Journal **TechInnovation**
Volumen 1, Número 2, 2022
Universidad Estatal del Sur de Manabí
ISSN-e: 2953-6472

ARTÍCULO DE REVISIÓN

Riesgos de seguridad de los datos en la web

Data security risks on the web

https://doi.org/10.47230/Journal.TechInnovation.v1.n2.2022.43-49

Recibido: 01-06-2022 **Aceptado:** 27-06-2022 **Publicado:** 31-07-2022

Geanfrank Isaias Cruz Lucas[1]
https://orcid.org/0000-0002-0881-6499

Luis Enrique Delgado Tejena[2]
https://orcid.org/0000-0003-4566-281X

Bryan Ricardo Ponce Solorzano[3]
https://orcid.org/0000-0002-0897-8965

Mario Javier Marcillo Merino[4]
https://orcid.org/0000-0001-5818-367X

1. Ingeniero en formación Carrera de Tecnología de la Información Facultad Ciencias Técnicas, Universidad Estatal del Sur de Manabí. Jipijapa, Manabí, Ecuador. cruz-geanfrank0339@unesum.edu.ec
2. Ingeniero en formación Carrera de Tecnología de la Información Facultad Ciencias Técnicas, Universidad Estatal del Sur de Manabí. Jipijapa, Manabí, Ecuador. delgado-luis3372@unesum.edu.ec
3. Ingeniero en formación Carrera de Tecnología de la Información Facultad Ciencias Técnicas, Universidad Estatal del Sur de Manabí. Jipijapa, Manabí, Ecuador. ponce-bryan1700@unesum.edu.ec
4. Ingeniero en Sistemas, Magister en Docencia Universitaria. Docente titular de la Universidad Estatal del Sur de Manabí. Jipijapa, Manabí, Ecuador. mario.marcillo@unesum.edu.ec

Volumen: 1
Número: 2
Año: 2022
Paginación: 43-49
URL: https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/18
***Correspondencia autor:** cruz-geanfrank0339@unesum.edu.ec

RESUMEN

En el mundo actual, la información y los datos son un activo valioso para cualquier organización. Sin embargo, con el aumento del uso de la tecnología y la dependencia de internet, los riesgos de seguridad de los datos en la web se han vuelto cada vez más preocupantes. Los ataques cibernéticos, el robo de identidad, y la pérdida de datos confidenciales son solo algunos de los riesgos que enfrentan las empresas y los usuarios en línea. Una de las principales preocupaciones es la vulnerabilidad de los sitios web y las aplicaciones móviles a los ataques de hackers. Los ciberdelincuentes utilizan técnicas sofisticadas para acceder a los sistemas y robar información confidencial, como contraseñas y números de tarjetas de crédito. Los ataques de phishing y malware son comunes, y pueden infectar los dispositivos de los usuarios y robar información personal. La privacidad de los usuarios también se ve amenazada en línea. Los sitios web y las aplicaciones suelen recopilar información personal de los usuarios, como su historial de navegación y preferencias, y compartirla con terceros sin su consentimiento. Los datos recopilados pueden ser utilizados para crear perfiles de los usuarios y dirigir publicidad personalizada. Es importante que las empresas implementen medidas de seguridad adecuadas y los usuarios deben tomar medidas para proteger sus dispositivos y redes. Además, es importante ser consciente de cómo se utiliza la información personal en línea y tomar medidas para proteger la privacidad.

Palabras clave: Ataques Dos, Ciberdelincuentes, Ciberseguridad, Spam.

ABSTRACT

In today's world, information and data are a valuable asset for any organization. However, with the increased use of technology and reliance on the internet, data security risks on the web have become increasingly concerning. Cyberattacks, identity theft, and loss of sensitive data are just a few of the risks that businesses and users face online. One of the main concerns is the vulnerability of websites and mobile applications to hacker attacks. Cyber criminals use sophisticated techniques to break into systems and steal sensitive information, such as passwords and credit card numbers. Phishing and malware attacks are common, and they can infect users' devices and steal personal information. User privacy is also threatened online. Websites and apps often collect users' personal information, such as their browsing history and preferences, and share it with third parties without their consent. The data collected may be used to create user profiles and target personalized advertising. It is important that companies implement adequate security measures and users must take measures to protect their devices and networks. Additionally, it is important to be aware of how personal information is used online and take steps to protect privacy.

