TRABAJO FINAL DE MAESTRIA EN AUDITORIA EN TECNOLOGIAS DE LA INFORMACION

Validez de una rúbrica para la auditoría de redes en el contexto de una institución pública de Guayaquil

Propuesta de artículo presentado como requisito parcial para la obtención del título:

Magister en Auditoría en Tecnologías de la Información

Por el estudiante:
Kléber David VILLACÍS REAL

Bajo la dirección de:
Francisco Joseph BOLAÑOS BURGOS

Universidad Espíritu Santo
Maestría en Auditoría en Tecnologías de la Información.
Guayaquil - Ecuador
Marzo del 2018

Validez de una rúbrica para la auditoría de redes en el contexto de una institución pública de Guayaquil

Kleber David VILLACÍS REAL[1]
Francisco Joseph BOLAÑOS BURGOS[2]

Resumen

El objetivo del estudio es validar en el contexto de una institución pública de Guayaquil, un instrumento para la auditoría de Seguridad de Redes aplicable a los firewalls; Para esto, se elaboró una escala de Likert con 19 dimensiones y 68 items, distribuidos conforme a la ISO27002 considerando Aspectos Organizativos de la seguridad de la Información (7), Control de Accesos (17), Seguridad Física y Ambiental (6), Seguridad Operativa (18), Seguridad en Telecomunicaciones (20). En cuanto, a la validación del instrumento para medir la calidad se utilizó la Teoría de la Generalizabilidad y el software Edug1.6-e; el diseño de la medida consta de 3 facetas: Unidad de Negocio, Items y Auditores. Por otra parte, los resultados en el análisis de la Teoría G muestran coeficientes ρ igual 0, lo que indica que el instrumento es fiable y valido. En relación a los trabajos futuros, el instrumento plantea un diagnóstico exploratorio como punto de partida para una auditoría de red técnica, donde, la eficacia operativa de los controles de seguridad pueda ser evaluada.

Palabras clave: auditoría de redes, seguridad de redes, revisión de seguridad de redes, ISO 27000, NIST 800-53ª

Abstract

The objective of the study is to validate an instrument for network security auditing, applicable to firewalls; for this, a three-level Likert scale was developed, consisting of 5 clauses, 10 categories and 68 items, distributed according to ISO27002 in Organization of Information Security (7), Access Control (17), Physical and Environmental security (6), Operations Security (18), Communications Security (20). As for the validation of the instrument, the reliability was measured with the G Theory and the software Edug1.6-e; The design of the measure consists of 3 facets: Business unit, Items and Auditors. On the other hand, the results in the analysis of Theory G show coefficients ρ equal 0, which indicates that the instrument is reliable. In relation to future work, the instrument proposes an exploratory diagnosis as a starting point for a technical network audit, where the operational effectiveness of safety controls can be evaluated.

Key words: network audit, network security, network security review, ISO 27000, NIST 800-53ª

[1] Estudiante de Maestría en Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail kvillacis@uees.edu.ec.

[2] Magister en Seguridad Aplicada. Director de la Maestría en Auditoría en Tecnologías de la Información, Universidad Espíritu Santo – Ecuador. E-mail fcobolanos@uees.edu.ec.

INTRODUCCIÓN

El avance tecnológico ha generado en las Tecnologías de la Información y Comunicación (TIC) un incremento de los servicios informáticos que se ofrecen en las instituciones públicas y privadas (Dhillon y Backhouse, 2000). Por ello, los Sistemas de Información (SI) están expuestos en el ciberespacio al riesgo de ciberataques, que se han incrementado de manera proporcional al crecimiento tecnológico, provocando preocupación por la Confiabilidad, Integridad y Disponibilidad (CID) de la información (Alhomoud, Munir, Disso, Awan, y Al-Dhelaan, 2011; Mendoza, 2017). Asimismo, lo anuncia Shen (2014), recalcando que el aumento de los ciberataques a los SI, pone en alerta a las instituciones, por las repercusiones financieras, legales, de imagen y depreciación del precio de las acciones que genera este tipo de incidentes. Por otra parte, ESET(2017) de manera alentadora demuestra que existe 5% de incremento en el uso de Controles de Seguridad (CS) de la información en relación al año 2016, no obstante, la eficacia de estas contramedidas crean dudas en la protección de los SI .

En este sentido, Sahibudin, Sharifi y Ayat (2008), concuerdan en la existencia de varios marcos de trabajo, normas, modelos, instrumentos, herramientas y estándares para la gestión de las Tecnologías de la Información (TI) y SI para las instituciones. De la misma manera, Pardo, Pino, Garcia, Baldassarre y Piattini (2013), indican que se observa una variedad de estándares que pueden ser tomados como referencia para mejorar los CS de una institución, como las que ofrece la norma ISO 27000 para la Gestión de la SI.

Por otro lado, Gossels y Mackey (2007); Granneman (2013), expresan que la ISO 27000 es una norma de seguridad de la información que puede ser aplicada en cualquier tipo institución por ser un mecanismo práctico para evaluar y afirmar las políticas de seguridad. De manera similar, la NIST SP 800-53ª es el estándar para las agencias Estado Unidenses, no obstante, podria ser usada en cualquier tipo institución. En este sentido, Bodeau y Graubart (2013), señalan que 77% de los controles estan orientados a la CID de los SI. Asimismo, Fitzgerald (2017) expresa que no es suficiente implementar los controles de los marcos de trabajos mencionados a manera de primera línea de defensa, sino mediante auditorías internas para ejercer mayor control en una tercera línea de defensa.

En ese orden de ideas, Disterer (2013); Kayrak (2014b), plantean que las instituciones han llevado al uso de nuevos y renovados instrumentos de auditoría, conduciendo un cambio fundamental en el entorno de la seguridad de la información. Por otro lado, ISACA (2014) señala que los instrumentos y técnicas representan material complementario que sustenta la auditoría y existe una variedad de herramientas adecuadas que deben ser seleccionadas para alcanzar el objetivo deseado. De la misma manera, Sizemore, Nigel, Franke, y Kalyanaramani (2013), expresan que el uso de las herramientas innovadoras de expertos deben de considerarse para las auditorías en caso de ser apropiadas; Además, Sizemore et al. (2014), destaca que el auditor no necesita la experiencia del experto para el uso de la herramienta, sin embargo, necesita tener el suficiente conocimiento para conducir y supervisar su uso durante el desarrollo de la auditoría.

Por otra parte, en el estudio presentado de auditoría de seguridad de una institución mediana por Lo y Marchand (2004) se enfocan en auditar componentes específicos de infraestrutura de red, sistemas de políticas, contraseñas, redes inalámbricas y accesos remotos; en cuanto a la auditoría de infraestructura de red, el objetivo principal a revisar es el firewall, por ser la primera línea de defensa contra los ciberataques. De manera similar, Zhang et al. (2010) proponen un modelo y una estrategia general de protección del SI basado en características del *China Smart Grid* y los nuevos requisitos de protección para la seguridad de la información donde señalan que la seguridad básica de la infraestrutura empieza por la seguridad fronteriza, red y dispositivos.

Conforme a los estudios realizados por ESET (2016) muestran en su información histórica que el antivirus, firewall y respaldo de información han sido en los últimos 7 años las principales contramedidas más aplicadas en las instituciones. Un año más tarde, ESET (2017) en la encuesta realizada a 4500 instituciones latinoamericanas demuestra que estas contramedidas siguen ocupando las mismas posiciones de aplicabilidad: 83% antivirus, 75% firewall y 67% respaldo de información.

De manera similar, Bellovin (2008), señala que el firewall puede ser de valiosa ayuda a la seguridad de información en ambientes apropiados con las configuraciones correctas que cumplen las políticas de seguridad, no obstante, si los controles

aplicados son muy sencillos, este no cumplirá su objetivo. Por otro parte, para elevar el nivel de robustez en las políticas implementadas, es necesario realizar auditorías internas con instrumentos validados y adaptados al contexto para ejercer mayor control en los dispositivos de red.

