SISAP
Sistemas Aplicativos

Proyecto Final 2023

Fortalecimiento de la Ciberseguridad: Integrando Educación y Respuesta Efectiva

27 NOVIEMBRE

IRSI
Creado por:
Mariana David
Ronny Juárez
José William Vargas

IRSI Information Risk & Security Institute

Detalles de documento

Detalles de contacto

Nombre: Mariana David Sosa
Teléfono: +502 30110780
Correo electrónico: natydaso3@hotmail.com

Nombre: José William Vargas Hernández
Teléfono: +505 58338279
Correo electrónico: vjosewilliam@gmail.com

Nombre: Ronny José Juárez Juárez
Teléfono: +505 81932354
Correo electrónico: ronnyjuarez1996@gmail.com

Distribución del documento

Nombre	/	Puesto
Mariana David		Estudiante/IRSI-SISAP
Ronny Juárez		Estudiante/IRSI-SISAP
William Vargas		Estudiante/IRSI-SISAP
Mario Rivera		Instructor/IRSI-SISAP
Antonio Cabrera		Director/IRSI-SISAP

Historial del documento

Versión	Fecha	Modificado por	Observaciones
1.0	20/11/2023	Integrantes	Versión Inicial
2.0	27/11/2023	Integrantes	Versión Final

Introducción

La era digital ha llevado consigo innumerables beneficios, pero también ha suscitado desafíos significativos en términos de seguridad cibernética. Este informe aborda la problemática emergente de la creciente amenaza de ciberataques, afectando tanto a usuarios individuales como a organizaciones en línea. La falta de conciencia y preparación en ciberseguridad se manifiesta en un aumento alarmante de incidentes, poniendo en riesgo la seguridad de datos y sistemas, y evidenciando la necesidad urgente de medidas preventivas y correctivas.

El principal objetivo de este proyecto es analizar y abordar la creciente amenaza de ciberataques mediante la implementación de soluciones integrales. Se busca desarrollar una página web informativa sobre ciberseguridad, destinada a proporcionar recursos y orientación para mejorar la conciencia y preparación en seguridad digital. Estos objetivos se centran en fortalecer la ciberseguridad, proporcionando tanto recursos educativos a largo plazo como una capacidad de respuesta activa para enfrentar las amenazas emergentes.

La elección de abordar la ciberseguridad surge de la observación de un entorno digital cada vez más hostil. El aumento en la frecuencia y gravedad de los ciberataques, combinado con la falta de cumplimiento de leyes y regulaciones, destaca la necesidad de una acción inmediata. El impacto negativo de la falta de conciencia se manifiesta en pérdida de datos, daño a la reputación y pérdidas financieras, justificando así la importancia de este proyecto.

Este proyecto se enfocará en la creación de una página web informativa sobre ciberseguridad para abordar la problemática desde la conciencia hasta consultas directas por medio de vía mail que estará habilitado para comentarios, dudas entre otros.

La metodología de investigación implica la identificación de la problemática a través de la observación del entorno, seguida de la delimitación del problema y la identificación de soluciones alternativas, el cual consiste en la creación de una página web. Además, se evalúa las consecuencias de cada opción y se seleccionarán las más pertinentes y efectivas para no confundir al usuario y que sea interactiva.

Índice

Antecedentes

La elección de abordar la ciberseguridad como tema central de este proyecto surge de la observación y análisis del entorno digital actual. En un mundo cada vez más interconectado, la omnipresencia de la tecnología ha propiciado un aumento significativo en la frecuencia y gravedad de los ciberataques. Esta problemática se manifiesta no solo en la amenaza constante de malware, phishing y ataques de denegación de servicio, sino también en la falta generalizada de conciencia y preparación en ciberseguridad.

El contexto actual revela una realidad donde la seguridad de datos y sistemas está en riesgo debido al crecimiento exponencial de incidentes de seguridad cibernética. Las estadísticas documentan no solo la magnitud de estos incidentes, sino también la complejidad y diversificación de las amenazas. Este escenario, caracterizado por la falta de cumplimiento de leyes y regulaciones relacionadas con la ciberseguridad, destaca la necesidad imperativa de abordar esta problemática de manera integral.

