Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio

Cristian Bracho-Ortega[1], Fabián Cuzme-Rodríguez[1], Carlos Pupiales-Yepez[1], Luis Suárez-Zambrano[1], Diego Peluffo-Ordoñez[1], César Moreira-Zambrano[2]

[1] Carrera de Ingeniería en Electrónica y Redes de Comunicación, Universidad Técnica del Norte, Av. 17 de Julio 5-21 y Gral. José María Córdova, Ibarra, Ecuador, código postal 100105.

[2] Departamento de Data Center, Escuela Superior Politécnica Agropecuaria de Manabí MFL, Sitio Limón Km 3/2 vía Tosagua, Calceta, Ecuador, código postal 130250.

Autores para correspondencia: {clbrachoo, fgcuzme, chpupiales, lesuarez, dhpeluffo}@utn.edu.ec, cmoreira@espam.edu.ec

Fecha de recepción: 16 de mayo de 2017 - Fecha de aceptación: 12 de julio 2017

RESUMEN

Este artículo explica la metodología utilizada en una auditoría de seguridad informática, tomando como referencia las recomendaciones de la metodología OSSTMM versión 3 que engloba 5 canales fundamentales. Para la comprensión de su aplicabilidad en un entorno práctico, se tomó como caso de estudio al Gobierno Autónomo Descentralizado del Cantón Mira. La metodología permite medir la seguridad actual de cinco canales diferentes, los mismos que son: humano, físico, comunicaciones inalámbricas, telecomunicaciones y de redes de datos. Del mismo modo, se consideran tres medidas importantes para el cálculo de cada canal: la porosidad (OpSec), los controles y las limitaciones. Los resultados finales, una vez realizado el análisis pertinente, permiten determinar los valores numéricos de cada uno de estos ítems, siendo necesario acogerse a las recomendaciones de los tipos de pruebas que la metodología recomienda para su cálculo. Una vez aplicada la metodología, esto ayuda a comprender, en cada ámbito de aplicación, las deficiencias o excesos de los controles operacionales de seguridad que se manejan en una empresa u organización. Esto constituye un punto importante para controlar las vulnerabilidades que se detecten internamente y poder solucionarlas en su debido momento.

Palabras clave: OSTMM, porosidad, controles, limitaciones, canales, auditoria, seguridad.

ABSTRACT

This article explains the methodology followed in computing auditing in terms of security where OSSTMM version 3 was taken as reference methodology and implemented in GAD-Mira. The current methodology allows to measure the security aspects of five different channels such as human, physical, wireless communications, telecommunications, and networking. At the same time, it includes porosity (OpSec), controls, and limitations as three important measures in each channel which allow to calculate and get the numerical values that explain the importance and influence of each item in the computing audit. Additionally, results obtained after the application of the described methodology allowed to understand deficiencies or excesses in terms of security controls that exist in a company or organization in each channel, being an important point to analyze the internal vulnerabilities that need to be solved.

Keywords: OSSTMM, porosity, controls, limitations, channels, audit, security.

1. INTRODUCCIÓN

En la sociedad actual, la administración de la justicia se ha visto profundamente transformada con la aparición de las nuevas tecnologías de la información y comunicación (TICs). Las omnipresentes computadoras, interconectadas en la red mundial llamada Internet, son el signo más evidente del impacto que tienen hoy. En base a una publicación de la revista *La Verdad*, se asegura que, para las telecomunicaciones, el tráfico comercial y el entretenimiento, estás tecnologías son prácticamente indispensables (Chiluiza, 2015). Sin la ayuda de esta valiosísima herramienta, en la actualidad es prácticamente imposible alcanzar resultados económicos aceptables y beneficiosos, tanto como para la administración en particular, como para la administración de la justicia en la sociedad en general. Por esto, este principio es perfectamente aplicable al sistema judicial ecuatoriano, que, para poder cumplir con su función de administrar la justicia, debe tratar con información en cantidades ascendentes.

De los casos suscitados en Ecuador en cuanto a delitos informáticos, de enero a diciembre del 2010, se recibieron más de 866 denuncias en diferentes fiscalías del país por delitos tradicionales cometidos por, y con, mecanismos informáticos. De estos, 697 fueron debidos a apropiación ilícita; 86 fueron denuncias propiamente de delito informático, como vulneración a páginas de servicio público; 82 fueron debidas a páginas de servicio privado; y, 1 por estafa utilizando medios informáticos (Cuenca Espinosa, 2012).

A partir del año 2010 se presenta un importante crecimiento en el porcentaje de casos reportados por este tipo de delitos. El más importante ocurrió en el año 2015, cuando *cyber* atacantes accedieron a equipos informáticos de 17 firmas privadas e instituciones públicas de Quito, Guayaquil y Cuenca. En los últimos cuatro años, entre los sitios web atacados, se encuentran el de la Policía Nacional, de los Gobiernos Autónomos Descentralizados Municipales de Chone (Manabí), Durán (Guayas), Baños (Tungurahua) y varios de la Provincia de Chimborazo, a esto se suman *cyber* ataques dirigidos a las páginas web de la Asamblea Nacional, cuerpo de Bomberos de diferentes ciudades, Casa de la Cultura, Ministerios: del Ambiente, Transporte y Obras Públicas, Desarrollo Urbano, Finanzas Producción, entre otros (Bravo, 2015).

