INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 5 Núm. 2 (27-29 Octubre, 2021), pp. 119-128ISSN https://doi.org/10.33936/isrtic.v5i2.3952 | 2550-6730

Recibido: 17/09/2021
Aceptado: 12/10/2021

Instrumento para la auditoría técnica de seguridad informática en pequeños proveedores de Internet

Marlon Navia [1], Walter Zambrano-Romero [1]

[1]Departamento de Tecnologías de la Información y Comunicación, [1]Universidad Técnica de Manabí
[1]marlon.navia@utm.edu.ec [1]walter.zambrano@utm.edu.ec

RESUMEN Una auditoría de seguridad informática permite evaluar el nivel de seguridad de la infraestructura tecnológica de una organización. Su realización es muy importante, en especial en empresas que brindan servicios tecnológicos a muchos clientes. En este trabajo se presenta una herramienta que pretende facilitar la realización de este tipo de auditoría en pequeños Proveedores de Servicio de Internet, en los cuales no siempre es aplicable todo estándar o metodología de auditoría, debido a que su infraestructura está orientada a brindar servicios más que a ejecutar procesos. La herramienta está basada en la metodología OSSTMM, y tiene dos componentes: una ficha para recolección de datos, y una hoja electrónica para determinar los valores que requiere la metodología para evaluar la seguridad. Para elaborar la misma se tomó en cuenta las características propias de este tipo de negocios. La aplicación de esta herramienta permite reducir el tiempo de realización de una auditoría en este tipo de proveedores de servicio, al tiempo que sirve de guía para el levantamiento de información.

Palabras claves: Evaluación de seguridad; auditoría informática; OSSTMM.

A tool for the Technical Audit of Computer Security in small Internet providers

ABSTRACT Computer security audits allow evaluating the level of security of an organization's technological infrastructure. Its realization is very important, especially in companies that provide technology services to many clients. This paper presents a tool that aims to facilitate the performing of this type of audit in small Internet Service Providers, in which not all audit standards or methodology are always applicable, because their infrastructure is focused on offer services instead of perform processes. The tool is based on the OSSTMM methodology, and has two components: a data sheet for performing data collection, and an electronic sheet to determine the values required by the methodology to assess security. To create the tool, the characteristics of this type of business were considered. The application of this tool makes it possible to reduce the time required to perform an audit in this type of service provider, while at the same time it serves as a guide for gathering information for auditing.

KEYWORDS: Security assessment, computer audit, OSSTMM.

1. Introducción

La seguridad informática es un tópico de gran interés no solo para los profesionales del área, sino para el mundo en general, debido a la informatizacion de datos y procesos que vivimos actualmente. Según IT Governance [1] en el año 2020 se reportaron más de mil grandes violaciones de seguridad informática, que significaron más de 20000 millones de registros de datos perdidos o robados. A nivel económico, se espera que el daño por el crimen cibernético llegue a los 6 billones de dólares este 2021,

esto a pesar de que se afirma que el 80 % de los ataques pueden ser evitados aplicando acciones básicas de seguridad que mitiguen los riesgos [2].

Dado que los ataques a la seguridad informática o cyberataques se dan a través de las redes de datos, este recurso es el primero que debe asegurarse. Sin embargo, a pesar de los mecanismos o estrategias de seguridad que puedan implantarse, es prácticamente imposible conseguir un 100 % de seguridad. Por lo tanto, se hace necesario evaluar la seguridad tanto de sistemas informáticos como de las redes de datos que estos utilicen [3]. Para evaluar de forma práctica la seguridad de una infraestructura tecnológica, mediante la búsqueda de vulnerabilidades, existen varios métodos y técnicas [4]. Así mismo, hay disponibles varios estándares o metodologías para realizar una auditoría de seguridad, como ISO 27000, COBIT, ITIL, entre otros; que definen los lineamientos para evaluar la seguridad de los recursos tecnológicos [5].

