REVISTA INCAING
ISSN 2448 9131

(Marzo-Abril 2021), pp. 35-44

Servicio de Pentesting, basados en la propuesta de auditoria interna con la norma ISO 27001.

Mtra. Angélica González Páramo, Dr. Luis Armando García de la Rosa, Martha Fernanda Araujo Valdés
agonzalez@itesg.edu.mx, lgarcia@itesg.edu.mx, fernanda_mar815@hotmail.com
Tecnológico Nacional de México/Instituto Tecnológico Superior de Guanajuato. México.

Resumen.
El objetivo del proyecto se enfocó en identificar y disminuir vulnerabilidad en la red de datos del Instituto Tecnológico Superior de Guanajuato, bajo la metodología PTES y la norma ISO27001, en esta se evaluaron varias etapas, soportadas con software y herramientas gratuitas; las cuales permitieron pruebas de testeo, para el diagnóstico actual de la seguridad en la red, donde participaron docentes, administrativos y alumnos.

Los campos de estudio fueron los laboratorios de mayor demanda, sala de docentes y área administrativa. Con base en el desarrollo de pruebas de vulnerabilidades, se determinó que la Institución de educación, no tiene un adecuado control sobre políticas de seguridad informática y el cómo aplicar estás, esto fue demostrado bajo la metodología PTES que permitió medir el nivel de impacto y criticidad de las vulnerabilidades encontradas, las cuales serán mitigadas bajo los siguiente controles: Políticas de seguridad de la información, seguridad relativa de los recursos humanos, organización de la seguridad de la información, gestión de activos, control de acceso, seguridad de las comunicaciones y adquisición, desarrollo y mantenimiento de los sistemas de información, permitiendo garantizar los elementos principales de la seguridad informática, disponibilidad, confiabilidad e integridad.

Palabras claves.
Seguridad perimetral, vulnerabilidades, metodología PTES, ISO27001.

Introducción.

El mundo cambia, y en esta etapa de cambios se encuentra la seguridad informática o computacional que está adquiriendo un impacto significativo en todo el mundo, dadas las cambiantes condiciones y las nuevas plataformas tecnológicas que hasta hoy se conocen.

La tendencia de la digitalización conlleva a que más personas usen tecnologías, que más servicios estén conectados a Internet, e incluso que dependan de sistemas de información para su funcionamiento, lo que implica que se incrementen las vulnerabilidades, riesgos y amenazas.[8].

Por lo cual las Instituciones de Educación tampoco están exentas de sufrir algún ataque cibernético, esto basado en la encuesta realizada por ESET en el 2018**,** donde indica que "el 67% de las instituciones que participaron aseguró haber sufrido al menos un incidente de seguridad."

Esto debido a que toda Institución Educativa cuenta con amplios volúmenes de datos personales, médicos, socioeconómicos de alumnos, docente, administrativos y estos últimos también con la exposición de salarios. Lo que puede desencadenar que se genere una divulgación de información, que puede exponer datos sensibles y privados, afectando la integridad social y personal de cada una de las víctimas.

Y desde otra perspectiva del lado tecnológico, perdida de dispositivos digitales (computadora, impresora, tabletas, celulares, etc.), alteración de servicios (Internet), lo que puede provocaría atraso de pagos salariales, envío de información relévate (a través del correo electrónico), accesibilidad al sitio web de la universidad, entre otros. Esto podría llevar al desprestigio de la Institución si la información obtenida del personal es alterada para fines lucrativos o acoso, agrediendo así su vida personal o familiar.

Atendiendo a los peligros que cualquier Institución pública o privada de Educación está expuesta, este trabajo tiene como objetivo la implementación de Hardening en la red Institucional del Tecnológico de Guanajuato esto con el fin de disminuir las vulnerabilidades actuales y prepararse para futuras amenazas.

Y enfatizando en lo anterior se determina realizar el proyecto bajo las características de Hardening pues permite generar un conjunto de actividades con la finalidad de reforzar la seguridad en un componente. Entre las herramientas que se utilizan esta: Kali Linux, Wireshark, nmap, setoolkit y páginas web como haveibeenpwned que permitirá visualizar si existen correos expuestos de docentes, alumnos, y administrativos, otra página será;hackerstorm esta permite visualizar información geográfica de IP, nombres de domino válidos, reputación de sitios web que visitan con mayor frecuencia los alumnos, entre otros.
Las herramientas que se utilizan en este trabajo, al igual que el sistema operativo (Kali Linux) permiten llevar acabo la metodología PTES.