Cabe señalar que, de acuerdo con un estudio realizado por GMS y Kaspersky, los delitos informáticos en Ecuador crecieron en un 360% en 2010, en comparación con 2009, dejando una pérdida aproximada de un millón de dólares. Estas estadísticas guardan relación con los reportes de la Fiscalía General del Estado, que indican que, solo en los tres primeros meses del año 2011, se han denunciado 1,308 delitos informáticos entre enero y diciembre del 2011. Esta cifra se incrementó considerablemente para año 2012, llegándose a receptar 3,662 denuncias de este tipo de delitos (Cuenca Espinosa, 2012).

1.1. Seguridad Informática

Es común hablar de seguridad informática y de seguridad de la información, como si fueran el mismo término y, a primera vista, parecería ser. Sobre todo si se tiene en cuenta que, en la actualidad, gracias al constante desarrollo tecnológico, se tiende a digitalizar todo tipo de información y a manejarla a través de un sistema informático. Sin embargo, aunque se tenga la necesidad de trabajar en armonía, cada uno de estos aspectos tiene objetivos y actividades diferentes.

Por seguridad informática se entiende al conjunto de políticas, reglas, estándares, métodos y protocolos que se utilizan para la protección de la infraestructura de computadoras y toda la información contenida o administrada por ella (Toth, 2014). No solo se debe prestar atención a los ataques intencionales, sino también a posibles fallas de software o hardware que atenten contra la seguridad, tratando de minimizar los riesgos asociados al acceso y utilización de un determinado sistema de forma no autorizada o malintencionada, para revelar, utilizar, modificar o destruir accidental o intencionalmente la información que en este se encuentre. Para ello, se deben evaluar y cuantificar los bienes a proteger, y en función de este análisis, implantar medidas preventivas y correctivas que eliminen o reduzcan los riegos asociados hasta niveles manejables.

Por otra parte, seguridad de la información se refiere a todas aquellas medidas que procuren resguardar la información ante cualquier irregularidad. La principal diferencia, entre seguridad informática y seguridad de la información, es que la primera se encarga de la seguridad en un medio informático y la segunda se interesa en la información en general, pudiendo ésta estar almacenada tanto en un medio informático como en cualquier otro. Por ejemplo, un manual de procedimientos escrito en

papel, el conocimiento que poseen las personas, escrituras en pizarras y papeles que se descartan, son fuentes importantes de información (Toth, 2014).

1.2. Auditoria de seguridad informática

Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información es el estudio que comprende el análisis y gestión de los sistemas informáticos, realizado por una persona o grupo de personas, denominados auditores, que pueden ser del propio personal o ajeno a la organización; para identificar y posteriormente corregir las diversas vulnerabilidades que se pudieran presentar en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores (Costas Santos, 2010).

Las auditorias de seguridad informática, en el momento de su realización, permiten conocer cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad operacional, y así mejorar la rentabilidad y la eficacia del sistema, mediante la exposición de las debilidades y disfunciones que se van encontrando en el proceso, para luego levantar un informe final donde se indica los planes de acción para eliminar dichas falencias, a modo de recomendaciones (Costas Santos, 2010).

Para elegir un tipo de prueba adecuado, lo mejor es entender primero cómo sus módulos están diseñados para trabajar. Dependiendo de la minuciosidad, negocio, asignación de tiempo y los requisitos de la auditoría, el analista puede programar los detalles de la misma, realizada por fases. En la metodología OSSTMM, versión 3, hay cuatro fases en su ejecución: Fase de Inducción, de Interacción, de Indagación y de Intervención (Herzog, 2010).

Fase de Inducción

En esta fase, el analista comienza la auditoría entendiendo los requisitos, el alcance y las limitaciones de la misma en dicho alcance. A menudo, el tipo de prueba se determina mejor después de esta fase (Herzog, 2010).

Fase de interacción

Para que la auditoría de seguridad se desarrolle correctamente, será necesario elaborar un plan de auditoría. El objetivo de esta planificación es la recopilación de información de la organización y de sus sistemas informáticos, para obtener una información global del área a auditar. La recopilación de información se deberá realizar a través de observaciones, entrevistas con los agentes que interactúan con el sistema y con la solicitud de documentos e información a los responsables de la organización. Con esto, el auditor ya será capaz de definir concretamente el objetivo general del estudio, el alcance que la auditoría deberá tener y el programa desarrollado de las tareas de auditoría (Chicano Tejada, 2014).

Fase de indagación

La fase de indagación consiste en la realización de una serie de pruebas cuyos resultados permitan detectar debilidades y fortalezas del sistema de información auditado y justifiquen la detección de las evidencias (Chicano Tejada, 2014).

Fase de intervención

Estas pruebas se centran en los recursos de los objetivos requeridos en la aplicación, mismos que se pueden intercambiar, cambiar, sobrecargar, o morir a causa de la penetración o interrupción. Esto, a menudo constituye la fase final de una prueba de seguridad, para asegurar que las interrupciones no afecten a las respuestas de las pruebas menos invasivas y porque la información, para hacer estas pruebas, no puede ser conocida hasta que otras fases se han llevado a cabo (Herzog, 2010).