Sin embargo, estos estándares y metodologías suelen estar enfocados a organizaciones de tamaño grande, con una infraestructura considerable. Por lo que su aplicación a pequeños y medianos Proveedores de Servicio de Internet (ISP) no siempre es factible, y debe adaptarse a las características de los mismos. Por otro lado, existen regulaciones y normas legales que obligan a los proveedores de servicios de Internet realizar auditorías o evaluaciones de la seguridad de sus redes, para prevenir riesgos de seguridad [6], sin importar el tamaño o cobertura de estos. En este trabajo se presenta un instrumento metodológico, basado en el Manual de la Metodología Abierta de Pruebas de Seguridad (OSSTMM por sus siglas en inglés), para aplicar una auditoría de seguridad informática en pequeños ISP, de tal forma que se pueda cumplir con los requerimientos de seguridad necesarios para realizar un trabajo confiable, así como los que imponen los organismos reguladores para su operación.

En la siguiente sección se analiza la motivación del uso de la metodología OSSTMM como base para este instrumento. Después se describe el instrumento, su fundamento, en que consiste y cómo se aplica. Por último se presentan las conclusiones de este trabajo.

2. OSSTMM y su difusión

2.1. Estructura de OSSTMM

De acuerdo a sus autores el Manual de la Metodología Abierta de Pruebas de Seguridad (que de aquí en adelante llamaremos simplemente Metodología OSSTMM) proporciona un camino para realizar pruebas o auditorías exhaustivas de seguridad, con un enfoque abierto. Esta metodología puede ser aplicada en conjunto con estándares y normativas reconocidas a nivel mundial o local, y actualmente se encuentra vigente la versión 3.0 de la misma [7].

Esta parte del artículo no pretende exponer detalladamente todo lo que comprende OSSTMM, sino solo lo más importante para entender la propuesta que se presenta. La metodología busca cuantificar la seguridad mediante métricas cuantitativas. Para esto divide los aspectos a auditar (la “Seguridad Operacional” u OpSec) en canales, los cuales se agrupan en 3 clases. En el cuadro 1 se muestran y describen brevemente los 5 canales considerados en OSSTMM.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 5 Núm. 2 (27-29 Octubre, 2021), pp. 119-128ISSN https://doi.org/10.33936/isrtic.v5i2.3952 | 2550-6730

Tabla 1: Canales definidos en OSSTMM.

Clase	Canal	Breve descripción
Seguridad Física (PHYSSEC)	Humano (HUMSEC)	Comprende el elemento humano de la comunicación.
	Físico	Comprende los elementos tangibles, no electrónicos. Por lo general se lo toma como lo que es sí PHYSSEC.
Seguridad de espectro (SPECSEC)	Inalámbrico	Abarca las comunicaciones mediante ondas electromagnéticas.
Seguridad de Comunicaciones (COMSEC)	Telecomunicaciones	Abarca las redes de telecomunicaciones sobre líneas telefónicas.
	Redes de datos	Comprende los sistemas electrónicos y cableado que constituyen las redes de datos.

Para evaluar cada canal, se miden cuentan criterios separados en 3 grupos: Operaciones, Controles y Limitaciones. Cada grupo comprende una parte del funcionamiento y seguridad de un sistema o infraestructura, así como de sus falencias. La Figura 1 muestra estos criterios, así como su relación.

Los criterios mostrados en la Figura 1 permiten obtener los RAV (Risk Assesment Value, Valor de Evaluación de Riesgos), que son una escala de medida de una posible superficie de ataque, y se calcula como un balance cuantitativo entre las operaciones, los controles, y las limitaciones. El valor del RAV idealmente debe ser cercano al 100 %, un valor menor indica que hay debilidades en la seguridad, y uno mayor muestra que hay más controles de seguridad de los necesarios.

