Polo del Conocimiento

Pol. Con. (Edición núm. 70) Vol. 7, No 7
Julio 2022, pp. 2615-2626
ISSN: 2550 - 682X
DOI: 10.23857/pc.v7i7

Implementación y evaluación de un sistema seguridad anti phising para la protección de la información utilizando un firewall en procedimientos académicos en línea para el Instituto Superior Tecnológico Riobamba

Implementation and evaluation of an anti-phishing security system for the protection of information using a firewall in online academic procedures for the Instituto Superior Tecnológico Riobamba

Implementação e avaliação de um sistema de segurança anti-phishing para proteção de informações utilizando firewall em procedimentos acadêmicos online para o Instituto Superior Tecnológico Riobamba

Marco Vinicio Estrada Velasco [I]
mestrada@institutos.gob.ec
https://orcid.org/0000-0001-5222-2287

Cristian Geovanny Merino Sánchez [II]
c_merino@espoch.edu.ec
https://orcid.org/0000-0003-3645-5165

María Fernanda Girón Bonilla [III]
fernanda.giron@epemapar.gob.ec
https://orcid.org/0000-0002-4088-909X

Greta Nataly Chancusi Camalle [IV]
greta.chancusi@espoch.edu.ec
https://orcid.org/0000-0002-7191-9079

Correspondencia: mestrada@institutos.gob.ec

Ciencias de la Computación
Artículo de Investigación

*** Recibido:** 23 de mayo de 2022 ***Aceptado:** 12 de junio de 2022 *** Publicado:** 31 de julio de 2022

I. Coordinador de la Carrera Tecnología Superior en Desarrollo de Software, Docente, Ecuador.
II. Docente de la Escuela Superior Politécnica de Chimborazo, Ecuador.
III. Jefe de Catastro y Medición de la Unidad de Dirección Comercial Empresa Municipal de Agua Potable y Alcantarillado del Cantón Riobamba, Ecuador.
IV. Ingeniera en Sistemas Informáticos, Ecuador.

Resumen

El objetivo fue implementar y evaluar un sistema de seguridad anti phishing para dar una protección de la información del instituto Superior Tecnológico Riobamba implementando las normas ISO 27001, se llevaron a cabo pruebas en dicha plataforma informática y así detectar vulnerabilidades, utilizando el sistema de seguridad basado en la norma ISO 27001 para su prevención. La detección de vulnerabilidades se basó en 5 de los riesgos de seguridad encontrados mediante el Open Source, utilizando como herramientas de escaneo y explotación a Nessus, Vega, BurpSuite y Zenmap, Kali Linux (metasploit), lo que facilitó identificar fallas de seguridad como: inyección de código malicioso, pérdida de autenticación, exposición de datos sensibles, pérdida de control de acceso, control de seguridad incorrecta, uso de componentes con vulnerabilidades conocidas y registro y monitoreo insuficientes; además que la plataforma informática presentó todos las 7 vulnerabilidades establecidas, por lo tanto, se concluyó que la plataforma un 100% de verse afectada Una de las acciones que ayudan a mitigar estos problemas, es establecer una seguridad perimetral lógica afín de poner una barrera o frontera que sea imposible de penetrar entre una red interna y el internet, para restringir y tener un control sobre los datos que entran y salen de la organización, siendo la principal ventaja permitir al administrador concentrarse en los puntos de entrada, sin olvidar la seguridad del resto de servidores internos de la red, para protegerlos frente a una posible intrusión. (Díaz, 2013)

La seguridad de la información ha sido un tema de vital importancia para el sector empresarial y como ende de ella la seguridad perimetral. En los últimos años este concepto ha sufrido algunos cambios y ello ha estado condicionado según al incremento de las brechas en las redes, los sistemas operativos, los equipos de uso cotidiano, la evolución de la tecnología, el uso de mecanismos de comunicaciones móviles y el almacenamiento de información en la nube, siendo necesario integrar a este concepto accesos lógicos y físicos. (Bohórquez_Gutiérrez, 2018).