1.3. Legislación Ecuatoriana que regula los delitos informáticos

A pesar de que en el Ecuador no se tomaba en cuenta a los delitos informáticos en materia de jurisprudencia, en la legislación ecuatoriana actual se amparan leyes y decretos que establecen apartados

y especificaciones acordes con la importancia de la información y de las tecnologías, entre ellas se tienen:

- Ley orgánica de transparencia y acceso a la información pública.
- Ley de comercio electrónico, firmas electrónicas y mensajes de datos.
- Ley de propiedad intelectual.
- Ley especial de telecomunicaciones.
- Ley orgánica de garantías jurisdiccionales y control constitucional.
- Código Orgánico Integral Penal (COIP).

En base a declaraciones de (Acurio del Pino, 2012), los departamentos, tanto de la Fiscalía General del Estado como los de la Policía Judicial, sirven como puntos de contacto nacionales para una cooperación internacional formal o informal basada en redes transaccionales de confianza entre los agentes de aplicación de la Ley; lo cual es posible mediante la aplicación del artículo 226 de la Constitución y la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

La cooperación multinacional de grupos especiales multinacionales puede resultar particularmente útil; y, efectivamente, existen casos en que la cooperación internacional ha sido muy efectiva en la resolución de algún tipo particular de delito electrónico.

2. MATERIALES Y MÉTODOS

Para la aplicación de la metodología se plantea realizar un caso de estudio con la finalidad de demostrar la aplicabilidad de la misma.

2.1. Caso de estudio

En esta parte se hace una breve descripción de los principales datos de relevancia del Gobierno Autónomo Descentralizado del Cantón Mira (GADM-Mira), basándose en la información proporcionada por el funcionario a cargo del Área de Sistemas, quien se encarga de administrar toda la infraestructura de la red de datos la entidad, y visitas técnicas a las instalaciones físicas donde se encuentran los diferentes dispositivos de comunicaciones.

Red activa actual

La red LAN es de tipo Ethernet y posee una distribución topológica tipo árbol, como se aprecia en la Figura 1. Al momento de su implementación, se pensó en una red escalable en el tiempo, teniendo actualmente 75 puntos de red para computadoras de escritorio y portátiles.

Equipos de enrutamiento

El GADM-Mira no cuenta con un equipo propio de enrutamiento, mantiene un *router* proporcionado por la empresa proveedora de servicios de Internet, que más allá de brindar un protocolo de enrutamiento dinámico, sirve como salida hacia la Internet a los usuarios de la red LAN, mediante el uso de enrutamiento estático.

Enlace WAN

El GADM-Mira posee un contrato por concepto de servicios de Internet con la empresa CNT E.P. con un ancho de banda total de 13 Mbps simétricos, por medio de una conexión de Fibra Óptica *mono modo* sin *backup*, como se puede ver en la Figura 2. Para control del tráfico de red, tanto de entrada como de salida, desde y hacia la Internet se hace uso del servicio de *Firewall*.

Direccionamiento

El direccionamiento asignado para los equipos de comunicación, los ordenadores y/o dispositivos terminales del GADM-Mira hace uso de un direccionamiento clase C, teniendo así 254 direcciones IP

disponibles para *hosts*. Por el hecho de ser una red parcialmente pequeña, a la fecha, no se requiere más de 100 direcciones disponibles, pero sí se ha considerado un porcentaje de escalabilidad en el tiempo.

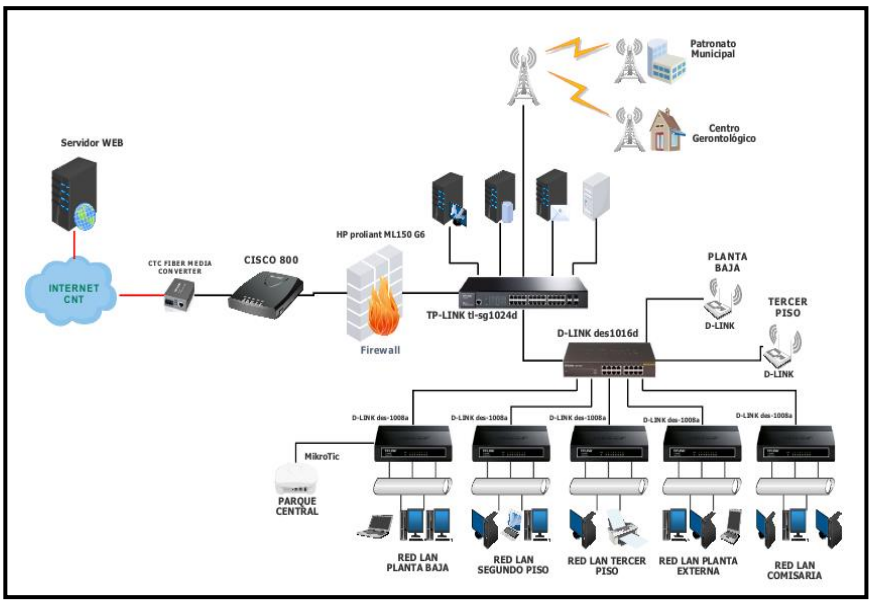


Figura. 1. Topología física de la red LAN del GADM-Mira.