En ese sentido, en los estudios presentados por los autores Karabacak y Sogukpinar (2006), Bandopadhyay, Sengupta y Mazumdar (2011) y Karin Huijben (2014), se evidencia la creación de modelos similares al presentado, sin embargo, carecen del uso de una metodología, como recomienda (Escobar-Pérez y Cuervo-Martínez, 2008) para la validez del contenido y (Mendo, Martínez y Morales, 2010) para la fiabilidad del instrumento. De manera que el objetivo del presente estudio es validar un instrumento para una auditoría de seguridad de redes de un firewall. Para ello, se ha tomado como base fuente la ISO27002:2013 y la NIST 800-53ª r5, dentro del contexto de una institución pública del país.

MARCO TEÓRICO

Seguridad de la Información

De acuerdo con Alberts y Dorofee (2003)**,** definen a la seguridad de la información como actividades que proveen protección a los activos de información contra los riesgos de acceso no autorizado, uso indebido, divulgación, modificación o destrucción. Asimismo, enumeran las áreas principales donde se enfocan la seguridad de la información: activo de información, amenaza, vulnerabilidad y riesgo. De manera similar, Ross, Viscuso, Guissanie, Dempsey y Riddle (2015), describe que: *"La protección de la confidencialidad, integridad y disponibilidad de los SI contra el acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción de la información". (p b4).* Por otra parte ISO/IEC (2016), establece que la seguridad de la información es un objetivo alcanzado a través de la aplicación de CS que protegen la CID de la información.

Seguridad de redes

Onwubiko y Lenaghan (2007;2009)**,** conciben la seguridad de redes como la protección que tiene como objetivo preservar la CID de las redes y servicios ofrecidos por TI contra los ciberataques, esto incluye hardware, software, firmware, SI y telecomunicaciones. Asimismo Sheth y Thakker (2011), plantean como objetivo de seguridad de redes a la protección de la información de accesos no autorizados para mantener la CID de la información, no obstante, destacan que es indispensable para alcanzar los objetivos de las organizaciones. Por otra parte Pan, Yuan y Mishra (2011)**,** señala que la combinación de tecnologías como firewalls, detección de intrusos IDS y cifrado aumenta la seguridad en las redes, no obstante, para mejorar la resistencia a los ciberataques se deben de revisar periódicamente las políticas, procedimientos y CS.

Auditoría

Lo y Marchand (2004), señalan que la auditoría de SI es una actividad de diferentes áreas que podría implicar la auditoría tradicional, gestión de SI y ciencias del comportamiento. Por otra parte, Pan et al. (2011) la definen como una evaluación o revisión sistemática de controles comparados con una norma, estándar o política, donde los resultados son reportados a los interesados. De manera similar, Kayrak (2014b), plantea que la auditoría de SI, se puede establecer como una auditoría de TI de una institución, operaciones de TI, gobierno y gestión de TI y otros procesos de TI relacionados. En ese sentido, la auditoría se plantea como una revisión y verificación formal para corroborar que las políticas, contramedidas y registros están basados acorde a un estándar y que cumplen los objetivos de seguridad de la institución.

Clasificación de las auditorías

De acuerdo con Onwubiko (2009), existen varios tipos de auditoría de SI que una institución podría utilizar para proteger los activos de información; desde la prueba de CS a firewalls, sistema de detección de intrusos con el fin de detectar puertas de seguridad abiertas hasta la verificación regulatoria del cumplimiento de las mejores prácticas o normas implementadas. Por otra parte Jackson (2010), define que las auditorías pueden desglosarse en diferentes tipos como el análisis de la arquitectura de seguridad basada en el criterio del auditor, hasta una auditoría integral de extremo a extremo basada a un estándar o marco de seguridad como la norma ISO27001. Con respecto a lo antes planteado, los autores concuerdan en dos tipos de auditorías de SI; la primera que comprende la parte de pruebas o testeo, y la segunda, que se enfoca en la revisión de cumplimiento de normas, políticas o estándares.

Tabla 1
Tipos de Auditoría de SI

Autor	Tipo de Auditoría	Técnica
Onwubiko (2009)	Auditoría Técnica de SI	Pruebas de Testeo Pen TEST
	Auditoría de SI	Revisión de Cumplimiento de políticas Normas Estándares Buenas Prácticas
Jackson (2010)	Revisión de Seguridad	Pruebas de Testeo Pen TEST Escaneo de vulnerabilidad Análisis de riesgo
	Auditoría de Seguridad	Auditoría de cumplimiento Auditoría de políticas

Auditoría de Seguridad de Redes

Hayes (2003), concibe que una auditoría de seguridad informática es una evaluación técnica metódica y mensurable de cómo se emplea una política de seguridad de la institución en un lugar determinado. Onwubiko (2009) explica que la auditoría de seguridad de red busca garantizar: Primero, el cumplimiento normativo y de seguridad establecido en la compañía. Segundo, la protección de los activos de información valiosos o críticos, y los mecanismos de protección funcionen según lo establecido. Tercero, los procesos se encuentren en sitio y en mejora continua. Finalmente, que se apliquen los CS.

Por otra parte, acorde con Jackson (2010) la auditoría de seguridad de redes revisa, examina y realiza un análisis brecha de los controles implementados, conforme al cumplimiento de la norma adoptada en la institución, con el fin de medir el estado actual de las políticas de seguridad. Por otro lado, Pan et al. (2011), conceptualiza que es un reporte que propone mejoras de una revisión metódica de las políticas, procedimientos, sistemas y aplicaciones que no cumplieron con el estándar o las mejores prácticas de la industria de la seguridad de redes.

Normas, Metodologías y Estándares

ISO2700, es una norma Internacional de seguridad de la información publicada por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC). En ese sentido ISO/IEC:27002(2013), establece que es una guía de buenas prácticas que describe los objetivos y mecanismos de control para el proceso de implementación y certificación de la ISO/IEC:27001 (2013). De acuerdo con Disterer (2013), los requerimientos codificados en ISO 27001 desarrollan y explican en ISO 27002 a manera de una guía de prácticas comunes, conocidas como mejores prácticas, que pueden ser adaptadas a requerimientos específicos de las instituciones interesadas en la seguridad de la información. Por otro lado ISO/IEC (2016), revela que la estructura de la norma contiene 14 cláusulas de CS que contienen un total de 35 categorías principales de seguridad y 114 controles.

NIST SP 800-53, es una abreviatura de *Instituto Nacional de Estándares y Tecnología Publicación Especial 800-53*, que provee un catálogo de CS y privacidad para los sistemas de información y organizaciones federales estadounidense. Sin embargo, acorde con NIST (2014), se motiva a los gobiernos estatales, locales, tribales y organizaciones del sector privado el uso de estos CS. Por otra parte Duncan & Whittington (2014), señala que la NIST SP 800-53 ha venido evolucionando en los estándares de seguridad antes de la evolución de la computación en la nube incorporando los controles ISO 27002 con otros marcos gubernamentales y no gubernamentales. Por otro lado NIST (2014), muestra la estructura de los CS y privacidad organizados en 24 familias, cada una contiene controles relacionados con el tema específico de cada familia. Los CS y privacidad involucran aspectos de políticas, supervisión, procesos manuales y mecanismos automatizados que son implementados por sistemas o acciones de individuos.

