Universidad EAN Facultad de Ingeniería

Programa Académico Ingeniería de Sistemas

Desarrollo de una aplicación web para capacitación en seguridad cibernética: una herramienta para el crecimiento de ManageEngine en Chía

Proyecto de Grado

Proyecto de Integración

Autor:

Juan Sebastián Narváez Molina

Director:

Emanuel Elberto Ortiz Ruiz

Bogotá, 2024

Resumen Ejecutivo

Actualmente en una era que se torna en pro de la transformación digital, las empresas en el sector de Chía en Colombia afrontan diversas y crecientes tipos de amenazas cibernéticas en su interacción con el ciber espacio. Esas amenazas pueden conllevar graves repercusiones tanto en el plano operativo como en uno de los aspectos cruciales para cualquier compañía, la afectación de la confianza de sus clientes. Según las nuevas tecnologías se desarrollan, las tácticas, estrategias y herramientas de los cibercriminales, por lo que las empresas afrontan un maro de vulnerabilidades cambiantes, como se menciona en (Rodríguez Zambrano & Moreno Tamayo, s/f).

La pérdida de los datos confidenciales resulta no solo en daños a la reputación de una empresa sino también en problemáticas financieras pueden acabar progresivamente con la salud de una compañía. Adicionalmente, las regulaciones establecidas respecto a la seguridad cibernética son día a día más rigurosas aumentando así la necesidad de abordar este problema con la seriedad que lo amerita.

Este estudio tiene como principal objetivo analizar y evaluar las ciber amenazas a las que es expuesta la empresa ManageEngine situada en Chía con la finalidad de desarrollar una aplicación que permita de primera mano capacitar a los empleados del común frente a dichos riesgos expuestos al adentrarse al mundo digital resaltando la importancia de la capacitación cibernética como se menciona en (Ortiz Osorio, 2021). Los objetivos específicos abordan la identificación las amenazas más comunes, la medición de los esfuerzos de concientización en ciberseguridad, el análisis de los planes de respuesta junto con su respectiva recuperación de incidentes, resaltar el impacto económico de los ataques cibernéticos como se menciona en (Gil

López et al., 2021), comprender las herramientas de desarrollo modernas parala escalabilidad de la aplicación y entender como la realización de un diseño con buenas prácticas de interfaz de usuario puede conllevar a una mejor interacción con la aplicación.

Este proyecto se basa en su relevancia social, concurrencia, valor teórico y utilidad metodológica. Las ciber amenazas afectan la confianza del cliente, la salud económica y la integridad de los datos comprometidos. Lo que hace de este desarrollo una pieza crucial para el fortalecimiento empresarial moderno. Además, se busca contribuir al cuerpo de conocimiento en la seguridad cibernética y servir de modelo para futuros estudios y desarrollos en otras regiones y contextos.

Palabras clave:

Amenazas Cibernéticas, Aplicación, Seguridad Cibernética, ManageEngine, Chía, Resiliencia Empresarial, Concienciación en Ciberseguridad, Planes de Respuesta a Incidentes, Protección de Datos, Experiencia de Usuario.

Tabla de contenido

Introducción

Teniendo en cuenta el crecimiento exponencial y transición tecnológica que menciona (Botero Zuluaga et al., 2023), las compañías se enfrentan a un escenario de oportunidades y amenazas sin precedentes. Este avance tecnológico ha desatado muchas ciber amenazas de crecimiento y evolución constante que pueden socavar las operaciones comerciales y la confianza depositada por los clientes actuales y potenciales hacia la compañía. En el informe proporcionado por SONICWALL para el año 2022 se revela un crecimiento constante en la prevalencia de amenazas cibernéticas, lo que denota la urgente necesidad de abordar esta problemática.

La empresa ManageEngine al ser una empresa del sector tecnológico enfrenta importantes desafíos en cuanto a seguridad cibernética se refiere, dentro de dichos desafíos se incluyen la propagación de malware, las amenazas internas, el phishing, los ataques de ransomware, entre otros tipos de ataques. Estos desafíos como lo menciona (Patiño, 2023) atentan contra la capacidad de las empresas para mantener su operación con normalidad.

En este sentido la ciberseguridad no solo es un problema tecnológico, sino que también se torna en un asunto de vital importancia económica y social. Los problemas financieros y daños en la reputación son resultado de la pérdida de datos confidenciales, en este sentido se busca analizar y evaluar el panorama de las amenazas de seguridad cibernética que enfrenta la empresa ManageEngine. Por lo que a razón de ello surgen otros inconvenientes de análisis como lo son la identificación de las amenazas cibernéticas más comunes, la medición los esfuerzos de concientización, la relevancia de la capacitación en seguridad cibernética, el entendimiento de como lo visual impacta en el aprendizaje, la comprensión sobre el análisis de los planes de

respuesta y como promover conocimiento a una generación de crecimiento tecnológico exponencial. Por todo lo anteriormente descrito surge la pregunta ¿Existe alguna aplicación web desarrollada para la empresa ManageEngine que provea el entendimiento sencillo y práctico del fortalecimiento de la seguridad cibernética?

Objetivos

Objetivo general

Desarrollar una aplicación web que permita facilitar funciones o ambientes para capacitar a los colaboradores en principios de ciberseguridad para la empresa ManageEngine.

Objetivos específicos

- Medir la concientización y capacitación sobre temas de seguridad cibernética: Estudiar y clasificar el nivel de conocimiento de los individuos de una empresa respecto al mundo cibernético ahondando en las buenas prácticas a la hora de interactuar en el ciberespacio.
- Identificar las amenazas más comunes en el ciberespacio: Observar las ciber amenazas que predominan en el ciber espacio y que afronta la empresa ManageEngine, dentro de las que se incluyen el *malware*, *phishing*, el *ransomware*, las amenazas internas y más.
- Visualizar el impacto económico que dejan los incidentes cibernéticos: Dar visibilidad de las repercusiones monetarias que se deben afrontar tras sufrir un ataque cibernético.

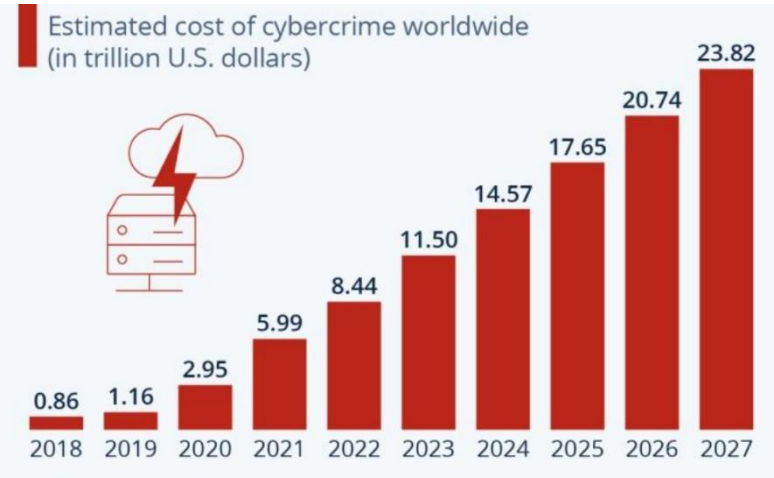
- Seleccionar un entorno de desarrollo y lenguaje de programación escalable: Establecer un entorno actual que compile un código capaz de alcanzar todos los requerimientos para una aplicación web, además de seleccionar un lenguaje moderno mundialmente utilizado que permita el crecimiento del proyecto cuando lo requiera.
- Construir una base de datos estructurada: Recolectar, organizar y almacenar toda la información que será expuesta en la aplicación web con el propósito de contar con un centro de información que pueda ser fácilmente gestionado y actualizado.
- Desarrollar el frontend de la aplicación web: Realizar el desarrollo de la visualización de la aplicación web de manera que se muestre intuitivo y fácil de usar.
- Integrar la base de datos con el frontend: Realizar la integración de la base de datos de conocimientos con lo que se va a visualizar de la aplicación web de manera que esta termine como un desarrollo *fullstack.*

Problema de investigación

Las empresas están enmarcadas en un mundo cada vez más digitalizado. El cambio y la creación masiva de tecnologías ha traído consigo ventajas competitivas en cuanto a eficiencia y acceso a nuevas oportunidades de negocio. Sin embargo, pese a dichos beneficios, la transformación y transición tecnológica también han abierto una amplia gama de amenazas cibernéticas que cada día van en aumento según lo menciona (Ruddin & Subhan Zein SGN, 2024).

Figura 1

Costo Estimado de los Ciber Ataques en el Tiempo

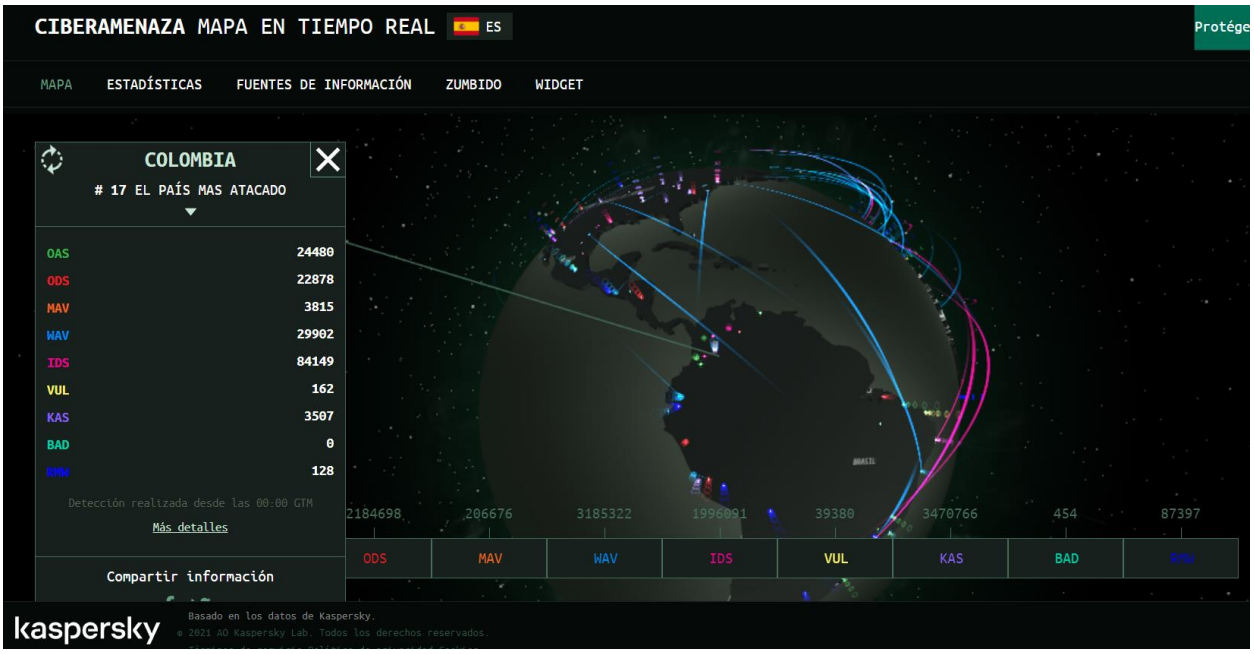


Nota. Datos expresados en trillones de dólares. Reproducida de Tecnología Hecha Palabra, (*Los ciberataques descontrolados son una amenaza creciente para la frágil economía mundial*, 2023)

Chía, uno de los principales centros empresariales de Colombia, un país que está en el puesto 17 en el ranking mundial de ataques cibernéticos según el mapa en tiempo real de amenazas cibernéticas (Kaspersky), enfrenta desafíos importantes en cuanto a la seguridad cibernética se refiere. Estos desafíos incluyen la propagación de *software* malicioso, técnicas de ingeniería social combinadas con *phishing* cuya finalidad es robar información sensible, ataques de tipo de denegación de servicio o denegación de servicio distribuido que bloquean el acceso a datos valiosos y los riesgos que pueden surgir desde dentro de la propia compañía. Estas problemáticas descritas resultan en la repercusión de la capacidad de las empresas para operar con normalidad y para mantener la confianza de sus clientes y socios según (Patiño, 2023).

Figura 2

Mapa de Ciber Amenazas en Colombia



La principal raíz de este problema nace de la convergencia entre el rápido crecimiento de la tecnología digital y las estrategias e innovación de aquellos que buscan explotar sus vulnerabilidades. Con el transcurso del tiempo y a medida que las empresas adoptan nuevas tecnologías que buscan mejorar sus operaciones, también se exponen a nuevas vulnerabilidades que los ciberdelincuentes pueden aprovechar. El desaforado crecimiento de las tácticas, técnicas y procedimientos de ataque significa que las empresas constantemente se encuentran luchando por mantenerse actualizados respecto a la información relacionada con las últimas amenazas y medidas de seguridad.

Este problema se acrecienta aún más debido a la cantidad de información sensible que las empresas manejan en sus operaciones. Dichos datos pueden variar desde datos personales de los clientes hasta información financiera, el perder estos datos puede resultar en consecuencias graves. Los problemas financieros se pueden suscitar junto con daños a la reputación y la buena

credibilidad de la empresa, de manera que dichos efectos afecten fuertemente a la integridad de la compañía misma.

Existe también una presión adicional ejercida a esta problemática en donde las regulaciones como la ISO/IEC 27032 que trata temas sobre la gestión de la ciberseguridad día a día más estrictas en cuanto a la protección de datos y privacidad se refiere. En consecuencia, se vuelve imperativo que las empresas garanticen que sus prácticas cumplan con estos estándares, considerando que el incumplimiento de dichas regulaciones puede resultar en multas y sanciones, aumentando la necesidad de abordar la seguridad cibernética muy común.

En este sentido, la necesidad de abordar estas amenazas cibernéticas se vuelve un tema urgente. La empresa de tecnología ManageEngine debe no solo ser conciente de la importancia de la capacitación en la prevención de posibles ataques, sino que también debe estar preparada para responder de la mejor manera posible si estos ataques llegan a ocurrir. Esta compleja problemática abarca una amplia gama de aspectos, desde los tecnológicos y organizacionales hasta los humanos.

Gran parte de la población como lo menciona (Maggi Murillo & Gómez Gómez, 2021) no comprende la importancia de la seguridad cibernética además de no contar con herramientas que sirvan como fuente de conocimiento en varios de los aspectos principales para el entendimiento de dicho tema. Por lo que, de quedarse atrás, los ciber delincuentes pueden devastar con una mayor facilidad la integridad de las empresas establecidas como objetivos de ataque al aumentar sus conocimientos y aprovechar la desinformación de sus víctimas.