La ausencia de conciencia y preparación en ciberseguridad se traduce en consecuencias tangibles, desde la pérdida de datos confidenciales hasta daños a la reputación y pérdidas financieras. La necesidad de una intervención efectiva se hace evidente, respaldada por la urgencia de mitigar los riesgos y mejorar la resiliencia frente a las crecientes amenazas cibernéticas. En este contexto, el proyecto propone una respuesta proactiva y eficiente, fusionando la creación de una página web educativa con la formación de un equipo de respuesta a incidentes para abordar la problemática desde diversas perspectivas.

Marco teórico

Planteamiento del problema

La problemática identificada resalta la creciente amenaza de ciberataques a la que se enfrentan tanto los usuarios individuales como las organizaciones en línea. En la actualidad, la omnipresencia de la tecnología y la interconexión global han creado un entorno propicio para la proliferación de amenazas cibernéticas, que van desde ataques de malware y phishing hasta intrusiones más sofisticadas.

Un aspecto crítico de esta problemática es la falta generalizada de conciencia y preparación en materia de ciberseguridad. Muchos usuarios y organizaciones aún subestiman la importancia de adoptar medidas proactivas para protegerse contra posibles amenazas en el ciberespacio. La insuficiente comprensión de las mejores

prácticas de seguridad digital y la falta de implementación de protocolos adecuados aumentan la vulnerabilidad frente a posibles ataques.

Este panorama se ve agravado por el constante aumento de incidentes de seguridad cibernética que afectan a nivel mundial. Desde la pérdida de datos confidenciales hasta interrupciones en los servicios en línea, la magnitud de los daños causados por estos ataques subraya la necesidad urgente de abordar las deficiencias en la ciberseguridad.

Además, se observa una marcada carencia en el cumplimiento de leyes y regulaciones relacionadas con la ciberseguridad. Las normativas existentes destinadas a salvaguardar la integridad y confidencialidad de la información digital a menudo son pasadas por alto, ya sea debido a la falta de recursos, la complejidad normativa o simplemente la falta de conciencia sobre la importancia de su cumplimiento.

Para contrarrestar esta problemática, es esencial promover una mayor conciencia pública sobre los riesgos cibernéticos y fomentar la educación en ciberseguridad. Asimismo, las organizaciones deben implementar medidas robustas de seguridad digital, incluyendo la actualización regular de sistemas, la capacitación del personal y la adopción de tecnologías avanzadas de detección y prevención de amenazas. Además, el fortalecimiento de la aplicación de leyes y regulaciones relacionadas con la ciberseguridad resulta fundamental para crear un entorno digital más seguro y resistente ante las crecientes amenazas cibernéticas.

Descripción de la problemática

En el actual panorama, se observa un notable incremento en los ciberataques, generando una creciente vulnerabilidad en la seguridad de datos y sistemas. Las estadísticas disponibles revelan no solo un aumento en la frecuencia de estos incidentes, sino también un incremento en su gravedad, señalando la magnitud del desafío que enfrentamos en el ámbito de la seguridad cibernética.

Dentro de las amenazas específicas que se destacan, se encuentran el malware, el phishing y los ataques de denegación de servicio, cada uno representando una faceta distinta de la compleja red de riesgos que enfrentan usuarios individuales y organizaciones en línea. Estos ataques no solo comprometen la integridad de los datos, sino que también tienen el potencial de causar daño significativo a la reputación de las entidades afectadas, así como provocar pérdidas financieras considerables.

Una de las cuestiones fundamentales que agravan esta problemática es la falta generalizada de conciencia y preparación en ciberseguridad. Este vacío de conocimiento

contribuye directamente a consecuencias adversas, como la pérdida de datos confidenciales, el menoscabo de la reputación de las instituciones y la ocurrencia de pérdidas económicas. Ante este escenario, resulta imperativo impulsar iniciativas educativas que promuevan la conciencia sobre los riesgos cibernéticos y fomentar la implementación de medidas proactivas para fortalecer la seguridad digital en todos los niveles.