La seguridad lógica hace referencia a la aplicación de mecanismos y barreras para mantener el reguardo y la integridad de la información dentro de un sistema informático, la seguridad es una herramienta valiosa para cualquier negocio, lo cual conlleva a cuestionarse sobre la manera en que se puede formalizar la intención que tiene la misma en las organizaciones. En el contexto actual cuando se habla de seguridad sobre las tecnologías de la información (TI) se definen o establecen desde diversas áreas, tales como la seguridad informática, la seguridad de la información y la Ciberseguridad. (Pírez, 2018)

Palabras Clave: sistema seguridad anti phishing; firewall; procedimientos académicos en línea.

Abstract

The objective was to implement and evaluate an anti-phishing security system to protect the information of the Instituto Superior Tecnológico Riobamba by implementing ISO 27001 standards, tests were carried out on said computer platform and thus detect vulnerabilities, using the security system based on in the ISO 27001 standard for its prevention. The detection of vulnerabilities was based on 5 of the security risks found through Open Source, using Nessus, Vega, BurpSuite and Zenmap, Kali Linux (metasploit) as scanning and exploitation tools, which made it easy to identify security flaws such as: malicious code injection, loss of authentication, exposure of sensitive data, loss of access control, incorrect security control, use of components with known vulnerabilities, and insufficient logging and monitoring; In addition, the computer platform presented all the 7 established vulnerabilities, therefore, it was concluded that the platform was 100% affected. One of the actions that help mitigate these problems is to establish a logical perimeter security in order to put a barrier or border that is impossible to penetrate between an internal network and the Internet, to restrict and have control over the data that enters and leaves the organization, the main advantage being to allow the administrator to concentrate on the entry points, without forgetting the security of the rest of the internal servers of the network, to protect them against a possible intrusion. (Diaz, 2013)

Information security has been a topic of vital importance for the business sector and, as a result, perimeter security. In recent years this concept has undergone some changes and this has been conditioned by the increase in gaps in networks, operating systems, equipment for daily use, the evolution of technology, the use of mobile communication mechanisms and the storage of information in the cloud, being necessary to integrate logical and physical access to this concept. (Bohórquez_Gutiérrez, 2018).

Logical security refers to the application of mechanisms and barriers to maintain the protection and integrity of information within a computer system, security is a valuable tool for any business, which leads to questioning the way in which it can be formalize the intention that it has in organizations. In the current context, when we talk about information technology (IT) security, they are defined or established from various areas, such as computer security, information security and cybersecurity. (Pírez, 2018)

Keywords: anti phishing security system; firewall; online academic procedures.

Resumo

O objetivo foi implementar e avaliar um sistema de segurança anti-phishing para proteger a informação do Instituto Superior Tecnológico Riobamba através da implementação das normas ISO 27001, foram realizados testes na referida plataforma informática e assim detectar vulnerabilidades, utilizando o sistema de segurança baseado na Norma ISO 27001 para sua prevenção. A detecção de vulnerabilidades foi baseada em 5 dos riscos de segurança encontrados através do Open Source, utilizando Nessus, Vega, BurpSuite e Zenmap, Kali Linux (metasploit) como ferramentas de varredura e exploração, o que facilitou a identificação de falhas de segurança como: código malicioso injeção, perda de autenticação, exposição de dados confidenciais, perda de controle de acesso, controle de segurança incorreto, uso de componentes com vulnerabilidades conhecidas e log e monitoramento insuficientes; Além disso, a plataforma computacional apresentou todas as 7 vulnerabilidades estabelecidas, portanto, concluiu-se que a plataforma foi 100% afetada. Uma das ações que ajudam a mitigar esses problemas é estabelecer um perímetro lógico de segurança para colocar uma barreira que é impossível penetrar entre uma rede interna e a Internet, restringir e ter controle sobre os dados que entram e saem da organização, sendo a principal vantagem permitir que o administrador se concentre nos pontos de entrada, sem esquecer a segurança do resto dos servidores internos da rede, para protegê-los contra uma possível intrusão. (Díaz, 2013)

A segurança da informação tem sido um tema de vital importância para o setor empresarial e, consequentemente, a segurança perimetral. Nos últimos anos este conceito sofreu algumas alterações e isso tem sido condicionado pelo aumento de lacunas nas redes, sistemas operativos, equipamentos de uso diário, a evolução da tecnologia, a utilização de mecanismos de comunicação móvel e o armazenamento de informação na nuvem, sendo necessário integrar o acesso lógico e físico a este conceito. (Bohórquez_Gutiérrez, 2018).