Justificación

El presente proyecto propuesto sobre el desarrollo de una aplicación web que permita capacitar e informar sobre las diversas amenazas cibernéticas en beneficio de la protección en la interacción con el ciber espacio destinado principalmente a la empresa de tecnología ManageEngine localizada en Chía Colombia cuenta con una gran pertinencia y utilidad en múltiples dimensiones del sector empresarial, no solo para la compañía sino también para el empleador y sus respectivo equipo de trabajo, como consecuencia este desarrollo se impulsa por su significado en los términos de brindar un espacio de información relevante y accesible basada en la importancia social, la concurrencia, las implicaciones prácticas, el valor teórico, la utilidad metodológica y la importancia de comprender como una aplicación para la capacitación en seguridad cibernética puede conllevar a diferentes veneficios como lo son la comprensión de la protección de los datos sensibles, el entendimiento del cumplimiento normativo, la concientización junto con la respectiva prevención, la reducción de los costos empresariales y la competitividad al tener la confianza del cliente. Donde a lo largo de la justificación se presenta el porqué de cada término.

Primeramente, en la investigación cualitativa de (Núñez Reiz et al., 2019) realizada en grupos empresariales, similares a los de ManageEngine, evidencia una fuerte afectación de la confianza entre los clientes después de un incidente cibernético. En su gran mayoría, las entrevistas con las personas afectadas revelan cómo los datos comprometidos dan lugar a sentimientos de vulnerabilidad, causando así que los clientes se muestren reacios a participar digitalmente en las empresas. Estos hallazgos enfatizan los costos intangibles de los incidentes

cibernéticos, lo que subraya la confusión emocional que experimentan los usuarios cuya información personal se ve comprometida.

Cuando se trata de la concurrencia se hace necesario entender que en una era denotada por el aumento de las amenazas cibernéticas y los vectores de ataque en constante evolución simultáneamente también existen las herramientas para tratarlos como bien lo puede ser el *darknet monitoring* que como se menciona en (Charan et al., 2023) responde al tráfico malicioso dirigido a direcciones "IP" maliciosas. En este sentido cobra relevancia el conocimiento sobre el panorama de la ciberseguridad en la empresa de tecnología ManageEngine. La confluencia que existe entre la creciente sofisticación de los ciber ataques y los avances tecnológicos requieren de la realización de un examen de vulnerabilidades y sistemas de mitigación, además de también reforzar la seguridad principal de la empresa pues como se menciona en (Gandal et al., 2023) al emplear mayores precauciones en ámbito de la seguridad se reducen en gran medida las probabilidades de sufrir un incidente cibernético.

Teniendo en cuenta que el contexto que presenta las empresa ManageEngine es similar al que presentan las compañías de todo el mundo sobre temas de interacción con la tecnología en donde nace una dependencia cada vez mayor de los medios y plataformas digitales para poder operar adecuadamente, la protección de los datos confidenciales se convierte en un tema de interés principal, esto a causa de que las empresas actúan como pilares críticos en la economía local y por lo tanto como lo menciona en (Rawindaran et al., 2023) su vulnerabilidad a las ciber amenazas puede conllevar a efectos cascada en la seguridad laboral, la confianza para los inversionistas y generalmente la estabilidad económica. Por lo que se hace necesario proteger de ataques tales como el *phishing* que como menciona en (Hillman et al., 2023) es uno generalmente más afrontan las empresas en cualquier parte del mundo.

Otro punto clave de respecto a los conceptos tratados en el proceso de investigación, es la relevancia social de la misma donde como menciona (Krawczyk-Sokołowska & Caputa, 2023) las empresas dependen cada vez más de las plataformas digitales para realizar sus operaciones y como consecuencia de ello se presentan los objetivos estratégicos de la protección de la información, en donde se incluyen los registros financieros, los datos de los clientes e incluso la información comercial patentada, también está el punto de la preservación de la privacidad esto debido a que las personas confían su información comercial en las empresas esperando que esta sea manejada responsable y se salvaguarde la integridad de los datos, lo anteriormente descrito se dfine técnicamente con un término denominado CTI el cual por sus siglas representa *Cyber Threat Intelligence* la cual como se menciona en (Ainslie et al., 2023) es el conocimiento y entendimiento de las amenazas en la información de las organizaciones que abarca temas de objetivos, intenciones, limitaciones, estrategias y vulnerabilidades.

La relevancia social de la seguridad ciberseguridad en el entorno empresarial es destacada por una gran cantidad de evidencia cuantitativa que muestra los impactos tangibles y de gran alcance de las amenazas cibernéticas en las personas, las empresas y la sociedad en su conjunto.

En un análisis intersectorial realizado por (*Martinez v. Johnson & Johnson Consumer Inc., 471 F. supp. 3d 1003*, 2020) se estableció cuantitativamente que el tiempo necesario para recuperarse de un incidente cibernético era directamente proporcional a la gravedad de la infracción. En promedio, las empresas experimentaron un tiempo de interrupción en sus operaciones de 6,2 días para infracciones menores, sin embargo, esto aumentó a 20,8 días alarmantes para infracciones importantes. El impacto cuantificable en la productividad, la

generación de ingresos y el servicio al cliente durante tiempos de inactividad tan prolongados resalta el estrecho vínculo que existe entre la ciberseguridad y la continuidad del negocio.

Otro de los aspectos clave de la relevancia social es la estabilidad económica del país, porque al presentarse interrupciones en las operaciones comerciales, se provocan pérdidas financieras e incluso recortes de personal, alineado con lo mencionado se puede presentar la resiliencia a las cadenas de suministro porque muchas empresas están interconectadas a través de estas, por lo que en el punto en que una de estas empresas sufre un ataque cibernético genera un efecto domino que perjudica a todos sus socios comerciales. También se tiene en juego frente a un ciber ataque la confianza del consumidor ya que un cliente pierde la confianza en una compañía que no solo es constantemente vulnerada cibernéticamente, sino que también le cueste recuperarse tras el incidente. Uno de los puntos más cruciales es la protección de la infraestructura crítica que se explica como menciona (Cano-Martínez, 2022) en el ataque que afecta también los servicios esenciales como la energía, el transporte, la atención médica, entre otros.

La información que contendrá la aplicación tras pasar por todo el proceso previo de investigación busca contar con implicaciones prácticas directas para la empresa de tecnología ManageEngine basadas en conocimientos adquiridos como el “LATAM-DDoS-IoT” que como se menciona en (Almaraz-Rivera et al., 2022) es una metodología de detección de anomalías especializada en ataques de tipo “DoS” y “DDoS”. Esto a razón de que el identificar las amenazas y vulnerabilidades cibernéticas de mayor predominancia mediante el uso de ataques con entornos controlados, con la finalidad de entender la perspectiva del atacante cómo se menciona en (Hendi Muhammad et al., 2023) permite encontrar brechas de seguridad en las defensas de la compañía, lo que a su vez brinda la posibilidad de un fortalecimiento empresarial

tratando sus mecanismos de protección frente al entorno digital. Las estrategias recomendadas para la prevención, detección y respuesta mejoran la continuidad operativa, la confianza del cliente y la integridad de los datos, alineando así los objetivos comerciales bien sean individuales o conjuntos de cada empresa con prácticas digitales más seguras.

La información que se busca exponer contribuye teóricamente al profundizar la comprensión de la compleja interacción que existe entre las amenazas de la seguridad cibernética y la resiliencia empresarial, cuando se enfatiza en los detalles del entorno empresarial en Chía la investigación enriquece el cuerpo de conocimiento existente en el campo, adicionalmente, los hallazgos del estudio amplían potencialmente los marcos de seguridad cibernética existentes y las teorías fomentando así una comprensión holística respecto a los desafíos que afrontan las compañías de este contexto geográfico y socioeconómico único.

En lo que respecta al rigor metodológico empleado en el estudio incluyendo la recopilación, análisis e interpretación de datos relacionados o no entre sí, además del uso de *middleboxes* que como se menciona en (Odegbile et al., 2023) que ofrecen opciones poderosas y flexibles como *firewalls*, detección de intrusiones, *proxyng* y captura de tráfico monitoreado servirán para beneficiar la no solo a la empresa ManageEngine sino también a la comunidad académica y de investigación en general, a razón de que se pueden plantear estudios haciendo uso del modelo de la aplicación para entornos similares en otras regiones del país o en otros espacios en el mundo, fomentando un enfoque colaborativo para comprender las amenazas de la seguridad cibernética.

Es importante resaltar que una aplicación web permite que en un mundo digitalizado cuyas empresas manejan altos volúmenes de información sensible de sus clientes exista una herramienta que permita comprender la importancia de esos datos sensibles, que muestre el

cumplimiento normativo de manera conjunta y clara la ley de protección de los datos particularmente para Colombia.

La aplicación busca fortalecer la concientización y prevención respecto al mundo cibernético, ya que al mostrar evidencias de casos de uso las personas que interactúan con la aplicación pueden comprender de forma ejemplificada por qué tomar ciertas acciones dependiendo de la situación presentada, adicionalmente se busca destinar un apartado cuya finalidad es exponer las ventajas del comprender sobre ciberseguridad para temas de reducción de costos y competitividad frente a la confianza del cliente ampliando dicha información con gráficas el compromiso por el crecimiento.

El estudio propuesto sobre las amenazas de seguridad cibernética en la empresa ManageEngine situada en Chía para el desarrollo de la aplicación web, posee una concurrencia convincente, relevancia social, implicaciones prácticas, valor teórico y utilidad metodológica y muestra ventajas como exponer la información relevante donde se describen la importancia de la protección sensible de los datos, el cumplimiento normativo, la concientización y prevención, la reducción de costos y la competitividad para ganar la confianza del cliente al mostrar una vía sobre la intersección.

Análisis de Requerimientos

En el contexto de este proyecto de grado enfocado en la seguridad cibernética y el desarrollo web en pro del beneficio de la empresa de chía ManageEngine, se busca el entendimiento de las necesidades específicas tanto de la empresa como de los usuarios finales

donde se definen los requisitos funcionales y no funcionales que brinden una base de diseño para el desarrollo de la aplicación web.

El análisis de requerimientos para este proyecto de grado cobra una gran relevancia ya que permite comprender las necesidades del cliente a través de la identificación de necesidades, la definición de funcionalidades además de alinearse con objetivos alcanzables, definir las características de la aplicación e identificar posibles restricciones y riesgos lo cual proporciona una base sólida tanto para el desarrollo como para la implementación satisfactoria de la aplicación web de capacitación en seguridad cibernética para la empresa ManageEngine.

En este sentido este análisis de requerimientos se deriva también en dos temas principales cruciales los cuales son las restricciones directas del proyecto y los componentes tecnológicos y de innovación.

Restricciones directas del proyecto

Dentro de las restricciones encontradas se encuentran limitaciones de naturaleza financiera, temporal, técnica y legal como las siguientes:

- Recursos financieros: El proyecto se encuentra limitado según el presupuesto asignado debido a que se requiere adquisición de herramientas de tecnología y la contratación de personal capacitado
- Tiempo: El tiempo resulta una principal limitante ya que completar el proyecto en un espacio temporal definido afecta directamente tanto la planificación como la ejecución de las actividades.

- Capacidad técnica: A la hora de implementar funcionalidades o tecnologías avanzadas se ven directamente relacionadas las habilidades y conocimientos técnicos con los que debe contar el equipo de desarrollo.
- Requisitos legales y normativos: Es de vital importancia que el proyecto cumpla con regulaciones y estándares legales que cuenten con relación con la seguridad de la información y la protección junto con el tratado de datos.
- Disponibilidad de datos: Es de vital importancia que el proyecto cumpla con regulaciones y estándares legales que cuenten con relación con la seguridad de la información y la protección junto con el tratado de datos.

Componentes tecnológicos y de innovación

- Desarrollo web moderno: Se busca hacer uso de tecnologías actuales y *frameworks* de desarrollo como HTML5, CSS3 y JavaScript de manera que se logre desarrollar una interfaz dinámica con una alta experiencia de usuario
- Aplicación interactiva: Dentro de la aplicación web se componentes dinámicos e interactivos que capturen la atención del usuario, como lo pueden ser evaluaciones de conocimientos y direccionamiento a sitios que complementen la información suministrada.
- Integración de datos: Se integrará una base de datos MySQL que almacenará la información del tipo de usuario y sus resultados en los exámenes.
- Capacitación en seguridad cibernética: La aplicación web contara con módulos de capacitación interactivos que les permitan a los empleados de la empresa ManageEngine aprender sobre mejores prácticas de seguridad cibernética además

de brindar concientización sobre los principales riesgos a los que se está expuesto al navegar en internet.

Adicionalmente, para el desarrollo de este proyecto, surgen como restricciones económicas contar con un presupuesto que sea destinado para las funciones de pago para el equipo de desarrollo del *frontend* de la aplicación en donde como lo revelan estudios de (Sharma, 2021) el costo estimado para el desarrollo de una aplicación web simple oscila desde los 3000 hasta los 17000 dólares. También se deben tener en cuenta los costos de mantenimiento que como se menciona en (Weisheim, 2022) el cual es un sitio especializado en dominios web, los precios del mantenimiento varían desde los 60 hasta los 6000 dólares por año y los costos de infraestructura o de compra de un dominio son en promedio de 10 a 15 dólares por año en donde estos se encuentra supeditados a múltiples factores como lo pueden son el registrador que se elija o incluso la protección adicional de privacidad (Betania, 2022).

Por otra parte, existen también restricciones legales cuando se desarrolla una aplicación web para la capacitación en seguridad cibernética que van desde el cumplimiento de leyes de protección de datos, el cumplimiento de normativas de seguridad cibernética con estándares como NIST junto con las políticas de seguridad digital proporcionados por el MinTIC en Colombia como se menciona en (*Política de Seguridad Digital - Política de Seguridad Digital*, s/f) y la propiedad intelectual.

Marco de Referencia

La evolución institucional del ciberespacio en Colombia y su relación con la interacción civil-militar, según el estudio realizado por Villamil et al. (2020), es un aspecto crucial que requiere atención, en este contexto, resulta evidente que las empresas en Chía se vean expuestas a diversas amenazas cibernéticas, dichas amenazas van desde ataques de phishing hasta ransomware y malware, lo cual puede causar un impacto significativo en la continuidad de las operaciones comerciales y la confidencialidad de la información.

Como parte de una estrategia integral de ciberseguridad y ciberdefensa, es imperativo que las empresas se preparen para contrarrestar estas amenazas.

La política gubernamental en materia de ciberseguridad y ciberdefensa tiene como objetivo influir en las prácticas de seguridad de las empresas en Chía. Las regulaciones y directrices establecidas pueden moldear la forma en que las empresas deben salvaguardar sus activos digitales y responder a incidentes cibernéticos. Según el Ministerio de Tecnologías de la Información y las Comunicaciones, MinTIC, estas políticas buscan que “las empresas conozcan e identifiquen los riesgos a los que están expuestos en el entorno digital y aprendan como protegerse, prevenir y reaccionar ante los delitos y ataques cibernéticos” (Política de seguridad digital, s. f.).

Es importante destacar que muchas empresas, especialmente las PYMEs, a menudo son blanco de ciberataques debido a sus limitaciones financieras para invertir en medidas de ciberseguridad. Como lo indica la investigación de Rawindaran et al. (2023), la falta de recursos dificulta la implementación de medidas de seguridad adecuadas.