Definiciones de términos importantes relacionados con el tema

Ransomware
El ransomware es un tipo de software malicioso que cifra los archivos o bloquea el acceso a sistemas informáticos y solicita un rescate para restaurar el acceso. Se propaga a través de correos electrónicos fraudulentos, descargas de software comprometido o vulnerabilidades en sistemas no actualizados. El pago del rescate no garantiza la recuperación de los datos y puede alentar más ataques.

Phishing
El phishing es una técnica de ingeniería social donde los atacantes se hacen pasar por entidades confiables para engañar a las personas y obtener información confidencial, como contraseñas, números de tarjetas de crédito o datos personales. Los correos electrónicos de phishing suelen contener enlaces maliciosos o adjuntos que, al hacer clic o descargar, comprometen la seguridad de la víctima.

Error Humano
Los errores humanos en ciberseguridad pueden ser involuntarios o resultado de falta de conciencia. Por ejemplo, la negligencia al hacer clic en enlaces desconocidos, revelar información confidencial por teléfono o correo electrónico, o no seguir prácticas de seguridad como actualizar contraseñas regularmente.

Ingeniería Social
La ingeniería social se centra en manipular psicológicamente a individuos para obtener acceso a información confidencial o realizar acciones que comprometan la seguridad. Esto puede involucrar el uso de pretextos, engaños o amenazas para persuadir a las personas a revelar datos sensibles o realizar acciones perjudiciales.

Malware
Término genérico que engloba todo tipo de software malicioso, como virus, gusanos, troyanos, spyware, adware, entre otros, diseñados para dañar, robar información o acceder de manera no autorizada a sistemas informáticos.

Firewall
Es un sistema de seguridad que controla el tráfico de red, permitiendo o bloqueando

ciertos tipos de datos en función de reglas de seguridad predefinidas. Sirve como barrera entre una red interna privada y redes externas como internet.

Vulnerabilidad
Es una debilidad o falla en un sistema que podría ser explotada por un atacante para comprometer la seguridad del sistema, acceder a información confidencial o causar daño.

Parches de Seguridad
Actualizaciones desarrolladas por los fabricantes de software para corregir vulnerabilidades conocidas en sus programas. Aplicar estos parches ayuda a mantener los sistemas protegidos contra posibles ataques.

Cifrado
Proceso de convertir información en un código secreto para protegerla de accesos no autorizados. Se utiliza para garantizar la confidencialidad de los datos, especialmente durante la transmisión a través de redes.

Autenticación de dos factores (2FA)
Un método de seguridad que requiere dos formas diferentes de identificación antes de otorgar acceso a un sistema, como la combinación de una contraseña con un código enviado al teléfono móvil del usuario.

Intrusión
Acceso no autorizado a un sistema informático o red, realizado por una persona no autorizada.

Ataque de denegación de servicio (DDos)
Un tipo de ataque informático que busca abrumar un sistema o red con un gran volumen de tráfico falso, impidiendo que usuarios legítimos accedan a los servicios.

Autenticación biométrica
Utiliza características físicas únicas, como huellas dactilares, reconocimiento facial o de voz, para verificar la identidad de un usuario.

Política de seguridad
Conjunto de reglas, procedimientos y prácticas establecidas para proteger los activos de una organización, incluyendo directrices sobre contraseñas, acceso a la red, almacenamiento de datos, etc.

Descripción de teorías que respalden la investigación

En el ámbito de la investigación sobre el uso de una página web de ciberseguridad, se encuentran diversas teorías y enfoques que respaldan el análisis desde distintas perspectivas. La Teoría de la Ciberseguridad destaca principios como la Defensa en Profundidad, abogando por implementar capas de seguridad para una protección integral, y el Principio de Menor Privilegio, que limita el acceso a sistemas y datos para reducir la superficie de ataque.

Desde la perspectiva del comportamiento del usuario, el Modelo de Razonamiento de la Tecnología de Protección (PTRM) examina las decisiones de seguridad, mientras que la Teoría de la Disonancia Cognitiva aborda la inconsistencia entre actitudes y comportamientos de seguridad, buscando comprender y reducir esta discrepancia.

