Maestro: GERARDO SALAZAR SA

LAZAR

Alumnos: Juan Sebastián Terán Ramírez

José Esaú Tovar Cruz

Tesina

8-C

26/02/2024

Índice

Resumen:

Actualmente estamos viviendo en un mundo en donde la tecnología cada vez forma más parte de la vida cotidiana, con nuestros celulares, computadoras, relojes, inclusive con aparatos domésticos que ya son “inteligentes”, dando con esto una infinidad de problemas de seguridad y gente que desea vulnerar estos aparatos, dando como resultado que se desarrollen distintos métodos y aplicaciones para prevenir y para remediar cuando ya has sido vulnerado, además de esto existe hasta cierto punto un escaso conocimiento para la población en general para poder afrontar y prevenir estos riesgos dando como resultado que ellos mismo sean los causantes de que sean vulnerados y con estos su integridad informática se vea afectada y por lo cual se decidió crear GuardianNet que es una aplicación que permitirá la fácil guía de los cuidados y recomendaciones a la hora de afrontar problemas en la red.

Introducción

Se ha comprado que los usuarios se ponen en peligro al entrar a la red en donde se identificaron varios comportamientos de riesgo, entre los que destacan el compartir información personal sensible en redes sociales, como direcciones, números de teléfono o detalles de cuentas bancarias. Además, el uso de contraseñas débiles o repetidas en múltiples cuentas aumenta la vulnerabilidad frente a ataques cibernéticos.

Otro aspecto preocupante es la descarga de software y archivos de fuentes no confiables, lo que puede resultar en la instalación de malware o virus en los dispositivos. Asimismo, la falta de actualizaciones regulares de software y sistemas operativos deja a los usuarios expuestos a vulnerabilidades de seguridad conocidas.

El phishing y el engaño en línea también son amenazas comunes, donde los usuarios pueden ser víctimas de estafas al proporcionar información confidencial a través de correos electrónicos fraudulentos o sitios web falsos.

¿Y cómo le podemos dar vuelta a la situación? GuardianNet es una página web con el objetivo de brindar a las personas guías de cómo se pueden cuidar tanto en la web y como en la vida común, de igual forma posibles soluciones y

recomendaciones a problemas con la ayuda de nuestro ayudante C.O.N.N.O.R., un sistema experto que nos ayudara a dar con las posibles soluciones y realizar tu perfil de seguridad.

Dado a que existen una gran cantidad de antivirus y opciones de seguridad, la verdad es que ninguno te ayuda para que tu como usuario tengas las herramientas y conocimientos necesarios para no ser víctima de los peligros informáticos, además de que las interfaces de estos mismo son muy abrumadoras haciendo que el usuario no sepa donde debe de clickear para iniciar un proceso de la misma aplicación.

La página se enfoca en proveer de conocimiento y guías al usuario de cómo puede protegerse para prevenir y como dar con las posibles soluciones cuando ya está vulnerado, todo esto con una interfaz sencilla, y un sistema experto con mucho conocimiento con información precisa y reciente sobre temas de seguridad.

Preguntas de la investigación

Para llegar a la idea de la página web, se formularon preguntas para poder comprender mejor estos temas, ¿Qué es un antivirus?, ¿Qué es un virus?, ¿Cómo funciona un antivirus?,¿Cuánto cuesta un antivirus?, ¿Qué tipo de prevenciones ofrecen los antivirus?, ¿Qué es un sistema experto?, ¿Cómo funciona un sistema experto?, ¿Son amigables las interfaces de los antivirus comerciales?, ¿Qué tanto conocen las personas sobre temas de ciberseguridad y seguridad en general?, con ayuda de estas preguntas se obtuvo un mejor panorama de hacia dónde enfocar el objetico de la página para de esta forma poder brindar a las personara una página que ayude de verdad.

Justificación del problema.

GuardianNet resulto ser una herramienta que se pensó de muchos tipos y formas, ya sea solo como una página que proporcionara información general o simples consejos básicos. Al seguir avanzando en la investigación y obtener resultados preliminares, se empiezan a identificar las principales fallas y problemas que

enfrentan los usuarios. Se hace evidente la necesidad de profundizar más y buscar enfoques novedosos, en lugar de limitarse a ofrecer información superficial sobre posibles problemas. sino que fuera algo que el usuario pudiera sentir como una herramienta verdaderamente útil y confiable es como llegamos a la solución de tener nuestra página GuardianNet que cuenta con la información necesaria para tener una prevención y uso adecuado sin peligros en la red.