Las empresas en Chía enfrentan una gran variedad de amenazas cibernéticas, que incluyen ataques de phishing, malware y ransomware, por esta razón, la necesidad de comprender dichas amenazas y su impacto en las organizaciones de la región es cada vez más

apremiante. La política de seguridad digital desempeña un papel crucial al proporcionar recursos y apoyo a estas empresas, permitiéndoles mejorar su postura de ciberseguridad y analizar cómo están siendo atacadas y cómo pueden defenderse de manera más efectiva.

Al enfrentarse día a día a estos ciberataques lo que busca la investigación de Almahmoud et al. (2023), es introducir modelos más eficaces de “machine learning” para automatizar la tarea de detectar, rastrear y bloquear malware e intrusos, aplicando enfoques que permitan incluir la identificación temprana de vulnerabilidades, la monitorización constante de la red y la implementación de medidas de seguridad avanzadas.

Analizando el impacto de estas estrategias en la reducción de la exposición al riesgo cibernético y en la mitigación de posibles pérdidas, incluyendo la evaluación de métricas clave como la disminución en el número de incidentes cibernéticos o la reducción del tiempo de recuperación después de un ataque, se evidencia que es importante implementar mecanismos que sean la clave para marcar la diferencia en la capacidad de las empresas de la ciudad para proteger sus activos digitales y salvaguardar la información sensible de sus clientes.

Según las investigaciones realizadas por Gandal et al. (2023) y Hillman et al. (2023), junto con el uso de tecnologías basadas en el aprendizaje automático que permiten la detección temprana de amenazas, también se destaca la importancia de evaluar la efectividad del entrenamiento en seguridad informática para los empleados de las empresas de tecnologías. Además, se sugiere que los resultados de este entrenamiento varían dependiendo del tipo de ataque, especialmente de aquellos altamente personalizados realizados con ingeniería social de por medio, es por esto que una aplicación como centro de capacitación de seguridad cibernética invita a la empresa ManageEngine a realizar un análisis exhaustivo del impacto de estos programas de capacitación, incluyendo la medición de métricas clave, como la reducción de los

informes de incidentes de phishing y la disminución de las brechas de seguridad relacionadas con el engaño por correo electrónico.

El fortalecimiento de la concienciación y las habilidades en seguridad cibernética de los empleados de la empresa ManageEngine situada en Chía se presenta como un elemento de vital importancia para disminuir la efectividad de los ataques informáticos y salvaguardar la información confidencial y los activos digitales de la organización.

Para hacer frente a las ciber amenazas en constante evolución, la Inteligencia Cibernética (CTI) y herramientas como DKaaS (DARK-KERNEL as a Service) desempeñan un papel fundamental en la protección de las organizaciones en Chía, como señalan las investigaciones de Ainslie et al. (2023) y Charan et al. (2023). La CTI se enfoca en recopilar, analizar y utilizar información sobre amenazas cibernéticas para tomar decisiones informadas.

En este contexto, es crucial comprender cómo los empleados de la empresa ManageEngine utilizan la CTI y herramientas como DKaaS para anticipar y responder a las amenazas cibernéticas. Esto implica evaluar cómo se recopila y comparte la información, cómo se implementa DKaaS y cómo contribuye a la toma de decisiones estratégicas en cuanto a seguridad cibernética corresponda.

Dado que las amenazas cibernéticas se vuelven más específicas y dirigidas a sectores particulares, los datos genéricos ya no son suficientes. Por otro lado, los datos de la red oscura, donde el tráfico va a direcciones IP no utilizadas, son una fuente valiosa de inteligencia sobre amenazas empresariales. DKaaS se basa en el monitoreo activo de la red oscura, capturando el tráfico entrante de manera detallada y específica a través de un sensor de nivel de kernel que utiliza un protocolo de enlace de tres vías en lugar de una observación pasiva. Esto permite recopilar información más precisa sobre las amenazas cibernéticas. Siendo de gran utilidad para

las empresas de todo el mundo.

La inversión en ciberseguridad es esencial para proteger a cualquier empresa que opere en el ciber espacio y más aún si se trata de una organización de tecnología como lo es ManageEngine, esto debido a que toda compañía en constante desarrollo enfrenta diversos desafíos cibernéticos. No se trata solo de gastar más dinero, sino de asignar los recursos de manera inteligente para abordar las amenazas críticas.

Para tomar decisiones de inversión en ciberseguridad, las organizaciones pueden emplear metodologías como la técnica "Best-Worst". En lugar de calificaciones absolutas, esta técnica permite a los evaluadores seleccionar la mejor y la peor opción de un conjunto de alternativas según criterios específicos, ya sean cualitativos o cuantitativos. Luego se utiliza el análisis de estos resultados para priorizar las alternativas según su frecuencia como la elección más viable.

Esta metodología es fundamental para desarrollar estrategias efectivas de inversión que puedan destinar empresas como ManageEngine tal como lo menciona la investigación de Muhammad et al. (2023).

Proponer una nueva forma de proteger las empresas en Chía mediante una mejora en la tecnología de seguridad de red, es una idea interesante como sugiere la investigación de Odegbile et al. (2023). En este contexto, las "middleboxes" son dispositivos de red que desempeñan múltiples funciones de seguridad, como cortafuegos, filtrado de contenido y detección de accesos no autorizados.

Sin embargo, la actual tecnología de "middleboxes" en la ciudad puede tener limitaciones en cuanto a su capacidad para enfrentar amenazas cibernéticas cada vez más sofisticadas, así como problemas de escalabilidad y eficiencia. La propuesta de una nueva arquitectura busca

mejorar la manera en que se aplican las medidas de seguridad en las redes tradicionales de Chía, que no utilizan la tecnología de Redes Definidas por Software (SDN, por sus siglas en inglés).

Este planteamiento analiza en detalle las deficiencias de la arquitectura actual en la aplicación de políticas de seguridad y cómo la nueva propuesta puede solucionar estos problemas. La investigación de Odegbile et al. (2023) respalda la importancia de esta iniciativa y ofrece una base sólida para explorar enfoques novedosos en el campo de la ciberseguridad en Chía.

En un entorno cibernético en constante cambio, mejorar la infraestructura de seguridad de la red es fundamental para asegurar la resistencia de la ciudad ante las amenazas cibernéticas.

El crecimiento exponencial de la compañía ManageEngine trae consigo la posibilidad de enfrentar ataques con una mayor frecuencia, Gracias a la inteligencia artificial (AI) y la introducción del internet de las cosas (IoT) surgen nuevos vectores de ataque en donde tanto empresas como consumidores tienen sus cuentas conectadas a varios dispositivos, por lo que el riesgo de que alguno sea vulnerable a un ataque aumenta (Xia, L et al 2023). No es suficiente, ni viable, esperar que una plataforma se cierre para evitar ataques internos, ya que ataques enfocados a otro dispositivo en la misma red o usando las mismas credenciales son capaces de penetrar estas defensas momentáneas, es por esto que no basta con que las empresas tomen medidas de este tipo, sino que además es necesario que tanto los trabajadores directos de ManageEngine, como sus clientes tengan un conocimiento del manejo que se le puedan dar a estos ataques, que vaya más lejos de simplemente conocer su existencia.

Es importante también mencionar que, aunque estos ataques son siempre malignos, no siempre provienen de un ente que sea conocido como maligno por sí mismo. Es posible tener tecnología que monitoree por ataques, que a su vez se encarga de hacer un *“Data scraping”,* es

decir recopilar información de los usuarios que después se puede vender a terceros. Es por esto que la importancia de la seguridad de la información y la privacidad deben prevalecer y ser el foco del desarrollo y la protección de sistemas de encriptación de datos para garantizar la seguridad de esta información.

Así mismo, es importante tener en cuenta que no es suficiente con garantizar la protección contra los ataques cuando se están ejecutando, al contrario, muchos de estos ataques, tales como los de denegación de servicios dirigida (DDoS) ya no se pueden repeler al ser ejecutados sin un gasto de recursos adicionales, peleando contra el atacante para asegurar que el daño ya realizado no se propague. Por otra parte, deben buscarse nuevas formas de asegurar la protección, ya sea en tiempo real, o incluso antes de que sucedan, tal como el uso de AI para la detección temprana. Esto se hace monitoreando el tráfico normal de la página del negocio u otras, o la entrada y uso de las credenciales de manera anónima, para así mantener la protección de la privacidad con el fin de identificar un uso que no sea normal (Nguyen, Xuan-Ha. Le, Kim-Hung. 2023). El tráfico de comportamiento inusual como lo es el envío masivo de peticiones que tiene como propósito sobrecargar los servicios, el acceso a cuentas desde lugares lejanos, con direcciones IP o MAC que no sean comunes o las habituales, entre otros, buscan alterar la continuidad de las operaciones en la organización.

Para esto existen los llamados sistemas claves de gestion (KMS), los cuales deben ser actualizados constantemente, incluso, diariamente ya que las vulnerabilidades son explotadas en el momento que se encuentran, ya sea por quienes las descubren o por venta de información de un tercero. Es importante que toda compañía se mantenga al tanto de la búsqueda de nuevas vulnerabilidades, las cuales siempre están presentes con cada actualización que realicen en sus sistemas volviendo el ataque y la defensa cibernética una competencia constante, ya que cada

actualización a las bases de inteligencia que poseen los negocios causa la aparición de otro posible punto de entrada que debe ser encontrado y reparado antes de que un atacante lo explote para beneficio propio.

Existen bases y sistemas claves de gestión muy utilizados, que tienen vulnerabilidades incluso conocidas, que no son arregladas por el costo inmediato, y aun así las empresas deben estar vigilantes. El hecho de que un actor no abuse de un punto de entrada no significa que no exista, y el ahorrarse dinero y tiempo a corto plazo al no arreglar estas vulnerabilidades, encontradas, pueden causar una perdida mucho más grande en el futuro.

Un paso proactivo para defender el entorno económico en una zona de los ciber ataques es el desarrollo e índice de divulgación para las empresas de Chía sobre la resiliencia cibernética.

Se debe fomentar el conocimiento la apertura, la rendición de cuentas y la adhesión a las mejores prácticas. Esta herramienta es vital en un mundo como el que se afronta hoy en día donde se interactúa constantemente con diversos dispositivos tecnológicos.

Es importante mencionar “HEAD” donde se debe saber que este es un marco integral creado con la finalidad de respaldar la creación y administración eficiente de una arquitectura empresarial. Debido a su adaptabilidad, las empresas lo pueden implementar en una amplia gama de escenarios, incluidos los que trabajan con internet, uno de los casos es el de la empresa “Smart Manufacturating Inc” donde se implementó el metamodelo “HEAD” y de esa forma la organización creo la hoja de ruta para la adopción de “IoT” al trazar su arquitectura estatal actual y delinear su arquitectura futura, haciendo uso de eso, se pudieron identificar brechas cibernéticas además de disminuir el tiempo de inactividad, todo gracias a fomentar una colaboración multifuncional entre equipos de operaciones de tecnologías de la información junto con equipos de investigación y desarrollo.

Cuando se trata de recomendaciones para mejorar la resiliencia cibernética de los negocios lo primero que se debe trabajar es la muy conocida “Capa 8” esta hace referencia al factor humano el cual es el eslabón más vulnerable de la actualidad en el entorno cibernético, a raíz de esto surge la necesidad implícita de hacer una capacitación periódica del personal presente donde se traten los temas de las amenazas del ciber espacio y las principales precauciones que debe tomar cada uno de los trabajadores para salvaguardar, no solo su información personal sino también la de la empresa, puesto que los empleados generalmente actúan como puente de enlace entre el cibercriminal y la compañía objetivo.

Para proteger a una compañía de los ataques a los que está expuesta al operar en internet, además de la capacitación del personal, también es importante el uso de las buenas prácticas como la contenerización en la cual se segmenta un rol corporativo netamente para operaciones del trabajo, dejando así todo tipo de dispositivo personal con un uso ajeno a lo referente a la compañía. La principal razón de la anterior medida tiene su fundamento en que todos los dispositivos de la empresa pueden ser programados con estándares de seguridad validados por un equipo profesional de ciberseguridad comprobados tanto por un “Blue Team” que hace referencia al equipo especializado en la defensa, como por un “Red Team” o también denominado el equipo de ataque, en un informe. Esto busca conseguir, que independiente a los cambios de dispositivos personales de los trabajadores la línea de dispositivos de trabajo corporativo principal no se veá comprometida tan fácilmente.

En caso que infortunadamente una empresa resulte víctima de un ataque cibernético, se adiciona otro paso en la línea de la ciberseguridad, el cual es la recuperación frente a incidentes, este paso ha presentado un mayor cambio con el transcurso de los años, particularmente desde la implementación del *machine learning*, pues como lo define (Núñez Reiz et al., 2019) este hace

parte de una disciplina del campo de las inteligencias artificiales que opera a través de algoritmos para dotar así a los computadores de la capacidad de identificación de patrones masivos de comportamiento. Por lo tanto, se puede hacer uso de esta práctica para identificar patrones de recuperación de otras empresas y así implementar las mejores soluciones y pasos a seguir según el ataque al que hayan sido expuestos.

Para una empresa es bueno tener conocimientos de recuperación tras un ataque por parte de un personal capacitado pues si bien el *machine learning* brinda un apoyo para este apartado, no es la solución absoluta frente al problema ya que requiere de alguien que lo gestione; en ese sentido una buena línea de recuperación de incidentes cibernéticos está conformada por un profesional del campo de recuperación de incidentes que sepa identificar el tipo de ataque, su fuente y además tenga la capacidad de usar herramientas externas como el *machine learning* para potenciar sus conocimientos y tomar decisiones sobre las mejores medidas que se deben adoptar para recuperarse rápidamente del incidente y permitirle así a la empresa seguir ejerciendo su actividad económica.

Otro de los aspectos que se deben tener en cuenta para el ámbito de la ciberseguridad es la gestión que se le da a los hogares inteligentes, puesto que estos están dotados de todo tipo de artefactos tecnológicos y por lo tanto su relación con el entorno cibernético es directa. Los routers son dispositivos que se encargan de recibir y transmitir datos mediante protocolos específicos, lo cual indica que toda la información transita por este medio y como consecuencia se vuelve crucial hacer una buena administración de quien tiene acceso a la red, para esto una persona del común puede simplemente filtrar a su criterio quien considera, no es una potencial amenaza. Por otra parte, existen métodos más complejos como la configuración del router para que éste solo permita el flujo de información de las direcciones de *media access control* o

también denominadas direcciones “MAC” preestablecidas, estas direcciones son únicas de cada dispositivo y sirven para identificar a cada uno en la web como se menciona en (Santos González, M).

Para las empresas, como se mencionó previamente, es fundamental mantener capacitado a su personal sobre las ciber amenazas con la finalidad de evitar grietas en la seguridad de la compañía y esto conlleva a otro de los factores que un ciber atacante puede explotar, las redes sociales. Es importante que se maneje de manera adecuada la información que se sube a cualquier tipo de red social y más si dicha información es publica pues si el contenido es delicado se abre una brecha para la realización de ingeniería social y posteriormente un tipo de ataque acorde a la víctima. De esta manera surgen recomendaciones como lo son la gestión de las amistades en las redes, no subir contenido que pueda mostrar datos sobre una ubicación personal, no ingresar a cualquier enlace sin antes verificar mínimamente mediante comentarios la veracidad del mismo y sobre todo nunca publicar datos sensibles como usuarios y contraseñas de manera pública.