A segurança lógica refere-se à aplicação de mecanismos e barreiras para manter a proteção e integridade da informação dentro de um sistema informático, a segurança é uma ferramenta valiosa para qualquer negócio, o que leva a questionar a forma como se pode formalizar a intenção que tem em organizações. No contexto atual, quando falamos em segurança de tecnologia da informação (TI), elas são definidas ou estabelecidas a partir de diversas áreas,

como segurança de computadores, segurança da informação e segurança cibernética. (Pirez, 2018)

Palavras-chave: sistema de segurança anti-phishing; firewall; procedimentos acadêmicos online.

Introducción

La tecnología ha ido evolucionando con el pasar de los tiempos y las entidades que manejan este recurso han facilitado el uso de datos para varias operaciones en cuanto a los servicios de internet. Las empresas envían la información a través de los servicios web, que al encontrarse en una libre disposición tienen un fácil acceso por personas externas a la entidad.

Las plataformas informáticas son herramientas conformadas por hardware y software que dan a las empresas servicios del sistema informático tradicional como: accesibilidad, disponibilidad e integridad mediante diferentes conexiones web.

La evolución de varias plataformas como de aplicaciones web y móviles han hecho que también los ciberataques sean capaces de penetrar varias seguridades de diferentes entidades públicas y privadas que están colgadas en la web. Para esto se debe brindar la seguridad, otorgando la protección de la información; evitando de esta manera problemas fraudulentos ocasionados por terceras personas al no conocer sobre el tema.

El Instituto Superior Tecnológico Riobamba al ser una institución de educación pública maneja información propia y de otros establecimientos, es por esto que, al no resguardar su información de manera adecuada, estos recursos han presenciado el intento de ser vulnerados debido al libre acceso por estudiantes, docentes y público en general.

Con este trabajo de investigación se propone diseñar e implementar un modelo de seguridad evitando la fuga de información y el acceso no autorizado de personas externas a la institución ya que la importancia de los datos en la plataforma digital académica son muy delicados y propensos a ser modificados.

Fundamentos Teóricos

Los firewalls al configurarse adecuadamente funcionan como un escudo para nuestro ordenador, analizando entrada y salida de datos. Hay que considerar que el termino open source alcanza un acceso código fuente.

Los programas open source colaboran a usuarios que configuren las funciones de su red. Una de las características que facilitan un escudo de protección son: firewall, antivirus, servicios antispam y filtros web. (Fernández, 2020).

El phishing se define como el delito de manipular a un usuario para que comparta su información personal por medio de chantajes recibiendo mensajes en su correo electrónico. El mensaje hace que la víctima realice un clic en el sitio web y así el hacker pueda descargar la información. (Malwarebytes, 2021)

El Antiphishing son aquellos programas utilizados para detectar aquel contenido que se infiltra en los sitios web como phishing. Lo importante de este software es bloquear datos y contenido para que no tenga libre acceso. (Avast Software, 2020)

Materiales y Métodos

Los métodos para la presente investigación se han decidido los siguientes:

1. Obtener una fuente bibliográfica para tener considerable material teórico (Registros, Internet, bibliografía científica, investigaciones realizadas en el país y estadísticas oficiales).
2. Experimentación: Se realizará distintos casos para comprobar que la implementación de un firewall es una gran solución para controlar el tráfico que soporta el sistema académico del Instituto Superior Tecnológico Riobamba.
3. Análisis de la información, exacta y real.
4. Observación de campo: se realizará mediciones para comprobar la efectividad de la investigación.

