Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final de la Especialización

Metodología de testeo de seguridad

Análisis de la Metodología OSSTMM para comprobar la seguridad operacional de una organización

Autor

Leticia Elena Ferreira González

Tutor del Trabajo Final

Juan Pedro Hecht

2020

Cohorte 2017

Declaración jurada de origen de los contenidos

“Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual”.

Leticia Elena Ferreira González

DNI: 95.736.835

Resumen

El presente trabajo final de especialización se enfoca en analizar y en describir en detalle el Manual de la Metodología Abierta de Comprobación de Seguridad, OSSTMM por sus siglas en inglés (*Open Source Security Testing Methodology Manual*). Primero se expone el concepto de la seguridad de la información y cuál es el estado actual en la región de Latinoamérica con base estadísticos sobre las preocupaciones de las organizaciones y como estos están preparados para resguardar sus activos.

Se describe las distintas formas de auditar, comprobar y evaluar la seguridad de la información en las organizaciones y se resalta la importancia que estas evaluaciones se basen en una metodología y contar con un proceso periódico en el tiempo, para descubrir los puntos débiles de la seguridad en la organización que afectan directamente a los activos.

Luego se estudia el Manual de la Metodología Abierta de Comprobación de Seguridad con un enfoque de los conceptos utilizados en la metodología y se proporciona descripciones específicas sobre las pruebas de seguridad operacional en los canales operativos, como ser la seguridad humana, física, inalámbrica, telecomunicación y de redes de datos.

Posteriormente se comparte un caso de estudio para visualizar la aplicación de la metodología en un alcance de infraestructura de una organización, y se demuestra que se obtienen métricas útiles para la evaluación sobre la correcta implementación de los procesos, políticas y controles sobre los activos.

Se destaca que el presente trabajo final de especialización está basado en el *Open Source Security Testing Methodology Manual,* considerado una metodología completa para pruebas de penetración y seguridad, análisis de seguridad y la medición de la seguridad operativa. Finalmente se complementa con los conceptos del trabajo de tesis de Gastón Alejandro Toth con el nombre “Implementación de la guía NIST SP800-30 mediante la utilización de OSSTMM”, los cuales se detallan en la bibliografía general.

Palabras clave: OSSTMM, Auditoría, Análisis, Seguridad, Vulnerabilidad, Activo, Riesgo, Proceso, Control, Métrica.

Índice General

Índice de Ilustraciones

Índice de Tablas

Agradecimientos

A mi familia quien me acompaña y apoya incondicionalmente en mi crecimiento personal y profesional.

A los docentes y compañeros de la especialización por los conocimientos adquiridos y las experiencias compartidas durante la cursada.

Al Programa Nacional de Becas de Postgrado en el Exterior “Don Carlos Antonio López” por otorgarme la oportunidad de formarme y especializarme para fortalecer y afianzar mis capacidades profesionales.

1- Introducción

La información representa el activo más valioso de toda organización, por lo cual es necesario, sino obligatorio, que se cumpla con requisitos de calidad y de seguridad en los procesos que la utilizan. [1]

La seguridad de la información se encarga de proteger la información de una amplia gama de amenazas, a fin de garantizar la continuidad comercial del negocio, minimizar los daños y maximizar el retorno sobre las inversiones y las oportunidades, normalmente se logra implementando un conjunto adecuado de controles que abarcan políticas y procedimientos, involucrando recursos humanos, hardware y software. [1]

Las organizaciones y sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o negación de ataques de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas. [2]

1.1- Reporte de seguridad en Latinoamérica

1.1.1- Como se producen los ataques

Dada la amplia variedad de amenazas que puede afectar a las organizaciones, es importante identificar cuáles son los diferentes vectores por los cuales puede llegar un ataque para luego tomar las medidas de control más adecuadas. Si bien muchas veces los ataques llegan desde fuera de la organización, es posible que ocurran dentro de la empresa, incluso por descuidos o malas prácticas de seguridad. [3]

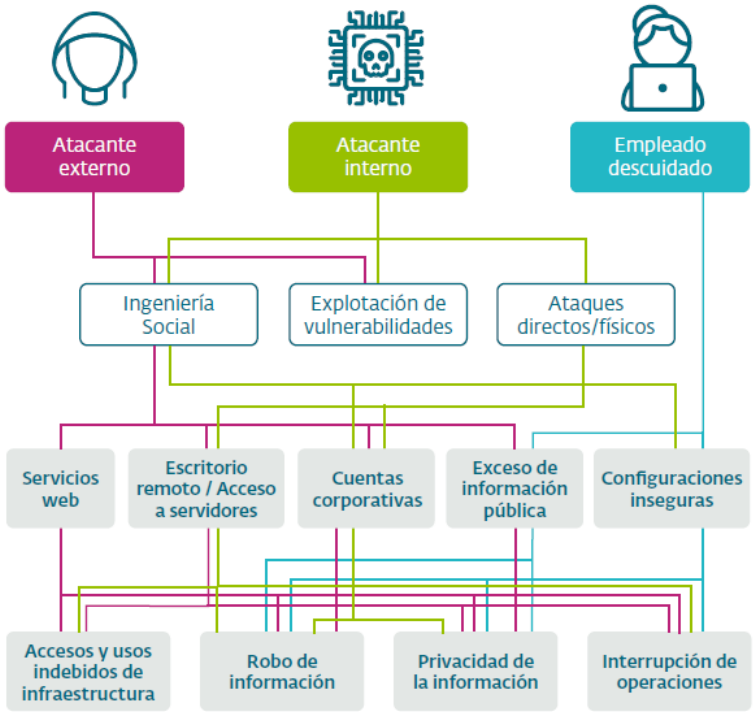


Ilustración 1: Cómo ocurren los ataques [3] [4]

Se debe considerar a la seguridad de la información como aspecto integral en los procesos de la organización.

De no hacerlo, se tendrá problemas asociados a bases de datos mal configuradas, por ejemplo, filtraciones de información masivas por una mala configuración de servidores, y que la adopción de nuevas tecnologías que buscan brindar mayor seguridad genere más problemas que soluciones, por ejemplo, cámaras, controles de acceso biométricos. [3]

1.1.2- Preocupaciones en materia de seguridad

El panorama de incidentes y amenazas demuestra la preocupación de las organizaciones por la seguridad de su información. Al disponer en un orden es como sigue, un 60% de las organizaciones afirma que su principal preocupación es el acceso indebido a la información. El podio lo completan el robo de información (56%) y la infección con códigos maliciosos (53%). [3]