Las redes neuronales como otros de los avances del tiempo moderno hacen parte del *machine learning* pues permiten reducir esfuerzo humano automatizando procesos mediante la identificación de patrones, a causa de ello, hoy en día es viable para una empresa destinar cierto presupuesto con el fin de mantenerse a la vanguardia en el ámbito de la ciberseguridad, es importante hacer uso de estos recursos, puesto que los ciber criminales también conocen este tipo de herramientas por lo que para una empresa contar con menos ventajas tecnológicas, que las que dispone su atacante abre una brecha de vulnerabilidades que pueden ser explotadas ya que el tiempo que utiliza un dispositivo que implemente redes neuronales como lo menciona (Izaurieta

& Saavedra, s/f) le permite llegar a conclusiones, en la mayoría de los casos, de una manera más rápida que a un ser humano.

Finalmente, con todo lo visto previamente se puede evidenciar que en gran parte de las empresas de Chía, no cuenta con el conocimiento sobre las buenas prácticas que se deben tener en el ciberespacio para salvaguardar la confidencialidad de los datos gestionados por dicha empresa y por consiguiente se debe adoptar un cambio en la forma en la que se ve la tecnología, no es solo resumirse a no usarla y mantenerse en lo tradicional pues esto trae desventajas competitivas frente a una industria digitalmente creciente como la que se está experimentando hoy en día, se trata de hacer uso de la tecnología realizándolo de una forma responsable y velando por proteger los datos de los usuarios mediante la implementación de las buenas prácticas mencionadas previamente como lo son, la capacitación del personal, el uso de las tecnologías emergentes, la buena gestión de todos los sitios donde se almacene información, la buena gestión de las redes sociales y la investigación junto con el adquirir conocimiento a la vanguardia para entender lo que sucede en el mundo digital del momento.

Diseño metodológico

Para el diseño metodológico se establece un enfoque mixto, de manera, se realice un análisis tanto cuantitativo como cualitativo. Adicionalmente el alcance de la investigación se divide en estas dos fases mencionadas previamente.

Fase cuantitativa:

- Esta fase se centrará en obtener información cuantitativa que perita abordar los objetivos 2, 3 y 4.
- La población objetivo será tanto el área de tech latam como el área de marketing de la empesa de tecnología ManageEngine
- Se utilizará una encuesta estructurada como instrumento de recolección de datos.
- La encuesta se diseñará para medir la frecuencia y gravedad de las amenazas cibernéticas, así como para evaluar los esfuerzos de concientización y capacitación en ciberseguridad en estas empresas, adicionalmente también busca recopilar información sobre los mejores frameworks e IDEs de desarrollo para una aplicación escalable.
- Se aplicará la encuesta a una muestra representativa tanto del área de tech latam como del área de marketing de la empresa ManageEngine, seleccionadas de forma estratégica de manera que toda la información suministrada aporte valor a través del conocimiento y experiencia de los encuestados.
- Los datos cuantitativos se analizarán utilizando técnicas estadísticas, como análisis descriptivo y análisis de correlación, para identificar patrones y relaciones.

Fase cualitativa:

- Esta fase se centrará en obtener información cualitativa que perita abordar los objetivos 1, 5, 6 y 7

- Se llevarán a cabo entrevistas semiestructuradas con profesionales del área de ciberseguridad y SEO en la empresa ManageEngine. Estas entrevistas permitirán profundizar en la comprensión de la importancia sobre una plataforma que fomente la capacitación en ciberseguridad para la empresa, además de entender sobre aquellos factores de alcance que se pueden lograr con un desarrollo de este tipo y analizar según su experiencia el costo vs beneficio que traería una implementación de este tipo.
- Se seleccionarán a los participantes de las entrevistas utilizando un muestreo intencional, buscando la representación de áreas relevantes en seguridad cibernética y posicionamiento en internet.
- Los datos cualitativos se analizarán mediante análisis de contenido, identificando temas y patrones emergentes en las respuestas de los entrevistados.

Diseño de Investigación

Diseño explicativo secuencial:

Se dará comienzo con la fase cuantitativa para recopilar datos de que permitan dar respuesta al cumplimento de los objetivos planteados. Luego, se usarán los resultados cuantitativos para informar la selección de participantes y el diseño de las entrevistas en la fase cualitativa. Finalmente, se combinan los hallazgos cuantitativos y cualitativos para obtener una comprensión más completa de la seguridad cibernética.

Población y muestra

Población

Para esta investigación, debido a que su enfoque se centra en la empresa ManageEngine situada en chía Colombia, la población es se compone de dos grupos los cuales son el área técnica de la empresa y el área de marketing.

- **Especialistas Tecnológicos del Área Técnica de la Empresa:** Este grupo incluye integrantes del área técnica de los dominios Unified Endpoint Management and Security (UEMS) y Ciberseguridad segmentada en Identity and Access Management (IAM) y Security Information and Event Management (SIEM) de la empresa ManageEngine.

- **Especialistas en SEO del Área de Marketing de la Empresa:** Este grupo se compone de especialistas en posicionamiento de aplicaciones web y gestión de contenido en internet. Se prestará una atención particular a aquellos empleados involucrados en posicionamiento de blogs sobre seguridad cibernética, la gestión de la información y la toma de decisiones relacionadas con las tecnologías de la información (TI).

Muestra

Teniendo la población ya establecida, lo siguiente es diseñar una muestra de estudio que represente los grupos y sectores mencionados anteriormente. Por ende, existen dos muestras de estudio en esta investigación.

- **Especialista en seguridad cibernética de la empresa ManageEngine:** En donde Se selecciona un individuo el cual actúa en representación del área de seguridad cibernética. El encuestado cuenta con cargo de consultoría técnica en su dominio, de manera que se pueda cumplir con el propósito de recopilar información cualitativa en términos de sus prácticas de seguridad cibernética, percepción de amenazas, y buenas metodologías de desarrollo.

- **Especialista en SEO de la empresa ManageEngine:** En donde se selecciona un individuo el cual actúa en representación del área de posicionamiento SEO y marketing. La persona encuestada cuenta con cargos de especialista en posicionamiento de marca, por consiguiente, se busca obtener información desde otra perspectiva que complemente la información suministrada desde un enfoque menos técnico.

Selección de Métodos

Métodos cualitativos

- **Entrevistas Semiestructuradas:** Realizar entrevistas en profundidad con especialistas de áreas de tecnología y marketing de la empresa ManageEngine para comprender en detalle las prácticas, desafíos y percepciones en el entorno cibernético.

Métodos cuantitativos

- **Encuestas:** Diseñar encuestas estructuradas que permitan recopilar datos cuantitativos sobre los gastos destinados para la formación en ciberseguridad, la adopción de tecnologías emergentes, la percepción de amenazas cibernéticas y los mejores IDEs y *frameworks* de desarrollo para una aplicación móvil.
- **Análisis de Datos Cuantitativos:** Utilizar análisis estadísticos para examinar si existe alguna relación entre las variables estudiadas, como el gasto en ciberseguridad y la frecuencia de incidentes cibernéticos, o la capacitación en seguridad informática y la eficacia de la seguridad.

Variables de Investigación

Variables cuantitativas

- Ocurrencia de malware: Se analiza la frecuencia con la que se reportan incidentes de malware en un lapso de tiempo determinado, por ejemplo, cada mes.
- Clasificación de malware: Se analiza la variedad de malware encontrado y se clasifica en categorías como virus, troyanos, spyware y ransomware en función de sus características y modus operandi.
- Métodos de penetración de malware: Incluyen métodos de ataque mediante correos electrónicos malintencionados, páginas web comprometidas y dispositivos de almacenamiento externos.

- Frecuencia de intentos de phishing: Hace referencia a la cantidad de intentos de phishing realizados por un empleado o sistema en un período de tiempo determinado.
- Efectividad de los ataques de phishing: Se calcula la proporción de intentos de phishing exitosos en comparación con el número total de intentos realizados.
- Educación para prevenir el phishing: Hace referencia a la cantidad de personal que participa en entrenamientos contra el phishing y sus comentarios sobre la eficacia de estos programas.
- Incidentes de amenazas internas: Se refiere a la cantidad de incidentes causados por amenazas internas en una organización durante un período de tiempo determinado.

  Incidentes de ransomware: el número de ataques de ransomware que sufre una organización en un período de tiempo determinado.
- Rescates de Ransomware Pagados: Se lleva la cuenta de las ocasiones en las que la organización ha tenido que pagar un rescate tras un ataque de ransomware.
- Recuperación de Ataques de Ransomware: Se mide el tiempo y los costos asociados con la recuperación de ataques de ransomware, incluyendo la restauración de sistemas y el soporte técnico.
- Ataques DDoS: Se contabiliza la cantidad de ataques por denegación de servicio distribuido que enfrenta la organización en un periodo dado.
- Duración de Ataques DDoS: Se mide la duración de los ataques DDoS, generalmente en horas o minutos.

- Consecuencias de Ataques DDoS: Se evalúa el impacto de estos ataques en términos de inactividad del sitio web y sobrecarga de los servidores.
- Asistencia a Capacitaciones: Se calcula el porcentaje de empleados que asisten a sesiones de formación en ciberseguridad respecto al total de empleados aptos.
- Campañas de Sensibilización en Ciberseguridad: Se cuenta la frecuencia con la que se realizan campañas de sensibilización en ciberseguridad por parte de la organización.
- Impacto de Campañas de Sensibilización: Se mide la efectividad de estas campañas a través de indicadores como visitas web, visualizaciones de videos y engagement en redes sociales.
- Opinión del Personal sobre Formación en Ciberseguridad: Se recoge la retroalimentación del personal sobre la efectividad de los programas de formación y sensibilización a través de encuestas y entrevistas.
- Detección y Respuesta a Incidentes: Se mide el tiempo que toma detectar y responder a un incidente de ciberseguridad, desde su ocurrencia hasta la resolución.
- Medidas de Contención de Incidentes: Se evalúa la eficacia de las acciones tomadas para contener y mitigar incidentes de ciberseguridad.
- Recuperación de Incidentes Cibernéticos: Se cuantifica el tiempo y el costo involucrado en la recuperación completa tras un incidente cibernético.
- Pérdidas Financieras por Incidentes Cibernéticos: Se calculan las pérdidas monetarias totales que la organización sufre a causa de incidentes cibernéticos.

- Costos de Respuesta a Incidentes: Se resume el total de gastos asociados con la respuesta, recuperación y remediación de incidentes cibernéticos.
- Impacto en la Reputación Tras Incidentes: Se mide el efecto negativo en la reputación de la marca o la confianza del consumidor tras un incidente cibernético.
- Satisfacción del Cliente Post-Incidente: Se recopilan datos sobre la satisfacción y confianza del cliente tras un incidente de ciberseguridad.
- Gastos Legales por Incidentes Cibernéticos: Se calculan los costos legales resultantes de incidentes cibernéticos, incluyendo multas y honorarios legales.

Variables cualitativas

- Tipos de amenazas internas: Se refiere a la categorización de amenazas internas según la intención, incluidas acciones no intencionales, intencionales o maliciosas, para obtener una comprensión más profunda del panorama de amenazas.
- Indicadores comunes de amenazas internas: Se refiere a la identificación y documentación de signos de comportamiento o relacionados con el sistema que indican posibles amenazas internas, como patrones de acceso anormales o transferencia de datos.
- Tipos de amenazas cibernéticas (ingeniería social, ataques a la cadena de suministro): Clasificar las amenazas cibernéticas en categorías como ataques de

ingeniería social y ataques a la cadena de suministro para analizar diferentes vectores de amenazas.

- Temas tratados en campañas de concientización: Enumerar los temas y temas abordados en las campañas de concientización sobre ciberseguridad, como seguridad de contraseñas, concientización sobre phishing, navegación segura, etc.
- Ajustes realizados en función de la retroalimentación para mejorar los programas: Documentar los cambios o mejoras realizadas en las iniciativas de formación y sensibilización en función de la retroalimentación de los empleados, mejorando la eficacia de estos programas.
- Conciencia y comprensión de los empleados sobre los procedimientos de respuesta a incidentes: Realizar encuestas o entrevistas para medir el nivel de comprensión y conciencia que tienen los empleados sobre los procedimientos y protocolos de respuesta a incidentes.
- Revisión posterior al incidente y lecciones aprendidas para mejorar los planes de recuperación: Analizar y resumir los conocimientos y lecciones obtenidas de las revisiones posteriores al incidente, destacando áreas de mejora en los planes de recuperación y la gestión de incidentes.

Recolección de datos

Para profundizar en este tema y comprender mejor las amenazas, los desafíos, las estrategias de mitigación en de ciber incidentes en la empresa ManageEngine e información sobre las mejores prácticas de desarrollo, se han llevado a cabo entrevistas con dos expertos en

ciberseguridad y posicionamiento de marca, así como una encuesta diseñada para recopilar datos valiosos sobre la percepción y las prácticas de seguridad cibernética en el entorno empresarial de la ciudad.

Nuestros dos expertos, el Andrés Cabra consultor de soluciones de Unified Endpoint Management and Security (UEMS) y Sara Pinto, especializada en posicionamiento de marca en el área de marketing, comparten una variedad de conocimientos y perspectivas sobre los temas de seguridad cibernética presentes en sus áreas.

Además de las entrevistas, se ha llevado a cabo una encuesta en la que participaron empleados de la organización tanto de la parte técnica como administrativa. Esta encuesta tuvo como objetivo recopilar datos cuantitativos y cualitativos para analizar la percepción de las amenazas cibernéticas, las prácticas de seguridad y uso de buenas prácticas para el desarrollo de aplicaciones web.

Procesamiento y análisis de resultados

Entrevista a la parte técnica

Para el caso de esta entrevista se señalaron como principales los siguientes puntos:

- Indicadores Comunes de Amenazas Internas: Aunque no se proporcionaron ejemplos específicos de indicadores en la entrevista, es importante señalar que la detección de amenazas internas a menudo se basa en la identificación de patrones de comportamiento anormal, tanto intencionales como no intencionales. Por

ejemplo, la actividad inusual en una cuenta de usuario o un patrón de acceso inusual podrían ser indicadores de una amenaza interna.

- Tipos de Amenazas Cibernéticas: Los tipos de amenazas cibernéticas pueden categorizarse en diversas modalidades, como ataques de ingeniería social y ataques a la cadena de suministro. Los ataques de ingeniería social involucran la manipulación psicológica de las víctimas para obtener información confidencial. Los ciberdelincuentes se valen del desconocimiento de las personas y su falta de conciencia sobre cómo proteger sus datos. Utilizan técnicas como el envío de mensajes fraudulentos que pueden hacer que las víctimas hagan clic en enlaces maliciosos, descarguen archivos adjuntos peligrosos o revelen información personal, como contraseñas y datos de tarjetas de crédito. Mientras que los ataques a la cadena de suministro implican aprovechar la infraestructura de proveedores o socios comerciales para acceder a la red de una organización. Los ciberdelincuentes se dirigen a organizaciones más grandes a través de sus conexiones más débiles, como sus socios comerciales o proveedores. Esto puede incluir ataques a través de sistemas de terceros que se utilizan en una cadena de suministro, lo que puede dar como resultado la exposición de información sensible y comprometer la seguridad. identificar estas categorías es fundamental para analizar diferentes vectores de amenazas y estar preparado para ellas.