OSSTMM, por sus siglas en inglés *Open Source Security Testing Methodology Manual* o *Manual de la Metodología Abierta de Testeo de Seguridad*. Según Jackson (2010), es la metodología de pruebas más completa y utilizada para la revisión de la seguridad. Por otra parte Herzog (2010), señala que la metodología de testeo contempla requerimientos en la NIST y especificaciones de la administración de seguridad de la información en la norma ISO:27001 e ISO:27002. Por otra parte, define la estructura de la metodología compuesta por 3 clases, las cuales contienen 5 canales de seguridad, donde los canales son los medios que interactúan con los activos de información. Asimismo, el enfoque de esta metodología es

proporcionar descripciones específicas para pruebas de seguridad operacional como pruebas de penetración, piratería ética, evaluaciones de seguridad y vulnerabilidad en todos los canales operativos.

Tabla 2
Normas de Seguridad de la Información

Norma	Proporciona	CID	Publicación
ISO 27002	Directrices para la selección, implementación y gestión de controles en base a los riesgo de SI de la organización.	Si	2013
NIST 800-53	Catálogo completo y flexible de controles de seguridad y privacidad	Si	2017
OSSTMM	Metodología científica para la caracterización precisa de la seguridad operacional	Si	2010

METODOLOGÍA

Participantes

La estructura organizacional de esta institución, está compuesta por 10 Unidades de Negocios (UN) y una sede principal, las cuales se encuentran separadas geográficamente en todo el Ecuador. Las UN que forman parte del modelo fueron seleccionados por conveniencia, cuya muestra está basada en la proximidad geográficas entre ellas y en la aproximación del promedio de la cantidad de usuarios que pertenecen a cada sitio.

Por otro lado, la infraestructura de red está compuesta por 12 Centro de Datos (CD), teniendo uno como principal donde convergen todos los servicios de la institución. Cabe mencionar que cada CD está dotado de un dispositivo de frontera de la misma marca y modelo. Asimismo, sus configuraciones son semejantes en los equipos. En vista de la importancia del servicio que ofrecen los firewalls y por ser la primera línea de defensa contra los ciberataques, se ha considerado una muestra de tres UN.

Tabla 3
Auditores

UN	Título	Experiencia	Capacitación
1	Ing. de sistemas	4 años	30 días de capacitacion, Universidad Huawei, Shenzhen, China
	Ing. en sistemas de información gerencial	8 años	Huawei Certified Network Associate, Universidad Huawei, Shenzhen, China
2	Ing. de sistemas	5 años	CCNA 1, CCNA 2, CCNA 3, CCNA 4
3	Ing. en computación, Magister en seguridad de la información	10 años	15 días de capacitacion, Universidad Huawei, Shenzhen, China

En ese sentido, se eligieron 4 auditores, estos fueron seleccionados con base en los siguientes criterios: disponibilidad, imparcialidad y cualidades como confianza en sí mismo, adaptabilidad, y que sus niveles de formación estén relacionados por educación, entrenamiento, experiencia y posición laboral. En cuanto al rango de instrucción, los 4 auditores son ingenieros en sistemas, poseen cursos y certificaciones inherentes a temas de redes. La experiencia del auditor de menor tiempo es de 4 años y el de mayor tiempo es de 10 años, sus cargos laborales están entre líderes y profesionales. Ver tabla 3.

Instrumento

Con el fin de reducir riesgos y evitar daños en los SI del sector público, el Gobierno Ecuatoriano a través del SNAP (2013) en el Registro Oficial No.88, dispone desarrollar un Esquema Gubernamental de Seguridad de la Información EGSI basado en la ISO 27000. Por ello, la norma de referencia seleccionada es la ISO27002:2013. Luego se realizó un análisis exploratorio de varias normas y se seleccionaron conforme al propósito y la aplicabilidad al cumplimiento de las regulaciones de acuerdo al contexto.

Tabla 4
Clasificación de controles de seguridad para instrumento

Cláusula	Controles	Items	Total
Aspectos Organizativos de la Seguridad de la Información (AO)	Segregación de Tareas (SF)	2	7
	Teletrabajo (TT)	5	
Control de Accesos (CA)	Control de Acceso a las Redes y Servicios Asociados (AR)	4	17
	Gestión de Altas/Bajas en el Registro de Usuarios (RC)	6	
	Gestión de los Derechos de Acceso con Privilegios Especiales (GD)	3	
	Revisión de los Derechos de Acceso a los Usuarios (RD)	1	
	Procedimientos Seguros de Inicio de Sesión (PR)	3	
Seguridad Física y Ambiental (SA)	Mantenimiento de Equipos (ME)	6	6
Segurida Operativa (SO)	Gestión de Cambio (GC)	4	18
	Gestión de Capacidad (CG)	2	
	Controles Contra Código Malicioso (CC)	3	
	Registro y Gestión de Eventos de Actividad (RG)	1	
	Sincronización de Relojes (SC)	1	
	Gestión de Vulnerabilidades Técnicas (GV)	7	
Seguridad en Telecomunicaciones (ST)	Controles de Red (CR)	13	20
	Mecanismos de Seguridad Asociados a Servicios de Red (MS)	4	
	Segregación de Redes (SR)	3	

De esta forma se seleccionó: OSSTMM 3 y NIST 800-53ª r4, donde las 3 normas cubren el CID y proporcionan directrices específicas para la seguridad de la información. En cuanto a la elección de los CS para evaluar el firewall dentro del contexto presentado, se realizó un análisis cualitativo de la ISO27002, obteniendo como resultado la tabla 4.

Por otra parte, para la alineación de las normas, se toma como base la organización dada por la ISO27002, clausula, categoría de control, controles y guía suplementaria. Luego, se realiza un cuadro comparativo de las estructuras de las normas y se definen 4 categorías: general, específica, instrucción y guía, las cuales sirven para mapear los componentes similares entre ellas, y clasificar sus componentes en niveles definidos, obteniendo un punto de partida para el mapeo y alineación de los CS. (Ver tabla 5). Asimismo, conforme a los CS seleccionados, se realiza un análisis comparativo y se alinean las tres normas de acuerdo a la equivalencia y clasificación de sus CS, obteniendo como resultado el producto de las tres normas.

Tabla 5
Alineación de la estructura de las normas

Norma	G	E	I	GS
ISO 27002	Cláusula	Categoría	Controles	GS
OSSTMM 3.0	Clase + Canal	Control	P	NA
NIST 800-53ª	Familia	P	Instrucción	GS

Nota. G: General; E: Especifica; I: Instrucción; GS: Guía Suplementaria; P: Procedimiento; NA: No aplica.

Mientras, se elabora el instrumento, la NIST, pública el borrador de la 800-53ª r5, de manera que permite realizar una revisión de lo elaborado y se actualiza los avances obtenidos, excluyendo la OSSTMM. De esta manera, se adapta agregando la guía suplementaria como otra categoría, que sirve como referencia para la elaboración, además se eliminan, confirman y aumentan CS para dar mayor robustez y alineación al instrumento. De modo que, se genera una actualización de la clasificación de las normas, obteniendo como resultado la alineación de los CS.

Como resultado, el instrumento es una guía exploratoria que consta de 68 ítems que evalúan el firewall, con el fin de medir el nivel de cumplimiento de las políticas de seguridad. Para ello, se usa una escala tipo Likert con un rango de 0 a 2 (No cumple, cumple con algo y cumple con el ítem). También, se agregó los datos del equipo a evaluar, un glosario de términos e indicaciones para que sirvan como referencia durante la ejecución del instrumento.