En el ámbito de la comunicación, la Teoría de la Agenda-Setting se centra en cómo los medios influencian la percepción pública, aplicándola al contexto de ciberseguridad para investigar la influencia de las páginas web en la conciencia del usuario.

La Teoría de Sistemas Complejos, específicamente la Teoría de Redes Complejas, puede analizar la infraestructura de la página web, comprendiendo la interconexión de componentes y su impacto en la resistencia del sistema.

Desde la Psicología Cognitiva, la Teoría de la Atención Selectiva examina cómo los usuarios procesan información de seguridad, guiando el diseño de la página web para captar y retener la atención del usuario.

La Teoría de Juegos, aplicada a la ciberseguridad, explora estrategias entre atacantes y defensores, modelando interacciones y decisiones para desarrollar estrategias óptimas de defensa.

Finalmente, la Teoría de la Privacidad, en particular la del Intercambio Social, analiza decisiones relacionadas con la privacidad y cómo los individuos evalúan costos y beneficios de compartir información en línea. La combinación de estos enfoques teóricos proporciona una comprensión integral para diseñar y evaluar eficazmente una página web de ciberseguridad, considerando aspectos tecnológicos, comportamentales y de comunicación.

Resumen de estudio e investigaciones

En el ámbito de la ciberseguridad, es fundamental comprender algunos términos clave. El ransomware es un software malicioso que cifra archivos o bloquea el acceso a sistemas, exigiendo un rescate. Por otro lado, el phishing es una técnica de ingeniería social que involucra engañar a las personas para obtener información confidencial. Los errores humanos, ya sean involuntarios o por falta de conciencia, también representan riesgos significativos, como hacer clic en enlaces desconocidos.

La ingeniería social busca manipular psicológicamente a individuos para obtener acceso a información confidencial. El malware, un término genérico, abarca diferentes tipos de software malicioso. Un firewall actúa como barrera de seguridad, controlando el tráfico de red. Las vulnerabilidades son debilidades en sistemas que podrían ser explotadas, y los parches de seguridad son actualizaciones para corregirlas. El cifrado, que convierte información en un código secreto, y la autenticación de dos factores son esenciales para proteger datos.

En cuanto a las teorías respaldando la investigación en páginas web de ciberseguridad, la Teoría de la Ciberseguridad aboga por la defensa en profundidad y el principio de menor privilegio. Desde la perspectiva del comportamiento del usuario, el Modelo de Razonamiento de la Tecnología de Protección y la Teoría de la Disonancia Cognitiva exploran cómo las personas toman decisiones de seguridad. La Teoría de la Comunicación, específicamente la Agenda-Setting, analiza cómo las páginas web pueden influir en la percepción pública. Además, la Teoría de Sistemas Complejos y de Redes Complejas ayuda a comprender la infraestructura de la página web.

Desde la Psicología Cognitiva, la Teoría de la Atención Selectiva examina cómo los usuarios procesan información de seguridad. La Teoría de Juegos Aplicada a la Ciberseguridad modela estrategias entre atacantes y defensores. Finalmente, la Teoría de la Privacidad, en particular la del Intercambio Social, evalúa las decisiones relacionadas con la privacidad. Integrar estos enfoques proporciona una comprensión holística para diseñar y evaluar eficazmente páginas web de ciberseguridad, considerando aspectos tecnológicos, comportamentales y de comunicación.

Desarrollo

Detalles del desarrollo del proyecto

En el desarrollo de nuestro proyecto, hemos seguido un enfoque integral para abordar los desafíos actuales en ciberseguridad. La creación de nuestra página web, que presenta una estructura clara y accesible, refleja nuestro compromiso con la conciencia y la educación en este campo crítico. A continuación, detallamos los aspectos clave de nuestro proyecto.

En la materialización del proyecto para la creación de la página web de ciberseguridad, se optó por utilizar tecnologías clave que contribuyen a un desarrollo eficiente y robusto. La implementación se llevó a cabo con React Native, aprovechando su versatilidad para el desarrollo de aplicaciones móviles mediante el uso de JavaScript. React Native permite construir interfaces de usuario dinámicas y fluidas, brindando una experiencia interactiva a los usuarios.