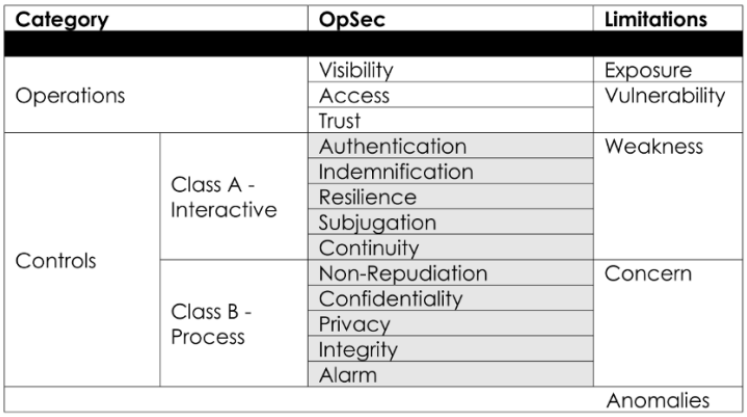

Figura 1: Mapeo de los criterios de Operación y Control con los de Limitaciones.

Los creadores de OSSTMM han puesto a disposición, en el sitio web de la organización, una hoja electrónica con fórmulas para calcular automáticamente el RAV de un canal, pero se deben determinar previamente los valores de los elementos de cada uno de los 3 criterios mencionados.

2.2. Casos de aplicación

Son varios los casos de aplicación de esta metodología. Como se explica a continuación, su estructura ha permitido se plantee su aplicación desde organizaciones pequeñas hasta grandes infraestructuras. Veamos algunos ejemplos.

[8]Analizan un caso de estudio de la aplicación de esta metodología como herramienta marco, para la evaluación de la seguridad en pequeñas empresas de asesoría contable en Colombia. En otro estudio, se aplica OSSTMM para auditar la seguridad de la infraestructura tecnológica de una institución de educación superior en Ecuador [9]. En ambos casos, se utilizó la metodología combinada con herramientas de hacking ético. [10] por su parte, lo aplicaron en la auditoría informática de un gobierno municipal.

Sin embargo, su aplicabilidad en infraestructuras más grandes también ha sido estudiada. En su investigación, [11] plantean esta metodología para evaluar las vulnerabilidades informáticas de un sistema SCADA en una infraestructura crítica, como lo es un sistema interconectado de electricidad. Sobre este aspecto, [12] plantean una versión expandida de OSSTMM, que permite calcular los RAV de una forma más completa, de tal forma que pueda ser mejor aplicada en infraestructuras críticas.

[13] Lo toman como referencia para plantear una arquitectura que permita lograr una seguridad modular en sistemas complejos, que pueden incluir desde pequeños dispositivos sensores, así como sus controladores o coordinadores, hasta equipos más grandes. Este mismo grupo de investigación utiliza esta metodología para evaluar un framework de control de un sistema de seguridad, basado en algoritmos genéticos [14].

Como hemos visto en todos estos ejemplos, OSSTMM es lo suficientemente versátil como para poder ser aplicada en la auditoría de organizaciones de distinto tamaño.

3. Descripción de la Propuesta

En esta sección primero se describirán los criterios y enfoques tomados para creación de la herramienta. Posteriormente se describe la herramienta en sí; y por último se dan las indicaciones para su aplicación, a la vez que se comenta su aplicación en dos casos reales de auditorías.

3.1. Enfoque de aplicación

Muchas de las metodologías o estándares de seguridad o de auditoría se enfocan en evaluar la Gestión de Seguridad de la organización. Sin embargo, en el caso de los ISP considerados “pequeños”, la mayoría de estándares o metodologías no son fácilmente aplicables. Para la propuesta que aquí se presenta, se entiende por un ISP de tamaño pequeño a aquel que tiene una cobertura que no abarca toda una provincia, pero que si puede llegar a varias localidades.

