CIBERSEGURIDAD PARA PYMES: ¿CÓMO PROTEGER TU NEGOCIO?

Jose Espinosa, Jostin Roa, Sebastian Rojas

2023

1 Introducción

El propósito de este trabajo consiste en abordar una problemática de alcance global: los ciberataques. El enfoque primordial de este proyecto radica en la búsqueda de soluciones para contrarrestar esta preocupante situación. Para lograrlo, se plantea la implementación efectiva de medidas de ciberseguridad en el entorno empresarial de Colombia. Esta estrategia se erige como respuesta a la constante amenaza que representan los ciberataques en el país, tal como lo indican diversos estudios que registran múltiples incidentes a lo largo del año

2 Problematica

La problemática a tratar en este proyecto, será sobre la ciberseguridad en empresas mas especificamente en las pymes, y como estas se han visto afectadas debido a la gran cantidad de ciberataques que han ocurrido estos últimos años. Estas empresas han sufrido graves consecuencias, lo cual lleva a que pierdan mucha de su información y datos importantes. Este problema tambien puede llevar a que las empresas pierdan datos de los usuarios o empleados, y ademas los efectos de estos ataques repercuten en toda la infraestructura empresarial bloqueando sus sistemas e incluso, pudiendo paralizar sus procesos de produccion.

3 Justificación

con esta problematica podriamos solucionar cosas como:

- Porque gracias a la programcion o conocimientos de la tecnologia podriamos ayudar a muchas empresas y solucionar tantos ataques de ciberseguridad
- ¿Qué pasaría si se resolviera el problema? Bajaria los ataques de ciberseguridad y puede apliar los empleos por que tiene que estar renovando la seguridad de la empresa

- ¿Qué pasaría si NO se resolviera el problema? Podrian subir los ataques y las empresas empezarian a perder informacion que llevaria a perdidas de dinero o clientes

4 Estado del Arte

La ciberseguridad es un tema crítico para las empresas de todos los tamaños. Los ciberataques son cada vez más sofisticados y pueden tener un impacto devastador en las empresas, tanto en términos financieros como reputacionales. Para protegerse de los ciberataques, las empresas deben implementar una serie de medidas de seguridad, como la implementación de software antivirus y antimalware, la formación de los empleados en ciberseguridad y la realización de copias de seguridad de los datos. Además de estas medidas básicas, las empresas también deben estar al tanto de las últimas tendencias en ciberseguridad, como el aumento del uso de la inteligencia artificial y la computación en la nube. En resumen, la ciberseguridad es un tema complejo que requiere una atención constante. Las empresas que implementen las medidas de seguridad adecuadas podrán protegerse de los ciberataques y mantener sus sistemas y datos seguros.

5 Pregunta generadora

¿Como pueden las pequeñas empresas mantenerse al dia con los temas de ciberseguridad y ademas protegerse de los ciberataques?

6 Objetivos del proyecto

- Objetivo General: El objetivo general de nuestro proyecto es que las pymes puedan estar al tanto de los temas relacionados con la ciberseguridad, y ademas que se mantengan protegidas usando nuestro sistema que permite detectar cualquier tipo de antivirus y ademas dar recomendaciones para no ser victima de ningun ciberataque.
- Objetivos específicos:
  - Lograr que las pymes conozcan las ultimas tendencias en ciberseguridad.
  - Lograr que las pymes implementen las medidas de seguridad adecuadas.
  - Identificar las necesidades de las pymes.
  - Desarrollar el sistema de deteccion de antivirus.
  - Evitar ciberataques en las pymes.

7 Marco teórico

El principal objetivo es ayudar a las pequeñas, una teoría clave que se ve o que se observó, (las pequeñas empresas) no prestan tanta atención al cuidado de sus datos con la ciberseguridad. Se hace la lectura de diferentes libros y artículos, podemos entender y saber que hacer para encontrar una solución a este inconveniente. Con las referencias tomadas previamente se hace una indagación para tener más certeza a la hora de cumplir el objetivo del proyecto. Se planteó una solución que puede dar una mayor seguridad al momento de cuidar los datos (pequeñas empresas).

8 Metodología

Para abordar de manera efectiva la seguridad de las PYMES, el primer paso fundamental sería llevar a cabo una indagación de los problemas que enfrenta la empresa cuando se convierte en blanco de ataques cibernéticos. Esta investigación nos permitirá comprender las vulnerabilidades específicas a las que se enfrentan y diseñar un programa de seguridad adaptado a sus necesidades. Simultáneamente, es esencial comunicar a estas PYMES la importancia de un programa de seguridad, así como la asistencia disponible para mejorar su protección cibernética. La concienciación sobre la ciberseguridad es un componente crucial, ya que muchas PYMES subestiman los riesgos que enfrentan. Una vez establecido este primer paso, el desarrollo de un programa integral que proponga soluciones efectivas para proteger los datos de estas empresas, junto con recomendaciones concretas en materia de seguridad, se convertirá en un recurso esencial para garantizar la continuidad de sus operaciones y proteger su información crítica.

9 Desarrollo - (¿Describa como serian las etapas?)

Para abordar los desafíos que enfrentan las pequeñas empresas en el ámbito de la ciberseguridad, se inicia con un análisis exhaustivo de la problemática existente. A partir de esta evaluación, se procede al diseño de un software eficiente que ofrezca soluciones efectivas, junto con valiosos consejos para las PYMES. Este software se pone a disposición mediante un modelo de suscripción, permitiendo su implementación en las empresas de menor tamaño. A medida que se avanza, se realizan actualizaciones periódicas para mejorar el software, y se lleva a cabo una revisión mensual de los resultados obtenidos, con el fin de identificar errores y rescatar aspectos positivos en su evolución constante.