- Campañas de Concientización: Se destacó que la concienciación y la capacitación de los empleados son fundamentales para prevenir ataques cibernéticos, y esto se

debe a varias razones cruciales como lo son las amenazas en constante evolución y la explotación del factor humano.

- Amenazas en constante evolución: Con la rápida evolución de las amenazas cibernéticas, es imperativo que los empleados estén al tanto de los últimos métodos utilizados por los ciberdelincuentes. Las campañas de concientización garantizan que el personal esté actualizado sobre las amenazas más recientes.
- Es el eslabón más débil: Como mencionó el experto, el factor humano a menudo es considerado como el eslabón más débil en la cadena de seguridad cibernética. Los ciberdelincuentes explotan la falta de conocimiento y las vulnerabilidades de los empleados, lo que resalta la importancia de educarlos.
- Reducción de riesgos: Con la capacitación adecuada, los empleados pueden reconocer señales de posibles ataques, como correos electrónicos de phishing o sitios web maliciosos. Esto permite una respuesta más rápida y, en última instancia, reduce los riesgos de que se materialicen los ataques.
- Protección de datos críticos: La ciberseguridad es esencial para proteger la información confidencial, datos de clientes y la reputación de la empresa. Las campañas de concientización ayudan a los empleados a comprender la importancia de salvaguardar esta información.
- Conciencia de los empleados: En la entrevista se detalló la falta de conciencia y capacitación en el personal de las organizaciones con respecto a los procedimientos de respuesta a incidentes. Esta falta de conocimiento puede resultar en una respuesta inadecuada ante un incidente, lo que puede agravar sus consecuencias. Es crucial que los empleados sepan a quién deben informar en

caso de un incidente y estén familiarizados con los procedimientos, ya que una respuesta deficiente puede afectar significativamente la reputación de la empresa, lo que a su vez puede llevar a la pérdida de confianza de los clientes y la desacreditación de la empresa en el mercado.

Entrevista a la parte administrativa

- Tipos de amenazas cibernéticas: Se definen como principales vectores de ataque específicamente la ingeniería social y los ataques de ransomware a través de correos electrónicos como formas comunes de amenazas.
- Campañas de concientización: Como bien se mencionó anteriormente que uno de los puntos clave son las mismas personas de concientización, se mencionan temas relacionados con la conciencia sobre ciberseguridad, como lo son la importancia de no compartir contraseñas, cambiar contraseñas con regularidad y tener precaución con todo tipo de archivos, más aún si su origen no es fiable.
- Concientización y comprensión de los empleados en la respuesta a incidentes: Es discutida también la importancia de que los empleados comprendan los procedimientos de respuesta a incidentes, ya que esto permite una mejora en los tiempos de recuperación al interiorizar los pasos a seguir y genera conciencia en las diversas áreas que tiene la organización. Si bien no todas las áreas de la empresa trabajan directamente en la recuperación después de un incidente, el hecho de que todas las áreas se vean así sea levemente involucradas en el proceso de recuperación permite una ampliación de los conceptos de buenas prácticas para la prevención de ataques cibernéticos.

- Elementos para que una aplicación web sea llamativa: Se menciona la importancia de una buena interfaz gráfica de manera que esta permita enganchar a los usuarios para que puedan seguir interactuando y adquieran también más ganas de apropiar el conocimiento expuesto en el sitio web.

Realizacion de Encuestas

- Grupo Demográfico:

Figura 3

Grupo demográfico, edad y género

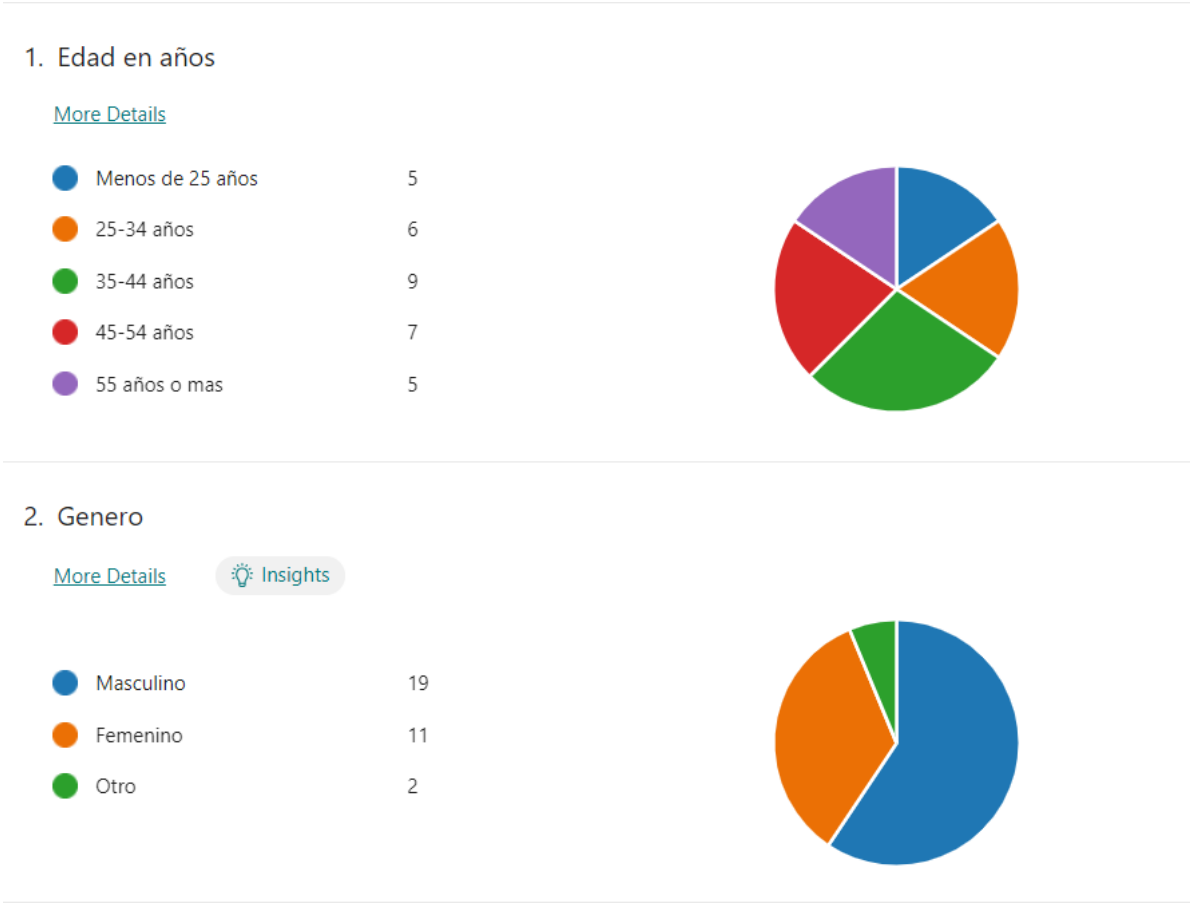


Figura 4

Grupo demográfico, nivel de escolaridad

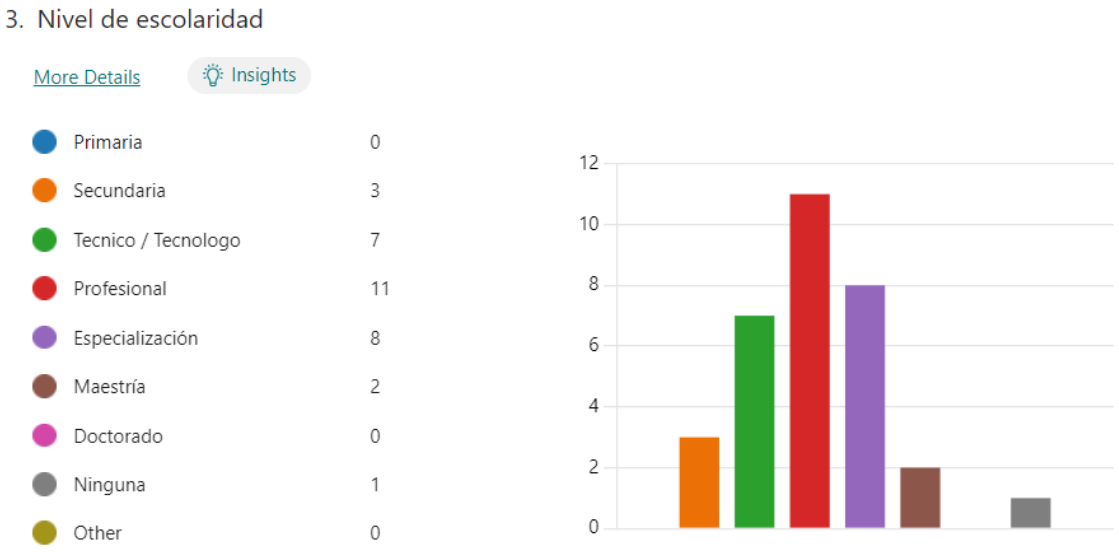
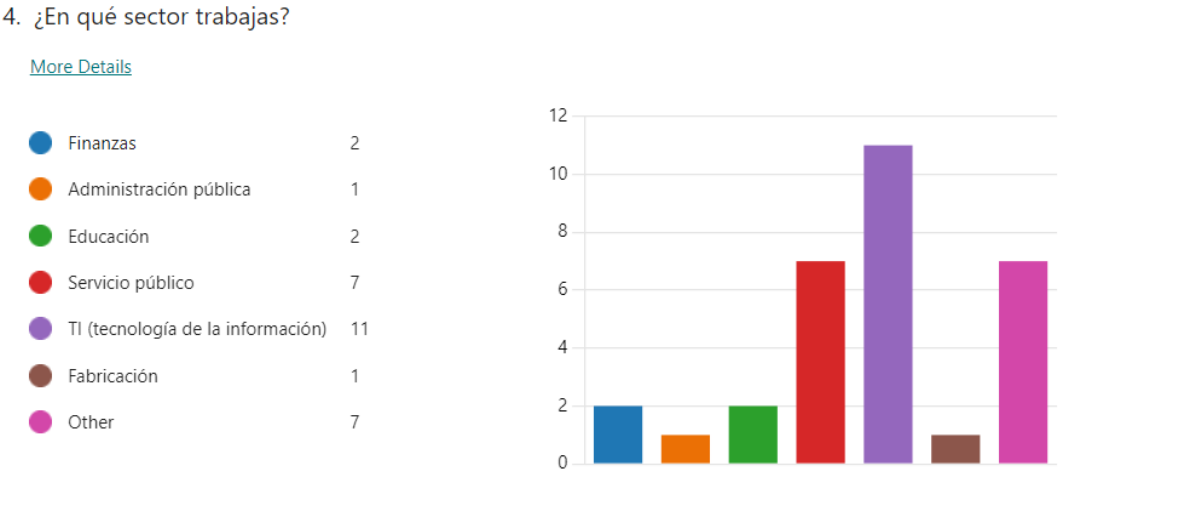


Figura 5

Grupo demográfico, sector de trabajo

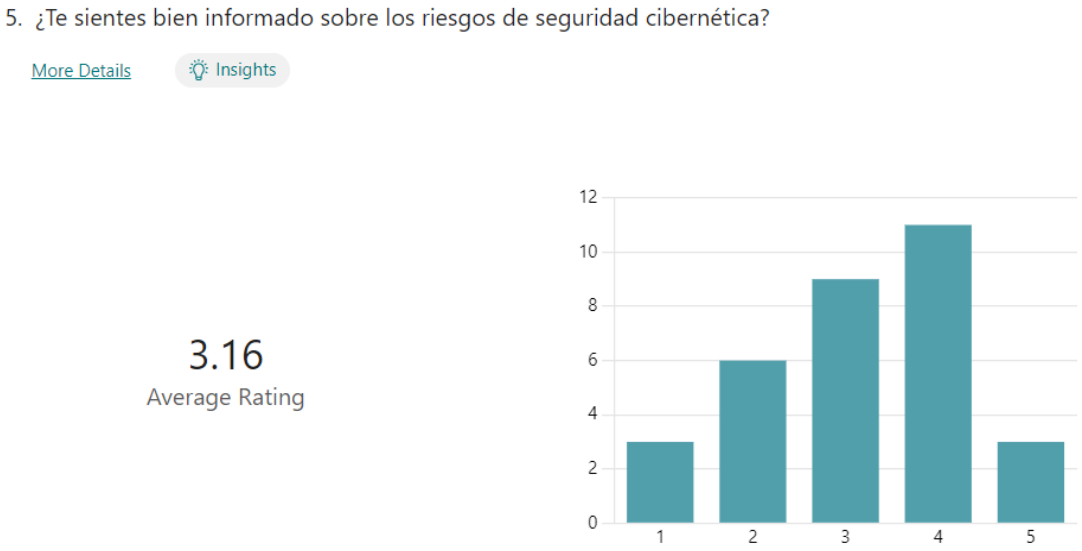


El grupo demográfico de esta encuesta son las personas de la empresa ManageEngine, de edades variadas. Entre estas se puede ver que la mayoría tiene entre 35-44 años, seguidas por una mayor entre 45-54 años. Entre estas personas, la mayoría son hombres y se encuentran muchas menos personas que se identifican como “otro”. Fue una encuesta pequeña por lo que los resultados pueden variar al hacerse a una escala mayor. La mayoría de estas personas trabajan en algo relacionado con TI, seguido por el sector público y “otros”. De estas personas, la mayoría tienen un nivel escolar profesional, seguido por una especialización. Ninguna se encuentra en un nivel de primaria, de doctorado u “otro”.

- Información ante los riesgos:

Figura 6

Nivel de información ante riesgos



Una de las preguntas realizadas a las personas fue su nivel de información al respecto de la seguridad cibernética. Como se puede ver, la mayoría de las personas se encuentran en un nivel

medio-alto, con muy pocas que se encuentren en los niveles más bajos o más altos de información.