Otra parte importante que visualiza este trabajo, es el uso de seguridad perimetral que perfila el fortalecimiento de la seguridad lógica, a través del uso de pfSense que es una distribución de firewall de red gratuita.

El software pfSense, con la ayuda del sistema de paquetes, puede proporcionar la misma funcionalidad o más de los firewalls comerciales comunes, sin ninguna de las limitaciones artificiales. Ha reemplazado con éxito todos los firewalls comerciales de renombre que pueda imaginar en numerosas instalaciones en todo el mundo, incluidos Check Point, Cisco PIX, Cisco ASA, Juniper, Sonicwall, Netgear, Watchguard, Astaro y más [19]. Todo lo anterior permite disminuir riegos que están presentes y se desconocían por falta de análisis de vulnerabilidad, y preparar infraestructura para mejorar el rendimiento de los equipos que pueden estar expuestos por falta de mantenimiento y segmentación de red.

Objetivo General.
Analizar fallas desconocidas y puntos débiles dentro de la infraestructura de la red de un sector privado o público, así como en su página web, empleando la metodología PTES (estándar de ejecución de pruebas de penetración) y la norma de auditoria de ISO 27001 para determinar posibles escenarios de explotación de vulnerabilidades analizando el

comportamiento y la resistencia de un sistema para la gestión de seguridad en información.

Metodología.

Metodología PTES.

El estándar de ejecución de pruebas de penetración consta de siete secciones principales. Estos cubren todo lo relacionado con una prueba de penetración, desde la comunicación inicial y el razonamiento detrás de un pentest, pasando por las fases de recopilación de inteligencia y modelado de amenazas donde los evaluadores trabajan detrás de escena para obtener una mejor comprensión de la organización probada, a través de la investigación de vulnerabilidades, explotación y post explotación, donde la experiencia técnica en seguridad de los evaluadores juega y se combina con la comprensión comercial del compromiso, y finalmente con la presentación de informes, que captura todo el proceso, de una manera que tiene sentido para el cliente y proporciona valor para ello[20].

Fases de la Metodología PTES.

El Estándar para la Ejecución de Pruebas de Penetración o PTES (Penetration Testing Execution Standard), es un proyecto constituido por diversas organizaciones y empresas. Está compuesto por siete fases [11]

A. Interacciones previas al compromiso.

Se llega a un acuerdo con el cliente de la profundidad de las pruebas a realizar, permisividad de ataques, enfoque del test, presentación de evidencias.

B. Recolección de información.

Se levanta la información publicada en motores de búsqueda que da una idea del objetivo y de las personas que trabajan en ella.

C. Modelado de amenazas.

Se realiza el modelado de amenazas, donde se definen las líneas de negocios existentes y los activos más importantes a fin de definir las pruebas de ataques siguientes.

D. Análisis de vulnerabilidades.

Se realiza el escaneo de puertos y servicios identificando vulnerabilidades existentes; se valida las posibles opciones reales de ataque y se comprueba que pueden darse con un riesgo derivado; así como la brecha que existe entre las seguridades y vulnerabilidades.

E. Explotación.

Se contempla en la forma de evasión de contramedidas existentes desde el acceso físico hasta las redes Wireless, ataques web, entre otros.

F. Post-explotación.

Se centra en la recopilación de evidencias y en cómo valorar el impacto real de la intrusión y hasta donde se puede llegar si el sistema está vulnerable.

G. Reporte.

Se entregan los reportes ejecutivo y técnico, conteniendo las razones por las cuales se hicieron las pruebas, seguido de los posibles riesgos y su valoración, luego el análisis de las vulnerabilidades encontradas y la confirmación de que las mismas han sido podido ser explotadas junto con las contramedidas propuestas y probadas

Resultados.