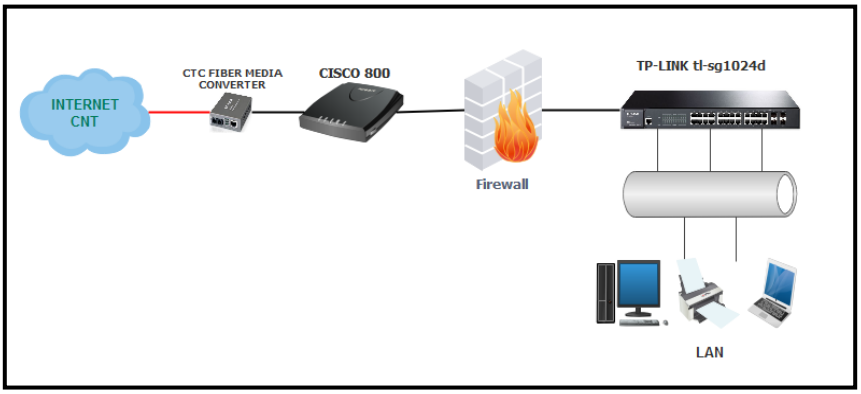


Figura. 2. Conexión hacia la Internet del GADM-Mira.

Equipos de conmutación

Los equipos de conmutación del GADM-Mira son no-administrables y se encuentran conectados en un orden jerárquico, basándose en el modelo de conexión en cascada que empieza por el *switch* de *core*; luego, al *switch* de distribución; y, finalmente, a los *switches* de acceso, como se mostró en la Figura 1. En caso de necesitar más puertos para las estaciones de trabajo, se deja un puerto libre en el *switch* de acceso y en este puerto se conecta otro *switch* de acceso, formando una cascada; y así se extiende la red, hasta que se logre satisfacer el número de estaciones de trabajo requeridas para cada planta del edificio.

Servidores

Básicamente el GADM-Mira hace uso de 5 servicios elementales como son: bases de datos, Internet, *Firewall proxy*, web y hosting para cuentas de correo electrónico. De estos, solo dos (bases de datos e Internet) se encuentran físicamente en el cuarto de telecomunicaciones. Los otros tres servicios son contratados a empresas privadas: *Firewall proxy* es un complemento al servicio de antivirus, prestado por la empresa ESET Smart Security, el de *servicios web* y *hosting* para cuentas de correo electrónico, son prestados por la empresa NIC.EC.

Enlaces inalámbricos

El GADM maneja dos enlaces principales, uno de radiofrecuencia, con su respectivo *back-up*, que se encuentra dirigido desde la terraza del edificio del GADM-Mira, hacia una pequeña torre de 5 m de altura que se articula en la terraza del edificio del ex Patronato Municipal. Este edificio fue seleccionado con la finalidad de aprovechar la elevación que tiene dicha infraestructura, en donde se puede repartir de mejor manera varios radioenlaces a diferentes instituciones y dependencias que forman parte de la jurisdicción administrativa de la institución, facilitando así su conexión al servicio de Internet.

El otro enlace que brinda el GADM-Mira es el que está dirigido a la ciudadanía de forma gratuita, ofreciendo el servicio de Internet gratuito o *Wi-Fi Zone* en el parque central de la cuidad.

Documentación

Como información tangible en documentos físicos el GADM-Mira posee la siguiente documentación, a la cual es posible acceder únicamente con el consentimiento del encargado del área de sistemas:

- Registro de direcciones IP
- Inventarios de los recursos informáticos
- Manual de uso del Internet
- Acuerdos de confidencialidad del uso de sistemas
- Diagramas topológicos de la red LAN cableada
- Diagramas topológicos de la red LAN inalámbrica
- Planos del cableado estructurado del edificio del GADM

2.2. Aplicación de la metodología

Es necesario indicar que el caso de estudio considerado para la aplicación de la presente metodología tiene la finalidad de obtener resultados reales de la aplicación de la misma. Sin embrago, se pueden seguir los pasos aquí descritos para adaptarla a cualquier ambiente organizacional, en el que se requiera obtener información importante de una auditoria de seguridad informática, y aplicable a todos los ámbitos de una organización.

En base a la metodología OSSTMM versión 3, se hace a continuación una breve descripción de 7 pasos que se deberían seguir para llevar a cabo una prueba de seguridad exitosa (Herzog, 2010):

1. Definir lo que se desea proteger, es decir los activos. Los mecanismos de protección de dichos activos son los *controles*, mismos que se probarán para identificar las *limitaciones.*
2. Identificar el área alrededor de los activos, en donde se deben incluir los mecanismos de protección y los procesos o servicios construidos en torno a los activos**.** Esto se conoce como la *zona de enfrentamiento*.
3. Definir todo fuera de la zona de enfrentamiento, esto es necesario para mantener a los activos operativos, tales como: electricidad, alimentos, agua, aire, suelo estable, información, legislación y reglamentos; y los ambientes y cosas con las que puede trabajar. Eso se conoce como el *alcance* de la prueba.
4. Definir cómo el alcance interactúa dentro de sí y con el exterior, para ello es necesario fraccionar los activos dentro del alcance, conforme la dirección de las interacciones tales como: del interior al exterior, del exterior al interior, en el interior para el interior, etc. Esto se conoce como los *vectores*. Idealmente, cada vector debería considerar una prueba separada con una duración corta, antes de que el ambiente de la prueba presente cambios notables.
5. Identificar los equipos que serán necesarios para cada prueba. Dentro de cada vector, las interacciones pueden ocurrir en varios niveles, mismos que se clasifican según su función en cinco *canales.* Los canales se los puede apreciar de mejor manera en la Tabla 1.
6. Determinar la información que se desea obtener de la prueba. El *tipo de prueba* debe ser definido de forma individual, sin embargo, identifica seis tipos: Blindaje o *Hacking* Ético, Caja Negra, Caja Gris, Caja Blanca, Secuencial y de Inversión; de los cuales, dependiendo de la cantidad de información que el auditor conoce acerca de los objetivos y lo que el objetivo espera

de la prueba, se deberá definir, individualmente, la que más se adapte a las necesidades del proceso a desarrollarse en la evaluación de cada uno de los canales.