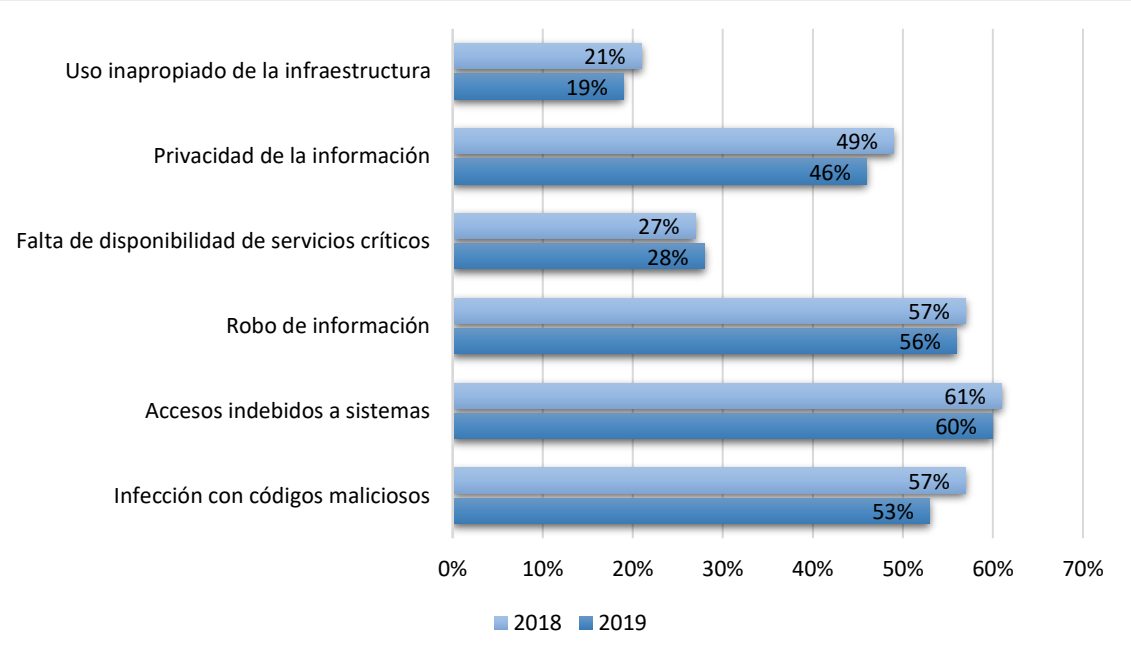


Ilustración 2: Preocupaciones relacionadas con la seguridad [3] [4]

La gran mayoría de los ataques que pueden comprometer la seguridad de una empresa suele estar asociada a variantes del *malware*[1]. Aprovechada en un amplio espectro de plataformas: desde computadoras hasta dispositivos móviles sin dejar afuera los dispositivos IoT[2], lo que hace que la infección mediante *malware* sea uno de los métodos más usados por los atacantes. [3]

[1] El *malware* es cualquier aplicación o software destinado a dañar un equipo, dispositivo móvil, sistema informático o red de equipos informáticos, o bien a asumir un control parcial de su funcionamiento, a menudo en un intento de acceder a la información personal. [33]

[2] IoT es la tendencia constante de conectar todo tipo de objetos físicos al Internet. Puede ser cualquier tipo de elemento, desde objetos domésticos comunes, como los refrigeradores y las bombillas; recursos empresariales, como las etiquetas de envío y los dispositivos médicos. [44]

1.1.3- Incidentes de seguridad

Según el tipo de incidente más recurrente y reconocido por las propias organizaciones es la base para evaluar qué controles se implementan a la hora de proteger las redes organizativas. [3]

En base a datos suministrados por organizaciones de toda Latinoamérica, se pude afirmar que un 60% de las empresas sufrió al menos un incidente de seguridad. [3]

Dentro de los incidentes relacionados a la infección con códigos maliciosos (32%), solo el 18% está relacionado al *ransomware*[3], lo que indica una incidencia del 6% sobre el total de las empresas. Esto se traduce en una caída respecto del 2019, año en el que el *ransomware* había registrado una incidencia del 8%. [3]

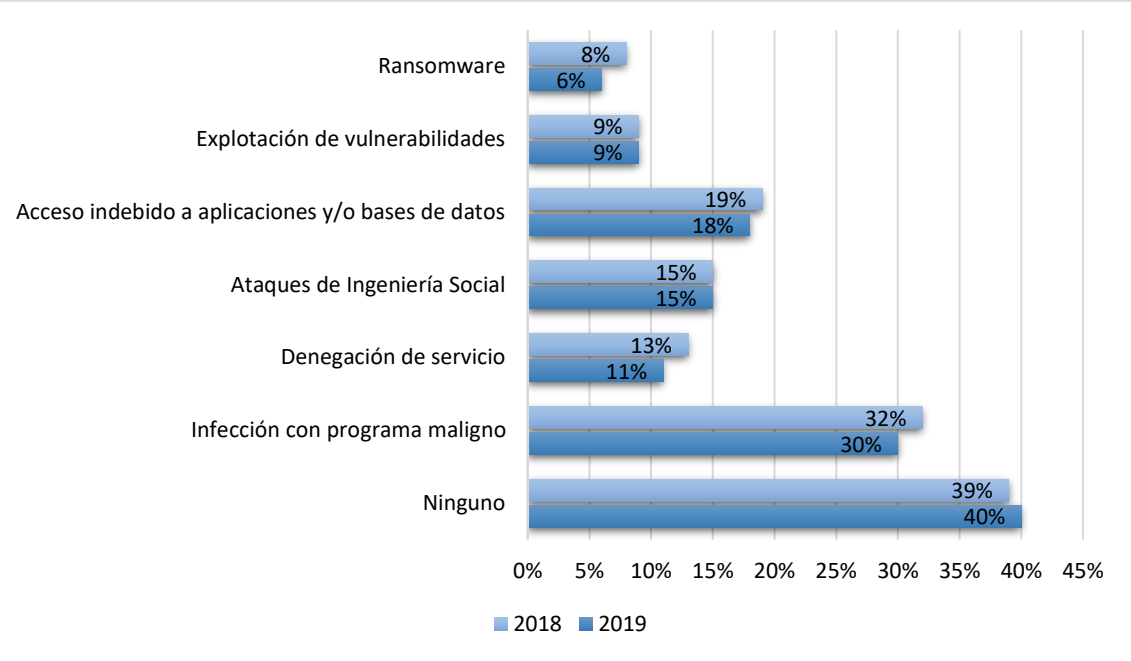


Ilustración 3: Incidentes de seguridad [3] [4]

1.1.4- Control y prevención de riesgos

La seguridad de la información debe abordarse desde un enfoque por capas: contar con tecnologías de protección, con políticas y planes para gestionar la seguridad de la información, así como también con planes continuos de capacitación a los colaboradores. [3]

En que casi el 98% de las empresas en la región cuenta con algún control basado en tecnología. Sin embargo, aún el 39% de las empresas no cuenta con políticas de seguridad y apenas un 28% clasifica su información. [3]

[3] El *ransomware* es un tipo específico de software malicioso utilizado para extorsionar. Cuando un dispositivo logra ser atacado con éxito, el *malware* bloquea la pantalla o cifra la información almacenada en el disco y se solicita un rescate a la víctima con los detalles para efectuar el pago.

Controles: seguridad antivirus, una copia de seguridad o una solución de *firewall*[4]; apenas alcanza el 48% en las organizaciones latinoamericanas. [3]

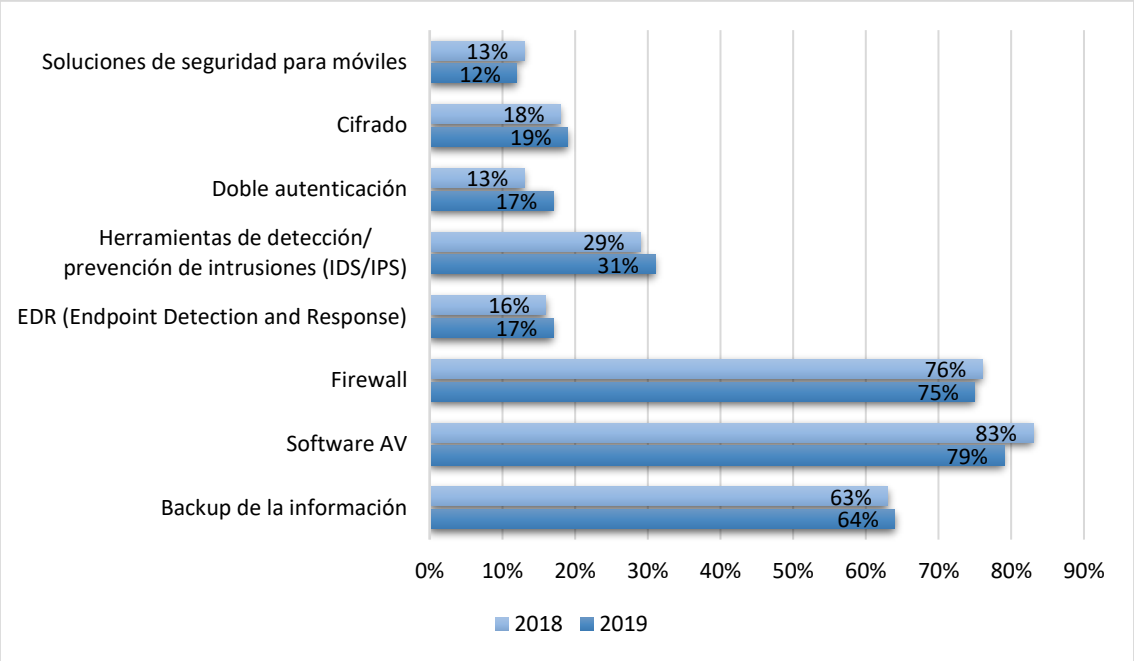


Ilustración 4: Controles basados en tecnología [3] [4]