Algunas de las características de la mayoría de ISP pequeños, de acuerdo a la experiencia de los autores de esta propuesta, que han sido tomados en cuenta para el planteamiento presentado, son las siguientes:

- El principal servicio que brindan es de acceso a Internet, pudiendo también ofrecer acceso a la red pública a equipos de sus clientes, es decir asignación de direcciones públicas a equipos de clientes.
- La mayoría no cuentan con un sistema de Gestión de Seguridad como tal, aunque si aplican políticas (por lo general no declaradas implícitamente) y mecanismos relacionados.
- Utilizan el servicio de terceros (portadores de telecomunicaciones) para el acceso a la red pública de Internet.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 5 Núm. 2 (27-29 Octubre, 2021), pp. 119-128ISSN https://doi.org/10.33936/isrtic.v5i2.3952 | 2550-6730

- Aunque algunos ofrecen algún servicio adicional (como televisión por cable o servicios de mantenimiento de equipos), prácticamente ninguno ofrece servicios de Internet como tal, como almacenamiento, computación en la nube, u otros similares.
- Sus clientes son principalmente de tipo domésticos, aunque también sirven a PYMES, y en algunos casos a instituciones públicas de menor tamaño.

Dado que es una organización que presta servicios de conectividad y relacionados, con una cobertura limitada, no todos los canales de OSSTMM son aplicables. En el cuadro 2 se muestran y explican brevemente que comprende cada canal considerado.

El canal Humano (HUMSEC) se lo deja como opcional por una razón: es posible que se pueda considerar como parte de este canal a los clientes del ISP, y sería complejo evaluarlos a todos. En todo caso, la evaluación de este canal queda limitada al personal del ISP, tanto a nivel operativo o técnico, como administrativo.

Tabla 2: Canales de OSSTMM considerados en la propuesta.

Canal	**Descripción**
Humano (HUMSEC)	Comprende el personal técnico y operativo del ISP (opcional).
Físico (PHYSSEC)	Comprende todo lo que tenga que ver con las ubicaciones físicas del ISP.
Redes de datos (COMSEC)	Comprende las redes, equipos, configuraciones y servicios

No se ha considerado el canal de Inalámbrico, dado que no se ofrece un servicio como tal de este tipo, y si lo hubiera es casi seguro que su funcionalidad caiga dentro de lo que abarca COMSEC. Tampoco se consideró el canal de Telecomunicaciones, ya que en la actualidad los servicios casi en su totalidad utilizan fibra óptica como medio de transmisión, y además la mayoría de estos ISP tampoco prestan el servicio de telefonía.

3.2. Herramienta para auditoría en ISP

La herramienta propuesta para la auditoría de seguridad de pequeños ISP consta de dos elementos o archivos. Ambos archivos tienen acceso abierto para quienes quieran consultar o hacer uso de las mismas. En la parte de Apéndice se indica cómo acceder a los mismos.

El primero es una Ficha para la recolección y análisis de datos. Esta ficha requiere como insumo documentos o elementos que debería tener un ISP, aunque no son obligatorios. Mediante el análisis de estos insumos, se puede determinar ciertos ítems que servirán para obtener los valores de los criterios para determinar un RAV. En caso de no tenerlos, también se puede determinar su valor mediante una inspección o análisis de la infraestructura, ya sea mediante pruebas de penetración, o simplemente mediante evaluación visual. Si bien la ficha indica que ítems se debe obtener, también es posible registrar otros, cuando el auditor lo considera conveniente. La Figura 2 muestra el encabezado y parte del contenido de esta ficha.

Una vez determinados estos ítems y sus cantidades, estos se ingresan en el segundo elemento, que es una hoja electrónica. En esta hoja electrónica, que además permite registrar la fecha de aplicación y la organización que se audita, se ingresan los valores correspondientes a los ítems, así como el canal y criterio al que pertenecen.