7. Asegurar que la prueba de seguridad cumpla con *las normas judiciales*, esto con el fin de asegurar que el proceso que se lleve a cabo no genere malentendidos, confusiones o falsas expectativas.

Tabla 1. Clasificación de los canales.

Clase	Canal	Descripción
Seguridad Física (PHYSSEC)	Humano	Comprende el elemento humano de la comunicación donde la interacción es tanto física o psicológica.
	Físico	Comprende el elemento tangible de la seguridad donde la interacción requiere esfuerzo físico o un transmisor de energía para manipular.
Seguridad Inalámbrica (SPECSEC)	Inalámbricos	Comprende todas las comunicaciones electrónicas, señales y emanaciones que tienen lugar sobre el espectro electromagnético EM.
Seguridad en las Comunicaciones (COMSEC)	Telecomunicaciones	Comprende todas las redes de telecomunicación, digitales o analógicas, donde la interacción se lleva a cabo a través de un teléfono determinado o similar a las líneas de la red telefónica pública.
	Redes de datos	Comprende todos los sistemas electrónicos y redes de datos donde la interacción se lleva a cabo a través de un cable establecido y líneas de la red cableadas.

Métricas de la seguridad operacional

La información de cada uno de los canales auditados se encuentra resumida en el *Rav*, que no es nada más que el balance de la porosidad, los controles y las limitaciones. Cabe señalar que el cálculo del valor final de la seguridad actual, se lo puede realizar de dos maneras: una de manera manual (aplicando varias fórmulas), o de manera automatizada (haciendo uso de una hoja de Excel).

La hoja de cálculo del *Rav* se la puede descargar del sitio web oficial de ISECOM (http://www.isecom.org/research/ravs.html), en la cual se debe ingresar los valores numéricos encontrados de cada ítem. El valor de la seguridad actual se obtiene de forma automática.

Para calcular el valor numérico de la seguridad actual de cada canal, que es la medida que permite evaluar el porcentaje de eficiencia de los controles operacionales implementados para cada uno, es necesario tomar en cuenta las recomendaciones que dicta la metodología para ponderar por separado cada uno de los ítems por los que está compuesto (Herzog, 2010):

- Porosidad: se mide como la suma de visibilidad (P_V), acceso (P_A) y confianza (P_T).
- Controles
  - ✓ Clase A: autenticación (LC_{Au}), indemnización (LC_{Id}), resistencia (LC_{Re}), subyugación (LC_{Su}), continuidad (LC_{Ct}).
  - ✓ Clase B: no-repudio (LC_{NR}), confidencialidad (LC_{Cf}), privacidad (LC_{Pr}), integridad (LC_{It}) y alarma (LC_{Al})
- Limitaciones: vulnerabilidad (L_V), debilidad (L_W), preocupación (L_C), exposición (L_E) y anomalía (L_A).

Para encontrar los valores de la debilidad, y la preocupación, es necesario hacer referencia a la Tabla 2, de donde se toman los siguientes criterios:

Tabla 2. Relación de la porosidad, controles y limitaciones.

Categoría	Seguridad operacional	Limitaciones
Operaciones	Visibilidad Acceso	Exposición

		Confianza	Vulnerabilidad
Controles	Clase A	Autenticación Indemnización Resistencia Subyugación Continuidad	Debilidad
	Clase B	No repudio Confidencialidad Privacidad Integridad Alarma	Preocupación
			Anomalía

La debilidad se calcula contabilizando cada defecto o error en los controles interactivos o de Clase A. Por lo tanto: $L_w = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}$

La preocupación se calcula contabilizando cada defecto o error en los controles de proceso o de Clase B. Por lo tanto: $L_c = FC_{NR} + FC_{Cf} + FC_{Pr} + FC_{It} + FC_{Al}$

El valor de la seguridad actual se mide en base a un nivel de referencia de 100 rav, donde más de 100 rav significa que se invierte un costo demasiado en controles, y menos de 100 rav significa que los controles operacionales, adoptados por la entidad, protegen a todo el sistema del canal auditado, pero con varias limitaciones.

2.3. Aplicación de las métricas para cada canal

Para este apartado es necesario indicar que sólo se muestra un ejemplo de la utilización de la hoja de cálculo del *Rav* en el canal humano. Para los demás canales, el procedimiento a seguir es el mismo.

Pruebas de seguridad humana

En primer lugar, para tener un punto de partida para evaluar este canal, fue necesario aplicar una encuesta a 10 empleados que interactúen en mayor frecuencia con el área de sistemas del GADM-Mira, mismos que se encuentran comprendidos por los departamentos del proceso habilitante de apoyo tomados de su Organigrama Institucional por Procesos.

Para calcular el valor de la porosidad en este canal, fue necesario aplicar varias técnicas de ingeniería social tales como: observación directa, observación y persuasión, y llamadas telefónicas falsas; esto con el fin de obtener los valores de la visibilidad, acceso y confianza, mismos que se resumen en la Tabla 3.

Tabla 3. Cálculo de la porosidad.