De acuerdo a la estructura de la metodología PTES, se obtienen los siguientes resultados, que permiten identificar puntos de mejorar y desarrollar habilidades de protección de datos y divulgación de información por canales adecuados.

Interacciones previas al compromiso.

En esta etapa se propuesto la reestructuración de la topología lógica que no estaba segmentada a la que se presenta en la figura 1, esto con el fin de mejorar el esquema lógico de conexión y prepárese para futuras

amenazas, identificando los posibles puntos de contaminación más vulnerables e integrando un firewall y punto de acceso para monitoreo de accesibilidad de páginas web, ya que de acuerdo a los compromisos de este proyecto, es reducir las vulnerabilidades en la red institucional, protegiendo la información que circula en está.

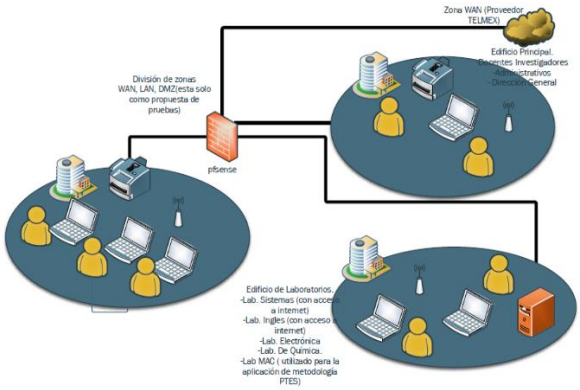

Figura 1. Propuesta de Hardening, para seguridad perimetral.

A. Recolección de información.

Gracias al desglose que la encuesta realizada a estudiantes, docentes, administrativos y alumnos, permito visualizar que sistema operativo es el más utilizado, dentro de la institución universitaria, y sí pueden identificar con claridad una página falsa, entre otros factores un ejemplo de la encuesta se muestra en la figura 3 y 4, en estas solo se muestran algunas preguntas.

Sobre todo los puntos vulnerables que se trabajaron en este proyecto se logró: control sobre el acceso al laboratorio de consulta, denegar que se descarguen programas y denegación de redes sociales, para evitar la saturación de ancho de banda, además de monitorear a que acceden alumnos, docentes y maestros con los nuevos punto de acceso ubiquiti, pues anterior a esto con los puntos de acceso antiguos, no se podía monitorear el uso del servicio de internet.

La figura 2, muestra parte del inicio de la encuesta, esto permitió identificar qué sistema operativo trabajan y el navegador con mayor demanda institucional.

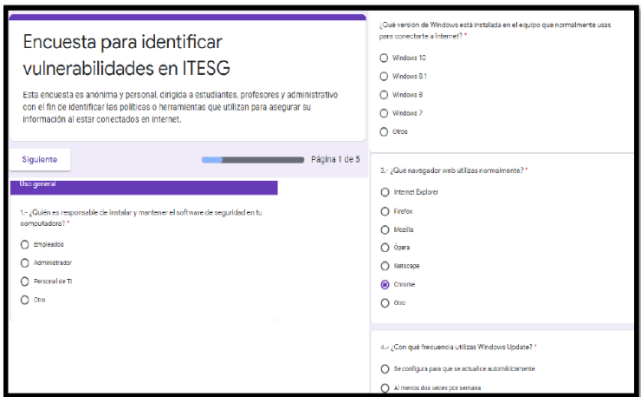

Figura 2. Parte I, detectar puntos débiles al momento de navegar en internet.

En la figura 3. Se muestra otra parte de la encuesta, en la cual permite observa que se buscó identificar el cuidado de cambio de contraseñas, identificación de e-mail y descarga de archivos.

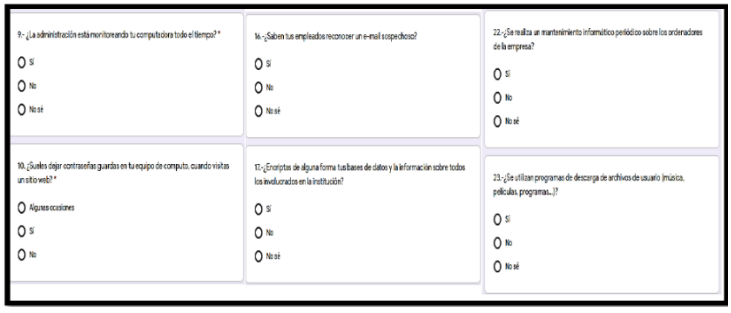

Figura 3. Parte 2, detectar puntos débiles al momento de navegar en internet.