Además, como agregado extra a nuestra página presentamos una herramienta propia de GuardianNet llamada C.O.N.N.O.R que en resumen es un asistente virtual basado en un sistema experto que está enfocado en resolver tus principales problemas sobre alguna vulnerabilidad que puedas llegar a tener o alguna duda el cual te proporcionara la información que estes buscando y así tener la información que necesites en ese momento sin tener que estar buscando entre grandes cantidades de textos o muchas páginas que no resuelven tu duda.

Objetivo de investigación.

Diseñar y desarrollar una herramienta para protegerse en la red, así como consejos de navegación segura y si se llega a vulnerar, obteniendo información de lo que podemos realizar al respecto y cómo podemos ayudar al usuario.

Hipótesis.

1. La presencia de un asistente virtual basado en un sistema experto podría mejorar la respuesta y la preparación de los usuarios ante amenazas de seguridad en línea
2. La creación de una herramienta como GuardianNet podría tener un impacto positivo en la conciencia y el comportamiento de los usuarios en línea
3. La falta de conciencia sobre la importancia de la seguridad cibernética en la vida cotidiana puede llevar a una subestimación de los riesgos en línea

Palabras clave

Virus, vulnerabilidades, sistema experto, guías, antivirus, ayuda personalizada.

Marco Teórico

En los tiempos cuando el internet como lo conocemos aun no existía, en la llamada ARPANET surgió un “virus” bautizado como Creeper y aunque sus intenciones no eran maliciosas dio como resultado la creación de Reaper un programa que detectaba a creeper en el sistema lo borraba para que este no viajara entre las pocas computadoras de esos tiempos, por esa razón a reaper se le adjudica el titulo como el primer antivirus (Pardo, D., 2024), que conforme fue pasado el tiempo los virus realmente maliciosos empezaron a surgir, la necesidad de una contramedida dio como resultado la rápida evolucionando de estos sistemas para poder dar frente a las necesidades de los usuarios, ¿Pero realmente que es un antivirus?

Un antivirus es un tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de una computadora (Verizon, 2024). Una vez instalados, la mayoría del software antivirus se ejecutan automáticamente en segundo plano para brindar protección en tiempo real contra ataques de virus.

Los programas antivirus y el software de protección para computadoras están diseñados para evaluar datos, como páginas web, archivos, software y aplicaciones, para encontrar y erradicar malware lo antes posible.

La mayoría de ellos brindan protección en tiempo real, que permite resguardar tus aparatos de las amenazas entrantes, escanean toda tu computadora de forma regular para encontrar amenazas conocidas y brindan actualizaciones automáticas, e identifican, bloquean y eliminan códigos y software maliciosos.

Debido a que varias actividades se realizan actualmente en línea y nuevas amenazas emergen continuamente, es más importante que nunca instalar un programa de protección antivirus. Por suerte, actualmente existe una gran cantidad de productos excelentes en el mercado para elegir. De igual forma existen tipos de antivirus los cuales son:

- Antivirus preventivos

- Identificadores
- Descontaminantes

Antivirus preventivos

Como indica la propia palabra, son los antivirus que avisan antes de que el posible virus infecte un equipo. Se encuentra en la memoria del equipo y monitorea la actividad del usuario. Por ejemplo, el caso más habitual es cuando nos avisa de que estamos a punto de ejecutar un archivo malicioso o de origen no confiable.

Un ejemplo de estos Antivirus seria Avira y Kaspersky

Antivirus identificadores

También están los antivirus de tipo identificadores. En este caso, se refiere al que es capaz de identificar programas infecciosos que pueden dañar al sistema. Es más, incluso rastrean secuencias de códigos que guardan relación con el virus.

Un ejemplo de estos Antivirus seria TotalAV y Avast

Antivirus descontaminantes

Los descontaminantes, se parecen a los anteriores. Sin embargo, se caracterizan por eliminar los programas malignos encontrados en el sistema, para así descontaminar el equipo infectado. Es decir, analiza en busca de infecciones y, si encuentra algo malicioso, te avisa para su eliminación.

