sugiere analizar a fondo la cobertura y estandarización de controles para diferentes tipos de PYMEs. Esto significa, en virtud de la propuesta, asegurarse de que el catálogo se amplíe para incorporar pivotes de referencia tales como los CIS Benchmarks, georeferenciarlo a los estándares clave como ISO/IEC 27001 y NIST CSF, y de igual forma, analizar diferentes alternativas técnicas para la recolección de evidencias como osquery, WMI/WinRM, o agentes en modo ligero, todo esto en el contexto de precisión, latencia y costo operativo; también se sugiere modelar la amenaza y ejecutar pruebas de resiliencia en adversos como pérdida de red o insuficiencia de permisos, esto para validar en el diseño o en el proceso de diseño la robustez en condiciones reales que se suponen difíciles de enfrentar.

En la segunda conclusión, respecto a la implementación y prueba del MVP, se sugiere que se aborden los problemas encontrados durante la ejecución. Para Windows, es necesario formular una política de acceso de menor privilegio para el uso de WinRM y automatizar la detección y recuperación del error 0x00000522, para Linux, se recomienda explorar AIDE en comparación con alternativas como Tripwire o osquery y establecer umbrales y frecuencias adecuadas para la verificación de integridad. El período máximo para la aplicación de parches no debe ser superior a 30 días, y el efecto de esta limitación debe evaluarse en términos de exposición al riesgo y tiempo de recuperación. Es necesario realizar un análisis comparativo antes y después de este período, considerando el cumplimiento y las vulnerabilidades abiertas como métricas técnicas, y para las métricas del proceso, la duración de la auditoría y el retrabajo, con el fin de entender el valor real de tales optimizaciones.

Para mejorar la validación práctica y educativa de la propuesta, se recomienda incluir a más expertos y usuarios, y presentar estadísticas básicas como el promedio, la desviación estándar y la confiabilidad interna para cada aspecto evaluado, también, para facilitar su uso sin hacer grandes cambios, se sugiere crear materiales de apoyo simples, como una hoja con los puntos clave, una guía paso a paso con un ejemplo práctico y una pequeña sección de preguntas frecuentes. Además, es importante medir cómo estos materiales afectan la experiencia del usuario usando herramientas reconocidas, y realizar pruebas que midan el tiempo y éxito al realizar tareas específicas.

La cuarta conclusión para avanzar en la producción y expansión implica trasladar la parte operativa y tecnológica usando herramientas como FastAPI, PostgreSQL, sistemas de acceso seguro, colas con Redis y garantizar alta disponibilidad con Docker o Kubernetes. También se

preparará documentación sobre costos y niveles de servicio. Igualmente, importante es el desarrollo de un plan de implementación mediante el cual las PYME integrarán la tecnología a través de proyectos piloto que evalúen las mejoras en el cumplimiento, la reducción de incidentes y el tiempo dedicado a las auditorías, todo monitoreado a través de un panel de control. Finalmente, se evaluarán los impactos de la tecnología en entornos de uso compartido, con medidas implementadas para proteger la privacidad y conservar la evidencia de auditoría necesaria.

Para difundir y comunicar los hallazgos y impactos, se recomienda elaborar un informe técnico y un artículo corto que documente la metodología, el conjunto de datos anonimizado y los hallazgos. Organizar seminarios o talleres para demostrar todo el flujo de trabajo y las recomendaciones más críticas es aconsejable. Además, es beneficioso producir breves videos instructivos (de 3 a 5 minutos de duración) que proporcionen una guía paso a paso para la implementación, el análisis, la generación de informes y la recuperación de resultados. Finalmente, debe haber un espacio dedicado para almacenar manuales, ejemplos prácticos, plantillas descargables y otros recursos que faciliten la modificación o aplicación en el mundo real de los flujos de trabajo descritos. Estas acciones ayudarán a fortalecer el trabajo académico, fomentar la transferencia de conocimiento y abrir nuevas oportunidades para estudiar cómo se adopta y funciona este método a largo plazo.