B. Modelado de amenazas.

En la tabla 1, se muestra de manera general los activos relevantes en la institución, esto permite visualizar las pruebas que se realizaran en la siguiente etapa.

Modelado de amenazas (activos)	
Tipo de activo	**Descripción del activo**
Activo de información	Datos de estudiar administrativos y docentes, datc proveedores, Documentos fís manuales. Inventarios de mobil y equipo de cómputo, contratos terceros, entre otros.
Software y licencias	Software de sistema operativo licencia, Software de aplicación licencia, licencias de uso de soft en outsourcing (impresoras).
Hardware	Características del hardware equipos, dispositivos de red (dispositivos móviles, equipos protección eléctrica.
Instalación de red eléctrica	Red e instalaciones eléctricas computadores, sistema protección de aterrizaje eléctrico
Servicios de terceros	Conectividad a internet.
Recurso Humano	Personal área informática.

Tabla 1. Inventario de activos.

C. Análisis de vulnerabilidades.

Se realiza el escaneo de puertos y servicios identificando vulnerabilidades existentes; se valida las posibles opciones reales de ataque y se comprueba los riesgos derivados; así como la brecha que existe entre la seguridad y la vulnerabilidad.

La tabla 2 muestra las amenazas usuales que se identificaron inicialmente, estas fueron comprobadas en la etapa de explotación.

Lugar de análisis	Vulnerabilidad	Amenaza	Riesgos
Hardware			
Edificio vertical (Site principal)	Falta de equipos UPS's para contingencias	Cortes de energía o sobrecargas en los equipos.	Pérdida d información, daños en lc equipos.
Software			
Laboratorio de Consulta. (edificio vertical) Laboratorio de inglés. (CADI)	Software no actualizado (Windows 7)	Virus informáticos, malware, utilización de exploit.	Acceso n autorizado en lc equipos d usuarios par modificación, eliminación robo d información.
Seguridad lógica			
Edificio principal Edificio vertical Edificio de laboratorios	Deficiente control de acceso a los sistemas	Suplantación de identidad	Robo de datos alteración, destrucción d estos. Suplantación d identidad d usuarios. Robo de clave de usuarios.
Redes de comunicaciones			
Edificio principal Edificio vertical Edificio de laboratorios	Navegación inadecuada en internet	Uso de correo institucional.	Sitios vulnerables, acceso a sitio web maliciosos.
Recurso Humano			
Area de docencia. Laboratorio de Consulta. (edificio vertical) Laboratorio de inglés (CADI)	Falta de políticas del uso adecuado de los recursos en red y servicio de Internet.	Ataques no intencionados, ingeniería social, phishing.	Borrado, eliminación d archivos, destrucción d S.O, robo d información personal.

Tabla 2. Análisis de vulnerabilidades.

D. Explotación.

Una vez que se identificaron las posibles vulnerabilidades es momento de desarrollar los ataques, para comprobar el nivel de riesgo de estas amenazas.

Análisis de identificación de riesgo en el dominio Institucional, a través del sitio web y correo.

En la figura 4, se visualiza como el domino no tiene hasta el momento anomalías que se hayan reportado, como uso de phishing, o que se haya comprometido. Esto es importante saberlo, debido a que el Instituto tiene el contrato de hosting con un tercero y no lo administra la universidad.

Figura 4. Búsqueda de anomalía en la página oficial de la universidad

Análisis de identificación de riesgo en el correo institucional.

En esta etapa, se comprobó solo con los 19 maestros de tiempo completo, que son el total que hasta el momento trabajan en la Institución, en esta etapa, los profesores de tiempo parcial no participaron, esto con el fin de identificar si abren los correos sin verificar sí el asunto es verídico o sí realmente es un integrante de la Institución y/o alumno, esto apoyado de la herramienta de MailTrack, que es una extensión para Google Chrome, que de acuerdo a los resultados de la encuesta, el 100% de los docentes trabajan con Google Chrome, pues el Instituto otorga a cada docente una cuenta, bajo este dominio.