Un ejemplo de estos Antivirus seria Kaspersky y Norton

Algunos de los Antivirus más utilizados son:

1. Norton

   Con más de 30 años en el mercado, Norton Antivirus es uno de los bestselleres. Es muy famoso y tiene un paquete de seguridad muy avanzado, incluso para hogares conectados, con control parental y muchas más funcionalidades. Es una apuesta segura para proteger los equipos a nivel doméstico o empresarial.

2. Bitdefender

En el caso del antivirus Bitdefender Total Security, nos proporciona una gran protección contra los virus y software malicioso. Es completo hasta el punto de que también nos protege de ransomware e incluye VPN gratis. Además, presenta una relación calidad-precio fantástica y es compatible con Linux, Windows y Mac.

3. Panda

Con años de trayectoria en el mercado, el antivirus Panda nos protege de todas las amenazas informáticas. En términos de compatibilidad, solo podemos ejecutarlo en Windows, macOS y Android. Pero sí viene con VPN, control parental y programa antivirus en USB.

4. McAfee

El antivirus del café es otro de los más populares y destaca por ser pionero en ofrecer protección para cien dispositivos a la vez. Es un paquete con protección superior frente al malware en Android o Windows. Pero sí hay que mencionar que la función de control parental no es tan pro como en el caso de los otros antivirus. pero sí nos encanta la posibilidad del gestor de contraseñas True Key.

5. Malwarebytes

Este otro antivirus de «Malwarebytes Anti-Malware» es de tipo descontaminante, dado que analiza y borra todo lo malicioso que tengas en el sistema. ¡Siempre encuentra algo! Es uno de los mejores ejemplos de antivirus descontaminantes.

En términos más técnicos, un virus informático es un tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo. Además, está diseñado para propagarse de un equipo a otro. Los virus se insertan o se adjuntan a un programa o documento legítimo que admite macros a fin de ejecutar su código. En el proceso, un virus tiene el potencial para provocar efectos inesperados o dañinos, como perjudicar el software del sistema, ya sea dañando o destruyendo datos. (Norton. (2023, 6 marzo).

Los Virus

Cuando un virus se adjunta a un programa, archivo o documento, el virus permanecerá inactivo hasta que el equipo ejecute su código. Para que un virus infecte un equipo, se debe ejecutar el programa infectado, lo cual provocará que el código del virus se ejecute. El virus podría permanecer inactivo en el equipo, sin mostrar grandes indicios o síntomas. Sin embargo, una vez que el virus infecta el equipo, puede infectar a otros de la misma red. Los virus pueden realizar acciones devastadoras y molestas, por ejemplo, robar contraseñas o datos, registrar pulsaciones de teclado, dañar archivos, enviar spam a sus contactos de correo electrónico e, incluso, tomar el control de su equipo.(verizon, 2024)

Los virus informáticos secuestran el código y los recursos de su sistema para reproducirse y causan problemas de rendimiento en todo tipo de dispositivos. Al ejecutarse, el virus informático libera su carga útil y comienza su ataque. Casi inmediatamente, empezará a verse lo que los virus informáticos pueden hacer. (Latto, N. (2022, 17 septiembre).

¿Qué le pueden hacer los virus a su ordenador? Estos son algunos de los efectos que pueden desencadenar:

- Rendimiento lento o congelación
- Archivos dañados o eliminados
- Ventanas emergentes constantes o adware
- Fallos del programa y del sistema operativo
- Un disco duro que gira constantemente
- Mal funcionamiento de aplicaciones, archivos y otros programas

Aparte de causar estos problemas de rendimiento, los virus informáticos también pueden robar información personal como nombres de usuario, contraseñas o números de tarjeta de crédito. Algunos virus pueden enviar mensajes a todos sus contactos e intentar engañarlos para que también descarguen el virus, que es otra forma de propagación.

Todos los dispositivos, incluso los Mac, pueden infectarse con virus. Los iPhones y los Android también pueden tener virus. De hecho, cualquier dispositivo con acceso a Internet puede recibir programa maligno, incluso otros dispositivos inteligentes como las cafeteras.