Gestión: clasificación de la información, plan de respuesta y continuidad, políticas de seguridad; los niveles de implementación de políticas de seguridad acumulan un alto porcentaje (61% de las organizaciones declararon contar con ellas); solo una tercera parte (33%) de las empresas encuestadas cuenta con un plan de continuidad del negocio. [3]

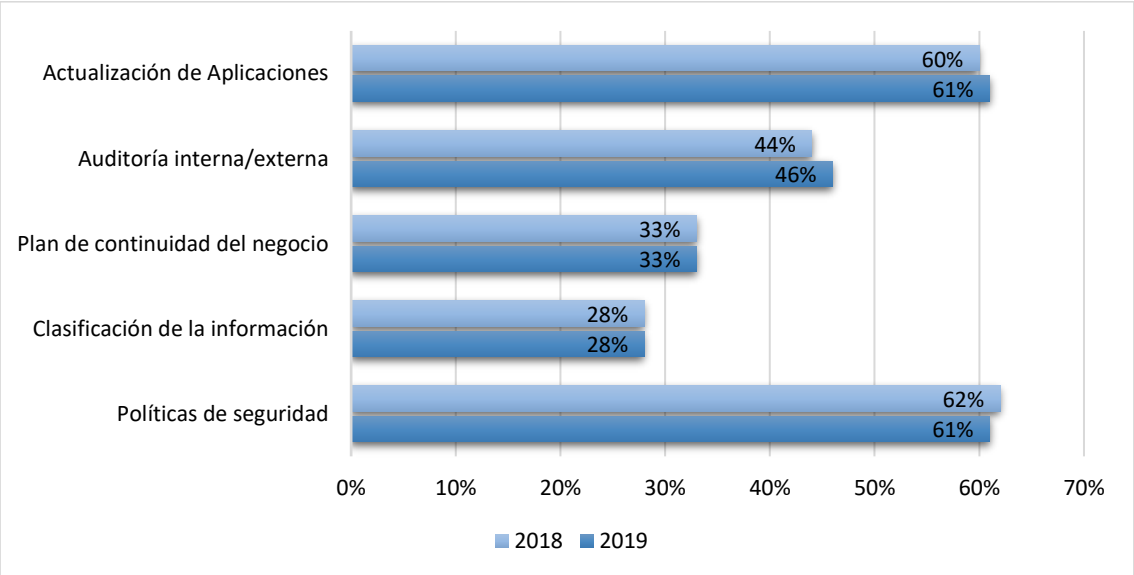


Ilustración 5: Controles basados en gestión [3] [4]

[4] Un firewall es un dispositivo de seguridad de la red que monitoriza el tráfico entrante y saliente y decide si debe permitir o bloquear un tráfico específico en función de un conjunto de restricciones de seguridad ya definidas. [34]

1.2- Evaluaciones de la seguridad

El aumento de amenazas ha hecho que cobren mayor importancia los análisis y evaluaciones de seguridad sometidas a las infraestructuras de tecnología de la información de las organizaciones. Estas se realizan de forma controlada tomando el auditor o el analista el rol de un potencial adversario o competidor. [5]

La Auditoría de seguridad es un proceso que permite evaluar e identificar de forma sistemática el estado de la seguridad con relación a una serie de criterios o normas. Mediante este proceso se trata de identificar diversas vulnerabilidades que pudieran afectar a la confidencialidad, integridad y disponibilidad de un aplicativo y de los sistemas asociados con éste. [6]

La evaluación de vulnerabilidades es el proceso de identificación de vulnerabilidades y riesgos en los sistemas. La vulnerabilidad no se explota. Simplemente se destaca los riesgos para que la organización pueda identificar los riesgos y planificar la remediación. [7]

La prueba de penetración es el proceso autorizado de encontrar y usar vulnerabilidades para realizar una intrusión en una red, aplicación o host en un período de tiempo predefinido. Una prueba de penetración explota la vulnerabilidad para asegurarse de que no sea un falso positivo. Durante una prueba de penetración, algunas pruebas pueden afectar las aplicaciones comerciales y provocar tiempo de inactividad. Por esta razón, se requiere conciencia a nivel gerencial y personal. [7]

La evaluación del equipo rojo es similar a una prueba de penetración, pero es más específica. El objetivo de una evaluación de equipo rojo es probar las capacidades de respuesta de una organización y actuar sobre las vulnerabilidades que cumplirán sus objetivos. [7]

1.3- Evaluaciones externas e internas

Las pruebas de seguridad externas se realizan desde fuera del perímetro de seguridad de la organización. Esto ofrece la posibilidad de ver la situación de seguridad del entorno tal como aparece fuera del perímetro de seguridad, generalmente visto desde Internet, con el objetivo de revelar vulnerabilidades que podrían ser explotadas por un atacante externo. [8]

Para las pruebas de seguridad interna, los asesores trabajan desde la red interna y asumen la identidad de un infiltrado de confianza o un atacante que ha penetrado las defensas del perímetro. Este tipo de prueba puede revelar vulnerabilidades que podrían explotarse y demuestra el daño potencial que podría causar este tipo de atacante. [8]

Las pruebas de seguridad abiertas implican realizar pruebas externas o internas con el conocimiento y consentimiento del personal de TI de la organización, lo que permite una evaluación integral de la postura de seguridad de la red o del sistema. [8]

El propósito de las pruebas encubiertas es examinar el daño o el impacto que puede causar un adversario; no se enfoca en identificar vulnerabilidades. Este tipo de prueba no prueba todos los controles de seguridad, identifica cada vulnerabilidad o evalúa todos los sistemas dentro de una organización. [8]

1.4- Metodología de pruebas de la seguridad de la información

En tiempo pasado, la verificación de seguridad requería un especialista interdisciplinario que entienda la seguridad como entienda sobre políticas, normas, leyes, procedimientos, operaciones, procesos y la tecnología involucradas.

Para garantizar que una prueba de seguridad obtenga valor es saber que la prueba se ha realizado correctamente, por esta razón resulta útil el uso de metodologías formales para cumplir este punto.

Actualmente el ambiente se ha vuelto más complejo debido a las operaciones remotas, virtualizaciones, y la computación en la nube. Por esta razón no es suficiente realizar pruebas de seguridad a nivel escritorio, servidores o equipos de enrutamiento.