Keywords: Cybersecurity, Cybercriminals, Dos Attacks, Spam.

Introducción

La seguridad de los datos en la web es un tema crítico en la era digital actual, pues, cada vez más información está siendo almacenada y compartida en línea. Los riesgos de seguridad incluyen desde el robo de información confidencial hasta la violación de privacidad y la interrupción de servicios. Con la creciente dependencia de la tecnología en la vida cotidiana, es esencial comprender estos riesgos y tomar medidas para proteger los datos personales y empresariales.

Uno de los principales riesgos de seguridad en la web es el robo de datos. Los ciberdelincuentes utilizan técnicas sofisticadas para acceder a información confidencial, como contraseñas y números de tarjetas de crédito. También pueden utilizar técnicas de phishing para engañar a los usuarios para que revele información confidencial. El robo de datos puede tener consecuencias graves, como el fraude financiero y la violación de privacidad.

Otro riesgo de seguridad en la web es la interrupción de servicios. Los ataques de denegación de servicio (DoS) y distribuidos (DDoS) buscan sobrecargar los sistemas para interrumpir el acceso a servicios en línea. Estos ataques pueden tener un impacto significativo en las empresas, ya que pueden causar pérdidas financieras y dañar la reputación.

La seguridad de los datos también es amenazada por la vulnerabilidad de los sistemas y aplicaciones en línea. Las debilidades en el código o las configuraciones pueden ser explotadas por los atacantes para acceder a los sistemas y robar datos. Es esencial llevar a cabo un análisis de vulnerabilidades regular para detectar y corregir estas debilidades.

La privacidad es un riesgo importante en la web, los datos personales pueden ser recolectados, almacenados y compartidos sin el conocimiento o el consentimiento del usuario. Los usuarios deben ser conscientes de las políticas de privacidad de las aplicaciones y sitios web que utilizan y tomar medidas para proteger sus datos personales.

Hoy en día, la seguridad de los datos en la web es un problema crítico en la era digital actual. Los riesgos incluyen el robo de datos, la interrupción de servicios, la vulnerabilidad de los sistemas y la privacidad. Es esencial que las empresas y los individuos tomen medidas para proteger sus datos y minimizar.

Desarrollo

Los riesgos de seguridad de los datos en la web son variados y pueden ser causados por una variedad de factores. Uno de los principales riesgos es la falta de privacidad y seguridad en las transacciones en línea. Los datos personales, como los números de tarjeta de crédito, pueden ser interceptados por ciberdelincuentes y utilizados para cometer fraude. Los sitios web que no utilizan protocolos de seguridad, como SSL y TSL, son especialmente vulnerables a este tipo de ataques.

Otro riesgo importante es el phishing, donde los delincuentes utilizan correos electrónicos y sitios web falsos para obtener información confidencial de los usuarios. Los ciberdelincuentes también pueden utilizar malware y software malicioso para robar información y controlar dispositivos.

La seguridad de los datos también puede ser comprometida por errores internos, como una mala configuración de seguridad o una falta de capacitación en seguridad para el personal. Los ataques de denegación de servicio (DoS) y distribuidos (DDoS) estos pueden causar interrupciones en el funcionamiento de un sitio web y exponer información confidencial.