Del total de profesores participantes, el 80% accedió al correo, permitiendo ver una debilidad de identificación de correos falsos, además de que algunos de ellos, se puede visualizar el sistema operativo que tiene para futuros ataques, figura 5.

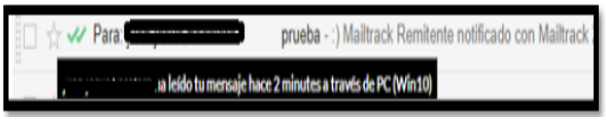

Figura 5. Seguimiento de correo.

Verificación de datos comprometidos, a través del correo institucional.

Para este ejercicio, nuevamente se tomaron de referencia a los 19 docentes de tiempo completo, en los cuales se encontraron que de acuerdo a la página https://haveibeenpwned.com/, 5 docentes estuvieron expuestos en 2017 para la divulgación de su información personal en una plataforma educativa en la cual se registraron, aquí la recomendación es que utilicen otra cuenta de correo alternativa, aun cuando no fue filtrada su información, el sitio si tuvo problemas de seguridad, figura 6.

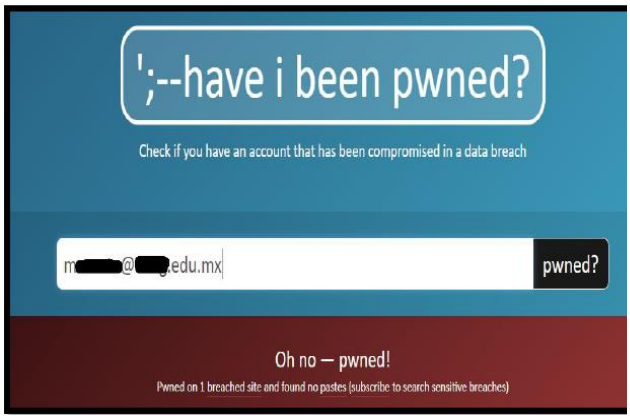

Figura 6, Ejemplo de cuentas de correos comprometidas.

Clonación de páginas web.

En esta etapa, se utilizó de prueba el laboratorio de consulta, el objetivo fue clonar páginas más visitadas por los alumnos, para comprobar la obtención de credenciales, pues aquí el servicio está totalmente abierto para que cualquier persona que pertenece a la institución, puede entrar y acceder al servicio de Internet, sin tener un tipo de restricción, lo cual provoca que accedan a redes sociales, la página oficial de la escuela y/o descarguen programas, películas, videos de cualquier página, saturando el ancho de banda, provocando mayor tráfico del normal y por ende, dejando sin servicio a otros equipos que se encuentran en la red.

¿Pero porque clonar una página web?

Esta es una técnica para realizar ataques phising que consiste en replicar la página web original, lo que puede provocar, no solo confusión a los usuarios, sino que estos faciliten a través de la web replicada, claves de acceso, datos privados sin saberlo. Entonces esta página fraudulenta podrá utilizar esos datos para su propio beneficio o incluso publicarlos en Internet [24].

Haciendo énfasis a lo anterior, se clono el sitio oficial del instituto, que de acuerdo a la figura 7, no se visualizan diferencias que puedan ser rápidas para identificarlas, en esta prueba de phising, se realizó con 250 alumnos, donde se solito que accedieran a su cuenta de control escolar, para monitorear sí está funcionaba de manera adecuada, después de una actualización.

Figura 7. Obtención de credenciales.

La figura 8, muestra un ejemplo de la obtención de credenciales de una víctima, después de esto, se les solicito a los alumnos que cambiaran su contraseña, y que ningún dato había sido alterado y se les explico que el principal motor para identificar una página falsa es la URL y que desde el navegador se aseguren que el icono de candado sea verde e indique que es un sitio seguro.

La obtención de credenciales, fue apoyada de la herramienta de Wireshark, que es el

analizador de protocolos de red más utilizado, permitiendo ver lo que sucede en la red a nivel microscópico[23], este es multiplataforma y todas las pruebas realizadas de este proyecto fueron a través del sistema operativo Kali Linux.