Pero vale la pena recordar la diferencia entre el programa maligno y los virus: un virus es solo *un tipo de programa maligno*. Y hay muchos tipos de infecciones que pueden dañar su dispositivo, robar sus datos y causar otros estragos.
Desde el ransomware al spyware pasando por los troyanos, hay algunas cepas desagradables de programa maligno con las que hay que tener cuidado en todos sus aparatos. Afortunadamente, muchas de estas amenazas pueden ser eliminadas y prevenidas con un software antivirus gratuito de confianza.

¿Cuáles son los Diferentes tipos de virus?

Virus de acción directa

El tipo de virus más común y el más fácil de crear, los virus de acción directa entran en su ordenador, causan el caos (normalmente adhiriéndose a un montón de archivos COM o EXE) y luego se borran solos.

Virus del sector de arranque

Como su nombre sugiere, estos virus se cuelan en su sector de arranque (el responsable de cargar el sistema operativo tras el inicio) para infectar directamente la memoria. Estos tipos de virus se transmiten normalmente a través de hardware, por ejemplo, discos flexibles, unidades USB o CD. A medida que esos dispositivos se vuelven obsoletos, este tipo de virus también está en vías de desaparecer.

Virus residentes

Un virus residente es otro tipo de virus que infecta la memoria y se instala en su RAM (memoria de acceso aleatorio), que permite que el virus persista incluso si se elimina el infector original. También borra archivos y destruye la memoria de la placa base del ordenador.

Virus multipartitos

Los virus multipartitos son devastadores ya que aumentan su potencia al infectar archivos y el espacio de arranque. Son muy difíciles de erradicar porque pueden esconderse en los archivos o en el espacio de arranque

Virus polimórficos

Los virus polimórficos, otro tipo de virus muy resistente, cambian de forma para esconderse. Cuando se replican, sus clones son ligeramente diferentes unos de otros, lo que ayuda a evitar su detección.

Virus de macro

Los virus de macro están diseñados para ocultarse dentro de documentos de Word, como los archivos DOC o DOCX. Al descargar el archivo, se le pide que habilite las macros; en cuanto lo hace, el virus se activa

Sistemas Expertos

Los sistemas expertos son programas informáticos que tienen el objetivo de solucionar un problema concreto y utilizan la Inteligencia Artificial (IA) para simular el razonamiento de un ser humano. Se denominan sistemas *expertos* porque estos programas imitan la toma de decisiones de un profesionista en la materia. Actualmente, se consideran dentro del global de la Inteligencia Artificial. (UNIR México. 2024, 22 febrero).

Tipos de sistemas expertos

RBO (Rule Based Reasoning)

Están basados en reglas previamente establecidas y abordan las situaciones más complejas a través de reglas deterministas.

CBR (Case Based Reasoning)

Basados en casos. Es decir, solucionan problemas utilizando soluciones preexistentes y haciendo una analogía de problemas anteriores.

Basados en Redes de Bayes

Utilizan un conjunto de variables conocidas y su dependencia probabilística para deducir una solución. Se usan en la predicción, clasificación o el diagnóstico de enfermedades y en medicina.

¿Como funciona un Sistema Experto?

Los sistemas expertos están compuestos por una base de conocimiento, que representa hechos y reglas concretos con una fórmula determinista (si A entonces B). Además, incluyen un motor de inferencia que aplica estas reglas a unos hechos conocidos para deducir así nuevas situaciones. También disponen de módulos de comunicación, como un módulo de consulta y otro de trabajo.

Los sistemas expertos actuales, cuando se utilizan, suelen integrar capacidades de aprendizaje automático, como el machine o el deep learning. Esto les permite mejorar el rendimiento y sacar el máximo partido a la experiencia acumulada. Hace al sistema experto más experto.