En la estructuración del contenido, se emplearon tecnologías web fundamentales como HTML y CSS. HTML (Hypertext Markup Language) se utilizó para definir la estructura y los elementos de la página, facilitando la organización y presentación de la información. Por otro lado, CSS (Cascading Style Sheets) se empleó para dar formato y estilo a la página, mejorando la presentación visual y la experiencia del usuario.

Para optimizar el flujo de trabajo y la gestión de dependencias, se incorporaron herramientas esenciales como Webpack, Babel y ESLint. Webpack se encargó de empaquetar y gestionar los recursos, como scripts y hojas de estilo, simplificando la carga eficiente de la página. Babel permitió la transpilación del código JavaScript, asegurando la compatibilidad con diversos navegadores y garantizando un código más legible y mantenible. ESLint se integró para mantener altos estándares de calidad en el código, identificando posibles errores y aplicando consistencia en la escritura del código fuente. La combinación de estas tecnologías proporcionó una base sólida para la creación de una página web educativa y funcional en el ámbito de la ciberseguridad.

Además, como parte del desarrollo de la página web de ciberseguridad, se llevaron a cabo pruebas unitarias para garantizar la fiabilidad y el rendimiento del sistema. Estas pruebas, realizadas en distintas secciones y funcionalidades, permitieron identificar y corregir posibles fallos o inconsistencias en el código. La implementación de pruebas unitarias contribuyó a mantener altos estándares de calidad, asegurando que la página web respondiera de manera consistente a las interacciones del usuario y mejorando la robustez del proyecto en su conjunto.

Presentación de datos, hallazgos relevantes

Implementación de la Página Web
Hemos diseñado y desarrollado una página web centrada en la ciberseguridad, con secciones bien definidas, como "Inicio", "Sobre Nosotros", "Aprendizaje", "Incidentes" y "Contacto". La presentación visual de la página, junto con una interfaz intuitiva, busca facilitar la navegación y comprensión de la información por parte de los usuarios.

Contenidos Relevantes
Dentro de la sección "Aprendizaje", hemos proporcionado información de ciberseguridad y una guía de aprendizaje descargable en formato PDF. Esto garantiza que los usuarios tengan acceso a recursos educativos clave para mejorar su comprensión de los riesgos y las mejores prácticas en ciberseguridad.

Enfrentando Incidentes de Ciberseguridad
Dentro de la sección "Incidentes", abordamos diversas amenazas, como ransomware, phishing y errores humanos. Proporcionamos información detallada sobre estos temas, destacando la importancia de la prevención, la respuesta rápida y la conciencia constante para protegerse contra estos ataques.

Enfoque en Ransomware
Dedicamos una sección específica para abordar el ransomware, detallando qué es, cómo puede infectar sistemas y las mejores prácticas para prevenir y manejar este tipo de amenaza. Proporcionamos consejos prácticos, como realizar copias de seguridad regulares y mantener actualizados los sistemas y el software.

Educación Sobre Phising
La sección sobre phishing destaca la importancia de reconocer y evitar este tipo de ataques. Proporcionamos información sobre la historia del phishing, sus diversas formas y consejos para protegerse, como no hacer clic en enlaces sospechosos y verificar la autenticidad de los correos electrónicos.

Consideración del Error Humano
Abordamos el error humano como un aspecto crítico de la ciberseguridad. Identificamos los errores basados en habilidades y decisiones, destacando la necesidad de formación continua para mitigar estos riesgos. Proporcionamos ejemplos de errores comunes en las empresas y cómo evitarlos.

Prevención con Ingeniería Social
Destacamos la amenaza de la ingeniería social y cómo los atacantes pueden aprovechar la psicología humana para obtener información confidencial. Proporcionamos pautas para protegerse, como no proporcionar datos personales a desconocidos y configurar la privacidad en las redes sociales.

Canal de contacto
Para fomentar la interacción, hemos incluido una sección de "Contáctanos" que permite a los usuarios enviar mensajes directos. Esto facilita la comunicación y la retroalimentación, fortaleciendo nuestra relación con la audiencia.