Es importante que las empresas y los usuarios tomen medidas para proteger sus datos en línea. Esto incluye el uso de contraseñas seguras y la verificación de la autenticidad

de los sitios web antes de ingresar información confidencial. Además, las empresas deben implementar medidas de seguridad adicionales, como la encriptación de datos y la implementación de políticas de seguridad sólidas. También se deben tener presente ciertos términos que ayudarían a identificar ciertas amenazas y como poder combatirlas entre las amenazas más comunes se encuentran las siguientes:

Ingeniería de la seguridad de datos. - Pensar en seguridad de datos y construir defensas desde el primer momento es de vital importancia. Los ingenieros de seguridad tienen como objetivo proteger la red de las amenazas desde su inicio hasta que son confiables y seguras. Los ingenieros de seguridad diseñan sistemas que protegen las cosas correctas de la manera correcta. Si el objetivo de un ingeniero de software es asegurar que las cosas sucedan, el objetivo del ingeniero de seguridad es asegurar que las cosas (malas) no sucedan diseñando, implementando y probando sistemas completos y seguros.

Encriptación. - Si la ingeniería de seguridad de datos protege la red y otros activos físicos como servidores, computadoras y bases de datos, la encriptación protege los datos y archivos reales almacenados en ellos o que viajan entre ellos a través de Internet. Las estrategias de encriptación son cruciales para cualquier empresa que utilice la nube y son una excelente manera de proteger los discos duros, los datos y los archivos que se encuentran en tránsito a través de correo electrónico, en navegadores o en camino hacia la nube.

En el caso de que los datos sean interceptados, la encriptación dificulta que los hackers hagan algo con ellos. Esto se debe a que los datos encriptados son ilegibles para usuarios no autorizados sin la clave de encriptación. La encriptación no se debe dejar para el final, y debe ser cuidadosamente integrada en la red y el flujo de trabajo existente para que sea más exitosa.

Hacker. - es una persona que utiliza habilidades técnicas para superar las medidas de seguridad de un sistema informático o red. Los hackers pueden ser utilizados con fines maliciosos o legítimos, como detectar vulnerabilidades en un sistema para mejorar su seguridad. Los hackers maliciosos, también conocidos como crackers, utilizan sus habilidades para acceder a información confidencial, robar datos y causar daños en los sistemas. Los hackers éticos, también conocidos como white hats, utilizan sus habilidades para detectar vulnerabilidades y ayudar a mejorar la seguridad de los sistemas. (Banco Pichincha , 2022).

Análisis de vulnerabilidades. - es un proceso mediante el cual se identifican, evalúan y priorizan las debilidades o amenazas potenciales de un sistema o red. El objetivo es detectar las vulnerabilidades antes de que puedan ser explotadas por atacantes maliciosos. El análisis de vulnerabilidades puede ser llevado a cabo de manera manual o automatizada, y puede incluir técnicas como el escaneo de puertos, el análisis de código fuente y la evaluación de configuraciones. Es un paso importante en la gestión de la seguridad de la información y puede ayudar a proteger los sistemas y datos contra posibles ataques (Say Net, 2023).

Pruebas de intrusión - implican la ejecución de procesos manuales o automatizados que interrumpen los servidores, las aplicaciones, las redes e incluso los dispositivos de los usuarios finales para ver si la intrusión es posible y dónde se produjo esa ruptura. A partir de esto, pueden generar un informe para los auditores como prueba de cumplimiento (PowerData, 2022).

De la misma manera como existen múltiples amenazas, también se tiene que tener claro el ¿Por qué es importante la seguridad en la web? Y no solo eso, sino que así mismo se debe brindar una seguridad y ambos puntos se explican a continuación:

¿Por qué es importante la seguridad web?

En el mundo, cada día existen miles de páginas web, servidores web y dispositivos móviles que son el blanco de los llamados piratas informáticos. Sitios web que dejan de estar disponibles, información modificada o dañada, filtraciones de direcciones de correo electrónico, tarjetas de crédito, contraseñas, y un sinfín de problemas que se tienen que afrontar si no se protegen correctamente la web. Este el propósito principal de la seguridad web: prevenir ataques y proteger sitios web del acceso, uso, modificación, destrucción o interrupción no autorizados.

¿Cómo hacer un sitio web seguro?