Porosidad u Op-Sec		
Ítem	Prueba	Total
Visibilidad	Contabilizar qué departamentos o áreas del GADM-Mira están autorizados a realizar interacciones con el cuarto de telecomunicaciones	5
Acceso	Contabilizar los escenarios donde puede ocurrir una interacción sin que se necesite una autorización del empleado guardián de la información generada en su estación de trabajo	4
Confianza	Contabilizar el acceso a la información o a los activos físicos de empleados que no generaron o están a cargo de los mismos respectivamente	3

El siguiente paso para definir el *Rav* es calcular los controles, que no son más que los mecanismos de seguridad puestos en marcha para proteger las operaciones. Los resultados de estas medidas operacionales se resumen a continuación en la Tabla 4.

Tabla 4. Cálculo de los controles.

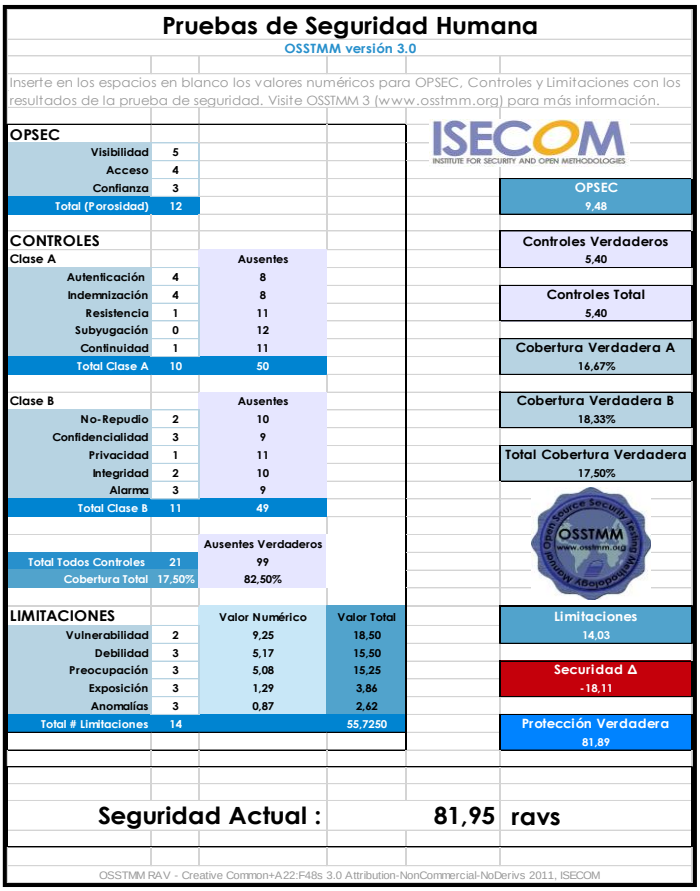
Controles		
Controles de interacción o de Clase A		
Ítem	Prueba	Total
Autenticación	Contabilizar los métodos por los cuales se puede interactuar con el personal de recepción	4
Indemnización	Contabilizar los documentos legales a los que deben someterse los empleados del GADM-Mira para resguardar la información generada o manejada por sus empleados	4
Resistencia	Contabilizar los empleados que permiten acceder sin autorización a los activos del cuarto de telecomunicaciones	1
Subyugación	Contabilizar los activos que pueden ser comunicados a través de canales en los cuales los controles no son necesarios, pueden ser eludidos o ignorados	0
Continuidad	Contabilizar el personal que genera conflictos en cuanto a retrasos de acceso	1
Controles de Proceso o de Clase B		
Ítem	Prueba	Total
No-repudio	Contabilizar quiénes del personal de recepción identifican y registran adecuadamente el acceso o las interacciones con los activos del GADM	2
Confidencialidad	Contabilizar los segmentos de comunicación con el personal dentro del alcance que son eficientes	3
Privacidad	Contabilizar los métodos eficientes para asegurar este control	1
Integridad	Contabilizar los métodos eficientes aplicados por el GADM para proteger y asegurar que la información de los activos físicos no pueda ser cambiados, conmutados, redirigidos o invertidos sin que las partes involucradas tengan conocimiento de ello	2
Alarma	Contabilizar la utilización de sistemas de advertencia o sistemas de alarma en todo el alcance	3

A continuación, se deben ponderar las *limitaciones*, mismas que se calculan de forma individual, para ellos se siguió el procedimiento mostrado en la Tabla 5.

Tabla 5. Cálculo de las limitaciones.

Limitaciones		
Ítem	Prueba	Total
Vulnerabilidad	Contabilizar las fallas o errores por las cuales una persona o proceso puede ganar o denegar el acceso a los demás	2
Debilidad	Contabilizar las posibles fallas o errores que pueden presentarse en los controles de Clase A	3
Preocupación	Contabilizar los posibles defectos o errores que puedan presentarse en los controles de Tipo B	3
Exposición	Contabilizar las acciones injustificadas, fallas o errores que proporcionen una visibilidad directa o indirecta de los activos dentro del alcance	3
Anomalías	Contabilizar los elementos desconocidos que no pueden tomarse en cuenta en las operaciones normales del GADM	3

Una vez que ya se han obtenido todos los valores individuales de cada ítem, se debe ingresar los mismos en los espacios en blanco dispuestos en la hoja de cálculo del *Rav*, y a continuación los demás valores se mostraran automáticamente, tal como se muestra en la Figura 3.