Materiales y Métodos

La presente investigación utiliza el método científico permitiendo hacer una de etapas que hay que recorrer para obtener un conocimiento válido desde el punto de vista científico, utilizando para esto instrumentos que resulten fiables, el cual consta de las siguientes etapas:

- Planteamiento del problema
- Formulación de las hipótesis
- Análisis e interpretación de resultados

- Comprobación de la hipótesis
- Difusión de resultados

Método deductivo debido que, al estudiar el riesgo generado por las no conformidades encontradas en la seguridad de la información, se trata de encontrar un marco de trabajo adecuado de seguridad que contenga las mejores características de las normas ISO 27001.

Este estudio se basa en fuentes de revisión de fuentes de información bibliográficas primarias como Pruebas y Observación de resultados y secundarias como:

- Revistas indexadas y no indexadas publicadas de prestigio
- Revistas electrónicas
- Páginas de internet que brinden información confiable

Población

Se define como el grupo de individuos puestos a prueba a ser evaluados, en la investigación. Se designó a la población de estudio a el Instituto Superior Tecnológico Riobamba que cuenta con 7 carreras un total de 2000 estudiantes, 80 personas entre docentes y personal administrativo. considerando el OWASP TOP 10-2017 verificando la exposición que tiene la plataforma ante 7 de 10 riesgos críticos que vulneran la seguridad de la plataforma mencionada.

Selección de la muestra

Para seleccionar una porción representativa de la población, que permita generalizar los resultados de la investigación, y por motivos de factibilidad relacionados con la disponibilidad de recursos se establece una muestra del tipo probabilístico tomada de los 125 funcionarios. Se decidió para esta investigación la plataforma del Instituto Tecnológico Superior Riobamba. Se determino como muestra 7 de 10 vulnerabilidades en el OWASPT Top 10-2017, obteniendo que 7 vulnerabilidades tienen relación con el presente estudio.

Chi Cuadrado

Mostramos la siguiente tabla las vulnerabilidades que vamos a analizar

$$X^2 = \frac{(7-4.5)^2}{4.5} + \frac{(0-2.5)^2}{2.5} + \frac{(2-4.5)^2}{4.5} + \frac{(5-4.5)^2}{2.5}$$

$$x^2 = \sum \frac{(FO - FE)^2}{FE}$$

$$x^2 = 5.377$$

$$x^2 \text{calculado} \leq x^2 \text{crítico}$$

$$x^2 \text{crítico} = 3.8415$$

Con los resultados obtenidos y como se puede observar en la gráfica se propone rechazar la Hipótesis nula (H0) aceptando la hipótesis alternativa (Hi) teniendo un nivel de confianza del 95% y 5% de nivel de significancia.

Resultados y Discusión

En la propuesta planteada referente a la seguridad perimetral de una red empresarial tipo, todo el tráfico de internet pasa por el equipo firewall para ser inspeccionada, de esa manera el diseño se vuelve efectivo.

Además en el equipo firewall se habilitan controles con la finalidad de proteger la red empresarial, en la cual se autoriza o se niega el paso del tráfico, además el firewall permite al administrador de la red monitorear y tener su control, prohibiendo la entrada o salida de información que puedan vulnerar los servicios de red, el equipo utilizado también permite realizar conexiones seguras por medio de una red privada virtual (VPN), se puede escoger el tipo de cifrado y autenticación, en la cual se necesite un nivel de seguridad más alto dependiendo del tipo de información que se esté transmitiendo.

Se está utilizando VPN sobre IPsec que es configuración de una VPN entre dos redes distintas a través de internet, IPsec es un protocolo que está sobre la capa de internet (IP), permitiendo a dos equipos conectarse de manera segura

En el capítulo III se analizan algunos ciberataques que sufren las pequeñas y medianas empresas, más de la mitad están relacionadas con la estafa como el phishing y el ransomware. El phishing consiste en suplantar la identidad de una empresa o persona para poder acceder a información

privada de sus víctimas. En el ransomware, los crackers secuestran los sistemas informáticos de empresas o personas, cifrando el contenido y pidiendo un rescate para descifrar la información. Es una negligencia por parte del responsable de seguridad de una Pyme no conocer las amenazas a las que está expuesta la empresa y las consecuencias que puede tener como una afectación en el normal funcionamiento empresarial hasta su cierre definitivo.