BIBLIOGRAFÍA

Abdullah, P., & Shukur, H. (2022). *Sistema de gestión de recursos humanos que utiliza computación en la nube para pequeñas y medianas empresas (PYME).* Obtenido de file:///C:/Users/carrielp/Downloads/TRKU31-5-2020PavelSubhiHananKarwan.pdf

Álvarez, A. (2024). *Estado del arte de técnicas de inteligencia artificial que aporten en la ciberseguridad.* Obtenido de Sitio web de la Universidad Politécnica Salesiana: https://dspace.ups.edu.ec/handle/123456789/27273

Aquino, R., Villarroel, G., & Cuevas, R. (2023). El modelo COBIT 5 para Auditoría Informática de los Sistemas de Información. *Innovación y Software, 4*(1), 63-81. Retrieved from https://www.redalyc.org/journal/6738/673874721005/673874721005.pdf

Beltran, D. (2022). *Implementación y evaluación de buenas prácticas de manufactura (BPM) para plantas procesadoras de lácteos.* Obtenido de file:///C:/Users/carrielp/Downloads/Implementacion_y_evaluacion_de_buenas_practicas_de.pdf

Bustillos, O., & Rojas, J. (2022). PROTOCOLO BÁSICO DE CIBERSEGURIDAD PARA PYMES. *Interfases, 2*(16), 166-184. Obtenido de https://www.redalyc.org/articulo.oa?id=730180375007

Bustillos, O., & Rojas, J. (2023). doi:https://doi.org/10.26439/interfases2023.n017.6246

Cano, J. J. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. *Revista Científica General José María Córdova, 20*(40), 814-832. doi:https://doi.org/10.21830/19006586.866

Casares, D. (2022). *Los estándares internacionales de sistemas de gestión.* Obtenido de https://www.researchgate.net/publication/28113120_Los_estandares_internacionales_de_sistemas_de_gestion

Chinthala, S. (2024). *Herramientas como SIEM.* Obtenido de https://www.researchgate.net/publication/387538937_Analyzing_the_Effectiveness_of_SIEM_Tools_in_Threat_Mitigation_A_Qualitative_Study_in_Cybersecurity

Cute DigitalMedia. (2024). *Chatbots y Servicio al Cliente: La Revolución de la IA*. Obtenido de Sitio web de Cute DigitalMedia: https://www.cutedigitalmedia.com/blog/chatbots-servicio-cliente-ia/

Garzón, M., Del Campo, G., & Loor, B. (2025). Análisis sistemático sobre la eficiencia comunicativa entre chatbots basados en reglas y modelos de lenguaje natural. *Universitas-XXI, Revista de Ciencias Sociales y Humanas, 42*, 167-192. doi:https://doi.org/10.17163/uni.n42.2025.07

INEC. (2024). *Registro Estadístico de Empresas (REEM) – 2023 (Definitivo)*. Obtenido de Sitio web INEC: https://www.ecuadorencifras.gob.ec/directoriodeempresas/

Linux. (2025). *Linux*. Obtenido de Sitio web Linux: https://www.linux.org/

López, L., Gómez, M., & Boumadan, M. (2025). Aplicaciones, beneficios, retos y áreas de desarrollo en el uso de IA-Chatbots. *Digital Education Review*. Retrieved from

https://repositorio.uam.es/bitstream/handle/10486/720545/aplicaciones_matosas_der_2025.pdf?sequence=1

Lores, S. A. (2024). Estrategia de ciberseguridad en la infraestructura. *Revista De Relaciones Internacionales, 19*(1), 13-29. doi:https://doi.org/10.18359/ries.6634

Microsoft. (2025). *Protege, adapta e innova con Windows Server*. Obtenido de Sitio web de Microsoft: https://www.microsoft.com/es-es/windows-server

Moran, B., & Chavez, Y. (2021). *Auditoria de Sistemas Automatizados.* Obtenido de file:///C:/Users/carrielp/Downloads/Auditoria_de_Sistemas_Automatizados.pdf

Mullo, A. H., Balseca, J. M., & Caicedo, N. E. (2024). Retos y oportunidades de la IA en la formación de profesionales. *Razón y Palabra, 28*(11), 28-43. doi:https://doi.org/10.26807/rp.v28i119.2107

NIST. (2023). *The NIST Cybersecurity.* Obtenido de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Peña, J. A., Giraldo, S., Arango, C. A., & Bucheli, V. A. (2022). Un chatbot para asistir a las necesidades de información en tiempos de COVID-19. *Ingeniería y competitividad, 24*(1). doi:https://doi.org/10.25100/iyc.24i1.11001

Prashant, J., & Sanchez, J. (2022). *Natural Language Processing: History, Evolution, Application, and Future Work.* Obtenido de https://www.researchgate.net/publication/350058919_Natural_Language_Processing_History_Evolution_Application_and_Future_Work

Puerta, J. (2022). *Dominio de Arquitectura Empresarial, Armonizando la Simulación de Procesos y la Metodología de Desarrollo de Arquitectura (ADM).* Obtenido de https://www.researchgate.net/figure/Fase-de-planeacion-de-la-auditoria-Etapa-2-Aplicacion-del-modelado-y-simulacion-a-traves_fig1_311160446