Procedimiento

La validez de contenido del instrumento mediante juicio de expertos, se basa en lo sugerido por los autores Escobar-Pérez y Cuervo-Martínez (2008), quienes presentan una guía para del proceso, en la que evalúa la suficiencia, claridad, coherencia y relevancia de los items. De esta manera, luego de obtener los resultados del juicio de expertos, se realizó algunas mejoras al instrumento, manteniendo la claridad semántica del mismo y su correlación con los CS. Previo a la ejecución del instrumento, se establecieron teleconferencias con el Director de Infraestructura y Telecomunicaciones, Profesionales de Infraestructura y Telecomunicaciones y Líderes de Tecnología de las UN involucradas, con el objetivo de plantear las directrices y capacitar a los elegidos a ser partícipes de este estudio. En cuanto a la confidencialidad de la información, la Dirección decidió manejarlo como un proceso de gestión interno, por lo tanto, no se firmaron acuerdos de confidencialidad entre las partes involucradas, sin embargo, se acordó de manera verbal utilizar el instrumento con las 10 UN. Los auditores recibieron en sus cuentas corporativas de correo electrónico el instrumento con las indicaciones respectivas para la ejecución de la auditoría. Cabe indicar, que los participantes recibieron una semana como periodo de tiempo para concluir y remitir los resultados.

Resultados

Briesch, Chafouleas, y Riley-Tillman (2010), señalan que la Teoría de la Generalizabilidad (Teoría G) puede ser aplicada en otras áreas de estudio que no sean la psicología, ni la educación. Por ello, debido a la naturaleza del estudio, esta técnica es pertinente para la validez de instrumentos. En ese sentido, acorde con Larraz, Allueva y Blanco-Villaseñor (2014), se considera este trabajo como un modelo apropiado en relación a la muestra y los niveles de las facetas del mismo. De igual modo, Mendo, Martínez y Morales (2010), enfatizan que la aplicación de la Teoría G permite estimar el grado de generalización de un diseño de medida con escenarios particulares a un valor teórico buscado. Para el análisis de los datos se utilizó el software EduG 6.1–e, que permite analizar modelos mixtos (Cardinet, Johnson y Pini, 2010).

Primero, en el plan de observación, se ha estipulado como facetas de diferenciación a: Unidades de Negocio (U), Items (I) y Auditores (A), cada uno de ellos está compuesto por distintos niveles. El universo de generalización para las facetas es: I de 1 a infinito y A de 4 a infinito, se consideran facetas aleatorias por que la muestra observada se extrae de un conjunto infinito.

Tabla 6
Resultados análisis de varianza aspectos organizativos de la seguridad de la información

				Componentes				
FV	**SC**	**GL**	**MC**	**A**	**M**	**C**	**%V**	**ES**
U	0.0952	2	0.04762	0	0	0	0	0.0032
I	7.2857	6	1.21429	0	0	0	0	0.0658
A	1.2381	3	0.4127	0	0	0	0	0.027
UI	2.0714	12	0.17262	0.006	0.006	0.006	0.9	0.0184
UA	0.4762	6	0.07937	0	0	0	0	0.0075
IA	28.429	18	1.57937	0.4769	0.4904	0.4904	76	0.1669
UIA	5.3571	36	0.14881	0.1488	0.1488	0.1488	23.1	0.0341
							ρ	**0.00**

Tabla 7
Resultados análisis de varianza de control de accesos

				Componentes				
FV	**SC**	**GL**	**MC**	**A**	**M**	**C**	**%V**	**ES**
U	0.91176	2	0.45588	0.0047	0.0047	0.0047	0.6	0.0049
I	63.31373	16	3.95711	0.21752	0.2171	0.2171	28	0.11228
A	1.45098	3	0.48366	0	0	0	0	0.00819
UI	3.42157	32	0.10692	0	0	0	0	0.00789
UA	0.93137	6	0.15523	0.00174	0.00174	0.00174	0.2	0.00469
IA	65.54902	48	1.3656	0.4133	0.42473	0.42473	54.9	0.09124
UIA	12.06863	96	0.12571	0.12571	0.12571	0.12571	16.2	0.01796
							ρ	**0.00**

Tabla 8
Resultados análisis de varianza seguridad ambiental y física

				Componentes				
FV	**SC**	**GL**	**MC**	**A**	**M**	**C**	**%V**	**ES**
U	2.1111	2	1.05556	0.0287	0.0287	0.0287	4.6	0.0318
I	11.944	5	2.38889	0.0935	0.0985	0.0985	15.7	0.1112
A	0.2778	3	0.09259	0	0	0	0	0.0207
UI	3.3889	10	0.33889	0.0546	0.0546	0.0546	8.7	0.0354
UA	0.8889	6	0.14815	0.0046	0.0046	0.0046	0.7	0.0133
IA	15.722	15	1.04815	0.3093	0.3202	0.3202	51.1	0.1203
UIA	3.6111	30	0.12037	0.1204	0.1204	0.1204	19.2	0.0301
							ρ	**0.00**

Tabla 9
Resultados Análisis de Varianza Seguridad operativa

				Componentes				
FV	**SC**	**GL**	**MC**	**A**	**M**	**C**	**%V**	**ES**
U	0.89815	2	0.44907	0.00018	0.00018	0.00018	0	0.00466
I	70.7037	17	4.15904	0.19862	0.20674	0.20674	25.2	0.11507
A	1.83333	3	0.61111	0	0	0	0	0.00882
UI	14.43519	34	0.42456	0.08932	0.08932	0.08932	10.9	0.02513
UA	0.47222	6	0.0787	0.00064	0.00064	0.00064	0.1	0.00225
IA	72.33333	51	1.4183	0.45034	0.45646	0.45646	55.6	0.09189
UIA	6.86111	102	0.06727	0.06727	0.06727	0.06727	8.2	0.00933
							ρ	**0.00**

Tabla 10
Resultados análisis de varianza seguridad en telecomunicaciones

				Componentes				
FV	**SC**	**GL**	**MC**	**A**	**M**	**C**	**%V**	**ES**
U	0.0333	2	0.01667	0	0	0	0	0.0008
I	14.333	19	0.75439	0.0235	0.0238	0.0238	10.2	0.0207
A	1.4	3	0.46667	0	0	0	0	0.0052
UI	2.9667	38	0.07807	0.0028	0.0028	0.0028	1.2	0.0049
UA	0.7	6	0.11667	0.0025	0.0025	0.0025	1.1	0.003
IA	26.267	57	0.46082	0.1313	0.1374	0.1374	58.9	0.0284
UIA	7.6333	114	0.06696	0.067	0.067	0.067	28.7	0.0088
							ρ	**0.00**

Nota: FV: Fuente de Varianza; SC: Suma de Cuadrados; GL: Grados de Libertas; MC: Media Cuadrática; AL: Aleatorio; M: Mixto; C: Corregido; %V: Porcentaje de Varianza; ES: Error Estándar; U: Unidad de Negocio; I: Item; A: Auditor; ρ: Coeficiente G.

Asimismo, U de 3 a 11, considerada variable fija, puesto que el número de UN en el estudio planteado es finito. De igual modo, el diseño de medida es A/UI, es un modelo mixto por cuanto, las facetas contienen extremos finitos e infinitos.

Segundo, en lo que se refiere al plan de estimación, es un modelo cruzado donde todos los firewalls son evaluados por todos los auditores y el diseño de medida utilizado es A/UI donde se evidencian dos facetas de instrumentación unidad de negocio e ítem, y una faceta de diferenciación auditor, por tanto, que son los que mayor varianza aportan sobre las medidas obtenidas. En cuanto, la Teoría G, se basa sobre las cláusulas de la ISO27002 utilizadas, pero no sobre sus categorías o controles, por cuanto existe un desbalance entre ellas. De manera general, en los escenarios planteados (Ver tablas 6,7,8,9,10), se observa que las fuentes de varianza que muestran un alto índice de variación son IA y UIA; lo que demuestra que una cantidad importante de variabilidad se debe a posibles facetas no incluidas o errores

aleatorios no considerados. Estos componentes representan en promedio 47.52%, y 19.1%, respectivamente.

En ese sentido, la fuente de variación IA proviene de la relación ítem y auditor, los resultados se ven afectados directamente por el auditor, donde se pueden considerar posibles factores externos o internos que afectaron al auditor al momento de realizar la ejecución del instrumento, como: proporciona una puntuación aleatoria severa por no tener claro el ítem. En cuanto, a la fuente de variación UIA corresponde a todos los posibles errores no considerados dentro del escenario planteado, en otras palabras, todos los demás errores inesperados.