Pruebas de Seguridad Humana

OSSTMM versión 3.0

Inserte en los espacios en blanco los valores numéricos para OPSEC, Controles y Limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM 3 (www.osstmm.org) para más información.

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC		
Visibilidad	5	
Acceso	4	
Confianza	3	
Total (Porosidad)	12	

OPSEC 9,48

CONTROLES		
Clase A		Ausentes
Autenticación	4	8
Indemnización	4	8
Resistencia	1	11
Subyugación	0	12
Continuidad	1	11
Total Clase A	10	50
Clase B		Ausentes
No-Repudio	2	10
Confidencialidad	3	9
Privacidad	1	11
Integridad	2	10
Alarma	3	9
Total Clase B	11	49
		Ausentes Verdaderos
Total Todos Controles	21	99
Cobertura Total	17,50%	82,50%

Controles Verdaderos 5,40

Controles Total 5,40

Cobertura Verdadera A 16,67%

Cobertura Verdadera B 18,33%

Total Cobertura Verdadera 17,50%

LIMITACIONES		Valor Numérico	Valor Total
Vulnerabilidad	2	9,25	18,50
Debilidad	3	5,17	15,50
Preocupación	3	5,08	15,25
Exposición	3	1,29	3,86
Anomalías	3	0,87	2,62
Total # Limitaciones	14		55,7250

Limitaciones 14,03

Securidad Δ -18,11

Protección Verdadera 81,89

Seguridad Actual : 81,95 ravs

Figura 3. Resultados obtenidos en la auditoria del canal humano en el GADM-Mira.

Pruebas de seguridad física, inalámbrica y de redes de datos

En la Tabla 6 se resume los valores numéricos obtenidos para la Porosidad, Controles y las Limitaciones, luego de haber realizado las diferentes pruebas que dicta.

Tabla 6. Valores numéricos de las métricas operacionales.

	Seguridad operacional		
Canal Ítem	Físico	Inalámbrico	Redes de datos
Visibilidad	11	4	21
Acceso	13	3	20
Confianza	0	1	1

	Controles		
Canal Ítem	Físico	Inalámbrico	Redes de datos
Autenticación	1	5	6
Indemnización	8	0	9
Resistencia	5	1	4
Subyugación	1	0	2
Continuidad	9	1	1
No-Repudio	1	0	1
Confidencialidad	1	1	0
Privacidad	2	2	19
Integridad	3	2	0
Alarma	0	0	2

	Limitaciones		
Canal / Ítem	Físico	Inalámbrico	Redes de datos
Vulnerabilidad	7	0	25
Debilidad	4	3	7
Preocupación	2	2	4
Exposición	3	0	2
Anomalía	0	1	1

Pruebas de seguridad de las telecomunicaciones

Para este canal en particular, (Herzog, 2010) recomienda que los vectores de ataque para este canal son:

- Pruebas de PBX
- Pruebas de buzón de voz
- Encuesta, sondeo y pruebas de FAX y módem
- Pruebas de Servicio de Acceso Remoto (RAS)
- Pruebas de líneas RDSI de respaldo
- Pruebas de voz sobre IP
- Pruebas de conmutación de paquetes en redes X.25

Para este canal solo existen dos objetivos que pueden ser probados dentro del GADM-Mira ya que solo se cuenta una central telefónica analógica y un sistema de fax; de los cuales, la central telefónica no sería considerada como un dispositivo de telecomunicaciones ya que está limitada para uso exclusivo dentro del espacio físico del GADM.

En consecuencia, para este canal se apelará al recurso que dicta Herzog (2010) para reportarlo como un "*objetivo no probado*", por el hecho de que el entorno de la prueba no permite recoger la información necesaria para emitir un informe que arroje resultados acordes a la realidad actual del GADM-Mira. Lo más recomendable es tomar este aspecto para futuras pruebas, y, en caso de que se cuente con los vectores necesarios a probar, se debe emitir un criterio sobre el grado de la seguridad operacional que tendrá este canal.

3. RESULTADOS

Existen dos expresiones que permiten realizar una interpretación de los valores obtenidos en la seguridad actual del canal auditado, la primera es *Seguridad* Δ como se muestra en la Figura 3, marcada de color rojo, que no es nada más que el equilibrio que existe entre los valores numéricos de la porosidad, los controles y las limitaciones. Por lo tanto, dependiendo del signo que éste posea: positivo (+) o negativo (-), se pueden considerar los siguientes aspectos: un delta positivo muestra lo mucho que se gasta en controles o, incluso, si el exceso de gasto es demasiado en un tipo de control; un delta negativo muestra una falta de controles o que se controlan a sí mismos con limitaciones que no pueden proteger adecuadamente al objetivo.

Al dar un orden prioritario a las limitaciones que se identificaron en el análisis de resultados de la metodología, se encuentra en primer lugar las de tipo financieras, por no asignar los recursos necesarios al departamento de sistemas para que se implementen los controles necesarios. En segundo lugar están las competencias estratégicas, debido a que no existen planes de capacitación continua para el personal que debe ofrecer seguridad a la información de la institución, así como crear políticas de acceso a recursos de la red.