- Percepción de Amenazas:

Figura 7

Percepción de amenazas, entrenamiento contra amenazas cibernéticas

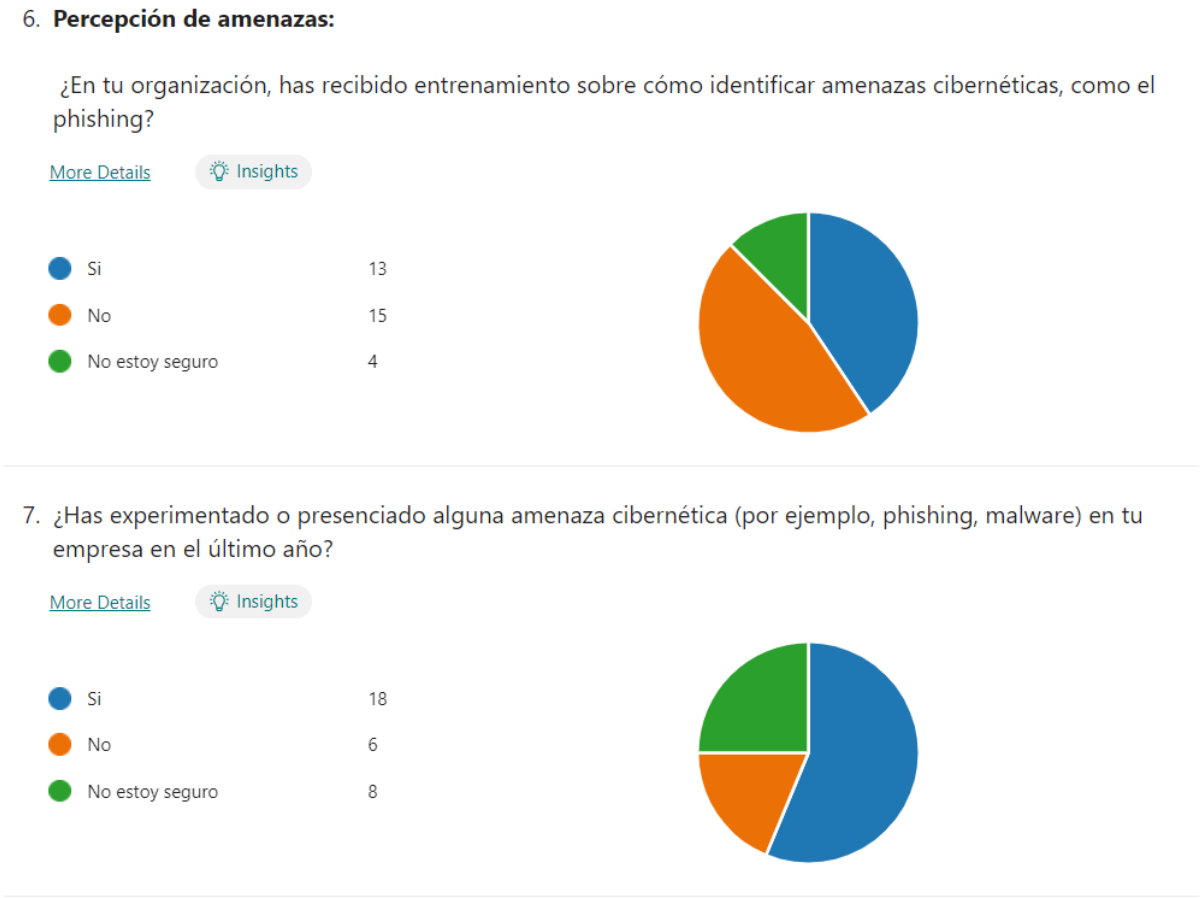
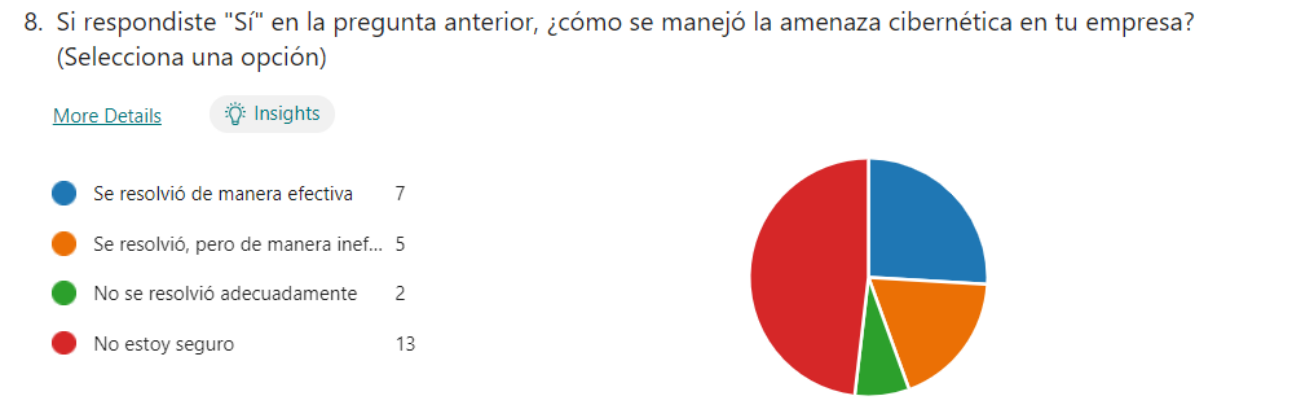


Figura 8

Posible manejo de amenazas cibernéticas



Posteriormente se preguntó a estas personas si habían recibido entrenamiento relacionado a la identificación de amenazas cibernéticas, donde hubo una separación relativamente equitativa de personas que si han recibido dicho entrenamiento y los que no. Sin embargo, viendo la siguiente pregunta, acerca de si se han presentado amenazas cibernéticas en las organizaciones, hay muy pocas de estas personas que no han presenciado un ataque cibernético, lo que puede dar a entender que el entrenamiento provisto por las empresas puede no ser el adecuado o no es eficaz para detener estas amenazas. Además, de las personas que, si han presenciado este tipo de ataques, muchas no son informadas acerca de estos ataques, o de los pasos que tomo la organización para resolverlos.

- Ciberamenazas:

Figura 9

Ciberamenazas, percepción de problemática y participación en capacitaciones

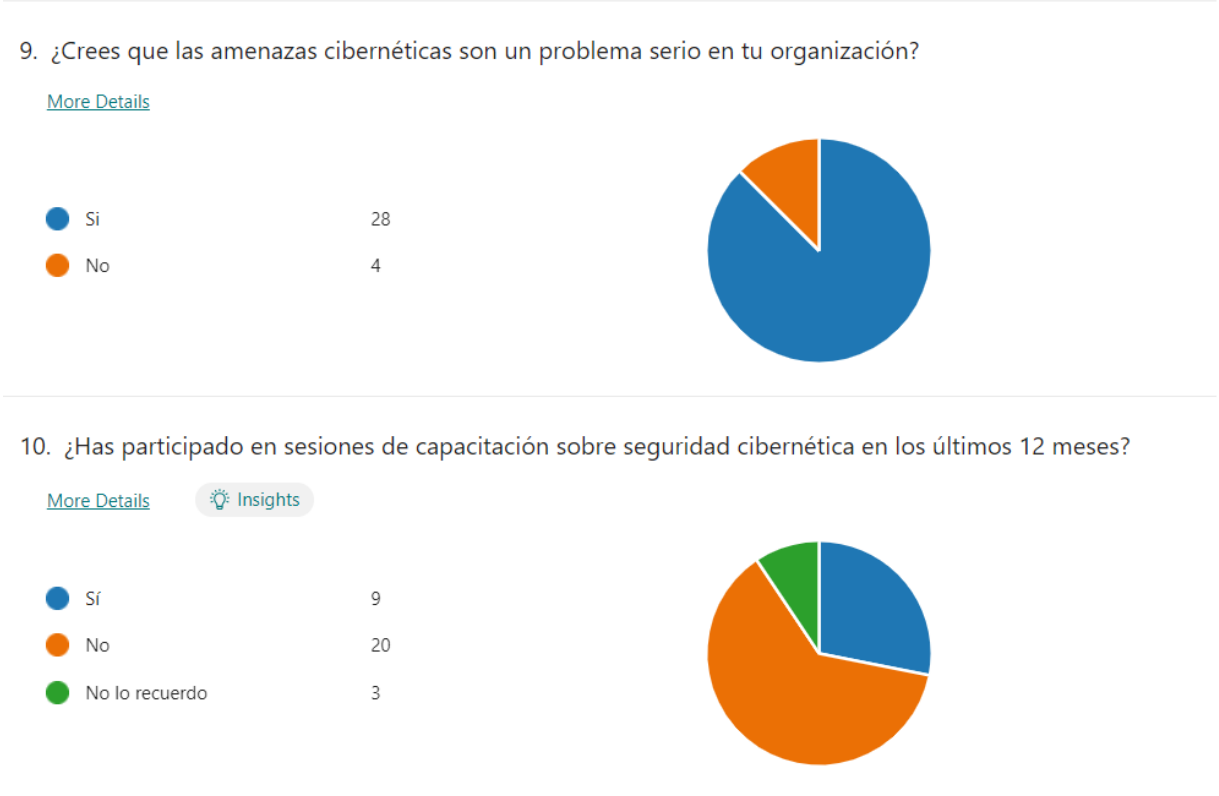
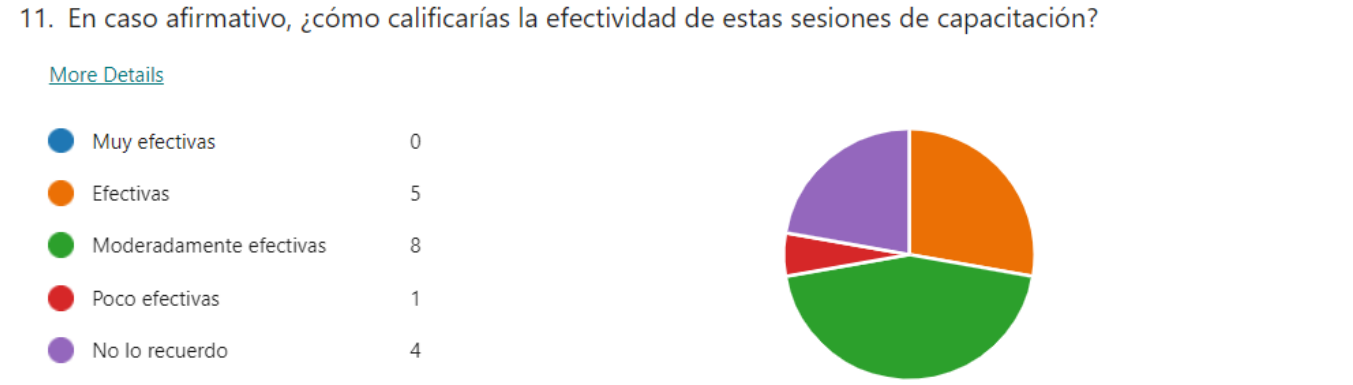


Figura 10

Percepción de efectividad acerca de las sesiones de capacitación

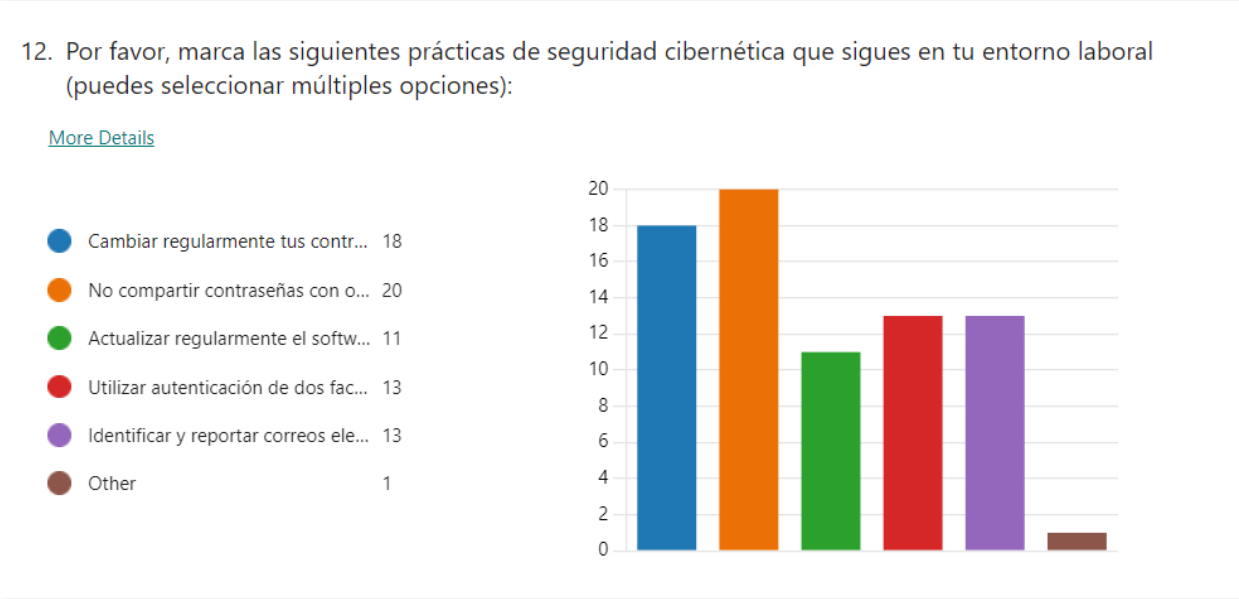


La mayoría de las personas encuestadas piensan que estas amenazas cibernéticas son un problema serio en la organización en la que se encuentran, y sin embargo estas organizaciones no proveen capacitaciones acerca de la seguridad cibernética, o en caso de que si las provean, muchas personas no ven la necesidad de participar, ya sea por su efectividad moderada u otro tipo de desinterés.

- Prácticas de Seguridad:

Figura 11

Prácticas de seguridad cibernética en el entorno laboral

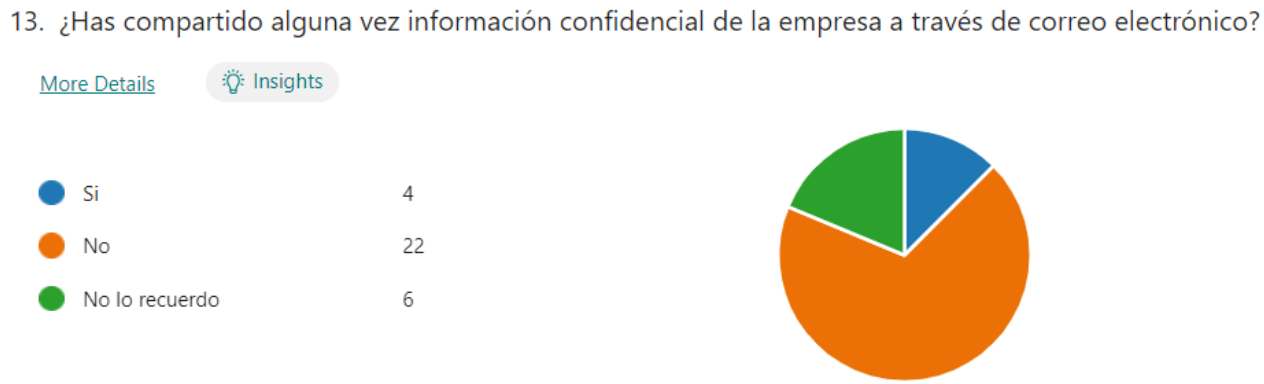


De las personas encuestadas, la mayoría toman una o más precauciones al momento de trabajar con la seguridad cibernética, la mayoría siguiendo algo simple como el no compartir contraseñas, seguido de cambiarlas regularmente. Sin embargo, tal vez por el entorno y la inhabilidad de estos de tener acceso a esta funcionalidad, no muchos actualizan regularmente el software para reparar posibles vulnerabilidades.