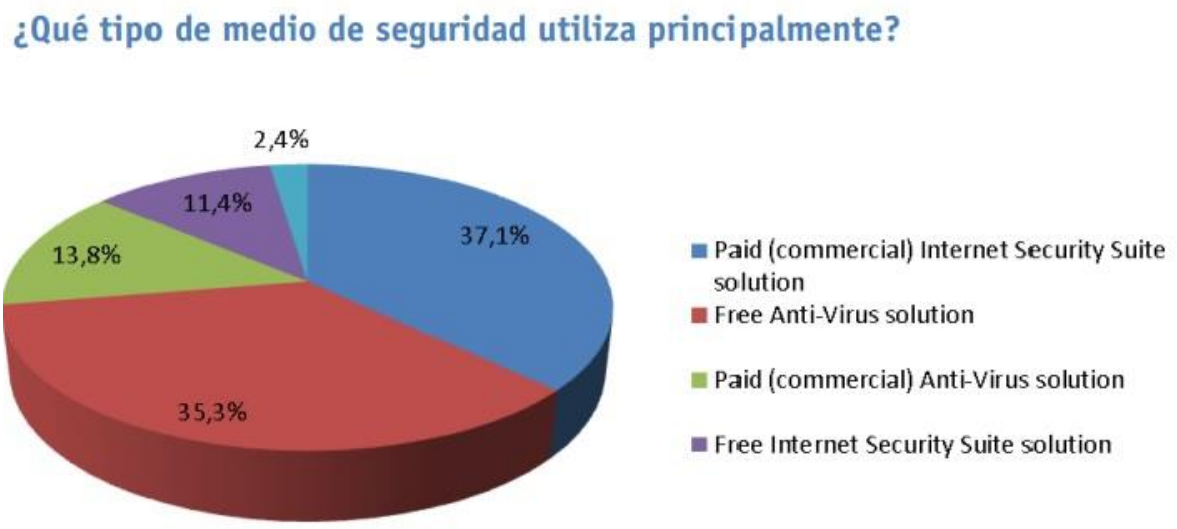
Entre las ventajas que ofrecen está la capacidad analítica y deductiva de mucha información muy rápida, lo que ahorra un tiempo valioso en la toma de decisiones que habrían tenido que tomar seres humanos. Es, por lo tanto, un ahorro de tiempo y recursos, pues estos sistemas una vez programados pueden replicarse

infinitamente y usarse por todo el mundo, con la ventaja añadida de que no envejecen.

Sus usos varían mucho según el campo para el que estén diseñados y, por ejemplo, en la industria y los negocios pueden realizar tareas de análisis de préstamos, optimización de almacenes logísticos, toma de decisiones financieras, gestión de datos, evaluación, control de procesos, etc.

La ingeniería Social

Aunque actualmente los antivirus son muy avanzados y te protejan de una gran cantidad de vulnerabilidades muchas personas, aunque en menor número no tienen instalado un antivirus y otros no saben que es.
De acuerdo con un estudio de AV-Comparatives, mientras algo más de la mitad de los usuarios paga por una solución de seguridad, el 2,4% no utiliza ninguna. De hecho, la cifra de ordenadores desprotegidos a nivel mundial se sitúa alrededor del 5%. (Collado, V. (2024, 25 abril).



Otro porcentaje de la población manifiesta la necesidad de formarse en materia de seguridad en Internet. Una de cada cuatro desconoce qué es un cifrado de datos o

de documentos, otra medida de seguridad, y un 39,6% no sabe reconocer si su equipo está actualizado o no.

Dando como resultado el uso de la ingeniería Social que utiliza la influencia y la persuasión para engañar a las personas, convenciéndolas mediante la manipulación de que el atacante es alguien que no es. Como resultado, se obtiene información con o sin el uso de tecnología. (INCIBE 2022)

Algunas técnicas de Ingeniería Social y sus variantes:

Phishing

Técnica de ciberdelincuencia que utiliza el engaño y el fraude para obtener información de una víctima. El ciberdelincuente utiliza un cebo fraudulento y espera a que algún usuario caiga en la trampa, para de esta manera poder obtener credenciales u otro tipo de información sensible. Se podría decir que el cibercriminal tira el cebo y espera a “pescar” (fishing en inglés) víctimas. (de ahí su nombre)

• Smishing: (SMS+ phishing) Ataque de phishing realizado a través de un SMS. Por lo general, el contenido del mensaje invita a pulsar en un enlace que lleva a una web falsa, intentarán que la víctima introduzca información sensible o que descargue una aplicación que en realidad es un malware. Generalmente, con estos SMS se hacen pasar por servicios usados en la población, como bancos o servicios de reparto. Los usuarios saben de las estafas a través de email, pero no tanto con los SMS, es por eso que hay una falsa percepción de seguridad con la mensajería móvil y nos lleva a que este ataque sea más efectivo.