Interpretación de los resultados y relación con los objetivos

Nuestro proyecto no solo se centra en la creación de una página web visualmente atractiva, sino que también busca brindar contenidos educativos, prácticos y relevantes para empoderar a los usuarios en la protección contra amenazas cibernéticas. La estructura clara y la presentación visual buscan hacer que la información sea accesible para todos los usuarios interesados en mejorar su comprensión y prácticas en ciberseguridad.

Conclusiones

Para terminar, este proyecto aborda la creciente amenaza de ciberataques y la falta de conciencia en ciberseguridad con un enfoque integral. La creación de una página web educativa refleja una estrategia organizada, con secciones específicas para educación, incidentes y contacto. La identificación del problema se respalda con estadísticas sobre el aumento de incidentes de seguridad cibernética, destacando la urgencia de medidas inmediatas. La implementación de la página web, con enfoque en ransomware, phishing y errores humanos e ingeniería social, demuestra la comprensión de la necesidad de abordar amenazas en tiempo real. La valoración de soluciones alternativas propone la combinación de educación continua y capacidad de responder a preguntas por medio de correo como una estrategia integral e indispensable para fortalecer la seguridad en línea en un entorno digital vulnerable.

Recomendaciones

Para mejorar la efectividad y la atractividad de la página web dedicada a la ciberseguridad, se pueden considerar diversas recomendaciones que fortalezcan la experiencia del usuario y maximicen el impacto educativo. En primer lugar, la inclusión de elementos multimedia, como videos explicativos, puede enriquecer significativamente el contenido educativo. Estos videos podrían abordar conceptos clave de ciberseguridad, presentar escenarios prácticos y ofrecer demostraciones visuales de buenas prácticas de seguridad digital. Esta adición no solo haría la información más accesible, sino que también aumentaría el compromiso del usuario.

Además, se podría explorar la implementación de simulaciones interactivas que permitan a los usuarios enfrentarse a situaciones de ciberseguridad en un entorno controlado. Estas simulaciones ofrecerían la oportunidad de aplicar los conocimientos adquiridos y tomar decisiones prácticas en tiempo real, brindando una experiencia educativa más inmersiva y práctica. Incorporar juegos educativos relacionados con la ciberseguridad también podría ser una estrategia efectiva para hacer el aprendizaje más divertido y memorable.

La introducción de secciones de estudio de casos reales podría añadir un componente práctico y relevante a la página web. Analizar incidentes de seguridad pasados, sus causas y consecuencias, así como las lecciones aprendidas, proporcionaría a los usuarios una comprensión más profunda de los riesgos y desafíos en el ámbito de la ciberseguridad.
Además, se sugiere la inclusión de un espacio de preguntas frecuentes (FAQ) dinámico, donde los usuarios puedan plantear sus dudas y obtener respuestas claras y concisas. Esto fomentaría la interacción y la participación activa, creando un entorno educativo más colaborativo.

La implementación de webinars o sesiones en vivo con expertos en ciberseguridad podría ofrecer a los usuarios la oportunidad de interactuar directamente con profesionales del campo. Estas sesiones podrían abordar temas actuales, responder preguntas en tiempo real y mantener a la audiencia actualizada sobre las últimas tendencias y amenazas cibernéticas.

Por último, se podría explorar la posibilidad de incorporar una sección de historias de éxito, destacando casos donde la aplicación adecuada de medidas de ciberseguridad haya evitado o mitigado ataques exitosos. Estas historias podrían servir como inspiración y motivación para que los usuarios adopten prácticas seguras en sus propios entornos digitales.

Bibliografía

30 Estadísticas Importantes de Seguridad Informática (2022) | Prey Blog. (2022, February 17). https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica

Aumento de los ciberataques en Chile en 2023: Lo que dicen las cifras, las formas más frecuentes y las consecuencias. (n.d.). https://comentarista.emol.com/2294117/25308885/Emol-Social-Facts.html

Hacknoid. (2020, April 21). *Estadísticas de ciberataques en tiempos de COVID-19*. Hacknoid. https://www.hacknoid.com/sin-categorizar/estadisticas-de-ciberataques-en-tiempos-de-covid-19/

Ibermatica. (2023, May 24). *IMPORTANCIA DE LA CIBERSEGURIDAD: ¿POR QUÉ?* Ibermática Industria. https://ibermaticaindustria.com/blog/la-importancia-de-la-ciberseguridad-por-que-y-como-protegernos/#:~:text=Evitar%20enormes%20p%C3%A9rdidas%20econ%C3%B3micas.,%2C%20secuestro%20de%20datos%2C%20etc.