- Información Confidencial:

Figura 12

Pregunta de confidencialidad



De las personas encuestadas, la mayoría saben que no deben compartir información confidencial a través de correo electrónico, con unos pocos que no recuerdan si lo han hecho y otros menos que si lo han hecho.

- Uso de Contraseñas:

Figura 13

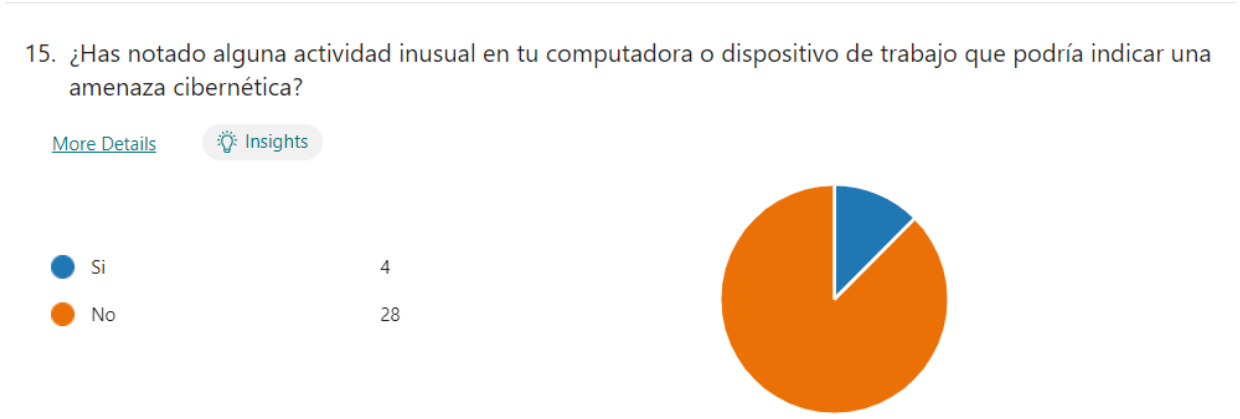
Uso de contraseñas fuertes

La mayoría de las personas están al tanto de su seguridad ya que utilizan contraseñas fuertes, las cuales pueden incluir mayúsculas, minúsculas o símbolos que hacen más difícil llegar a estas por fuerza bruta, además de contraseñas diferentes para sus cuentas que evitan que al descubrirse una se pueda acceder a todas sus cuentas.

- Actividad Inusual:

Figura 14

Percepción de actividad inusual

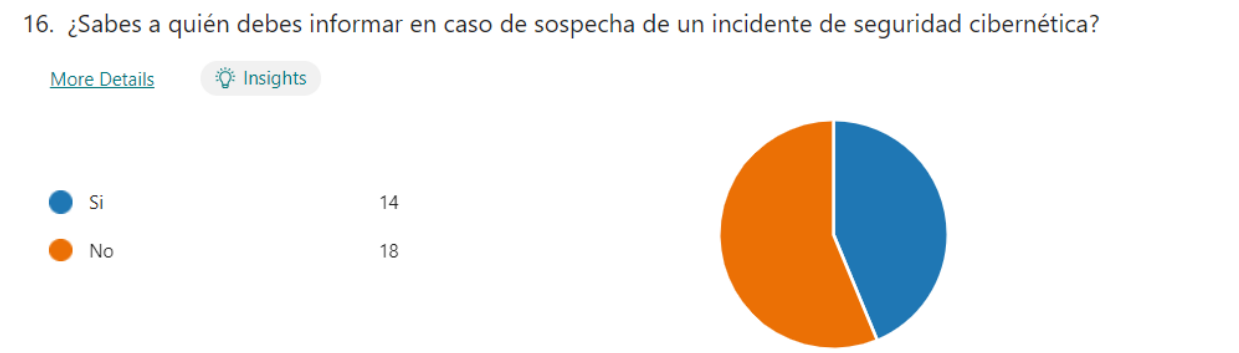


La mayoría de las personas no detectan actividad inusual en sus dispositivos de trabajo, aunque esto no significa que no hayan sido afectados por software malicioso de una u otra manera, ya que existen muchos ataques silenciosos que son difíciles de identificar para una persona que no tenga un entrenamiento extensivo.

- Entidad a la que Informar:

Figura 15

Entidad a la que informar



De acuerdo al gráfico, la mayoría de las personas no saben a quién deben informar en caso de que se presente un ataque, o la posibilidad de uno. Esto lleva a la conclusión de que la mayor parte de los ataques cibernéticos nunca son informados a la empresa, o que la empresa no tiene una manera de identificarlos correctamente.

- Respuesta Frente a Ataques:

Figura 16

Respuesta frente a ataques

La mayoría de las personas creen que su empresa no está preparada para responder de manera efectiva ante los ataques cibernéticos, que puede llevar a que estas no informen de dichos ataques a su empresa. Coincidentemente, la mayoría de las personas no han sido informadas de los procedimientos de respuesta de la empresa ante estos incidentes, lo que también contribuye al pensamiento de que estas empresas no son capaces de responder ante ataques cibernéticos.

Alternativa de Solución

Para promover el aprendizaje práctico, la plataforma busca incorporar contenidos interactivos como vídeos, con cuestionarios y simulaciones en su gama de cursos y módulos de formación en ciberseguridad. También uno de los puntos fundamentales es la función de supervisión y evaluación del progreso de los trabajadores, de manera que sea posible elaborar informes para la empresa, que permitirían una supervisión eficaz de la adherencia a la formación.

La aplicación debe contar con un apartado de ejercicios y simulaciones que permitan a los miembros del personal perfeccionar sus habilidades en escenarios reales controlados de ciberseguridad. Esto mejorará la preparación de los trabajadores para hacer frente a las ciberamenazas y les ayudará a desarrollar sus capacidades de detección y respuesta ante incidentes.

Otra opción que surge con un presupuesto más amplio sería la instalación de un sistema de gestión del aprendizaje (SGA) adaptado a las necesidades específicas de la empresa. Modificando un sistema de gestión del aprendizaje existente para la formación en ciberseguridad, podrían incluirse sólidas funciones de seguridad y posibilidades de personalización adecuadas. Esto permitiría incluir el seguimiento del progreso de los usuarios, materiales de formación e informes de cumplimiento eficaces.

Adicionalmente, también en una mayor escala podría considerarse la creación de una aplicación móvil complementaria. De manera que, al hacer uso de este software, los miembros del personal pueden acceder a materiales de formación móviles sobre ciberseguridad, ofreciendo un entorno de aprendizaje cómodo y adaptable. Las funciones de gamificación de la aplicación y la interfaz de usuario fácil de usar pueden animar a los usuarios a participar activamente en la formación y mejorar su memoria de la información.

Por último, otra de las estrategias que surge a una mayor escala es la formación especializada sobre temas relacionados con la empresa impartida a través de seminarios web, sesiones de formación presenciales y cursos en línea. La preparación de los empleados en materia de ciberseguridad podría reforzarse y el proceso de aprendizaje mejorarse invitando a especialistas en ciberseguridad a impartir sesiones de formación y promoviendo la interacción entre los participantes.

Análisis de Costos

Para el análisis de costos se ha dividido en dos apartados, en donde primeramente en la figura 17 se muestra una matriz con los costos directos y en la figura 18 se muestra la matriz respectiva para los costos indirectos.

Figura 17

Costos directos

Costo Principal	Sub Costos	Valor
Costos de Desarrollo de Software	Honorarios de desarrolladores y programadores.	167.000 COP a 292.000 COP por hora
	Licencias de software y herramientas de desarrollo.	No aplica
	Costos de adquisición de tecnologías y frameworks específicos.	No aplica
Costos de Diseño y UX/UI	Honorarios de diseñadores gráficos y de experiencia de usuario (U	2'800.000 COP mensual
	Software y herramientas de diseño.	142.000 COP (Ps y Ai)
Costos de Contenido de Capacitación	Creación o adquisición de contenido de capacitación en seguridad cibernética, como cursos, módulos de aprendizaje y	No aplica
	Honorarios de expertos en seguridad cibernética para la creación de contenido especializado.	No aplica
Costos de Seguridad y Pruebas	Contratación de servicios de pruebas de seguridad externas.	15.110 COP por hora
	Herramientas y software de seguridad para pruebas internas.	800.000 COP mensual
	Costos asociados con la implementación de medidas de seguridad adicionales durante el desarrollo.	No aplica
Costos de Infraestructura y Hosting:	Servicios de alojamiento web para la aplicación.	7.600 COP a 57.500 COP mensual
	Adquisición de servidores o recursos de computación en la nube.	No aplica
	Configuración de dominios y certificados SSL para garantizar la seguridad de la aplicación.	4.000 COP mensual
Costos de Capacitación y Soporte	Honorarios de capacitadores para la formación del personal en el uso de la aplicación y en conceptos básicos de seguridad	No aplica
	Costos asociados con la creación de materiales de capacitación y documentación de soporte.	No aplica
Costos de Implementación y Despliegue	Recursos humanos y técnicos necesarios para el despliegue de la aplicación en el entorno de producción.	167.000 COP a 292.000 COP por hora
	Pruebas finales de despliegue y configuración de la aplicación.	167.000 COP a 292.000 COP por hora
Costos de Gestión de Proyecto	Honorarios de gerentes de proyecto y coordinadores de proyecto.	No aplica
	Costos asociados con la gestión y coordinación de equipos de desarrollo y otros recursos.	No aplica
Costos de Marketing y Promoción	Gastos en estrategias de marketing digital para promover la aplicación entre los usuarios finales.	No aplica
	Costos asociados con la creación de materiales de marketing, como folletos, banners y contenido para redes sociales.	No aplica

Figura 18

Costos indirectos

Costo Principal	Sub Costos	Valor
Costos de Espacio de Oficina y Equipamiento	Alquiler de espacio de oficina para el equipo de desarrollo.	No aplica
	Costos asociados con servicios públicos, como electricidad, agua y conexión a internet.	No aplica
	Adquisición y mantenimiento de equipos de oficina y tecnología, como computadoras, impresoras y mobiliario.	No aplica
Costos de Gestión de Proyectos	Tiempo y recursos dedicados a la gestión de proyectos, como reuniones, planificación y seguimiento del progreso.	No aplica
	Costos asociados con el software de gestión de proyectos y herramientas de colaboración.	No aplica
Costos de Comunicación	Gastos de comunicación, como teléfono, correo electrónico y mensajería.	No aplica
Costos de Capacitación y Desarrollo de Personal	Gastos en programas de formación y desarrollo profesional para el equipo de desarrollo.	No aplica
	Costos asociados con la contratación de consultores externos o expertos en áreas específicas de seguridad cibernética.	1'842.000 COP mensual
Costos de Riesgos y Contingencias	Reserva de fondos para cubrir posibles sobrecostos o imprevistos durante el proyecto.	400.000 COP
	Costos asociados con la gestión de riesgos y la mitigación de posibles problemas durante el desarrollo.	400.000 COP
Costos de Tiempo de Inactividad y Productividad	Pérdida de productividad debido a interrupciones, errores o problemas técnicos durante el desarrollo.	No aplica
	Costos asociados con la recuperación de tiempo perdido y la gestión de tiempos de inactividad.	No aplica
Costos de Reubicación o Trabajo Remoto	Gastos de reubicación si el equipo de desarrollo necesita trasladarse temporalmente para trabajar en el proyecto.	No aplica
	Costos asociados con la implementación de políticas de trabajo remoto, como la adquisición de equipos y herramientas de comunicación.	No aplica
Costos de Seguro y Cumplimiento Legal	Primas de seguro relacionadas con la protección de la propiedad intelectual, responsabilidad profesional y otros riesgos.	No aplica
	Honorarios legales para garantizar el cumplimiento de las regulaciones y leyes pertinentes durante el desarrollo del proyecto.	167.000 COP a 292.000 COP por hora
Costos de Gestión de Cambios	Costos asociados con la gestión de cambios en el alcance del proyecto, incluyendo evaluación, aprobación y comunicación de cambios a las partes interesadas.	No aplica
	Recursos dedicados a la documentación y seguimiento de cambios en los requisitos y especificaciones del proyecto.	No aplica
Costos de Evaluación y Mejora Continua	Gastos en evaluaciones periódicas de calidad y rendimiento de la aplicación.	167.000 COP a 292.000 COP por hora
	Recursos dedicados a la implementación de mejoras continuas en función de retroalimentación de usuarios y cambios en el entorno tecnológico.	No aplica

Plan de Implementación

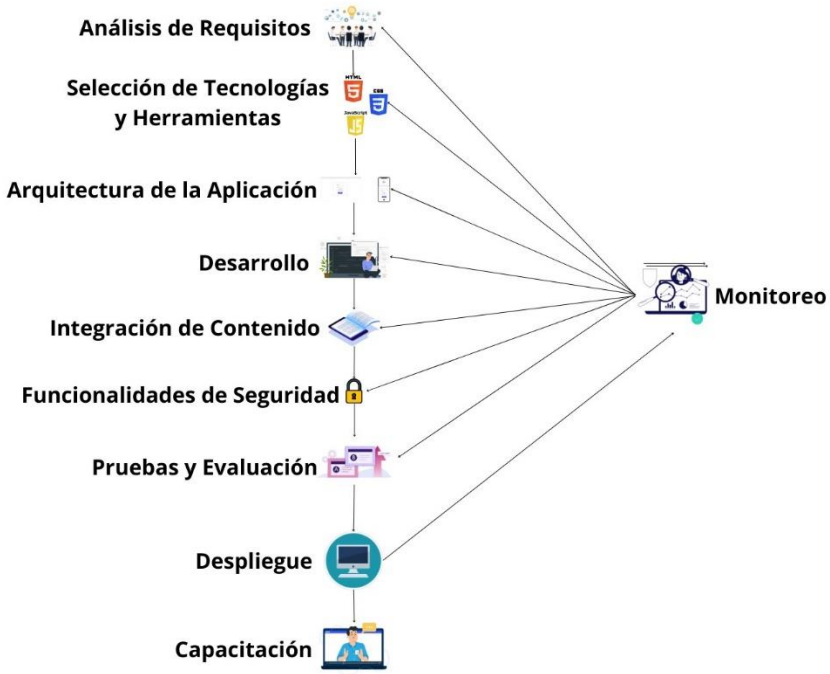
Se seguirá un plan de implementación como se detalla en la figura 19 que muestra el flujo de la operación desde una etapa de análisis de requerimientos hasta el monitoreo constante de la aplicación. En este sentido el primer paso que surge “Análisis de Requisitos” busca recabar información pertinente sobre tanto los requisitos funcionales como los no funcionales de la aplicación, posteriormente se pasa al proceso de “Selección de Herramientas y Tecnologías” en donde se consideran los lenguajes de programación pertinentes para el desarrollo de la aplicación, que en este caso al tratarse de una web se toman HTML5, CSS3 y JavaScript, posteriormente en el proceso de “Arquitectura de la Aplicación” se realizan los mockups que

permiten entender el flujo de uso de la aplicación y por consiguiente a la hora de realizar la etapa de “Desarrollo” sea más sencillo y se ahorre más tiempo en la creación de la aplicación al tener definidos los apartados de la aplicación. Una vez realizada la fase anterior ahora se pasa a la fase de “Integración de Contenido” en donde como su nombre lo indica se integran específicamente los temas relacionados en los espacios preseleccionados destinados para ello, luego en la fase de “Funcionalidades de Seguridad” se añaden funcionalidades de seguridad específicas como la integración con APIs y la creación de roles de acceso, para luego poder pasar a lo que respecta a las “Pruebas y Evaluación" que es todo el proceso de testing requerido al finalizar cualquier aplicación para verificar su comportamiento según la fluctuación de usuarios por segundo usando la aplicación y realizando peticiones a la base de datos.