Por otro lado, en los resultados de la fiabilidad, se obtuvo los valores esperados, todos los Coeficiente de generalizabilidad ρ tienen como resultado 0.00, lo que infiere que los evaluadores fueron concordantes en sus puntaciones. Lo cual corrobora lo que dice Blanco-Villaseñor, Castellano, Hernandez-Mendo, Sanchez-Lopez y Usabiaga (2014), que el coeficiente de generalizabilidad debe ser próximo a cero.

Tercero, en el plan de optimización, con la información proporcionada por los análisis en los planes precedentes, se pretende encontrar la mejor adecuación de los procedimientos de medida en función del plan de observación para lograr una optimización de la faceta de diferenciación y generalización del estudio. En cuanto, a los resultados obtenidos de los estudios de optimización (Ver tablas 11,12,13,14,15), se observa que mientras aumentan las unidades de negocio y las observaciones en las opciones de estudio presentadas, se mantiene el coeficiente de generalizabilidad a 0.00%, lo cual demuestra la fiabilidad del instrumento para el escenario planteado.

Por otra parte, acorde con la revisión de literatura, Sizemore et al. (2013); ISACA (2014), concuerdan en el uso de material complementario que sustenta la auditoría y que estos instrumentos deben de ser los adecuados para alcanzar el objetivo deseado. En este sentido, Karabacak y Sogukpinar (2006), definen una metodología cualitativa ajustable a los dominios existentes dentro de cualquier tipo institución, para evaluar el cumplimiento de la norma ISO 17999, demostrando que la encuesta utilizada proporciona resultados de cumplimiento en poco tiempo, asimismo, señalan que los controles los convirtieron a pregunta, sin realizar algún tipo de validación del contenido del instrumento realizado.

De manera similar, Bandopadhyay, Sengupta y Mazumdar (2011), plantean una metodología de análisis brecha para revisar las lagunas que existen en la implementación de controles de seguridad en una empresa cualquiera basado en ISO 27002:2005, no obstante, los cuestionarios no fueron objeto de revisión por juicios de expertos. De igual modo, Karin Huijben (2014), crean un marco de evaluación ligero y compatible con ISO 27002:2013 que revela cuán seguros son los procesos organizacionales de cualquier tipo de institución en un periodo de tiempo corto, al igual que las metodologías presentadas, utilizan cuestionarios, donde expertos con una encuesta de retroalimentación de 5 preguntas aprueban el uso del documento, no obstante, no se evidencia ninguna técnica estadística en la validación de este instrumento. Por ello, el instrumento validado de este estudio, permite plantear nuevas puertas de investigación en el ámbito propuesto, donde se puede profundizar sobre la validación de contenido y fiabilidad del mismo.

A pesar de que las normas, estándares y guías de auditoría para la seguridad de redes, plantean de manera holística recomendaciones y mejores prácticas a implementar; estas, no proporcionan la metodología de cómo llevar a cabo el proceso de auditoría según el contexto, asimismo, no incluyen los instrumentos para evaluar y mejorar la seguridad de redes conforme a la necesidad presentada por las organizaciones.

De manera que, presentado estos argumentos, este estudio, hace posible un análisis exploratorio de los aspectos de seguridad de redes como material suplementario para la auditoría basadas en las normas y estándares (ISACA, 2014; Sizemore et al., 2013). Por lo tanto, los resultados obtenidos manifiestan la validez y fiabilidad del instrumento propuesto para evaluar la seguridad de redes en los dispositivos de borde, desde un escenario en particular, de manera secuencial y ordenada que facilitan el proceso de auditoría.

Tabla 11
Resultados Teoría G aspectos organizativos de la seguridad de la información

Estudio de Optimización Teoría G			OP 1		OP 2		OP 3		OP 4		OP 5	
Facetas	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**
U	3	11	4	11	5	11	7	11	9	11	11	11
I	7	INF	7	INF	7	INF	7	INF	7	INF	7	INF
A	4	INF	4	INF	4	INF	4	INF	4	INF	4	INF
Observaciones	84		112		140		196		252		308	
ρ	**0**		**0**		**0**		**0**		**0**		**0**	

Tabla 12
Resultados Teoría G control de accesos

Estudio de Optimización Teoría G			OP 1		OP 2		OP 3		OP 4		OP 5	
Facetas	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**
U	3	11	4	11	5	11	7	11	9	11	11	11
I	17	INF	17	INF	17	INF	17	INF	17	INF	17	INF
A	4	INF	4	INF	4	INF	4	INF	4	INF	4	INF
Observaciones	204		272		340		476		612		748	
ρ	**0**		**0**		**0**		**0**		**0**		**0**	

Tabla 13
Resultados Teoría G seguridad ambiental y física

Estudio de Optimización Teoría G			OP 1		OP 2		OP 3		OP 4		OP 5	
Facetas	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**
U	3	11	4	11	5	11	7	11	9	11	11	11
I	6	INF	6	INF	6	INF	6	INF	6	INF	6	INF
A	4	INF	4	INF	4	INF	4	INF	4	INF	4	INF
Observaciones	72		96		120		168		216		264	
ρ	**0**		**0**		**0**		**0**		**0**		**0**	

Tabla 14
Resultados Teoría G seguridad operativa

Estudio de Optimización Teoría G			OP 1		OP 2		OP 3		OP 4		OP 5	
Facetas	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**
U	3	11	4	11	5	11	7	11	9	11	11	11
I	18	INF	18	INF	18	INF	18	INF	18	INF	18	INF
A	4	INF	4	INF	4	INF	4	INF	4	INF	4	INF
Observaciones	216		288		360		504		648		792	
ρ	**0**		**0**		**0**		**0**		**0**		**0**	

Tabla 15
Resultados Teoría G seguridad telecomunicaciones

Estudio de Optimización Teoría G			OP 1		OP 2		OP 3		OP 4		OP 5	
Facetas	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**	**NI**	**UNI**
U	3	11	4	11	5	11	7	11	9	11	11	11
I	20	INF	20	INF	20	INF	20	INF	20	INF	20	INF
A	4	INF	4	INF	4	INF	4	INF	4	INF	4	INF
Observaciones	240		320		400		560		720		880	
ρ	**0**		**0**		**0**		**0**		**0**		**0**	

Nota: U: Unidad de Negocio; I: Item; A: Auditor; ρ: Coeficiente G; NI: Nivel; UN: Universo; OP: Opción.

CONCLUSIONES

En el presente estudio, se realiza la validez de una rúbrica para auditorías de seguridad de redes, aplicado a los dispositivos de borde dentro del contexto de una entidad pública. Para cumplir con el objetivo de la investigación, se crea una escala de Likert con base en los controles de seguridad de ISO27002:2013 y NIST 800-53ª r5, luego se realiza juicio de expertos para validar el contenido y finalmente, se aplica la Teoría G para demostrar la fiabilidad del instrumento.

Por otra parte, de acuerdo con lo mencionado en la introducción de este artículo Sahibudin, Sharifi, y Ayat (2008); Pardo, Pino, Garcia, Baldassarre y Piattini (2013); (Sizemore et al., 2013), expresan que se observa una variedad de normas, modelos e instrumentos que pueden ser usados para las auditorías de seguridad. En este contexto, la principal herramienta para evaluar la seguridad de la información son los cuestionarios con base en las normas a evaluar, no obstante, estos no evidencian un proceso de validez de contenido y no demuestran la fiabilidad de los resultados del instrumento (Bandopadhyay et al., 2011; Huijben, 2014; Karabacak y Sogukpinar, 2006).