Ramirez. (2022). *Estrategias de la planeación en la auditoria.* Obtenido de file:///C:/Users/carrielp/Downloads/Estrategias_de_la_planeacion_en_la_auditoria.pdf

Ramirez, E. P., Pérez, H., Álvarez, M. A., & Aranda, R. (2023). Design, development, and evaluation of a chatbot for hospitality services assistance in Spanish. *Acta universitaria, 33*(e3645). doi:https://doi.org/10.15174/au.2023.3645

Rodríguez, I., Peña, M., Bermudez, A., & Famadas, A. (2021). Proyecto de gestión de redes. *Innovación y Software, 2*(1), 64-82. Retrieved from https://www.redalyc.org/journal/6738/673870838006/673870838006.pdf

Rubio, F. (2022). Innovación y buenas prácticas tecnológicas. *RUSC. Universities and Knowledge Society Journal, 9*(2), 80-85. Obtenido de https://www.redalyc.org/articulo.oa?id=78023425007

Sanchez, J. (2022). *Auditoría a la etapa de planificación y diseño del proceso de compensación.*

SCRUM ORG. (2024). *Welcome to the Home of Scrum!* Obtenido de https://www.scrum.org/

Sierra, O. J., & Mendes, A. M. (2024). Un debate entre la inteligencia artificial y la ideología. *Razón y Palabra, 28*(19), 1-14. doi:https://doi.org/10.26807/rp.v28i119.2090

Sierra, O., & Magnolia, A. (2022). *Un debate entre la inteligencia artificial y la ideología.* Obtenido de file:///C:/Users/carrielp/Downloads/2090Sierra.pdf

Tejedo, C. (2024). *Desarrollo de un ChatBot asistido por IA para analistas de ciberseguridad.* Obtenido de Sitio web de la Universitat Politécnica de Valencia: https://riunet.upv.es/entities/publication/c685c759-4d01-4f7b-81cf-3f6c813f5bbb

Vega, E. (2021). *Modelo Balanced Scorecard para los controles críticos de seguridad informática según el Center for Internet Security (CIS).* Obtenido de https://www.researchgate.net/publication/347811938_Modelo_Balanced_Scorecard_para_los_controles_criticos_de_seguridad_informatica_segun_el_Center_for_Internet_Security_CIS

Wunsch, L. P., & Nikolay, J. R. (2022). Chatbot: comunicación digital y religiosidad tras la pandemia en Latinoamérica. *Universitas-XXI, Revista de Ciencias Sociales y Humanas*(37), 101-121. doi:https://doi.org/10.17163/uni.n37.2022.04

ANEXOS

ANEXO 1

Objetivo del instrumento:

Recabar información de especialistas en seguridad de la información de PYMEs sobre el nivel de cumplimiento de buenas prácticas en servidores Windows y Linux, así como su percepción frente al uso de un chatbot como herramienta de auditoría.

Escala de valoración:

1 = Totalmente en desacuerdo
2 = En desacuerdo
3 = Ni de acuerdo ni en desacuerdo
4 = De acuerdo
5 = Totalmente de acuerdo

Datos generales del entrevistado:

- Empresa: _____
- Cargo: _____
- Años de experiencia en TI / Ciberseguridad: _____

Preguntas de la entrevista:

1. ¿Qué importancia tiene la seguridad de los servidores en el funcionamiento de su empresa?

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

2. ¿Con qué frecuencia realizan auditorías de seguridad en sus servidores Windows y/o Linux?

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

3. ¿Qué métodos o herramientas utilizan actualmente para verificar buenas prácticas de configuración?

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

4. ¿Cuáles son las principales dificultades que enfrentan al realizar auditorías de seguridad?

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

5. ¿Qué consecuencias han tenido debido a la falta de controles adecuados en sus servidores?

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

6. ¿Considera que una herramienta automatizada podría facilitar la auditoría de seguridad en su empresa?

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

7. ¿Qué características debería tener una herramienta de este tipo para ser útil en una PyME?

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

8. ¿Cree que un chatbot inteligente sería una alternativa práctica para asistir en auditorías de servidores?

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

9. ¿Qué limitaciones o riesgos percibe en el uso de un chatbot de auditoría?

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

10. ¿Qué impacto cree que tendría la implementación de una solución de este tipo en la seguridad de su empresa?

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

Anexo 2. Encuesta aplicada al personal de TI de las PYMEs

Objetivo del instrumento:

Evaluar el nivel de cumplimiento de buenas prácticas en servidores Windows y Linux, así como la percepción sobre el uso de un chatbot inteligente como herramienta de auditoría de seguridad.