Por lo tanto, la concientización a los directivos de la empresa es fundamental, comprender los riesgos que existen, ya que ello permitiría tomar las medidas adecuadas tanto para el personal como a los equipos informáticos, con la finalidad de mejorar la seguridad y minimizar las consecuencias de un potencial ataque.

Conclusiones

- Una vez implementando y realizadas las evaluaciones se ha comprobado las amenazas, vulnerabilidades y posibles debilidades que en los ciberataques pueden ser mal utilizados. La norma ISO: 27001 de la seguridad de la información y la guía OWASP Top10de vulnerabilidades más críticas da a conocer 7 vulnerabilidades del sistema académico del Instituto Superior Tecnológico Riobamba que están conectados directamente a la red pública.
- Los tres escenarios de prueba dos de posibles ataques dentro de la red y uno con la implementación del sistema de seguridad firewall ayuda a comprobar si se cumplen los requerimientos para lo cual fue elaborado, se logró mejorar el nivel de seguridad del Instituto Superior Tecnológico Riobamba reduciendo de 7 vulnerabilidades a 2.
- Con el diseño del sistema de seguridad anti-phishing se convierte en una fortaleza contra los ataques cibernéticos donde el firewall se encarga de filtrar el tráfico de red entrante y saliente por medio de una serie de reglas la cuales permitían su paso o rechazaban paquetes
- Con la implementación de un Firewall existe una mejora del 95% en relación al sistema anterior considerando que ningún sistema es cien por ciento seguro. El Firewall logra disminuir los riesgos que se pueden generar, esto debido a que el cortafuegos bloquea o permite el tráfico que se genera al nivel de capa 3, es decir las vulnerabilidades que se presentan al nivel de aplicación de debería contrastar con el uso muy posiblemente de IDS/IPS o PROXY.

Se ha realizado la implementación de un firewall (RIO_FIREWALL_01) y una red local denominada zona desmilitarizada (DMZ) para disminuir los riesgos de ataques informáticos al servidor web del ISTR, en donde el firewall se encargó de filtrar el tráfico de red entrante y saliente por medio de una serie de reglas la cuales permitían su paso o rechazaban paquetes. Por otro lado, se implementó una LAN DMZ dentro de la red interna de la organización, en donde se ubicó exclusivamente todos los recursos que tienen acceso a internet como es el caso de nuestro servidor web, permitiendo las conexiones procedentes tanto de internet como de la red local de la empresa, y negando las conexiones que van desde la DMZ a la red local, logrando con esto proteger las conexiones de red y actuando como un filtro entre el servidor web con conexión a internet y la red de ordenadores particulares.

Referencias

1. Analuisa, Henry. 2009. Implementación de un Firewall en los equipos Informaticos del Laboratorio de Instrumentación virtual ITSA. [En línea] 2009. [Citado el: 15 de Diciembre de 2021.] http://repositorio.espe.edu.ec/bitstream/21000/7863/1/T-ESPE-ITSA-000106.pdf.
2. AVAST. 2022. [En línea] 2022. [Citado el: 10 de Diciembre de 2021.] https://www.avast.com/es-es/c-phishing.
3. AVAST SOFTWARE. 2022. [En línea] 2022. [Citado el: 10 de Diciembre de 2022.] https://www.avast.com/es-ww/avast-online-security#pc.
4. Ballesteros, Andrea. 2018. Empresarial y Laboral. [En línea] 2018. [Citado el: 1 de Diciembre de 2021.] https://revistaempresarial.com/tecnologia/seguridad-informatica/vulnerabilidades-ciberneticas-y-su-impacto-organizacional/.
5. Bonilla, Jaime. 2016. Pontificia Universidad Católica del Ecuador. Diseño e Implementación de un Firewall L2 utilizando redes definidas por Software(SDN). [En línea] 2016. http://repositorio.puce.edu.ec/bitstream/handle/22000/13153/INFORME%20CASO%20DE%20ESTUDIO%20-%20ADRIAN%20BONILLA.pdf?sequence=1&isAllowed=y.
6. Corozo, Mayra. 2016. [En línea] Marzo de 2016. [Citado el: 15 de Diciembre de 2020.] http://dspace.espoch.edu.ec/bitstream/123456789/5468/1/98T00106.pdf.