La otra expresión permite analizar el riesgo de la superficie de ataque es la *Seguridad Actual* cuyos valores se pueden apreciar en la Tabla 7, en donde en promedio para los cuatro canales auditados posee un valor numérico de aproximadamente 80 rav, lo que se traduce en una deficiencia del alcance de aproximadamente un 20%. Por tanto, se puede asegurar que existe un porcentaje considerable de vulnerabilidades dentro del sistema de seguridad que se maneja dentro de la Institución.

Tabla 7. Resultados finales.

	Valores de análisis				
Canal / Ítem	Humano	Físico	Inalámbrico	Redes de datos	Promedio
OpSec	9.48	11.43	8.43	12.29	10.41
Limitaciones	14.04	16.12	11.76	20.10	15.51
Controles verdaderos	5.4	6.21	4.34	6.99	5.74
Seguridad Δ	-18.11	-21.34	-15.85	-25.39	-20.17
Protección verdadera	81.89	78.66	84.15	74.61	79.83
Seguridad actual	81.95 ravs	78.79 ravs	84.26 ravs	74.81 ravs	79.95 ravs

4. DISCUSIÓN

Se comparó los resultados que se obtienen con la Metodología OSSTMM versión 3 y su antecesora, es decir la versión 2, mostrando que la versión 3 brinda resultados de manera cuantitativa y cualitativa, haciendo uso de su propia unidad de medida para la seguridad operacional (*ravs*), mismos que reflejan el porcentaje de eficiencia, tanto para los canales auditados individualmente, como en un enfoque global de todo el sistema de seguridad. En cambio, la versión 2 no permite mostrar resultados cuantitativos, sino solamente cualitativos, para cada los subgrupos que ésta posee: seguridad de la información, de procesos, en las tecnologías de internet, en las comunicaciones, inalámbrica, y física; haciendo uso de pruebas de vulnerabilidad para enfocar las fallas más preponderantes de cada uno de los subgrupos mostrados anteriormente, lo que desencadena en que no se pueda tener un valor de medición de la eficacia de los mecanismos de seguridad operacional adoptados por una institución. Por otro lado, en la versión 3 de la metodología OSSTMM, se incluye un apartado en el que se explican las ventajas de cumplir con un régimen normativo, para llevar a cabo una auditoría de seguridad que cumpla con los marcos legales establecidos, no solo dentro de la institución, sino a nivel regional y así evitar que las pruebas de seguridad que se lleven a cabo generen malos entendidos o conflictos dentro de la institución. En la versión 2 no se cuenta con este importante recurso.

5. CONCLUSIONES

La aplicabilidad de esta metodología permite conocer resultados puntuales sobre los canales en los que se requiera una mayor atención, que permitan dar solución a ciertas vulnerabilidades que pueden darse dentro del entorno organizacional ya sea por limitaciones financieras, humanas, de procedimientos o estratégicas, así también la mala aplicación de los controles de seguridad que pueden verse subutilizados.

El caso de estudio considerado, para la aplicabilidad de la metodología, hace notar que en el GAD existen debilidades y limitaciones en sus controles de seguridad, que claramente son visibles una vez contabilizados en las *Rav*, teniendo un promedio de 20% de falencias de seguridad, y que son solucionadas mediante el mejoramiento y adopción de nuevos controles, y la generación de políticas de seguridad informática.

Esta metodología se puede orientar a cualquier ambiente organizacional que requiera tener un conocimiento amplio de la seguridad que cuenta su organización. Además, esta metodología puede complementarse con otras como COBIT, que permite la generación de políticas de seguridad, de forma que asegure los controles administrativos, físicos y técnicos, permitan asegurar la información de la empresa.

AGRADECIMIENTOS

Se agradece en primer lugar a los docentes de la Carrera de Ingeniería en Electrónica y Redes de Comunicación de la Universidad Técnica del Norte por el apoyo durante la ejecución de esta investigación; así como también al Gobierno Autónomo Descentralizado Municipal del Cantón Mira por la apertura para ser considerado como caso de estudio.

REFERENCIAS

Acurio del Pino, S. (2012). *Los delitos informáticos en el Ecuador (parte II)*. Disponible en http://www.inforc.ec/los-delitos-informaticos-en-el-ecuador-parte-ii/

Bravo, D. (2015). *Ecuador se muestra vulnerable a ciberataques*. El Comercio. Disponible en: http://www.elcomercio.com/actualidad/ecuador-muestra-vulnerable-ciberataques.html

Chicano Tejada, E. (2014). *Auditoría de seguridad informática.* Andalucía: IC Editorial.

Chiluiza, E. (2015). *Los delitos informáticos en el COIP: Efectos de los delitos informáticos en la administración de justica del Ecuador*. La Verdad. Disponible en http://www.revista-laverdad.com/2015/01/10/los-delitos-informaticos-en-el-coip/

Costas Santos, J. (2010). *Seguridad Informática.* Madrid: Ra-Ma Editorial.

Cuenca Espinosa, A. (2012). *El delito informático en el Ecuador: Una nueva tendencia criminal del siglo XXI, su evolución, punibilidad y proceso penal*. 24 pp. Disponible en http://www.egov.ufsc.br/portal/sites/default/files/el_delito_informatico_en_el_ecuador_una_tendencia_criminal_del_siglo_xxi-alexander_cuenca.pdf

Herzog, P. (2010). *OSSTMM 3. Manual de la Metodología Abierta de Testeo de Seguridad.* New York: ISECOM.

Toth, G. A. (2014). *Implementación de la guía NIST SP800-30 mediante la utilización de OSSTMM.* Neuquén, Argentina.