Si bien la hoja ya trae predeterminado a que criterio y canal debería corresponder cada ítem, es posible modificarlo. Además, aunque se han considerado los aspectos generales que indica la metodología

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

 https://doi.org/10.33936/isrtic.v5i2.3952 | 2550-6730

Información para evaluación de Métricas de Seguridad
Organización:
Canal de OSSTMM a evaluar: **Redes de Datos (COMSEC) y Físico (PHYSSEC).**
Fecha de toma de datos: .
Insumos para evaluación de métricas de seguridad en la auditoría

Insumo	Existe	Observación / Alcance	Ítem esperado	Cant.	Canal (Tipo)
1. Inventario de equipos y servicios en red			Dispositivos administrables visibles en el backbone o con IP publica		C (OpS)
			Cada tipo de servicio único que pueda ser accesible o utilizable en la red		C (OpS)
			Lugares o instalaciones con equipos de red del ISP		P (OpS)
2. Registro de configuración de red/servicios			Cada servicio activo en un dispositivo analizado (tipo de servicio único por host)		C (OpS)
			Cada tipo de servicio único que pueda ser accesible o utilizable en la red		C (OpS)
3. Planos de nodos o lugares con equipos de red			Lugares o instalaciones con equipos de red del ISP		P (OpS)
			Cada elemento por la que se podría acceder con cierta facilidad a alguna instalación		P (OpS)
			Cada ruta (física) interna o segura que pueda haber entre dos lugares hay equipos de red		P (OpS)
			Mecanismos físicos para realizar las tareas de forma privada ante externos (oficinas asiladas)		P (C.P.)
4. Planes de contingencia			Instancias a nivel de dispositivos/enlaces que aseguren que no se pueda causar interrupciones en el canal		C (C.I.)
			Instancias que proporcionan "fallo seguro" al acceder a configuración dispositivos o servicios		C (C.I.)
			Instancias o controles físicos sobre un recurso, que si uno falla el otro sigue funcionando (redundancia)		P (C.I.)

Figura 2: Parte del componente Ficha de recolección de datos.

y que pueden encontrarse en un ISP, se pueden registrar nuevos items cuando el auditor encuentra uno nuevo que no haya sido considerado en la hoja.

En la Figura 3 se muestra la hoja de ingreso de los valores para cada ítem considerado. En este caso, se estaría haciendo (de forma parcial) un análisis que abarca los canales PHYSSEC y COMSEC.

Información para evaluación de Métricas de Seguridad
Organización:
Canal de OSSTMM a evaluar: **Redes de Datos (COMSEC) y Físico (PHYSSEC).**
Fecha de toma de datos:
Insumos para evaluación de métricas de seguridad en la auditoría

Insumo	Existe (Si/No)	Ítem esperado	Cantidad	Criterio	Canal
1. Inventario de equipos y servicios en red	Si	Dispositivos administrables visibles en el backbone o con IP publica	6	Visibilidad	COMSEC
		Cada tipo de servicio único que pueda ser accesible o utilizable en la red	3	Acceso	COMSEC
		Lugares o instalaciones con equipos de red del ISP			
2. Registro de configuración de red/servicios	No	Cada servicio activo en un dispositivo analizado (tipo de servicio único por host)	3	Confianza	COMSEC
		Cada tipo de servicio único que pueda ser accesible o utilizable en la red	1	Confianza	COMSEC
3. Planos de nodos o lugares con equipos de red	No	Lugares o instalaciones con equipos de red del ISP	2	Visibilidad	PHYSSEC
		Cada elemento por la que se podría acceder con cierta facilidad a alguna instalación	2	Acceso	PHYSSEC
		Cada ruta (física) interna o segura que pueda haber entre dos lugares hay equipos de red	0		
		Mecanismos físicos para realizar las tareas de forma privada ante externos (oficinas asiladas)	1	Confianza	PHYSSEC

Figura 3: Parte de la hoja para ingreso de datos.

Si bien los valores que se ingresan en esta hoja son obtenidos de la ficha antes mostrada, es posible complementar los mismos con otras fuentes. Un caso particular tiene que ver con las Limitaciones del canal COMSEC, específicamente con las vulnerabilidades, que deberían ser determinadas mediante

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 5 Núm. 2 (27-29 Octubre, 2021), pp. 119-128ISSN https://doi.org/10.33936/isrtic.v5i2.3952 | 2550-6730

herramientas de test de penetración.