E. Post-explotación.

En esta etapa se muestra el análisis de la evaluación de los activos con los que trabajaron, se agruparon en las clasificaciones que se mostraron en la tabla número 1.

La realización de esta etapa se realizó bajo el uso de la norma 27001 que permite hacer la clasificación de amenazas y riesgos (figura 9).

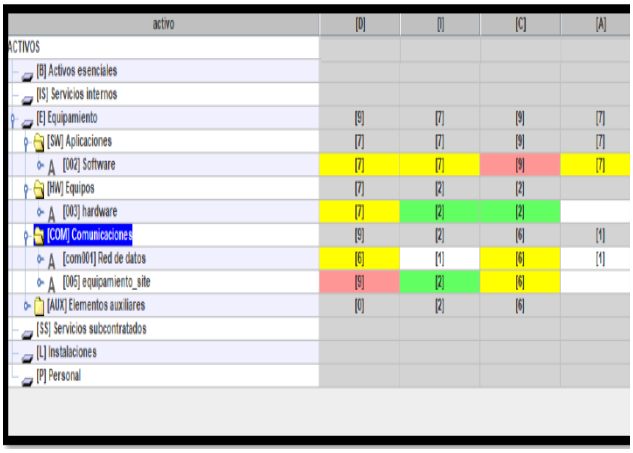

Figura 9. Nivel de impacto, después de la vulnerabilidad encontrada

F. Reporte.

En esta etapa, como se detectaron vulnerabilidades, donde se pudo comprobar que se necesita un firewall para bloqueo de páginas, como software actualizado y control de accesibilidad a los recursos en la figura 10, muestra un ejemplo básico de la aplicación de una regla para limitar el acceso a algunas páginas.

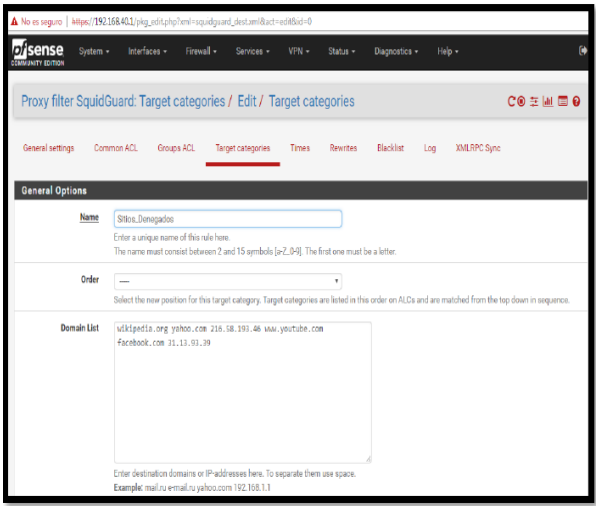

Figura 10. Creación de ACL.

En la figura 11, muestra la administración de los puertos que deben estar abiertos de acuerdo a la estructura física y de servicios con los que cuenta la escuela. Además de comprobar la división de las zona LAN y WAN.

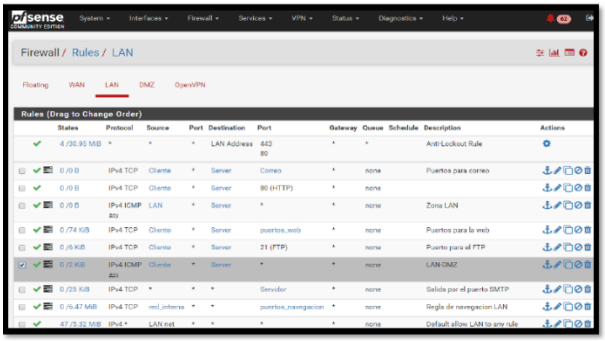

Figura 11. Creación de reglas de puertos.

Por último, de acuerdo a las pruebas realizadas, se obtuvo el nivel de crítico en el cual se encontraba la Institución, (figura 12).