7. CTMA consultores. 2021. Objetivo de la norma ISO. [En línea] 13 de Octubre de 2021. [Citado el: 10 de Agosto de 2021.] https://ctmaconsultores.com/objetivo-de-la-norma-iso-27001/.
8. Departamento de Tecnología Organización Inca. 2018. Políticas de Seguridad Informática (PSI). [En línea] 2018. [Citado el: 10 de Diciembre de 2021.] https://www.centroinca.com/centro_inca/documentos/politica_seguridad_informatica.pdf.
9. Fernández, Camilo. 2010. Introducción a OWASP. [En línea] The OWASP Foundation, Octubre de 2010. [Citado el: 10 de Diciembre de 2021.] https://owasp.org/www-pdf-archive/Introduccion_a_la_OWASP.pdf.
10. Ibáñez y Almenara. 2016. Técnicas para combatir el phishing. [En línea] 2016. [Citado el: 10 de Diciembre de 2021.] https://ialmenara.com/danos-causados-por-el-phishing-y-como-combatirlo/.
11. Jiménez, Edgar. 2014. Instituto Politécnica Nacional. [En línea] Febrero de 2014. [Citado el: 10 de Diciembre de 2021.] https://tesis.ipn.mx/jspui/bitstream/123456789/15606/1/I.C.E.%2044-14.pdf.
12. Malwarebytes. 2021. Phisihing. [En línea] 2021. [Citado el: 12 de Diciembre de 2021.] https://es.malwarebytes.com/phishing/.
13. Medina, Juan. 2016. [En línea] 2016. [Citado el: 12 de Diciembre de 2021.] https://repository.udistrital.edu.co/handle/11349/7440.
14. Muñoz, Facundo. 2021. We live security by eset. [En línea] 14 de Mayo de 2021. [Citado el: 20 de Diciembre de 2021.] https://www.welivesecurity.com/la-es/2021/05/14/que-es-virus-troyano-informatica/.
15. OCU. 2022. Phising. [En línea] 20 de Enero de 2022. [Citado el: 10 de Diciembre de 2022.] https://www.ocu.org/tecnologia/internet-telefonia/consejos/evitar-ataque-phishing.
16. OWASP. 2017. OWASP Top 10-2017. [En línea] 2017. [Citado el: 10 de Diciembre de 2021.] https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf.
17. Pilamunga, Norma. 2019. Dspace. [En línea] Enero de 2019. [Citado el: 1 de Diciembre de 2021.] http://dspace.espoch.edu.ec/bitstream/123456789/9694/1/20T01145.pdf.
18. Pinango, Álvaro. 2021. Dspace- ESPOCH. [En línea] Enero de 2021. [Citado el: 10 de Octubre de 2021.] http://dspace.espoch.edu.ec/handle/123456789/14516.

19. RAE. 2020. Real Academia de la Lengua. [En línea] 2020. [Citado el: 1 de Diciembre de 2021.] https://dle.rae.es/amenaza.
20. Torres, Gonzalo. 2021. AVG. Virus Informático. [En línea] 6 de Junio de 2021. [Citado el: 12 de Diciembre de 2021.] https://www.avg.com/es/signal/what-is-a-computer-virus.
21. UNIR. 2020. [En línea] 14 de Mayo de 2020. [Citado el: 1 de Diciembre de 2021.] https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/.
22. —. 2020. La Univerdidad en Internet. [En línea] 11 de Febrero de 2020. [Citado el: 1 de Diciembre de 2021.] https://www.unir.net/ingenieria/revista/hacking-etico/.
23. Valente, Roberto. 2018. DSPACE. [En línea] Octubre de 2018. [Citado el: 15 de Diciembre de 2021.] http://dspace.espoch.edu.ec/handle/123456789/9056.