Ingeniería social: definición. (2023a, April 19). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Ingeniería social: definición. (2023b, April 19). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Malwarebytes. (2019a, January 7). *¿Qué es el phishing? | Cómo protegerse de los ataques de phishing*. Malwarebytes. https://es.malwarebytes.com/phishing/

Malwarebytes. (2019b, May 8). *¿Qué es el malware? Definición y cómo saber si está infectado*. Malwarebytes. https://es.malwarebytes.com/malware/

Malwarebytes. (2019c, November 25). *Ransomware: qué es y cómo eliminarlo*. Malwarebytes. https://es.malwarebytes.com/ransomware/

Massoni, A. (2023, June 22). *Estadísticas Ciberseguridad junio 2023*. Hacknoid. https://www.hacknoid.com/hacknoid/estadisticas-ciberseguridad-junio-2023/

¿Por qué la ciberseguridad es tan importante? (n.d.). https://www.ironhack.com/mx/blog/por-que-la-ciberseguridad-es-tan-importante

Anexos

Link al repositorio

Aquí encontrara el código completo del proyecto. Adicional encontrará documentación en el README file. Donde se encuentra documentación importante del proyecto, como probarlo, el host y video.

- https://github.com/Marianadaso3/Proyecto-SISAP

Imágenes generales de la página Web

Figura 1. Página principal

Figura 2. Sección “Sobre nosotros”

Figura 3. Sección “Aprendizaje”

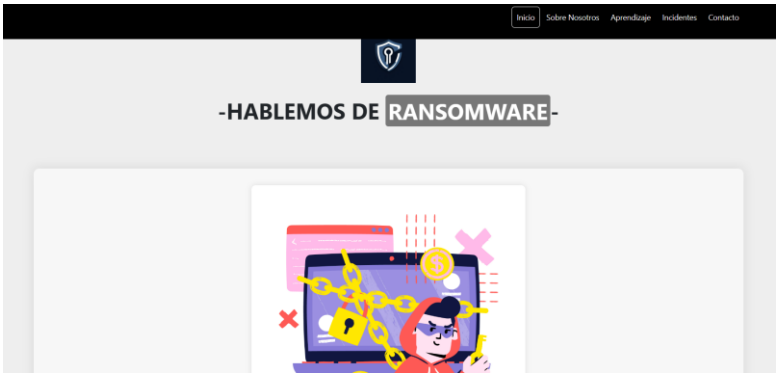

Figura 4. Sección “Incidentes-TEMA 1”

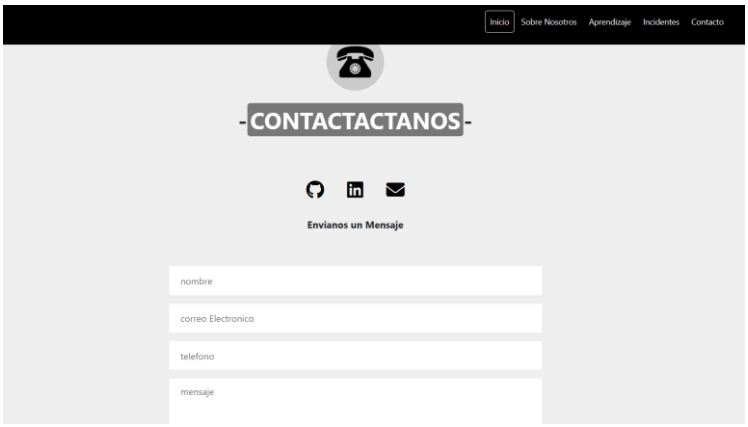

Figura 4. Sección “Contacto”

---------- ÚLTIMA PÁGINA ----------