Razón por la cual, la adopción de una metodología debe ser un proceso aplicado de manera iterativa y reiterada en el tiempo, con el fin de descubrir los puntos débiles de la seguridad que pueden provocar que los datos y los equipos se vean afectados en mayor o menor medida por ataques pasivos o activos. [9]

Una metodología define un conjunto de reglas prácticas y procedimientos que son ejecutados durante la evaluación de cualquier programa de seguridad de la información y permite ordenar y estandarizar este proceso. [9]. Cubre toda la variedad de pruebas que se deben realizar. Facilitan en gran medida la tarea al analista o auditor. Los resultados se trasladan al cliente de una forma más organizada y ordenada. Ayuda a realizar el proceso de una forma ética y legal. [5]

La metodología debe contener parámetros tanto para asegurar que la metodología se ha llevado a cabo correctamente como para comprender o calificar el resultado de la aplicación de la metodología.

Por lo tanto, es preciso aplicar métodos y políticas de seguridad, que mitiguen los riesgos, que son identificados de manera empírica, como la amplia distribución y utilización de *software* antivirus, la utilización de *firewalls* en áreas de la red, pero no son cubiertos todos los puntos y dejan abiertos ciertas zonas donde el ingreso ilegal permite tomar información. [10]

2- Introducción a OSSTMM

El Manual de la Metodología Abierta de Comprobación de Seguridad brinda una metodología para la comprobación de seguridad denominada auditoría de OSSTMM. Contribuye para medir con precisión la seguridad al nivel operacional. OSSTMM es un proyecto de código abierto, que permite la contribución de ideas para realizar las pruebas de seguridad más precisas,

accionables y eficientes. Asimismo, permite la difusión gratuita de información y propiedad intelectual.

Historia de OSSTMM a través de los años:

- 2000: abarcó todos los canales de seguridad con la experiencia aplicada de miles de revisores.
- 2005: no solo era un marco de mejores prácticas. Resultó ser una metodología para garantizar la seguridad a nivel operativo.
- 2006: es un estándar confiable para pruebas de seguridad, más que un informe de cumplimiento para una regulación o legislación.
- 2010: en su versión tres, incluye pruebas de todos los canales: redes humanas, físicas, inalámbricas, de telecomunicaciones y de datos.

En base a la última versión, se conceptualiza como una metodología para comprobar y medir la seguridad operativa de las ubicaciones físicas, las interacciones humanas y todas las formas de comunicación, como inalámbrica, por cable, analógica y digital.

Se utiliza el RAV[5] que es un conjunto de métricas para la superficie de ataque de un objetivo o alcance, apuntando a lo que se encuentra expuesto. Proporciona una representación gráfica y de los cambios en el estado a lo largo del tiempo. Esta métrica es precisa para medir la susceptibilidad a los ataques. Esto permite una métrica efectiva que no tiene ninguna desviación u opinión como el riesgo.

Por regulaciones legales y específicas de la industria frecuentemente se requiere una auditoría de seguridad como un componente para cumplir. Una auditoría OSSTMM es adecuada para ciertos casos de acuerdo con la región geográfica. Por lo tanto, las pruebas específicas de OSSTMM se pueden conectar con requisitos de normas formales de seguridad particulares, como ser PCI-DSS, NIST y la serie ISO/IEC 27000.

OSSTMM tiene como objetivo ser una herramienta directa para la implementación y documentación de una comprobación de seguridad.

2.1- Propósito del Manual OSSTMM

El propósito principal del manual es proporcionar una metodología científica para la estructura precisa de la seguridad operacional a través de la examinación y la correlación de los resultados de las pruebas de una manera consistente y confiable.

El segundo propósito es suministrar pautas que permitan al analista realizar una auditoría OSSTMM certificada. Estas pautas aseguran que la prueba se realizó a fondo e incluyó todos los canales necesarios; la postura de la prueba cumplió con la ley; los resultados se pueden medir de forma cuantificable, son consistentes y repetibles, y contienen solo hechos derivados de las pruebas mismas.

[5] RAV, *Risk Assessment Values*, por sus siglas en inglés.

2.2- Alcance del Manual OSSTMM

Proporcionar descripciones específicas para las pruebas de seguridad operacional en todos los canales operativos, como ser la seguridad humana, física, inalámbrica, telecomunicación y de redes de datos. El manual se enfoca en la seguridad operacional.

2.3- Responsabilidad

El manual OSSTMM cuenta con pruebas diseñadas para obtener una respuesta. Estas pruebas podrían ocasionar daños. Al utilizar esta metodología, el analista acepta asumir esta responsabilidad, de acuerdo con las leyes que rigen en el país donde se ejecuta el manual, así también como la ubicación de los sistemas probados.

2.4- Certificación y Acreditación

Para contar con una auditoría certificada por OSSTMM, se necesita que el Informe de Auditoría de Prueba de Seguridad, STAR[6] por sus siglas en inglés, sea revisado lo que fue y no fue probado, para ser aplicable a la certificación.

Una auditoría certificada OSSTMM ofrece beneficios: sirve como prueba de una prueba de hechos; responsabiliza al Analista de la prueba; proporciona un resultado claro para el cliente; ofrece una visión general más completa que un resumen ejecutivo; y proporciona métricas comprensibles.

3- Qué se necesitas saber acerca de OSSTMM

La seguridad operacional consiste en las diferentes políticas y procedimientos implementados por la administración de la instalación computacional [11]. La metodología OSSTMM mide el buen funcionamiento de la seguridad operacional.

Para que una amenaza sea efectiva en la seguridad operacional, debe interactuar o directa o indirectamente sobre el activo. Separar la amenaza del activo es evitar una posible interacción. Entonces, es posible contar con una seguridad total si la amenaza y el activo están completamente separados uno del otro. Las amenazas que no son factibles separar de los activos, se debe proporcionar mayor seguridad para que las interacciones causen un mínimo o nulo daño.

En el contexto de seguridad operacional, se llama seguridad a la separación de un activo y una amenaza *(security)*, y al control de una amenaza o sus efectos *(safety)*.

Es recomendable utilizar diferentes tipos de controles y es importante categorizarlos por lo que hacen en las operaciones, para asegurar el nivel de protección que ofrecen.

3.1- Seguridad (*security*)

Es la separación entre un activo y cualquier amenaza que existe o que no existe. Hay tres formas de lograr esta separación:

[6] STAR: *Security Test Auditing Report*

a- Mover el activo para crear una barrera física o lógica entre él y las amenazas.
b- Cambiar la amenaza a un estado inofensivo.
c- Destruir la amenaza.

Al analizar el estado de la seguridad, se identifica donde existe la posibilidad de interacción y dónde no. Se reconoce que interacciones son necesarias para las operaciones y cuáles no. El analista de seguridad no cuenta con el conocimiento de la razón de ser de todos los puntos interactivos, estos puntos interactivos se conceptualizan como la Porosidad.

La porosidad disminuye la separación entre una amenaza y un acceso. Cuenta con tres elementos como ser: la Visibilidad que es un medio para calcular la oportunidad de llegar al activo; el Acceso es la capacidad de interactuar y acceder al activo; y la Confianza es la aceptación de interacción libre entre dos activos u objetivos dentro del alcance. Por lo tanto, el aumento de la porosidad es la disminución de la seguridad.

3.2- Controles

Ante las amenazas, los controles proveen seguridad en las operaciones. Cuando se requiere interacción, los controles influyen en el impacto de las amenazas y sus efectos. Los controles se agrupan en interactivos y de proceso.

a- Controles Interactivos: Influyen directamente en la visibilidad, el acceso y en las interacciones de confianza.
   Se compone por [12]:
   1- Autenticación: es cada instancia de autenticación requerida para obtener acceso.
      Ej., en una auditoría de seguridad física en donde se solicita una tarjeta de identificación y la huella dactilar, se suma 2 a los controles de autenticación.
   2- Indemnización: son todas las instancias de métodos utilizados para la compensación por pérdidas referidas a los activos.
      Ej., un seguro que cubre el robo de 30 equipos de computación cuenta como 30.
   3- Resistencia: es cada instancia de acceso o confianza donde una falla en el sistema de seguridad no provea un nuevo acceso. Ej., existe un *webservice*[7] que solicita credenciales y las valida contra una base de datos, en el caso que este servicio pierda la conexión con la base, entonces no debe validar ninguna credencial hasta la restauración de la conexión. En caso de rechazar las credenciales, cuenta como 1 el valor de resistencia. Existe la posibilidad de que el servicio no esté correctamente diseñado y cuando pierde la conexión comience a validar todas

[7] Un *webservice* es un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones. [35]

las credenciales, inclusive las que no son correctas; en ese caso la resistencia es 0.