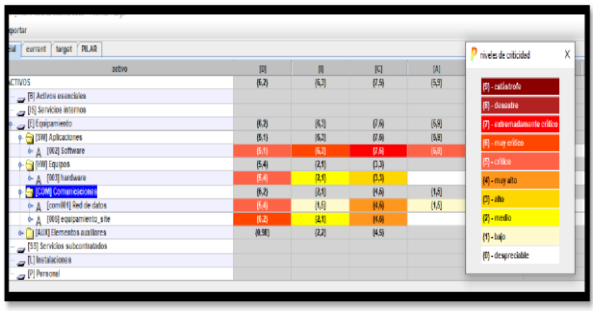

Figura 12. Nivel de criterio.

En la figura 13, se muestra la propuesta de soluciones, esto basado en el programa PILAR, que maneja los criterios de la norma 27001.

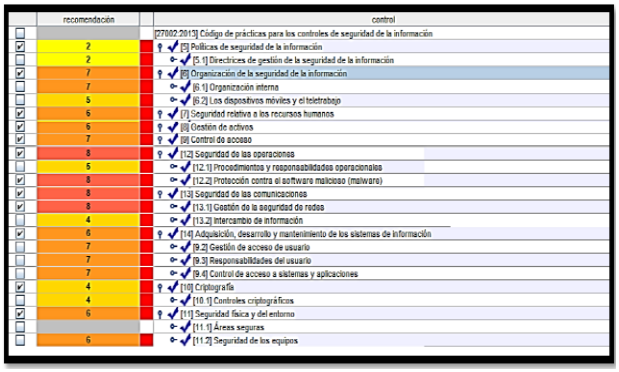

Figura 13. Recomendación de acuerdo a los criterios de vulnerabilidad encontrados.

Conclusiones.

Los resultados de este trabajo demuestran que cualquier organización pública o privada, independiente de su actividad que desempeñe, necesita implementar políticas de seguridad informática, que garanticen la evaluación de mejora continua en la divulgación de información, control de los recursos y monitoreo de la red, ya que de esta manera, permitirá que se utilicen de manera adecuada. Además con el desarrollo de este proyecto se logró identificar las vulnerables existentes en el Instituto Tecnológico Superior de Guanajuato, logrado modificar técnicas de monitoreo de red, control de acceso y asegurar los servicios que se divulgan en una red informática y medios de comunicación, donde se puede presentar perdida de infraestructura o interceptación de datos confidenciales, permitiendo verificar las etapas de la metodología PTES, que permitió generar pruebas de penetración para identificar los riesgos a los cuales estaba expuesto el ITESG, y así atender los diferentes puntos de ataque que puede realizar un intruso y explotar las vulnerabilidades presentes en la Institución. Otra área de oportunidad, fue poder mejorar los tres factores de la seguridad de la información, los cuales son: confidencialidad, integridad y disponibilidad.

Referencias Bibliográficas

[1] Almeida C. L & Pinca P. J. 2018. *Implementación de un laboratorio de seguridad de informática para la realización de técnicas de ataque y defensa (pentesting) en un ambiente real controlado, utilizando una distribución de Kali Linux dentro de la empresa industrial Siderurgica Andec S.A.*[tesis de ingeniería, Universidad de Guayaquil]. Repositorio Institucional. http://repositorio.ug.edu.ec/handle/redug/35450

[2] Avendaño M, A & Diaz P. D. & Tafur M. A, 2019. *Análisis de Seguridad Perimetral en la empresa Servitiendas de Colombia y Dsurtiendo* [tesis de ingenería , Universidad Cooperativa de Colombia Facultad de Ingenierias]. Repositorio Institucional. http://hdl.handle.net/20.500.12494/13835

[3] CCN(2020), *Guía de Seguridad de las TIC CCN-STIC 817***.** Centro Criptográfico Nacional. Consultado 28 de Mayo 2020. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

[4] Crespo, E., Carvajal, F., Astudillo, C., Orellana, M., Vintimilla, R., & Carvallo, J. P. (2018). Acometer contra un ERP con Software Libre. *Enfoque UTE, 9*(1), 138–148. https://doi.org/10.29019/enfoqueute.v9n1.253

[5] Cruz M. O.A.(2017). *Diseño e implementación de un proceso de hardening.*[tesis de Licenciatura]. Fundación Universitaria los Libertadores, Facultad de Ingeniería y Ciencias Basicas, Ingeniería de Sistemas, Bogotá d.c.