En este sentido, el área de seguridad de la información necesita profundizar los estudios en relación a la protección de la CID de la información en los dispositivos de borde para mejorar y alcanzar el nivel esperado en el diseño y la implementación de los CS. Frente a la importancia de mantener los SI seguros, este proyecto sirve como guía exploratoria dentro del proceso de auditoría de redes; Como resultado, la rúbrica muestra un modelo adaptado al contexto organizacional y es una referencia para el resto de las UN que conforman esta organización, creando un aporte diferenciador dentro de la gestión de TIC, auditoría y la seguridad de la información.

En cuanto, a la aplicación de juicios de expertos y los resultados obtenidos en el estudio de la generalizabilidad, han sido un aporte significativo y diferenciador a la elaboración del modelo donde se afirma la validez y fiabilidad del instrumento. Por ello, dentro del escenario planteado se puede generalizar el instrumento para todas las UN de la institución. Por lo consiguiente, se podría establecer como marco de trabajo desde la perspectiva de la metodología empleada, porque se evidencia la validez de contenido y la fiabilidad del modelo.

En lo que refiere, a limitantes, el alcance del estudio, proporciona un diagnostico exploratorio de la seguridad de la información en el firewall, sin embargo, acorde con Jackson (2010), estos resultados podrían ser un punto de partida para una auditoría técnica, como las pruebas de penetración, donde se mida la eficacia operativa del CS. Otro punto, se basa en la generalización del instrumento a través de las cláusulas seleccionadas; en donde el análisis del estudio de la Teoría G se debió considerar sobre los datos globales de estas cláusulas y no de manera específica, obligado por la diferencia en la sumatoria de ítems por cada cláusula; lo cual se determina como una limitante de la técnica.

En lo que respecta, a trabajos futuros, se plantea la ejecución del instrumento en las Unidades de Negocio restantes, con 7 auditores adicionales para ejecutar el mismo proceso, realizar el análisis respectivo y contrastar los resultados obtenidos en el plan de optimización de la Teoría G. Además, se podría aplicar la rúbrica en otra institución de similares características y con los resultados obtenidos analizar la fiabilidad. Por consiguiente, el instrumento genera un escenario para futuras investigaciones que servirán de ayuda a las partes interesadas; como aplicar el mismo procedimiento a un nivel más técnico y profundo en la seguridad de redes, como las pruebas de penetración, evaluar la eficacia operativa de los controles de seguridad, que servirían para dar un diagnóstico de las vulnerabilidades de los dispositivos de red y el funcionamiento de los controles de seguridad.

Para finalizar, el estudio expuesto se presenta como una alternativa que aporta al desarrollo del conocimiento en el área de la auditoría de seguridad de redes, brindando la oportunidad de proporcionar mayor confiabilidad para la obtención de los resultados y luego para el análisis de los mismos mediante el instrumento planteado.

BIBLIOGRAFÍA

Alberts, C. J., & Dorofee, A. J. (2003). *Managing information security risks : the OCTAVE approach*.

Alhomoud, A., Munir, R., Disso, J. P., Awan, I., & Al-Dhelaan, A. (2011). Performance evaluation study of Intrusion Detection Systems. *Procedia Computer Science*, *5*, 173–180. https://doi.org/10.1016/j.procs.2011.07.024

Bandopadhyay, S., Sengupta, A., & Mazumdar, C.

(2011). A Quantitative Methodology for Information Security Control Gap Analysis. *Proceedings of the 2011 International Conference on Communication, Computing & Security*, 537–540. https://doi.org/10.1145/1947940.1948051

Bellovin, S. (2008). Security by checklist. *IEEE Security and Privacy*, *6*(2), 88. https://doi.org/10.1109/MSP.2008.43

Blanco-Villaseñor, A., Castellano, J., Hernandez-Mendo, A., Sanchez-Lopez, C. R., & Usabiaga, O. (2014). Generalizabilidad y Gestión Deportiva Generalizability and Sports Management Generabilidade e gestão desportiva. *Servicio de Publicaciones de Universidad de Murcia*, *23*(1), 131–137.

Bodeau, D., & Graubart, R. (2013). Cyber Resiliency and NIST Special Publication 800-53 Rev . 4 Controls. *MITRE TECHNICAL REPORT MTR130531*, (September), 45.

Briesch, A., Chafouleas, S., & Riley-Tillman, C. (2010). Generalizability and dependability of behavior assessment methods to estimate academic engagement: A comparison of systematic direct observation and direct behavior rating. *School Psychology Review*, *39*(3), 408–421.

Cardinet, J., Johnson, S., & Pini, G. (2010). *Applying Generalizability Theory using Edug*. New York.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125–128. https://doi.org/10.1145/341852.341877

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *4*(2), 92–100. https://doi.org/10.4236/jis.2013.42011

Duncan, B., & Whittington, M. (2014). Compliance with standards, assurance and audit. *Proceedings of the 7th International Conference on Security of Information and Networks - SIN '14*, 77–84. https://doi.org/10.1145/2659651.2659711

Escobar-Pérez, J., & Cuervo-Martínez, Á. (2008). Validez De Contenido Y Juicio De Expertos: Una Aproximación a Su Utilización. *Avances En Medición*, *6*(September), 27–36.

ESET. (2016). Eset Security Report Latinoamérica 2016. *Eset Security Report Latinoamérica 2016*, *1*, 20.

ESET. (2017). Eset Security Report Latinoamérica 2017. *Eset Security Report Latinoamérica 2017*, 20.

Gossels, J., & Mackey, R. (2007). The Global Voice of Information Security ISO 2700X: A cornerstone of true security. *ISSA Journal*, (April), 33–35.

Granneman, J. (2013). IT security frameworks and standards: Choosing the right one. Retrieved November 28, 2017, from http://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

Hayes, B. (2003). Conducting a Security Audit: An Introductory Overview. Retrieved from https://www.symantec.com/connect/articles/conducting-security-audit-introductory-overview

Herzog, P. (2010). OSSTMM: The Open Source Security Testing Methodology Manual: v3. *Isecom*, 213. Retrieved from http://www.isecom.org/mirror/OSSTMM.3.pdf

Huijben, K. (2014). A lightweight, flexible evaluation framework to measure the ISO 27002 information security controls, 1–66. https://doi.org/10.4172/2168-9695.1000e118

ISACA. (2014). ITAF A Profesional Practice Framework for IS Audit/Assurance. *ITAF*, (3 edition), 181. Retrieved from www.isaca.org

ISO/IEC. (2016). ISO/IEC 27000:2016(E) Information technology — Security techniques — Information security management systems — Overview and vocabulary. *ISO.org [Online]*, *4th Editio*, 42. Retrieved from http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip

ISO/IEC:27001. (2013). ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements. *ISO.org [Online]*, *2nd Editio*, 23.

ISO/IEC:27002. (2013). ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. *ISO.org [Online]*, *2nd Editio*, 90. Retrieved from www.iso.org

Jackson, C. (2010). *Network Security Auditing*. *Cisco Press*. Indianapolis, IN, USA. https://doi.org/10.4018/978-1-60960-777-7.ch008

Karabacak, B., & Sogukpinar, I. (2006). A quantitative method for ISO 17799 gap analysis. *Computers and Security*, *25*(6), 413–419. https://doi.org/10.1016/j.cose.2006.05.001

Kayrak, M. (2014a). Information Technology Audit and The Practice of The Turkish Court of Accounts. *Alphanumeric Journal*, *2*(1).

Larraz, N., Allueva, P., & Blanco-Villaseñor, A. (2014). Estimación de la precisión de un programa educativo mediante la Teoría de la Generalizabilidad. *Revista Interamericana de Psicología*, *48*(1), 64–70.