• Vishing: Ataque de phishing realizado por teléfono o a través de un sistema de comunicación por voz. El cibercriminal se pone en contacto con la víctima a través de una llamada, y por ejemplo, haciéndose pasar por un servicio técnico, le pide a la víctima determinados requisitos para resolver la incidencia. Así pues, dependiendo de la estafa, intentará que la víctima revele información sensible, se instale alguna aplicación maliciosa, realice un pago, etc.

• Spear phishing: Ataque de phishing concretamente dirigido a una víctima o conjunto de víctimas. El ataque busca los mismos propósitos que los casos citados previamente, con la variante de que están personalizados, lo cual los hace más complicados de detectar. El atacante emplea técnicas de OSINT para obtener toda

la información disponible sobre la víctima, y de esta forma modelar y dirigir el ataque. Es vital conocer la información que publicamos en Internet sobre nosotros mismos.

• Whaling: Se trata de un ataque de spear phishing cuyo objetivo es un directivo o personal con un alto puesto en la organización. Los ciberatacantes consideran a los ejecutivos “High level” como “whales” de ahí el nombre del ataque.

SPAM

Cualquier email o mensaje recibido no deseado. Su envío se produce de forma masiva a un gran número de direcciones. No siempre es malicioso, aunque constituye una pérdida de tiempo y un gasto de recursos innecesario. Muchas veces puede tener enlaces maliciosos o difundir información que no es verdad.

• SPIM (spam over Internet messaging): Spam realizado sobre mensajería instantánea, es decir, mensajes que se reciben por Whatsapp, Telegram, DM de Facebook, etc. Suele ser más complicado de detectar que el spam “tradicional”.

Dumpster diving

Acción de “bucear” en la basura de una organización para obtener información de documentos. Una buena práctica es destruirlos para evitar que el reciclaje de estos documentos sea con un uso indeseado. Hay un dicho popular que define bien esta técnica: “La basura de una persona es el tesoro de otra”.

Shoulder surfing

Acción de mirar los datos que un usuario introduce por teclado y muestra en pantalla. De una manera aparentemente “casual”, el atacante puede obtener información sensible. Su nombre es muy descriptivo, ya que hace referencia a mirar por encima del hombro. Para evitar esto existen pantallas que se oscurecen o reflejan dependiendo del ángulo de visión, permitiendo que solo se vea correctamente desde el punto de vista del usuario del sistema.

Pharming

Redirección maliciosa hacia una web falsa, y de esta manera robar datos a las víctimas. Su nombre viene de la mezcla de phishing y farming. En general, este ataque viene después de otros ataques sobre DNS, y cuando se busca por el dominio, DNS traduce este nombre de dominio a una IP maliciosa de la que posee el atacante.

Comportamientos de Riesgo en Línea: El estudio de las acciones realizadas por las personas en línea revela varios comportamientos de riesgo. Entre estos, se destaca el compartir información personal sensible en plataformas de redes sociales, lo que aumenta la exposición a amenazas como el robo de identidad. El uso de contraseñas débiles o reutilizadas en múltiples cuentas también representa una vulnerabilidad significativa, facilitando el acceso no autorizado a información confidencial.

Descarga de Software y Archivos No Confiables: La descarga de software y archivos de fuentes no confiables constituye otra amenaza importante. Esta práctica puede resultar en la instalación inadvertida de programa maligno o virus en los dispositivos, comprometiendo la seguridad y la integridad de los datos del usuario. La falta de actualizaciones regulares de software y sistemas operativos también deja a los usuarios expuestos a vulnerabilidades conocidas.

Phishing y Engaño en Línea: El phishing y el engaño en línea representan tácticas comunes utilizadas por ciberdelincuentes para obtener información confidencial de los usuarios. Mediante correos electrónicos fraudulentos o sitios web falsos, los usuarios pueden verse inducidos a revelar datos personales o financieros, lo que los expone a riesgos de robo de información y fraude.