Una vez ingresados los valores en la hoja correspondiente, dentro del mismo documento se encuentra otra hoja con los resultados consolidados, que serán los que se ingresen en la hoja de cálculo de RAV. En la Figura 4 se muestra un resultado parcial del uso de la herramienta. Como se puede ver, el objetivo

CANAL:	PHYSSEC		CANAL:	COMSEC
Criterios:	Valor:		Criterios:	Valor:
OPSEC			OPSEC	
Visibildad	2		Visibildad	6
Acceso	2		Acceso	3
Confianza	1		Confianza	4
CONTROLES			CONTROLES	
C.A.-Autenticación	0		C.A.-Autenticación	0
C.A.-Indemnificación	0		C.A.-Indemnificación	0
C.A.-Resilencia	0		C.A.-Resilencia	0
C.A.-Subjugacicón	0		C.A.-Subjugacicón	0
C.A.-Continuidad	0		C.A.-Continuidad	0
C.B.-No Repudio	0		C.B.-No Repudio	0
C.B.-Confidenc.	0		C.B.-Confidenc.	0
C.B.-Privacidad	0		C.B.-Privacidad	0
C.B.-Integridad	0		C.B.-Integridad	0
C.B.-Alarma	0		C.B.-Alarma	0
LIMITACIONES			LIMITACIONES	
Vulnerabilidad	0		Vulnerabilidad	0
Debilidad	0		Debilidad	0
Preocupación	0		Preocupación	0
Exposición	0		Exposición	0
Anomalías	0		Anomalías	0

Figura 4: Hoja de datos de salida con valores para RAV.

principal de la herramienta es facilitar el trabajo del auditor, a la vez que se reduce el tiempo de la auditoría, cuando se quiere aplicar la metodología OSSTMM. Además, la herramienta no es totalmente rígida, sino que puede ser personalizada.

3.3. Aplicación de la Herramienta

Al momento de aplicar la herramienta, se deben tomar en cuenta algunas consideraciones:

- Dadas las características descritas anteriormente, mucha de la documentación no existirá, por lo que será necesario aplicar la observación para determinar los elementos a considerar en la auditoría.
- Si la documentación existe, es necesario interpretarla de forma adecuada.
- La ficha de la herramienta es una guía. Sin embargo, se puede (y debería) complementar con otras técnicas, como la entrevista.
- La información de las vulnerabilidades de dispositivos y servicios en el canal COMSEC debe ser determinadas mediante herramientas desarrolladas para ese objetivo, como has de hacking ético. Estas herramientas también pueden utilizarse para determinar (o confirmar si fuera el caso) la información de los equipos y servicios, así como sus configuraciones, para determinar otros criterios de este canal.

Para ver la utilidad de la herramienta propuesta, se la aplicó en la auditoría de dos ISP de tamaño pequeño (que cubrían entre 3 a 5 localidades) en Ecuador, a inicios del año 2021. Por motivo de la confidencialidad que se debe brindar en estos casos, no se muestran los resultados obtenidos en cada una, pero si se describe el proceso realizado, en el que se utilizó la herramienta, así como los resultados generales de su aplicación.

La realización de la auditoría se basó en las 4 fases descritas en OSSTMM:

1. Fase de inducción: Donde se define el alcance y se elabora el cronograma de la auditoría.
2. Fase de Indagación: Aquí se recopila información del ISP, tanto de forma interna como externa, incluyendo el descubrimiento y escaneo de los equipos de red.
3. Fase de Interacción: En esta fase se determinan las vulnerabilidades de la red, y se verifica la aplicación de controles de seguridad.
4. Fase de Intervención: Aquí se establece el nivel de seguridad de los canales, así como la elaboración del informe de la auditoría.