Para evitar riesgos innecesarios y proteger tu sitio web, se pueden aplicar acciones de seguridad como:

1. Instalar un certificado de seguridad: los certificados de seguridad son la medida básica y primordial para proteger la información y los datos en tránsito que una página web recolecta tales como: emails, números de tarjetas bancarias y hasta las contraseñas. Todos estos son aquellos que van desde el navegador de los usuarios hacia tu servidor.
2. Proteger tu página con un Firewall para Aplicaciones Web: un Firewall o cortafuegos, es un sistema de hardware o software que actúa como portero de discoteca. Es una especie de guardián que deja pasar los datos que fluyen entre dos redes. De esta forma, se impide que ciertos sistemas no autorizados puedan conectarse a tu sitio web.
3. Usar un escáner de seguridad de páginas web: como su nombre indica, sirve para escanear y revisar el sitio web cada cierto tiempo con el fin de detectar malware o actividades sospechosas. También nos informa de si la página web está en listas negras de motores de búsqueda (blacklists).
4. Actualizar el software frecuentemente: imprescindible para modernizar el software e implementar mejoras de seguridad.
5. Poner contraseñas fuertes: numerosos accesos a páginas webs o servidores tienen contraseñas débiles, teniendo así mayor exposición a ser hackeadas. Para una buena contraseña, esta debe tener más de 8 caracteres, combinar letras, números y símbolos, o no utilizar términos demasiado claros como el siguiente: “contraseña123”, lo mejor es que sean aleatorias pero fácil de recordar, ya que los programas que descifran contraseñas están diseñados para encontrar palabras de diccionarios o de Internet.
6. Limitar el acceso de usuario y permisos en el sitio web: lo ideal es otorgar a las personas los permisos justos y necesarios para poder trabajar en la web y realizar sus actividades. Estas deben ser por tiempo limitado y con el mínimo de derechos necesarios.
7. Cambiar ajustes preestablecidos del CMS o sistemas de gestión de contenido son muy intuitivos a la hora de utilizarlos, pero en ocasiones pueden ser vulnerables si mantienes la configuración preestablecida de tu cuenta. Como hemos visto, los bots suelen atacar a los sitios desactualizados o fáciles de descifrar.
8. Realizar copias de seguridad de la página web con frecuencia: una copia de seguridad ayuda a recuperar lo que existía antes del hackeo y poder recuperar información (nAFTiC, 2022).

Metodología

La metodología que se utilizó en el presente trabajo de investigación permitió analizar diferentes fuentes bibliográficas las que establecieron las bases sólidas de este estudio, a través de los métodos de investigación científica tales como:

El método de análisis - síntesis se basó en la búsqueda de información acerca de los riesgos de los datos en la web y luego la seguridad de datos en la web, así como sus respectivas ventajas, desventajas, características y funcionalidades, luego que se tuvo toda la información y se estudió todo el tema a profundidad se comenzó unir todo para hacer de la investigación una sola.

El método bibliográfico - documental permitió la recopilación y análisis de fuentes escritas, como libros, artículos, tesis, entre otros. La buscar y recopilar fuentes relevantes sobre los riesgos de seguridad de datos en la web, la lectura y análisis de las fuentes, la sistematización, comparación e interpretación ayudaron a obtener una información precisa sobre los riesgos a los que se enfrentas los datos de cada usuario dentro de la web.

El método histórico - lógico se utilizó en el estudio de la evolución de un fenómeno o problema a través del tiempo entre ellos se estudió el origen y la evolución de cómo era la seguridad anteriormente y como se podía aplicar seguridad a los datos o información que colguemos en la web, también como se utilizaron estos protocolos a lo largo del tiempo inclusive ayudo a investigar las tendencias en el uso de los protocolos, así como su propia evolución a lo largo del tiempo.

Resultados

Según un estudio realizado por el think tank internacional DQ Institute sobre el estado de la seguridad infantil en línea en 30 países, entre el 2017 y el 2019 el 60% de los niños entre 8 a 12 años que tuvieron acceso a internet fueron expuestos a riesgos cibernéticos, el 45% se ese ataque fue ciberacoso o ciberbullying, el 39% puso en riesgo su reputación personal, un 29% estuvo expuesto a contenido sexual o contenido violento, un 28% recibió ciberamenzas, el 17% de esa población tuvo contacto con números desconocidos un 13% estuvo a punto de padecer trastornos por el exceso de videojuegos y un 7% estuvo por padecer trastorno por el uso excesivo de redes sociales.