Metodología

La metodología que llevaremos a cabo para realizar nuestro proyecto es Scrum el cual es un marco de gestión de proyectos ágil que ayuda a los equipos a estructurar y gestionar su trabajo a través de un conjunto de valores, principios y prácticas. La razón por la cual decidimos utilizar Scrum como metodología es porque a menudo surgen nuevas amenazas y vulnerabilidades de las que debemos de cuidarnos y protegernos, por lo cual al utilizar Scrum permite ajustar las prioridades y el enfoque del proyecto en ciclos cortos (sprints), facilitando una rápida respuesta a los cambios.

Tecnologías de Desarrollo

Se desarrollará en HTML utilizando como editor de texto Visual Studio Code porque es un editor de texto ligero que inicia rápidamente y consume menos recursos del sistema además de que se pueden encontrar extensiones para casi cualquier necesidad, Para los diseños de nuestra página web utilizaremos CSS apoyado del framework de bootstrap el cual es muy fácil de integrar en una página web además de contar con muchas herramientas de diseño que facilitan el desarrollo y JavaScript en el backend ya que es un lenguaje dinámico y flexible que permite desarrollar y prototipar aplicaciones rápidamente permitiendo agregar interactividad y dinamismo a los sitios web , de igual forma manejaremos una base de datos NoSQL que será proporcionada por Firebase porque ofrece sincronizar datos entre clientes en tiempo real, haciendo más fácil construir aplicaciones colaborativas y con actualizaciones instantáneas y por ultimo utilizaremos GitHub para una mejor accesibilidad del proyecto el cual fue seleccionado por la razón de que es la plataforma que más usamos y en la que tenemos una mayor experiencia para la implementación del proyecto.

GuardianNet como Solución

Ante estos desafíos, surge la necesidad de una solución integral que eduque a los usuarios sobre las mejores prácticas de seguridad cibernética y brinde recursos para prevenir y mitigar los riesgos en línea. GuardianNet se presenta como una plataforma que cumple esta función, ofreciendo guías detalladas, soluciones prácticas y recomendaciones personalizadas.

El Rol de C.O.N.N.O.R: Central en la propuesta de GuardianNet es la inclusión de C.O.N.N.O.R, un sistema experto diseñado para proporcionar asistencia personalizada a los usuarios. Basado en un amplio conocimiento sobre seguridad cibernética, C.O.N.N.O.R ofrece respuestas precisas a consultas y problemas

específicos, brindando a los usuarios la orientación necesaria para protegerse en línea y actuar en caso de vulnerabilidad.

Referencias

Andrea. (2022, 16 junio). Tipos de antivirus y sus funciones. Copias de Seguridad En la Nube – tomado de: https://www.copianube.es/tipos-de-antivirus-y-sus-funciones/) mayo 2024.

Collado, V. (2024, 25 abril). Técnicas de ingeniería social. – tomado de : https://www.adaptixnetworks.com/tecnicas-de-ingenieria-social/. Mayo 2024

INCIBE (2022, 6 Febrero). El 92% de la población reconoce que necesita más formación sobre seguridad en Internet. – tomado de: https://www.incibe.es/incibe/sala-de-prensa/el-92-poblacion-reconoce-necesita-mas-formacion-seguridad-internet. Mayo 2024

Latto, N. (2022, 17 septiembre). ¿Qué es un virus informático y cómo funciona? ¿Qué Es un Virus Informático y Cómo Funciona? - Tomado de: https://www.avast.com/es-es/c-computer-virus

Prado D. (2024). Historia de los virus informáticos: Creeper y Reaper. –

Tomado de: https://pandorafms.com/blog/es/creeper-y-reaper/ Mayo 2024.

Norton. (2023, 6 marzo). ¿Qué es un virus informático? – tomado de: https://mx.norton.com/blog/malware/what-is-a-computer-virus. Mayo 2024

UNIR México (2024, 22 febrero). ¿Qué es un sistema experto? Usos y aplicaciones en la IA. - tomado de:https://mexico.unir.net/noticias/ingenieria/sistema-experto/#:~:text=Los%20sistemas%20expertos%20(SE)%20son,un%20profesionista%20en%20la%20materia.

Verizon (s. f.). Qué es un antivirus - Definición, significado y explicación. – tomado de: https://espanol.verizon.com/articles/internet-essentials/antivirus-definition/. Mayo 2024-