Dentro de estas fases, las actividades relacionadas a la herramienta se dieron de la siguiente manera:

- En la fase 2 se utilizó la ficha para obtener los datos (principalmente documentales o por observación) del ISP.
- En las fases 2 y 3 se complementó la información para llenar en la ficha, mediante la aplicación de pruebas de penetración y vulnerabilidad. Aquí se utilizó como guía las recomendaciones SP 800-115 [15]. Estas pruebas permitieron corroborar o determinar la información sobre los equipos del ISP, así como determinar las vulnerabilidades de los mismos.
- En la Fase 4 se ingresó la información obtenida a la hoja electrónica, para obtener los valores para el cálculo del RAV de cada canal evaluado.

Un resumen de las fases de la auditoría se muestra en la Figura 5. Se puede ver que la herramienta es útil en al menos 3 de las 4 fases, tal como se mencionó antes.

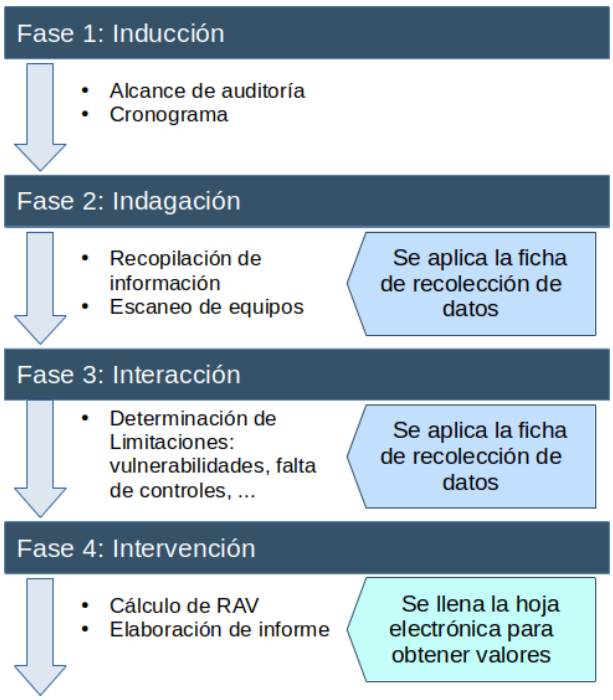

Figura 5: Esquema de las fases de la auditoría y de la aplicación de la herramienta.

Con la aplicación de los elementos de la herramienta, el tiempo de la parte operativa de la auditoría prácticamente se puede reducir hasta 3 días: uno para las evaluaciones internas, otro para las externas, y otro para la determinación de resultados, sin contar los tiempos de las fases preliminares, ni de la elaboración y aprobación del informe final. Este tiempo fue el que se llevó en cada una de las dos auditorías realizadas aplicando la herramienta.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 5 Núm. 2 (27-29 Octubre, 2021), pp. 119-128ISSN https://doi.org/10.33936/isrtic.v5i2.3952 | 2550-6730

4. Conclusiones

En este artículo se ha presentado una herramienta de ayuda para realizar auditorías de seguridad informática en pequeños ISP, basándose en la metodología OSSTMM. Esta herramienta busca ser una guía al momento de cuantificar el nivel de seguridad de este tipo de organizaciones, mediante el cálculo de RAVs.

La herramienta dispone de dos componentes: Una ficha para la obtención de datos, y una hoja electrónica para determinar los valores que se deben ingresar para el cálculo de los RAVs.

Además, se plantean que canales, de los mencionados por en OSSTMM, deben ser los que se evalúen en este tipo de ISP.

La aplicación de esta herramienta en auditorías realizadas a dos ISP pequeños en Ecuador, permitió determinar de forma rápida la valoración cuantitativa de seguridad estas empresas. En ambos casos, el tiempo para determinar la valoración fue bastante reducido.

Como futuros estudios, se podría analizar la valoración de esta herramienta en ISP de mayor tamaño, o en otro tipo de organizaciones.

Referencias

[1] Luke Irwin IT Governance. *2020 cyber security statistics.* 2021.

[2] Cyber Observer. *29 Must-know Cybersecurity Statistics for 2020.* 2020.