[6] Cyberpeace(2019). Hardening. Consultado 15 de agosto de 2020 https://www.cyberpeace.tech/

Delgado Q. B. A(2015). *Hardening en servidor web linux apache, php y configurar el firewall de aplicaciones modsecurity para mitigar ataques al servidor*.[tesis de maestria en seguridad informática aplicada]. Escuela Superior Politécnica del Litoral, Facultad de Ingeniería en Electricidad y Computación.

[7] ESET(2017).*67% de las instituciones educativas aseguró haber sufrido al menos un incidente de seguridad | ESET*. (n.d.)Consultado septiembre 6 de 2019. https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/67-de-las-instituciones-educativas-aseguro-haber-sufrido-al-menos-un-incidente-de-seguridad/

[8] Estrategia Nacional de Ciberseguridad(2017), *Ciberseguridad*, Consultado agosto 19 de 2019. www.gob.mx/ciberseguridad

[9] Fajardo, G. V., Marcela, D., Hurtado, M., Donado, S. A., Universitaria, I., & Mayor, C. (2018). *Diseño de un pentester de aplicaciones web utilizando raspberry PI 1*. 69–74.

[10] Franco, D. A., Perea, J. L., & Puello, P. (2012). Methodology for detecting vulnerabilities in data networks. *Informacion Tecnologica*, *23*(3), 113–120. https://doi.org/10.4067/S0718-07642012000300014

[11] González Brito, H. R., & Montesino Perurena, R. (2018). Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web. Revista Cubana de Ciencias Informáticas, 12(4), 52–65.

[12] ISECOM(2019). *OSSTMM*, ISECOM, https://www.isecom.org/research.html

[13] Laura, A., & Saucedo, H. (2015). *Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones Web*. ReCIBE. Revista Electrónica de Computación, Informática, Biomédica y Electrónica, 4(1), V.

[14] Martinez, J. M. ; Mejia, J. (2017). La Seguridad en Internet de las Cosas: Analizando el Tráfico de Información en Aplicaciones para iOS Security in the Internet of Things : Information Traffic. *ReCIBE*, *1*, 77–96.

[15] Martí T. R.M.(2016). *Desarrollo e implementación práctica de un PENTEST* [tesis de Licenciatura]. Universidad Politécnica de Valencia.

[16] Orellana Á. L. R.(2015). *Elaboración del hardening (aseguramiento) de una base de datos sql server de una empresa procesadora de tarjetas de crédito.*[tesis de Maestria en seguridad informática aplicada]. Escuela Superior Politécnica del Litoral, Facultad de Ingeniería en Electricidad y Computación.

[17] Ortigosa J. A.(2015). *Propuesta de implementación de una metodología de auditoría de seguridad informática.*[tesis de Licenciatura].Universidad Autonoma de Madrid.

[18] Panda (2019), *BlueKeep: la última vulnerabilidad de Windows más buscada por lo cibercriminales.* Panda, mediacenter. Consultado el 28 de junio de 2020. https://www.pandasecurity.com/spain/mediacenter/seguridad/bluekeep-vulnerabilidad windows-escaneo/

[19] Pfsense (2019) *Getting Started*. https://www.pfsense.org/getting-started/

[20] PTES(2014), *High Level Organization of the Standard*, PTES Technical Guidelines, Consultado el 16 de junio de 2020 http://www.pentest-standard.org/index.php/Main_Page

[21] Quiroz Zambrano, S., & Macías Valencia, D. (2017). Seguridad en informática: consideraciones. *Dominio de Las Ciencias*, *3*(3), 676–688.

[22] Solarte Solarte, F. N. J., Enriquez Rosero, E. R., & Benavides Ruano, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL*, *28*(5), 492–507.

http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321
[23] Wireshark. *About Wireshark, wireshark*. Consultado 22 de septiembre de 2020 https://www.wireshark.org/
[24]Wolters K. (11-10-2018 |). *Han clonado mi página web, ¿Qué hago?*. clarkemodet https://www.clarkemodet.com/news-posts/han-clonado-mi-pagina-web-que-hago/