4- Subyugación: son todos los puntos de acceso o confianza donde la interacción deba cumplir condiciones preestablecidas.
   Ej., el uso de PKI[8] para las comunicaciones entre un cliente y un servidor cuenta como 1 ya que la comunicación sólo puede establecerse si cumplen esa condición.
5- Continuidad: son todos los puntos de acceso o confianza donde una falla no cause una interrupción en la interacción.
   Dentro de los ejemplos para este punto se encuentran la redundancia y el balanceo de carga. En seguridad física, si una puerta se bloquea y no existe una entrada alternativa para los clientes entonces tiene continuidad 0 para ese vector.

b- Controles de Proceso: Utilizados para crear procesos defensivos. Protegen los activos una vez que la amenaza esté presente.
   Se compone por [12]:

6- No repudio: es cada acceso o confianza que provea algún mecanismo de no repudio, tal que exista alguna forma de determinar que la interacción se produjo en un tiempo determinado entre las partes identificadas.
   Dentro del canal de las redes de datos, los archivos de logs brindan mecanismos para el no repudio.
7- Confidencialidad: es cada instancia de acceso o confianza que provea mecanismos para evitar revelar información a terceros no autorizados.
   Un ejemplo claro de confidencialidad es el cifrado de la información.
8- Privacidad: es cada acceso o confianza donde el método de interacción sea ocultado. Esto no quiere decir que la información viaje codificada, sino que no se sepa que hay comunicación o que ésta sea ofuscada de alguna manera.
   En seguridad física, un cuarto cerrado donde se efectúe la comunicación entre personas provee privacidad.
9- Integridad: es cada acceso o confianza donde la interacción brinde algún mecanismo que permita conocer si la información fue modificada por terceros no autorizados.
   En el canal de las redes de datos, una función de *hash*[9] puede usarse para proveer integridad.
10- Alarma: es cada acceso o confianza que genere un registro o notificación cuando exista algún evento no autorizado o erróneo.
   En las redes de datos, los archivos de logs cuentan como alarma, aunque estos no generen una notificación inmediata. También se

[8] *Public Key Infrastructure*: Infraestrucutra de Clave Pública: todo lo necesario, tanto de hardware como de software, para las comunicaciones seguras mediante el uso de certificadas digitales y firmas digitales. [36]
[9] *Hash*: es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. [37]

debe sumar un punto por cada equipo monitoreado por un sistema de detección de intrusiones o antivirus.

3.3- Objetivos de garantía de la información

Al agrupar los controles de operación en referencia a los objetivos de la seguridad de la información, es como sigue:

Objetivos de garantía de la información	Controles de operación
Confidencialidad	Confidencialidad Privacidad Autenticación Resistencia
Integridad	Integridad No repudio Subyugación
Disponibilidad	Continuidad Indemnización Alarma

Tabla 1: Objetivos de garantía de información y Controles de operación [13]

3.4- Limitaciones

La limitación es el estado de la seguridad con respecto a las fallas y restricciones conocidas dentro del alcance de las operaciones. Son las vulnerabilidades, debilidades y problemas para mantener la separación entre un activo y una amenaza o para asegurar que los controles continúan funcionando correctamente.

Dentro del OSSTMM, las clasificaciones de Limitación son [12]:

a- Vulnerabilidad: es cada falla o error que pueda llevar a un acceso no autorizado o denegar un acceso legítimo.
Un ejemplo referido al canal de las redes de datos puede ser un proceso que permite la sobreescritura de áreas de memoria que lleven a la ejecución de código malicioso.

b- Debilidad: son todas las fallas o errores en los controles de interacción: autenticación, indemnización, resistencia, subyugación y continuidad.
Un ejemplo de debilidad en el canal de las redes de datos puede ser una pantalla que solicita credenciales de acceso que no posea límites en cuanto a la cantidad de intentos.

c- Preocupación: son todas las fallas en los controles de proceso: no repudio, confidencialidad, privacidad, integridad y alarma.
Un ejemplo de preocupación es un proceso que genere archivos de log con los datos de los participantes involucrados, pero no almacene correctamente la fecha y hora de la transacción.

d- Exposición: es cada acción no justificada, falla o error que provean visibilidad de los objetivos o activos, ya sea de forma directa o indirecta.
Un claro ejemplo de exposición son los banners que brindan información de la aplicación que está corriendo detrás de un puerto específico.

e- Anomalía: es cada elemento desconocido que no puede clasificarse dentro de las operaciones normales, ya que esto puede ser un síntoma para problemas de seguridad futuros.
Un ejemplo de anomalías dentro del canal de las redes de datos es una respuesta ICMP[10] proveniente de una dirección IP inexistente.

Para la comprender como las Limitaciones encajan en el marco de la seguridad operacional, es observa cuanto sigue:

Categoría		Seguridad Operacional	Limitaciones
Operaciones		Visibilidad	Exposición
		Acceso	Vulnerabilidad
		Confianza	
Controles	Clase A – Interactivo	Autenticación	Debilidad
		Indemnización	
		Resistencia	
		Subyugación	
		Continuidad	
	Clase B – Proceso	No repudio	Preocupación
		Confidencialidad	
		Privacidad	
		Integridad	
		Alarma	
			Anomalías

Tabla 2: Limitaciones en el marco de la seguridad operacional [13]

Las formas de gestionar las limitaciones es eliminar el área problemática que proporciona el punto interactivo, corregirlas o aceptarlas como parte de la actividad organizacional.

3.5- La seguridad real

El rol de los controles es reducir y manejar la porosidad. Las limitaciones entonces reducen la efectividad de la seguridad operacional y de los controles. El resultado de una auditoría que demuestra la seguridad, los controles y las limitaciones está exponiendo efectivamente la seguridad real. El término seguridad real hace referencia a una instantánea de la superficie de ataque en un ambiente operacional. [12]

3.6- Cumplimiento

El cumplimiento es un enfoque para la aplicación de las mejores prácticas en el área de tecnología de la información. El uso del OSSTMM está diseñado para que el analista vea y comprenda la seguridad y la protección. Por lo tanto, con el uso de esta metodología, cualquier cumplimiento es la producción de evidencia de gobernabilidad dentro del proceso de la seguridad organizacional.

[10] El protocolo ICMP, *Internet Control Messaging Protocol* (Protocolo de mensajes de control de Internet), sirve para informar de sucesos que han ocurrido en la red. Permite a los nodos intermedios enviar mensajes de control a los equipos que enviaron la información. [38]

4- Qué se necesita hacer con OSSTMM

4.1- Definición de alcance de una prueba de seguridad

La metodología cuenta con pasos y puede ser utilizada y adaptarla a cualquier organización en la que se requiera obtener información importante de una auditoria de seguridad de la información.