Instrucciones:

Marque con una "X" la opción que mejor refleje la situación en su empresa, según la escala siguiente:

Escala de valoración (Likert de 5 puntos):

1 = Totalmente en desacuerdo
2 = En desacuerdo
3 = Ni de acuerdo ni en desacuerdo
4 = De acuerdo
5 = Totalmente de acuerdo

Ítems de la encuesta

Pregunta 1. La seguridad de los servidores es crítica para la continuidad operativa de mi empresa.

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

Pregunta 2. Realizamos auditorías de seguridad a servidores Windows y/o Linux con una periodicidad establecida.

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

Pregunta 3. Utilizamos métodos y herramientas formales para verificar buenas prácticas de configuración en servidores.

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

Pregunta 4. Enfrentamos dificultades significativas (tiempo, personal, costo) para realizar auditorías de seguridad.

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

Pregunta 5. La falta de controles adecuados ha derivado en incidentes o riesgos relevantes en nuestros servidores.

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

Pregunta 6. Una herramienta automatizada facilitaría la auditoría de seguridad en mi organización.

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

Pregunta 7. Para que sea útil en una PyME, la herramienta debe ser fácil de usar, de bajo costo y con guías claras de remediación.

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

Pregunta 8. Un chatbot inteligente sería una alternativa práctica para asistir en auditorías de servidores.

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

Pregunta 9. El uso de un chatbot de auditoría implica riesgos o limitaciones que deben gestionarse (actualización, exactitud, privacidad).

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

Pregunta 10. La implementación de esta solución mejoraría la seguridad de la empresa y reduciría incidentes en servidores.

Escala	1	2	3	4	5
Marque	☐	☐	☐	☐	☐

Anexo 3. Juicio de Expertos

Universidad Israel

ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital " **Propuesta de Herramienta de Ciberseguridad fundamentada en un Chatbot basado en la ISO 27001 para la auditoría de buenas prácticas en Servidores Windows y Linux para las Pymes** ". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: ING. PAMELA CARRIEL CASTILLO
Título obtenido: INGENIERA EN SISTEMAS COMPUTACIONALES
C.I.: 0950415414
E-mail: pamelacarriel03@gmail.com
Institución de Trabajo:
Cargo: Ingeniera en QA
Años de experiencia en el área: 5

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: " Propuesta de Herramienta de Ciberseguridad fundamentada en un Chatbot basado en la ISO 27001 para la auditoría de buenas prácticas en Servidores Windows y Linux para las Pymes "

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia		x			
Aplicabilidad	x				
Factibilidad	x				
Novedad		x			
Fundamentación pedagógica			x		
Fundamentación tecnológica		x			
Indicaciones para su uso	x				
TOTAL	15	12	3		

Observaciones: El desarrollo obtiene un puntaje de 30 puntos según las variables evaluadas

Recomendaciones: Se recomienda incorporar como mejora mínima una guía rápida de uso (1 página) con pasos básicos y requisitos, más un ejemplo práctico de ejecución.

Lugar, fecha de validación: 1/09/2025

Firma del especialista
Pamela Carriel Castillo

Universidad Israel

ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital " **Propuesta de Herramienta de Ciberseguridad fundamentada en un Chatbot basado en la ISO 27001 para la auditoría de buenas prácticas en Servidores Windows y Linux para las Pymes** ". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: ING. IRVING GARZÓN SOLEDISPA
Título obtenido: INGENIERO EN SISTEMAS COMPUTACIONALES
C.I.: 0950901264
E-mail: Garzónsirving@gmail.com
Institución de Trabajo:
Cargo: Ingeniera en Implementación de proyectos
Años de experiencia en el área: 3

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: " Propuesta de Herramienta de Ciberseguridad fundamentada en un Chatbot basado en la ISO 27001 para la auditoría de buenas prácticas en Servidores Windows y Linux para las Pymes "

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia		x			
Aplicabilidad	x				
Factibilidad			x		
Novedad		x			
Fundamentación pedagógica		x			
Fundamentación tecnológica		x			
Indicaciones para su uso			x		
TOTAL	5	16	6		

Observaciones: El desarrollo obtiene un puntaje de 27 puntos según las variables evaluadas

Recomendaciones: Se recomienda incorporar como mejora mínima una guía rápida de uso (1 página) con pasos básicos y requisitos, más un ejemplo práctico de ejecución.

Lugar, fecha de validación: 1/09/2025

Firma del especialista
Irving Garzón Soledispa