Por último, la fase de “Despliegue” busca que el programa sea desplegado e implementado en el entorno de producción de la empresa, y con la fase de “Capacitación” se formará a los miembros del personal tanto en su uso como en los principios fundamentales de ciberseguridad. La seguridad y funcionalidad a largo plazo de la aplicación estarán garantizadas por un programa de mantenimiento y supervisión continuos. Esta minuciosa estrategia de implementación garantizará que la aplicación web de la organización ManageEngine se desarrolle con éxito. Desde este apartado de “Monitoreo” pueden surgir nuevos requerimientos u opciones de mejora de manera que es posible desde esta fase dar saltos a cualquiera de las fases anteriores con la finalidad de reestructurar o actualizar la aplicación conforme se vuelva necesario.

Figura 19

Plan de implementación de la aplicación web



Conclusiones

Este estudio ha alcanzado sus metas tras una profunda investigación en seguridad cibernética y la conceptualización de una aplicación web educativa en la materia. Un análisis meticuloso de las barreras económicas y tecnológicas, junto con un examen de la literatura previa, ha sentado una base robusta para el desarrollo de esta herramienta.

El proyecto se considera financieramente viable tras un examen y análisis según las matrices de los diferentes costos relacionados con la creación y ejecución de una aplicación web. En donde los elementos como costos de alojamiento del sitio, pruebas de seguridad, diseño y desarrollo son justos y acordes con las normas del mercado colombiano.

Adicionalmente, poner en marcha la aplicación web para la empresa ManageEngine tiene muchas ventajas que hacen que el coste merezca la pena. Entre ellas, se encuentran el aumento de la productividad gracias a la centralización de la información y la automatización de procesos, que permiten una gestión más eficaz. También, una aplicación web amplía el alcance de la empresa al permitirle conectar con un público más amplio sin verse limitada por la ubicación real de una tienda. Los servicios en línea están siempre disponibles, las veinticuatro horas del día, lo que permite incrementar la satisfacción del cliente, en complemento, el estudio de los datos de los usuarios ofrece información reveladora para tomar decisiones estratégicas. Estar presente digitalmente en el mercado actual es crucial para la competitividad, y tener una aplicación web que permita capacitar el personal de la empresa en seguridad cibernética de una forma sólida establece a una empresa como pionera en su campo.

Resultados del primer objetivo específico

Se ha identificado que ManageEngine, ubicada en Chía, es progresivamente más susceptible a ataques cibernéticos debido a la índole de su negocio. La necesidad de intensificar las medidas de protección y ofrecer formación especializada en seguridad cibernética a los trabajadores es clara y urgente.

Hallazgos del segundo objetivo específico

Al investigar el segundo objetivo, se ha verificado la viabilidad del desarrollo de la aplicación web sugerida. Las encuestas indican un interés marcado por parte de las empresas locales en programas de formación en seguridad cibernética, lo que subraya la pertinencia y la importancia del proyecto.

Resultados del tercer objetivo específico

Respecto al tercer objetivo, se considera que la aplicación web en cuestión tiene el potencial de aportar un valor considerable al capacitar al personal en la prevención de ataques cibernéticos. Este hallazgo enfatiza la importancia de la inversión en formación continua del personal como elemento clave de una estrategia de ciberseguridad efectiva.

Resultados de los objetivos específicos restantes

La implementación de una base de datos bien estructurada, junto con el diseño y desarrollo de una interfaz de usuario intuitiva, y la integración eficiente de esta con la base de datos, resultan pasos cruciales. Estas acciones han construyen una infraestructura robusta y operativa que satisface los estándares de un proyecto fullstack, proporcionando así una plataforma propicia para el progreso sostenido y la eficiencia del proyecto en el futuro.

Referencias

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security, 132*(103352), 103352. https://doi.org/10.1016/j.cose.2023.103352

Almahmoud, Z., Yoo, P. D., Alhussein, O., Farhat, I., & Damiani, E. (2023). A holistic and proactive approach to forecasting cyber threats. *Scientific Reports*, *13*(1). https://doi.org/10.1038/s41598-023-35198-1

Almaraz-Rivera, J. G., Perez-Diaz, J. A., Cantoral-Ceballos, J. A., Botero, J. F., & Trejo, L. A. (2022). Toward the Protection of IoT Networks: Introducing the LATAM-DDoS-IoT Dataset. *IEEE access: practical innovations, open solutions*, *10*, 106909–106920. https://doi.org/10.1109/access.2022.3211513

Ashfaq, R. A. R., Wang, X.-Z., Huang, J. Z., Abbas, H., & He, Y.-L. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. *Information Sciences*, *378*, 484–497. https://doi.org/10.1016/j.ins.2016.04.019

Botero Zuluaga, D. M., Hernández Zuluaga, J. C., & Rodríguez, E. M. (2023). Cripto-activos oficiales como medio de pago en Colombia. Transición tecnológica y ventaja competitiva. *Revista e-mercatoria*, *20*(1), 53–81. https://doi.org/10.18601/16923960.v20n1.02

Cano-Martínez, J. J. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. *Revista científica General José María Córdova*, *20*(40), 815–832. https://doi.org/10.21830/19006586.866

Charan, P. V. S., Ratnakaram, G., Chunduri, H., Anand, P. M., & Shukla, S. K. (2023). DKaaS: DARK-KERNEL as a service for active cyber threat intelligence. *Computers & Security*, *132*(103329), 103329. https://doi.org/10.1016/j.cose.2023.103329

Chauhan, V. S., Chakravorty, J., & Khang, A. (2023). Smart cities data indicator-based cyber threats detection using bio-inspired artificial algae algorithm. En *Advances in Computational Intelligence and Robotics* (pp. 436–447). IGI Global.

Chinchilla, E. J. S., & Allende, J. S. (2017). Riesgos de ciberseguridad en las Empresas. *Tecnología y desarrollo*, *15*(0). https://revistas.uax.es/index.php/tec_des/article/view/1174

Dabas, N., Ahlawat, P., & Sharma, P. (2023). An effective malware detection method using hybrid feature selection and machine learning algorithms. *Arabian Journal for Science and Engineering*, *48*(8), 9749–9767. https://doi.org/10.1007/s13369-022-07309-z

Estado del arte sobre la identificación amenazas no intencionales de ciberseguridad de parte de personal interno en instituciones públicas. (2021). *1*, 70–82. https://www.proquest.com/openview/4fc3316c510c3b225e5378667120e7e6/1?pq-origsite=gscholar&cbl=1006393

Gandal, N., Moore, T., Riordan, M., & Barnir, N. (2023). Empirically evaluating the effect of security precautions on cyber incidents. *Computers & Security*, *133*(103380), 103380. https://doi.org/10.1016/j.cose.2023.103380

Gil López, C. A., Fresneda Saldarriaga, I. C., & Molina Grajales, N. (2021). *Impacto económico y social que ha generado el delito cibernético sobre el comercio electrónico en Colombia durante el periodo 2019-2021*. Tecnológico de Antioquia, Institución Universitaria.

Hendi Muhammad, A., Dwi Santoso, J., & Fikri Akbar, A. (2023). Information security investment prioritization using best-worst method for small and medium enterprises. *Indonesian Journal of Electrical Engineering and Computer Science*, *31*(1), 271. https://doi.org/10.11591/ijeecs.v31.i1.pp271-280

Henkel, R., Guetebier, L., & Waltemath, D. (2022). CovidGraph: Integrating COVID-19 Data. En *Studies in Health Technology and Informatics* (Vol. 294). IOS Press.

Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security*, *132*(103364), 103364. https://doi.org/10.1016/j.cose.2023.103364

Igbinovia, M. O., & Ishola, B. C. (2023). Cyber security in university libraries and implication for library and information science education in Nigeria. *Digital Library Perspectives*, *39*(3), 248–266. https://doi.org/10.1108/dlp-11-2022-0089

Johnphill, O., Sadiq, A. S., Al-Obeidat, F., Al-Khateeb, H., Taheir, M. A., Kaiwartya, O., & Ali, M. (2023). Self-healing in cyber–physical systems using machine learning: A critical analysis of theories and tools. *Future Internet*, *15*(7), 244. https://doi.org/10.3390/fi15070244

Kashmar, N., Adda, M., Ibrahim, H., Morin, J.-F., & Ducheman, T. (2023). Instantiation and implementation of HEAD metamodel in an industrial environment: Non-IoT and IoT case studies. *Electronics*, *12*(15), 3216. https://doi.org/10.3390/electronics12153216

Krawczyk-Sokołowska, I., & Caputa, W. (2023). Awareness of network security and customer value – The company and customer perspective. *Technological Forecasting and Social Change*, *190*(122430), 122430. https://doi.org/10.1016/j.techfore.2023.122430

Larriva-Novo, X., Sánchez-Zas, C., Villagrá, V. A., Marín-Lopez, A., & Berrocal, J. (2023). Leveraging Explainable artificial intelligence in real-time cyberattack identification: Intrusion detection system approach. *Applied Sciences (Basel, Switzerland)*, *13*(15), 8587. https://doi.org/10.3390/app13158587

Maggi Murillo, G., & Gómez Gómez, O. S. (2021). Estudio preliminar sobre conocimiento de Ciberseguridad en usuarios de PYMEs: Caso de estudio en Riobamba. *Revista Perspectivas*, *3*(2), 45–53. https://doi.org/10.47187/perspectivas.vol3iss2.pp45-53.2021

Martinez v. Johnson & Johnson Consumer Inc., 471 F. supp. 3d 1003. (2020, julio 8). Casetext.com. https://casetext.com/case/martinez-v-johnson-johnson-consumer-inc

Nguyen, X.-H., & Le, K.-H. (2023). Robust detection of unknown DoS/DDoS attacks in IoT networks using a hybrid learning model. *Internet of Things*, *23*(100851), 100851. https://doi.org/10.1016/j.iot.2023.100851

Nikolaou, N., Papadakis, A., Psychogyios, K., & Zahariadis, T. (2023). Vulnerability identification and assessment for critical infrastructures in the energy sector. *Electronics*, *12*(14), 3185. https://doi.org/10.3390/electronics12143185

Núñez Reiz, A., Armengol de la Hoz, M. A., & Sánchez García, M. (2019). Big Data Analysis y Machine Learning en medicina intensiva. *Medicina intensiva*, *43*(7), 416–426. https://doi.org/10.1016/j.medin.2018.10.007

Odegbile, O., Ma, C., Chen, S., & Wang, Y. (2023). Policy enforcement in traditional non-SDN networks. *Journal of Parallel and Distributed Computing*, *177*, 39–52. https://doi.org/10.1016/j.jpdc.2023.02.005

Ogala, J. O., Ahmad, S., Shakeel, I., Ahmad, J., & Mehfuz, S. (2023). Strengthening KMS security with advanced cryptography, machine learning, deep learning, and IoT technologies. *SN Computer Science*, *4*(5). https://doi.org/10.1007/s42979-023-02073-9

Ortiz Osorio, M. (2021). *Importancia de las buenas prácticas en ciberseguridad en el trabajo remoto de entidades públicas de Colombia en época de pandemia*. https://repository.unad.edu.co/handle/10596/44501

Patiño, W. C. (2023, febrero 16). *Ciberseguridad: el gran desafío de las empresas en Colombia - Foros TIC*. Impacto TIC. https://impactotic.co/micrositios-tic/sectorti/ciberseguridad/ciberseguridad-el-gran-desafio-de-las-empresas-en-colombia-foros-tic/

Ramírez, M., Rodríguez Ariza, L., Gómez Miranda, M. E., & Vartika. (2022). The disclosures of information on cybersecurity in listed companies in Latin America—proposal for a cybersecurity disclosure index. *Sustainability*, *14*(3), 1390. https://doi.org/10.3390/su14031390

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

Rodríguez Zambrano, H. M., & Moreno Tamayo, C. H. (s/f). *Seguridad de la información y ciberseguridad: su importancia para los Estados, empresas y las personas, una revisión sistemática*. Colpap.org. Recuperado el 8 de abril de 2024, de https://colpap.org/wp-content/uploads/2023/12/Articulo-de-revision-sistematica-Ciberseguridad.pdf

Ruddin, I., & Subhan Zein SGN. (2024). Evolution of cybercrime law in legal development in the digital world. *Jurnal Multidisiplin Madani*, *4*(1), 168–173. https://doi.org/10.55927/mudima.v4i1.7962

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors (Basel, Switzerland)*, *23*(15), 6666. https://doi.org/10.3390/s23156666

Varpio, L., Paradis, E., Uijtdehaage, S., & Young, M. (2020). The distinctions between theory, theoretical framework, and conceptual framework. *Academic Medicine: Journal of the Association of American Medical Colleges*, *95*(7), 989–994. https://doi.org/10.1097/acm.0000000000003075

Xia, L., Semirumi, D. T., & Rezaei, R. (2023). A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis

on safeguarding citizen privacy. *Sustainable Cities and Society*, *98*(104771), 104771. https://doi.org/10.1016/j.scs.2023.104771

Zhang, Y., Malacaria, P., Loukas, G., & Panaousis, E. (2023). CROSS: A framework for cyber risk optimisation in smart homes. *Computers & Security*, *130*(103250), 103250. https://doi.org/10.1016/j.cose.2023.103250

Sharma, P. (2021, noviembre 9). *Costo de desarrollo de aplicaciones web: desglose de precios de 2021*. Cynoteck; Cynoteck Technology Solutions. https://cynoteck.com/es/blog-post/web-app-development-cost/

Weisheim, R. (2022, julio 11). *¿Cuánto cuesta mantener una página web en 2024? Un desglose completo de precios*. Tutoriales Hostinger. https://www.hostinger.co/tutoriales/cuanto-cuesta-mantener-una-pagina-web

Betania, V. (2022, febrero 15). *¿Cuánto cuesta un dominio web y por qué lo necesitas?* Tutoriales Hostinger. https://www.hostinger.mx/tutoriales/cuanto-cuesta-un-dominio-web

Política de Seguridad Digital - Política de Seguridad Digital. (s/f). MINTIC Colombia. Recuperado el 30 de abril de 2024, de https://mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/15430:Politica-de-Seguridad-Digital