Los 7 pasos que se propone seguir para llevar a cabo una prueba de seguridad exitosa se describen a continuación: [14]

a- Definir los activos que se desea proteger. Los mecanismos de protección de dichos activos son los Controles, mismos que se probaran para identificar las Limitaciones.
b- 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.
c- Definir todo fuera de la zona de enfrentamiento que 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.
d- Definir como 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. 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.
e- Identificar los equipos que serán necesarios para cada prueba. Dentro de cada vector, las interacciones pueden ocurrir en varios niveles, estos mismos se clasifican según su función en cinco canales.
f- Determinar la información que se desea obtener de la prueba. El tipo de prueba debe ser definido de forma individual, la metodología OSSTMM identifica seis tipos de pruebas; 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 de forma individual la que más se adapte a las necesidades del proceso a desarrollarse en la evaluación de cada uno de los canales.
g- Hay que 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.

El resultado final será una medida de su Superficie de Ataque. La superficie de ataque es la parte no protegida del Alcance de un Vector definido.

4.2- Alcance de los canales

Es el entorno de seguridad operativo total posible para cualquier interacción con el activo. El alcance se compone de tres clases, divididos en cinco canales:

Clase	Canal	Descripción
Seguridad Física PHYSSEC[11]	Humano	Comprende el elemento humano cuando la interacción es física o psicológica.
	Físico	Comprende el elemento tangible tales como el hardware, maquinaria, puertas, ventanas, pizarras, escritos.
Seguridad del espectro SPECSEC[12]	Medios Inalámbricos	Comprende todas las comunicaciones electrónicas, señales y emanaciones en el espectro electromagnético.
Seguridad de las Comunicaciones COMSEC[13]	Telecomunicaciones	Comprende todas las redes de telecomunicaciones, donde la interacción es a través de líneas telefónicas.
	Redes de datos	Comprende todos los sistemas electrónicos y redes de datos donde la interacción es a través de líneas de red cableadas.

Tabla 3: Canales de la metodología OSSTMM [13]

Un análisis completo de seguridad requiere una evaluación de los 5 canales mencionados, aunque en la práctica los análisis de seguridad tienden a ser más limitados, abarcando sólo algunos canales. [12]

4.3- Tipos de prueba

Existen tipos de pruebas que se diferencian por la cantidad de información que el analista conoce sobre los objetivos, y lo que el objetivo sabe sobre la auditoría.

#	Tipo	Descripción
1	*Blind*	El Analista se involucra con el objetivo sin conocimiento previo de sus defensas, activos o canales. El objetivo está preparado para la auditoría. Conocida como *Ethical Hacking*.
2	*Double Blind*	El Analista se involucra con el objetivo sin conocimiento previo de sus defensas, activos o canales. No se notifica al objetivo con anticipación sobre el alcance de la auditoría. Conocida como Prueba de Penetración o Caja Negra.
3	*Gray Box*	El Analista se involucra al objetivo con un conocimiento limitado de sus defensas y activos, y un conocimiento completo de los canales. El objetivo está preparado para la auditoría. Conocida como Prueba de Vulnerabilidad.

[11] PHYSSEC: Physical Security (Seguridad Física)
[12] SPECSEC: Spectrum Security (Seguridad del espectro)
[13] COMSEC: Communications Security (Seguridad de las Comunicaciones)

#	Tipo	Descripción
4	*Double Gray Box*	El Analista se involucra al objetivo con un conocimiento limitado y un conocimiento completo de los canales. Se notifica al objetivo sobre el alcance, pero no los canales a probar. Conocida como Prueba de Caja Blanca.
5	*Tandem*	El Analista y el objetivo conocen el alcance de la auditoría. Conocido como Auditoría Interna.
6	*Reversal*	El Analista se involucra al objetivo con pleno conocimiento de sus procesos y seguridad operativa, pero el objetivo no sabe qué, cómo o cuándo realizará la prueba. Llamado como Equipo Rojo.

Tabla 4: Tipos de pruebas que abarca la metodología OSSTMM [13]

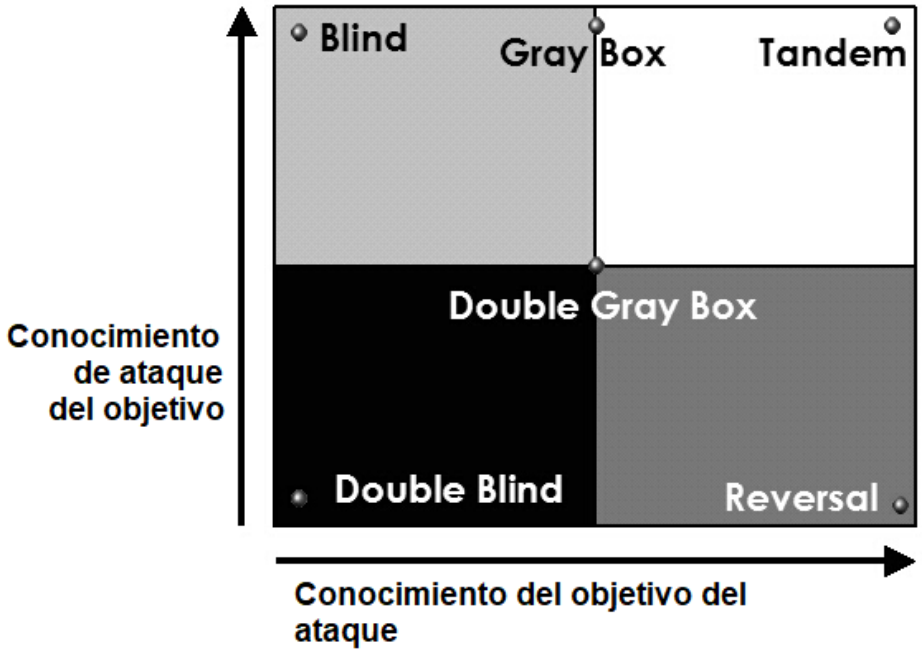


Ilustración 6: Conocimiento en base al ataque o el objetivo [13]

4.4- Reglas de compromiso

Estas reglas definen las pautas operativas de las prácticas aceptables en las pruebas de marketing y venta, la realización de trabajos de prueba y el manejo de los resultados de los compromisos de prueba:

a- Ventas y marketing
b- Evaluación / Entrega estimada
c- Contratos y negociaciones
d- Definición del alcance
e- Plan de prueba
f- Proceso de prueba
g- Informes

La descripción de las reglas de compromiso se podrá encontrar en forma explícita en el anexo Reglas de compromiso del presente Trabajo Final de Especialización.

5- Métricas de la seguridad operacional

Una métrica operativa es una medida constante que nos informa la comprobación de hechos en relación con el mundo físico en el que vivimos. Son operativas porque son números con los que podemos trabajar de manera constante, día a día, y de persona a persona.

Una métrica de seguridad adecuada debe evitar las tendencias inherentes a las evaluaciones de riesgos al garantizar que las mediciones tengan integridad. Estas cualidades se han combinado para crear los RAVs, una descripción imparcial y objetiva de una superficie de ataque.

5.1- Conociendo el RAV

La función básica del RAV es analizar los resultados de las pruebas y computar el valor actual de la seguridad basado en tres factores, seguridad operacional, controles y limitaciones. El resultado final es conocido como la puntuación RAV. Desde el punto de vista organizacional, el RAV, ayuda a optimizar y justificar las inversiones en medidas de seguridad. [15]

El RAV facilita exponer el tamaño de una superficie de ataque de dos formas prácticas. La primera forma es un cálculo directo, es el cálculo del Delta con escala 100, un número que describe la exposición específica de ese objetivo. En esta escala, 100 RAV es un equilibrio perfecto, por debajo es contar con pocos controles y por lo tanto una mayor superficie de ataque. Más de 100 RAV muestran más controles de los necesarios.

La segunda forma práctica de mostrar la superficie de ataque es comprender el panorama general. Esto se representa como la seguridad real.