Lo, E., & Marchand, M. (2004). Security audit: a case study. *Electrical and Computer Engineering, …*, 193–196. https://doi.org/10.1109/CCECE.2004.1344989

Mendo, A. H., Martínez, F. D., & Morales, V. (2010). Herramienta Observacional Para

Evaluar Las Clases De Educación Física 1. *Revista De Psicologia Del Deporte*, *19*(June 2010), 305–318.

Mendoza, M. A. (2017). Challenges and implications of cybersecurity legislation. *Trends 2017: Security Held Ransom*, 43–47. Retrieved from https://trends.fjordnet.com/trends/

NIST. (2014). Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations. *Sp-800-53Ar5*, 400+. https://doi.org/10.6028/NIST.SP.800-53Ar4

Onwubiko, C. (2009). A Security Audit Framework for Security Management in the Enterprise. In *Global Security, Safety, and Sustainability* (pp. 9–17).

Onwubiko, C., & Lenaghan, A. P. (2007). Managing Security Threats and Vulnerabilities for Small to Medium Enterprises. *2007 IEEE Intelligence and Security Informatics*, 244–249. https://doi.org/10.1109/ISI.2007.379479

Pan, Y., Yuan, B., & Mishra, S. (2011). *Network Security Auditing*. *Network Security, Administration and Management: Advancing Technology and Practice*. https://doi.org/10.4018/978-1-60960-777-7.ch008

Pardo, C., Pino, F. J., Garcia, F., Baldassarre, M. T., & Piattini, M. (2013). From chaos to the systematic harmonization of multiple reference models: A harmonization framework applied in two case studies. *Journal of Systems and Software*, *86*(1), 125–143. https://doi.org/10.1016/j.jss.2012.07.072

Ross, R., Viscuso, P., Guissanie, G., Dempsey, K., & Riddle, M. (2015). Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. *NIST Special Publication 800-171*, 1–76. https://doi.org/10.1613/jair.301

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. *Proceedings - 2nd Asia International Conference on Modelling and Simulation, AMS 2008*, 749–753. https://doi.org/10.1109/AMS.2008.145

Shen, L. (2014). The Nist Cybersecurity Framework Overview and Potential Impacts. *ThesciTechLawyer*, *10*(4), 16–19.

Sheth, C., & Thakker, R. (2011). Performance evaluation and comparative analysis of network firewalls. *Devices and Communications (ICDeCom), 2011 International Conference on*, 1–5.

Sizemore, S., Nigel, C., Franke, R., & Kalyanaramani, M. (2013). IS Audit and Assurance Standard 1206 Using the Work of Other Experts.

Sizemore, S., Nigel, C., Franke, R., Mackenzie, A., Namuduri, K., Sakagawa, K., … Smith, T. (2014). IS Audit and Assurance Guideline 2206 Using the Work of Other Experts. *ITAF*.

SNAP. (2013). Acuerdo MInisterial 166 - Esquema gubernamental de seguridad de la informacion EGSI, 1–47.

Todd J. Fitzgerald. (2017). Auditing Cyber Security: Evaluating Risk and Auditing Controls. *Isaca*, 15. Retrieved from https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Auditing-Cyber-Security.aspx

Zhang, T., Lin, W., Wang, Y., Deng, S., Shi, C., & Chen, L. (2010). The design of information security protection framework to support Smart Grid. *2010 International Conference on Power System Technology*, 1–5. https://doi.org/10.1109/POWERCON.2010.5666681

APENDICE A. Diseño del instrumento para la revisión de seguridad de redes

N°	ITEM
1	SF01. Se evidencia que las tareas y las áreas de responsabilidad de acceso están separados
2	SF02. Se evidencia que no existen modificaciones no autorizadas o uso indebido de las configuraciones del firewall
3	TT01. Se evidencia la autorización de los accesos remotos a los SI antes de permitir las conexiones
4	TT02. Se evidencia la monitorización y control de los métodos de accesos remotos a través del firewall a las redes internas de la compañía
5	TT03. Se evidencia el uso de mecanismos de cifrado para proteger los accesos remotos a través del firewall a las redes internas de la compañía
6	TT04. Se evidencia que todos los accesos remotos se enrutan por medio del firewall a las redes internas de la compañía
7	TT05. Se incluye en los inicios de sesión de los usuarios del firewall deshabilitar/desactivar/desconectar cuando no se evidencia actividad durante un período de tiempo establecido por la compañía
8	AR01. Se evidencia documentación y la definición de los tipos de usuarios para el firewall alineados a los objetivos y funciones de la compañía
9	AR02. Se evidencia la aprobación por parte del personal autorizado de la compañía para la creación de cuentas de usuarios en el firewall
10	AR03. Se evidencia la monitorización de las cuentas de usuario del firewall
11	AR04. Se evidencia el cumplimiento de los perfiles de usuarios asignados al firewall
12	RC01. Se evidencia en el firewall [desactivación/retiro] automático de las cuentas de usuarios [temporales/emergencia] durante los períodos de tiempos establecidos por la compañía para cada tipo de cuenta
13	RC02. Se evidencia en el firewall la desactivación automática de las cuentas de usuarios cuando su período de tiempo establecido por la compañía ha expirado
14	RC03. Se evidencia en el firewall la desactivación automática de las cuentas de usuarios cuando no están asociadas a un empleado de la compañía
15	RC04. Se evidencia en el firewall la desactivación automática de las cuentas de usuarios si infringe el cumplimiento de una política de la compañía
16	RC05. Se evidencia en el firewall la desactivación automática de las cuentas de usuarios cuando ya no están siendo utilizadas por ningún empleado de la compañía
17	RC06. Se evidencia en el firewall la desactivación automática de las cuentas de usuarios cuando las cuentas han estado inactivas por un período de tiempo definido por la compañía
18	GD01. Se evidencia en el firewall la administración de las cuentas de usuarios privilegiados de acuerdo a un esquema basado en roles que organiza el acceso al firewall y los privilegios permitidos en los roles
19	GD02. Se demuestra la prohibición de los accesos privilegiados a los usuarios externos (proveedores) en el firewall
20	GD03. Se evidencia la validación de los privilegios asignados a las cuentas de los usuarios del firewall en la frecuencia establecida por la compañía
21	RD01. Se demuestra supervisión de las asignaciones de roles privilegiados a las cuentas de los usuarios en el firewall
22	PR01. Se demuestra el cumplimiento de un número límite de intentos inválidos/fallidos consecutivos de inicio de sesión por parte de un usuario del firewall durante un período de tiempo definido por la compañía
23	PR02. Se evidencia en el firewall el bloqueo automático de una cuenta de usuario [durante un período definido por la compañía/hasta que sea liberado por un usuario administrador] cuando se exceda el número máximo de intentos
24	PR03. Se retrasa el próximo inicio de sesión [por un algoritmo de retraso/una acción] definida por la compañía cuando se exceda el número máximo de intentos
25	ME01. Se evidencia la programación de los mantenimientos, reparación o reemplazo de los componentes del firewall de acuerdo con las especificaciones del [fabricante/proveedor/requisitos de la compañía]