10 Conclusiones

A lo largo de este proyecto hemos aprendido lo siguiente: La ciberseguridad es un tema crítico para todas las empresas, independientemente de su tamaño. Las pymes son especialmente vulnerables a los ciberataques, ya que suelen tener menos recursos para invertir en seguridad. Existen una serie de medidas básicas que las pymes pueden implementar para protegerse de los ciberataques, como la instalación de software antivirus y antimalware, la formación de los empleados en ciberseguridad y la realización de copias de seguridad de los datos. Además de estas medidas básicas, las pymes también deben estar al tanto de las últimas tendencias en ciberseguridad, como el aumento del uso de la inteligencia artificial y la computación en la nube. En particular, he aprendido lo siguiente sobre la ciberseguridad en pymes: Las pymes suelen subestimar el riesgo de sufrir un ciberataque. Las pymes suelen tener dificultades para implementar las medidas de seguridad necesarias. Las pymes necesitan soluciones de ciberseguridad que sean asequibles, fáciles de usar y adaptadas a sus necesidades específicas. Estoy convencido de que este proyecto puede ayudar a las pymes a mejorar su ciberseguridad y reducir su riesgo de sufrir un ciberataque. El software que desarrollaremos ofrecerá soluciones efectivas, junto con valiosos consejos para las pymes. Además, el software estará disponible mediante un modelo de suscripción, lo que lo hará asequible para las empresas de menor tamaño. Estoy emocionado de seguir trabajando en este proyecto y ayudar a las pymes a proteger sus datos y su negocio.

11 Recomendaciones y trabajo futuro

Junto a mi grupo tenemos pensado seguir usando este proyecto en el futuro, sentimos que le podemos dar mas profunidad ya que los temas que tratamos nos interesan a todos. Si es posible nos gustaria darle continuidad a este proyecto en la proxima asignatura de pracitca, ya que, asi podemos mejorar lo que tenemos actualmente. Pensamos que la ciberseguridad en pymes es un tema que debe ser tratado realmente, por lo tanto, no queremos dejar el proyecto asi, sino que por el contrario nos gustaria poder nutrirlo mas en cada oportunidad que tengamos.

12 Referencias Bibliográficas y Anexos

- Martinez, Victor Gayoso, Luis Hernandez Encinas, and David Arroyo Guardeno. Ciberseguridad. Madrid, Spain: CSIC, 2020. Print.
- Oscar E. Rodríguez C., Raúl E. Dutari D., David A. Rodríguez F., Libertad Fernández G., Kevin J. Díaz R., Juan G. Quintero P., Humberto J. Chang M. (2022). Percepción de la ciberseguridad. Visión Antataura, 6(2).
- Pulido Daza. (2020). Seguridad y ciberseguridad: Realidad jurídica y práctica del documento electrónico. Universidad de La Salle.

- Raúl Manuel Arano Chávez, Jesús Escudero Macluf, and Luis Alberto Delfín Beltrán. "Una necesidad en las empresas: la ciberseguridad." Universita Ciencia 5 (2016): n. pag. Web.
- Chomczyk. (2020). Aspectos juridicos de la ciberseguridad (Beltran y O. Tejerina Rodriguez, Eds.). Ra-Ma.Direccion Nacional de Ciberseguridad de Israel. (2022). Recomendaciones de ciberseguridad y reduccion de riesgos ciberneticos para pequeñas empresas: mejores practicas en ciberseguridad. https://doi.org/10.18235/0004378
- Garrell Guiu, Antoni., and Llorenc. Guilera Aguella. La industria 4.0 en la sociedad digital. Barcelona Marge Books, 2019. Print.
- Escobar Macias, y Álvarez Galarza, M. D. (2022). Analisis de ciberataques sobre el uso de redes sociales en relacion a la proteccion de datos personales en Ecuador. Dominio de las Ciencias, 8(1), 1070–1079.
- Ramos Varon, Antonio Ángel et al. Hacking y seguridad de paginas web. Bogota: Ediciones de la U, 2015. Print.
- Villora Divino. (2018). Evaluacion y gestion de vulnerabilidades: Como sobrevivir en el mundo de los ciberataques. Universitat Politecnica de Valencia.
- Yndurain. (2022). Ciberataques: el riesgo digital constante. In Actualidad Economica (Madrid Spain) (p. 11–). Unidad Editorial Revistas S.L.U.
- Izaguirre Olmedo y Leon Gavilanez F. (2018). Analisis de los Ciberataques realizados en America Latina. INNOVA Research Journal 9 180–189. https://doi.org/10.33890/innova.v3.n9.2018.837
- Medina Chicaiza y Cando-Segovia M. R. (2021). Prevencion en ciberseguridad: enfocada a los procesos de infraestructura tecnologica. 3C TIC 10(1), 17–40. https://doi.org/10.17993/3ctic.2021.101.17-41
- Gomez Vieites Alvaro. Seguridad en equipos informaticos Madrid RA-MA Editorial 2014. Print.
- Olda Bustillos Ortega, y Javier Rojas Segura. (2022). Protocolo basico de ciberseguridad para pymes. Interfases 16 168–186. https://doi.org/10.26439/interfases2022.n016.6021