El RAV da a conocer los siguientes puntos fundamentales de seguridad:

a- La inversión que se debe realizar en seguridad.
b- Que se debe proteger primero.
c- Qué soluciones de protección se necesita y cómo configurarlas para mayor eficacia.
d- Las mejoras que se obtiene mediante adquisiciones y procesos de seguridad específicos.
e- Medición de los esfuerzos y las mejoras periódicas de seguridad con las auditorias regulares.
f- Con la auditoría a los controles se conoce la reducción de exposición a amenazas.
g- El RAV declara que tan bien se resiste a los ataques.
h- El RAV contribuye con el cumplimiento normativo

5.2- Cómo hacer un RAV

El RAV fue diseñado originalmente para pruebas de operaciones, donde el auditor se enfoca en el comportamiento del objetivo en lugar de la configuración.

Obtiene lo que sabe de lo que hay para un vector en particular y no hace suposiciones sobre lo que no está allí. Cuenta todo lo que es visible e

interactivo fuera del alcance y permite la interacción no autenticada entre otros objetivos en el alcance.

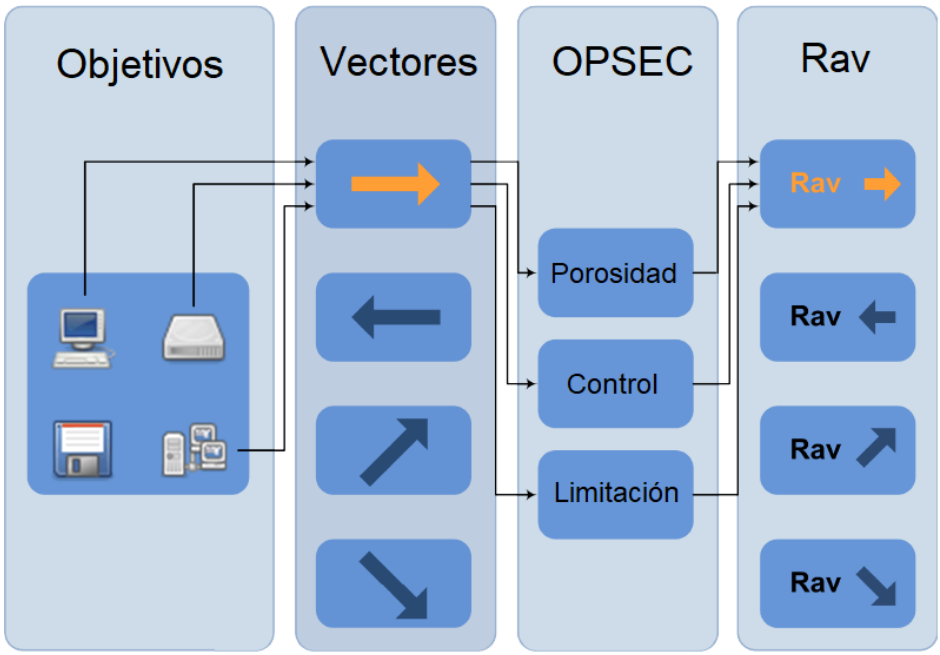


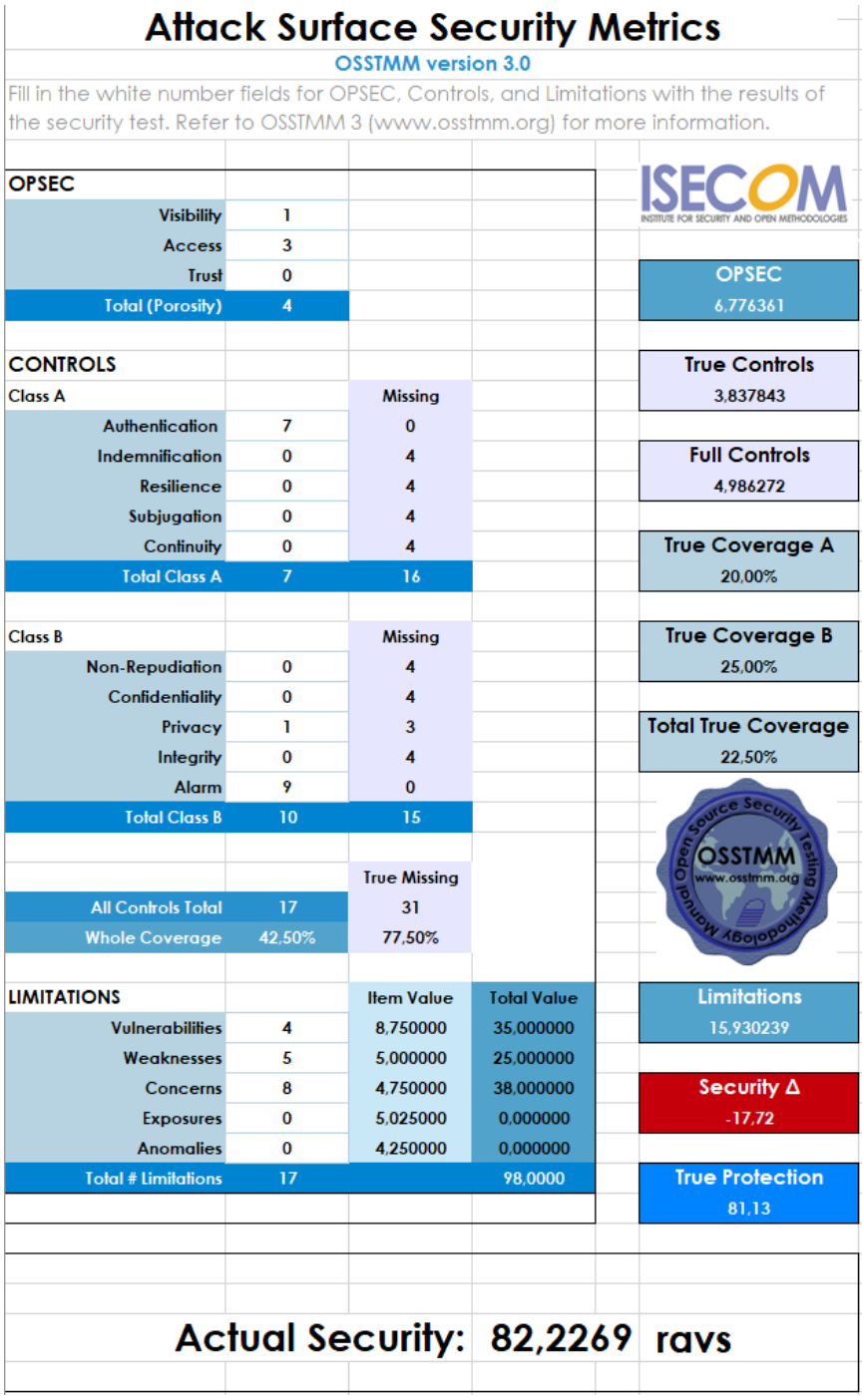
Ilustración 7: Cómo obtener el RAV [13]

La seguridad real solo se puede calcular por el alcance. Un cambio en el canal, vector o índice es un nuevo alcance y cálculo para la Seguridad Real.

Calculadora RAV: Una forma sencilla y directa de hacer RAVs es usar las hojas de cálculo creadas específicamente para calcular la superficie de ataque y varias métricas requeridas populares a partir de los datos de prueba. Esta hoja de cálculo está disponible en el sitio web de ISECOM[14].

La hoja de cálculo de RAV es para determinar el equilibrio entre porosidad, controles y limitaciones.

[14] El Instituto de Seguridad y Metodologías Abiertas (ISECOM) es una comunidad de investigación de seguridad abierta que ofrece recursos, herramientas y certificaciones originales en el campo de la seguridad.