Por otro lado, los ciberataques son tan comunes que una empresa de ciberseguridad revelo que ha aumento el robo de contraseñas en México, Brasil y chile en este 2022. En el mismo año las pequeñas y medianas empresas o conocidas como PyMes se han enfrentado amenazas que representan un peligro en su crecimiento, estos ataques tal y como se puede apreciar en la gráfica N°2 son los Troyanos, Los ataque por internet y ataque por Escritorio Remoto, estas amenazas permiten que los ciberdelincuentes puedan tener acceso a redes de la corporación y de esta manera pueden comprometer al negocio.

Figura 1. Los niños y la seguridad en línea. (Naranjo, 2021)

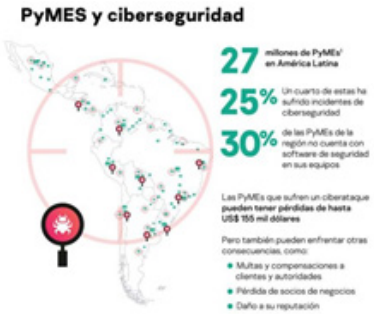

Figura 2. PyMES y Ciberseguridad. (Kaspersky, 2022)

En base a los resultados que se han podido apreciar acorde a diferentes años y a diferentes ataques, sin lugar a duda los riesgos de seguridad son cada vez más peligrosos por tal razón, es importante tomar medidas para proteger los datos personales y financieros al interactuar en línea, como utilizar contraseñas seguras, mantener el software actualizado y ser cuidadoso al proporcionar información personal a sitios web no confiables.

Conclusiones

La seguridad de los datos en la web es un tema crucial en la actualidad, cada vez son más las personas y las empresas que utilizan internet para almacenar y transmitir información valiosa. Los riesgos de seguridad en la web incluyen ataques cibernéticos, robo de información, suplantación de identidad y espionaje. Es importante tomar medidas para proteger los datos, tales como utilizar contraseñas seguras, mantener los sistemas actualizados y utilizar software de seguridad. Además, es fundamental concienciar a los usuarios sobre las precauciones que deben tomar para evitar caer en trampas en línea. En definitiva, aunque la web ofrece muchas ventajas, también conlleva riesgos de seguridad que deben ser abordados de manera proactiva para garantizar la protección de los datos.

Referencias

Banco Pichincha. (29 de Agosto de 2022). Obtenido de https://www.pichincha.com/portal/blog/post/que-es-un-hacker

Kaspersky. (17 de Diciembre de 2022). Prensario TI Latin America. Recuperado el 17 de Diciembre de 2022, de https://prensariotila.com/kaspersky-las-pymes-de-america-latina-enfrentan-un-creciente-numero-de-ciberataques/

nAFTiC. (2022). Obtenido de nAFTiC: https://naftic.com/la-importancia-de-la-seguridad-web/

Naranjo, S. C. (08 de Febrero de 2021). statista. Recuperado el 17 de Diciembre de 2022, de https://es.statista.com/grafico/24110/los-ninos-y-la-seguridad-en-linea/

PowerData. (2022). Obtenido de PowerData: https://www.powerdata.es/seguridad-de-datos

Say Net. (26 de Enero de 2023). Obtenido de https://saynet.com.mx/que-es-un-analisis-de-vulnerabilidades/

Cómo citar: Cruz Lucas, G. I., Delgado Tejena, L. E., Ponce Solorzano, B. R., & Marcillo Merino, M. J. (2022). Riesgos de seguridad de los datos en la web. Journal TechInnovation, 1(2), 43–49. https://doi.org/10.47230/Journal.TechInnovation.v1.n2.2022.43-49