N°	ITEM
26	ME02. Se evidencia la documentación de los mantenimientos, reparación o reemplazo de los componentes del firewall de acuerdo con las especificaciones del [fabricante/proveedor/requisitos de la compañía]
27	ME03. Se evidencia la revisión de los registros de los mantenimientos, reparación o reemplazo de los componentes del firewall de acuerdo con las especificaciones del [fabricante/proveedor/requisitos de la compañía]
28	ME04. Luego de aprobar los mantenimientos del firewall, se evidencia la monitorización de las actividades de mantenimiento realizadas en situ o de forma remota
29	ME05. Luego de aprobar los mantenimientos del firewall, se evidencia si las reparaciones de los componentes se realizan en situ o se retiran a otra ubicación
30	ME06. Se da seguimiento que todos los controles de seguridad y privacidad potencialmente impactados para verificar que los controles sigan funcionando correctamente después de las acciones de mantenimiento, reparación o reemplazo del firewall
31	GC01. Se evidencia los tipos de cambios en el firewall de la gestión de control de cambios definidos por la compañía
32	GC02. Se evidencia la revisión de las propuestas de cambios controlados por configuración para aprobación/desaprobación de tales cambios teniendo en consideración explicita el análisis de impacto de seguridad para el firewall
33	GC03. Se evidencia la implementación de cambios controlados por configuración aprobados en el firewall
34	GC04. Se evidencia el resguardo de los registros de los cambios controlados por configuraciones en el firewall por un período de tiempo definido por la compañía
35	CG01. Se evidencia el envio de alertas todo el tiempo al personal responsable de la administración del firewall cuando ocurren eventos de fallas de auditoria definidos por la compañía.
36	CG02. Se evidencia los límites de la segmentación del ancho de banda de los tráficos de comunicación de redes y el rechazo/retraso este trafico de red cuando sobrepasan los límites definidos por la compañía en el firewall
37	CC01. Se monitoriza en el firewall el trafico de comunicaciones de red entrantes y salientes durante un tiempo definido por la compañía para actividades o condiciones inusuales o no autorizadas (IDS).
38	CC02. Se evidencia el análisis del trafico de comunicaciones entre el firewall y puntos interiores definidos por la compañía para descubrir anomalías (IDS)
39	CC03. Se evidencia el análisis del trafico de comunicaciones y los patrones de eventos en el firewall
40	RG01. Se demuestra que los registros de auditoria contienen información que establezca que tipo de evento ocurrió, cuando ocurrió, donde ocurrió, el origen del evento, el resultado del evento y el identificador que generó el evento en el firewall
41	SC01. Se comprueba la sincronización del reloj interno del firewall con la fuente de tiempo autorizada por la compañía
42	GV01. Se evidencia la aplicación de técnicas y herramientas de análisis de vulnerabilidad en el firewall para que faciliten la interoperabilidad entre herramientas para la gestión de vulnerabilidades
43	GV02. Se evidencia la aplicación de técnicas, herramientas y/o uso de estándares en el firewall para enumeración de plataformas, fallas de software y configuraciones incorrectas
44	GV03. Se evidencia la aplicación de técnicas, herramientas y/o uso de estándares en el firewall para los formatos de verificación y procedimientos de prueba
45	GV04. Se evidencia la aplicación de técnicas, herramientas y/o uso de estándares en el firewall para medir el impacto de la vulnerabilidad
46	GV05. Se evidencia la corrección de las vulnerabilidades en el firewall durante los tiempos de respuesta definidos por la compañía de acuerdo con una evaluación de riesgo
47	GV06. Se evidencia el registro de pruebas o ambiente de pruebas para probar las actualizaciones de software y firmware con la corrección de fallas para el firewall para determinar la efectividad y los posibles efectos secundarios
48	GV07. Se evidencia la instalación de las actualizaciones de firmware y software relevantes para la seguridad del firewall dentro del período de tiempo definido por la compañía luego del lanzamiento de las actualizaciones
49	CR01. Se evidencia la monitorización y control de las comunicaciones en el firewall y en las redes importantes de la compañía
50	CR02. Se evidencia en el firewall conexiones a redes externas a través de interfaces gestionadas previstas de acuerdos con una arquitectura de privacidad y seguridad

N°	ITEM
51	CR03. Se evidencia en el firewall la implementación de interfaces gestionadas para cada servicio de telecomunicación externo
52	CR04. Se constata políticas/reglas de calidad de servicio para cada interfaz administrada en el firewall
53	CR05. Se resguarda la confidencialidad e integridad de la información que se transmite a través de cada interfaz en el firewall
54	CR06. Se evidencia política/regla en el firewall de denegación por defecto y permisión por excepción de las comunicaciones de red en las interfaces gestionadas
55	CR07. Se evidencia el enrutamiento del trafico de comunicación interno a redes externas a través del firewall en las interfaces gestionadas
56	CR08. Se constata en el firewall la detección y negación del trafico de comunicaciones salientes que pueden ser una amenaza para las redes internas de la compañía
57	CR09. Se constata en el firewall la permisión de la comunicaciones entrantes de fuentes autorizadas por la compañía se enruten a destinos autorizados definidos por la compañía
58	CR10. Se demuestra en el firewall el enrutamiento de todos los accesos privilegiados en red a través de una interface dedicada y administrada con fines de control de acceso y auditoria.
59	CR11. Se evidencia el impedimento de descubrimiento de componentes específicos del firewall de una interfaz gestionada
60	CR12. Existe constancia en el firewall de la implementación de direcciones de red independientes para conectarse a sistemas de información en diferentes dominios de seguridad
61	CR13. Se constata en el firewall la implementación de mecanismos criptográficos para impedir la divulgación no autorizada de información/detectar cambios en la información durante la transmisión
62	MS01. Se constata las autorizaciones de las conexiones desde el firewall a otros sistemas que utilicen acuerdos de seguridad de interconexión
63	MS02. Se evidencia la conexión directa de una red interna de la compañía a una red publica sin pasar por el firewall
64	MS03. Se evidencia en el firewall una política/regla de denegación de permisos, permiso por excepción para permitir que las redes de la compañía se conecten a redes externas o publicas
65	MS04. Se evidencia que los proveedores de servicios de comunicación (enlaces/internet) cumplan con los requisitos de privacidad y que empleen los controles de seguridad y privacidad definidas por la compañía
66	SR01. Se demuestra la segregación de las subredes de acceso publico (invitados) de las subredes de la compañía en el firewall
67	SR02. Se comprueba la denegación del trafico de red por defecto y se permite el trafico de red por excepción en las interfaces gestionadas del firewall
68	SR03. Se evidencia en el firewall la protección contra conexiones físicas no autorizadas en las interfaces gestionadas por la compañía.

APENDICE B. Mapeo de los controles de las normas

ISO27002:2013	NIST 800-53 R5								
CONTROL	INSTRUCCIÓN								
A.6.1.2	***AC-5**								
A.6.2.2	AC-3	***AC-17**	PE-17						
A.9.1.1	***AC-1**								
A.9.1.2	AC-2	AC-3	***AC-6**						
A.9.2.1	***AC-2**	***IA-2**	***IA-4**	***IA-5**	IA-8				
A.9.2.2	***AC-2**								
A.9.2.3	***AC-2**	AC-3	***AC-6**	CM-5					
A.9.2.4	IA-5								
A.9.2.5	***AC-2**								
A.9.2.6	***AC-2**	***PS-4**	PS-5						
A.9.3.1	IA-5								
A.9.4.1	AC-3	AC-24							
A.9.4.2	AC-7	AC-8	AC-9	IA-6					
A.9.4.3	IA-5								
A.9.4.4	AC-3	***AC-6**							
A.11.1.1	PE-3								
A.11.1.2	***PE-2**	PE-3	PE-4	PE-5					
A.11.1.4	CP-6	CP-7	PE-9	PE-13	***PE-14**	***PE-15**	PE-18	PE-19	PE-21
A.11.1.6	***PE-16**								
A.11.2.3	***PE-4**	PE-9							
A.13.1.1	***AC-3**	AC-17	AC-18	AC-20	***SC-7**	***SC-8**	SC-10		
A.13.1.2	***CA-3**	***SA-9**							
A.13.1.3	AC-4	***SC-7**							
A.13.2.1	AC-4	AC-20	AC-21	CA-3	PA-4	SC-7	SC-8		
A.13.2.2	AC-21	CA-3	PA-4	***PS-6**	SA-9				
A.13.2.3	SC-8								
A.13.2.4	PS-6								

Nota: Los controles de seguridad marcado con asterisco (*) es lo que se confirmó con la actualización de la NIST.
Los controles de seguridad que se añadieron están sin marcar.