[3] Régner Sabillón y Jeimy J Cano. «Auditorıéas en Ciberseguridad: Un modelo de aplicación general para empresas y naciones». En: *Revista Ibérica de Sistemas e Tecnologias de Informação* 32 (2019), págs. 33-48. DOI: https://doi.org/10.17013/risti.32.33-48.

[4] Matthew Metheny. «Chapter 10 - Security testing: Vulnerability assessments and penetration testing». En: *Federal Cloud Computing (Second Edition).* Ed. por Matthew Metheny. Second Edition. Syngress, 2017, págs. 379-400. ISBN: 978-0-12-809710-6. DOI: https://doi.org/10.1016/B978-0-12-809710-6.00010-X.

[5] Diego Arcentales-Fernández y Xiomara Caycedo-Casas. «Auditoría informática: un enfoque efectivo». En: *Dominio de las Ciencias* 3.3 mon (2017), págs. 157-173. ISSN: 2477-8818. DOI: https://doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.157-173.

[6] Arcotel. *Norma Técnica para coordinar la Gestión de Incidentes y Vulnerabilidades que afecten a la seguridad de las redes y servicios de telecomunicaciones.* 2019.

[7] P Herzog. «OSSTMM 3 - The open source security testing methodology manual». En: *Institute for Security and Open Methodologies: ISECOM* (2010).

[8] Héctor Darío Jaimes Parada, Olga Lucía Roa Bohórquez y Jaime Fernando Pérez González. «Scheme for the integration of the evaluation of computer security for the recognition phase. Case study: Company in the Colombian accounting sector». En: *2017 Congreso Internacional de Innovacion y Tendencias en Ingenieria (CONIITI).* 2017, págs. 1-6. DOI: 10.1109/CONIITI.2017.8273359.

[9] Diego Sebastián Gordón Revelo. «análisis de estrategias de gestión de seguridad informática con base en la metodología open source security testing methodology manual (osstmm) para la intranet de una institución de educación superior». Tesis de mtría. Universidad Especialidades Espíritu Santo UEES, 2017.

[10] Cristian Bracho, Fabián Cuzme-Rodríguez, Carlos Yépez, Luis Suárez Zambrano, Diego Peluffo y Cesar Moreira Zambrano. «Auditoría de seguridad informática siguiendo la metodología OSSTMMv3 : caso de estudio». En: nov. de 2017, págs. 307-319. ISBN: 1390-6143.

[11] Fabián Andrés Medina Becerra, Jesús Alberto Tirano Vargas y Diego Alexander Vargas Barrera. «Metodologıéa para la Ejecución de Evaluación de Ciber-Vulnerabilidades en los Sistemas ICS-SCADA de los Agentes del Sistema Interconectado Nacional». En: *Infometric@-Serie Ingenierıéa, Básicas y Agrıécolas* 2.1 (2019), págs. 61-67.

[12] Andrea Tortorelli, Andrea Fiaschetti, Alessandro Giuseppi, Vincenzo Suraci, Roberto Germanà y Francesco Delli Priscoli. «A security metric for assessing the security level of critical infrastructures». En: *International Journal of Critical Computer-Based Systems* 10.1 (2020), págs. 74-94. DOI: https://doi.org/10.1504/IJCCBS.2020.108685.

[13] Andrea Fiaschetti, A Morgagni, Martina Panfili, A Lanna y S Mignanti. «Attack-surface metrics, osstmm and common criteria based approach to "composable security" in complex systems». En: *WSEAS Transactions on Systems* 14 (2015), págs. 187-202.

[14] Alessandro Giuseppi, Andrea Tortorelli, Roberto Germaná, Francesco Liberati y Andrea Fiaschetti. «Securing Cyber-Physical Systems: An Optimization Framework based on OSSTMM and Genetic Algorithms». En: *2019 27th Mediterranean Conference on Control and Automation (MED)*. 2019, págs. 50-56. DOI: 10.1109/MED.2019.8798506.

[15] Karen A Scarfone, Murugiah P Souppaya, Amanda Cody y Angela D Orebaugh. *Sp 800-115. technical guide to information security testing and assessment*. 2008.