Attack Surface Security Metrics

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

OPSEC			
Visibility	1		
Access	3		
Trust	0		
Total (Porosity)	4		

CONTROLS			
Class A		Missing	
Authentication	7	0	
Indemnification	0	4	
Resilience	0	4	
Subjugation	0	4	
Continuity	0	4	
Total Class A	7	16	
Class B		Missing	
Non-Repudiation	0	4	
Confidentiality	0	4	
Privacy	1	3	
Integrity	0	4	
Alarm	9	0	
Total Class B	10	15	
		True Missing	
All Controls Total	17	31	
Whole Coverage	42,50%	77,50%	

LIMITATIONS		Item Value	Total Value
Vulnerabilities	4	8,750000	35,000000
Weaknesses	5	5,000000	25,000000
Concerns	8	4,750000	38,000000
Exposures	0	5,025000	0,000000
Anomalies	0	4,250000	0,000000
Total # Limitations	17		98,0000

OPSEC	6,776361
True Controls	3,837843
Full Controls	4,986272
True Coverage A	20,00%
True Coverage B	25,00%
Total True Coverage	22,50%
Limitations	15,930239
Security Δ	-17,72
True Protection	81,13

Actual Security: 82,2269 ravs

Ilustración 8: La hoja de cálculo de RAV [13]

5.3- Convertir resultados de prueba en una medición de superficie de ataque

a- Seguridad operacional:

La medición de la superficie de ataque requiere las mediciones de visibilidad, confianza y acceso en relación con el alcance. A medida que se determina la visibilidad, su valor representa el número de objetivos en el alcance. La confianza es cualquier interacción no autenticada con cualquiera de los objetivos. El acceso es el número de puntos de interacción con cada objetivo.

b- Controles:

   El siguiente paso para calcular el RAV es definir los controles; los mecanismos de seguridad establecidos para brindar seguridad y protección durante las interacciones.

c- Limitaciones:

   Las limitaciones se verifican cuando es posible. Los valores de limitación se calculan en función de la porosidad y los controles del objetivo en el que se pueden encontrar.

6- Las diez propiedades de confianza

La descripción de las propiedades de confianza se podrá encontrar en forma explícita en el anexo Las diez propiedades de confianza del presente Trabajo Final de Especialización.

7- Flujo de trabajo

El flujo de OSSTMM comienza con una revisión de la postura del objetivo. La postura es la cultura, reglas, normas, contratos, legislación y políticas que definen el objetivo. Termina con comparaciones de resultados con alarmas, alertas, informes o registros de acceso.

Esta metodología separa lo que se debe hacer en este formato jerárquico:

a- Canal
b- Módulo
c- Tarea

El trabajo se detalla en la descripción del módulo para cada auditoría de canal en particular. Algunas auditorías se aplican a tecnologías que pueden abarcar el límite entre dos o más canales. Para todos los objetivos, el Analista debe anticipar la necesidad de definir una auditoría para incluir múltiples canales.

Esta metodología se aplica a los cinco canales. Tiene 17 módulos y las mismas propiedades se aplican a los cinco canales. Cada módulo tiene una entrada y una salida. La entrada es la información utilizada para realizar cada tarea. El resultado es la conclusión de las tareas completadas. Esta salida puede o no ser datos analizados para servir como entrada para otro módulo y esta salida puede servir además como entrada para más de un módulo o sección.

Algunas tareas no producen salida, lo que significa que existirán módulos para los que no hay entrada. Las tareas que no tienen salida resultante pueden significar que el canal se obstruyó de alguna manera durante la realización de las tareas; las tareas no se realizaron correctamente; las tareas no eran aplicables; los datos del resultado de la tarea se analizaron incorrectamente; o que la tarea revela una seguridad superior.

En la metodología OSSTMM, cada módulo comienza como una entrada y termina como una salida exactamente por la razón de mantener la parcialidad mínima.

El tiempo de prueba con los módulos es relativo al plan. Es importante determinar el alcance adecuado basado en el vector porque puede haber objetivos fuera del vector y dentro del alcance que no constituirán el alcance de la prueba actual. Esta metodología no determina el tiempo permitido antes de regresar con los datos de salida, depende del Analista, el objetivo, el entorno de prueba y del plan de prueba.

7.1- Las fases de prueba de la OSSTMM

Es preciso corroborar las configuraciones referidas a la seguridad, para un mejor análisis, también debe probar que el sistema en cuanto a su funcionamiento, para comprobar que todo se comporte como se espera. [12]

Dependiendo del negocio, la asignación de tiempo y los requisitos de la auditoría, el analista puede programar los detalles de la prueba por fase. El proceso de cuatro puntos para pruebas de seguridad está diseñado para una eficiencia, precisión y minuciosidad óptimas para garantizar la validez de la prueba. [13]

El proceso de cuatro puntos considera el análisis del entorno, la interacción directa, las emanaciones del objetivo y la modificación del ambiente, asegurando una revisión integral. [12]

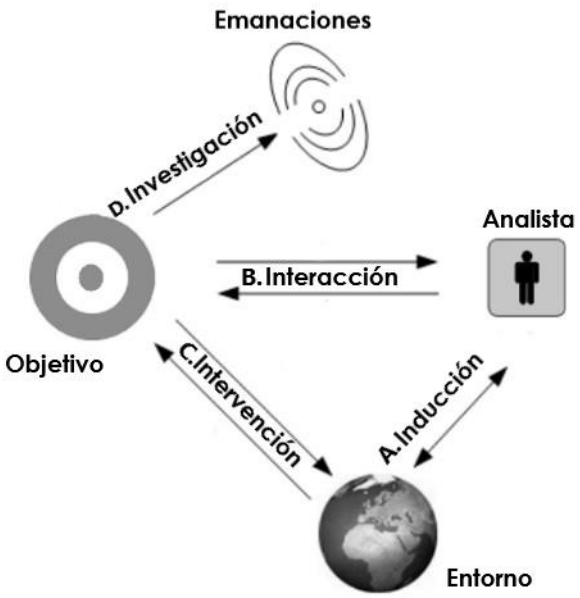


Ilustración 9: Interacciones dentro del proceso de 4 puntos [13]

La ejecución de la metodología OSSTMM se cuenta con las siguientes fases [16]:

a- Fase de inducción

El Analista estudia el entorno donde reside el objetivo, debido a que de una manera y otra condiciona su comportamiento y muchas veces dicho comportamiento deriva directamente de la influencia que recibe del ambiente. El entorno puede ser un sitio web, se debe identificar cual es el sitio web que se va a evaluar.

b- Fase de interacción

Interactuar directamente con el objetivo y observar las respuestas obtenidas. La interacción puede ser haciendo consultas, aplicando pruebas en el módulo de control de acceso, ver cómo responde, realizando conexiones de distintas formas, a través de distintos protocolos. Esta fase define el alcance.

c- Fase de investigación

Analizar las emanaciones que provengan del objetivo, así también como cualquier pista o indicador de las emanaciones mencionadas.

d- Fase de intervención

Estas pruebas se centran en los recursos que los objetivos requieren en el alcance. Modificar los recursos del entorno que necesita el objetivo y observar cómo responde.

Cada una de estas fases se divide en diferentes etapas que llevan el análisis a distintos niveles de profundidad, sin embargo, ninguna de ellas es ni más ni menos importante que la otra. [12]

La descripción de estas fases se podrá encontrar en forma explícita en el anexo Proceso de cuatro puntos del presente Trabajo Final de Especialización.

7.2- OSSTMM como una metodología

Poner todos los módulos en un grupo provee una metodología para conocer y trabajar. Esta es una metodología que es aplicable a todos y cada uno de los tipos de pruebas de seguridad. Ya sea que el objetivo sea un sistema, una ubicación, una persona, o un proceso en particular, esta metodología garantiza que la prueba sea completa y eficiente.

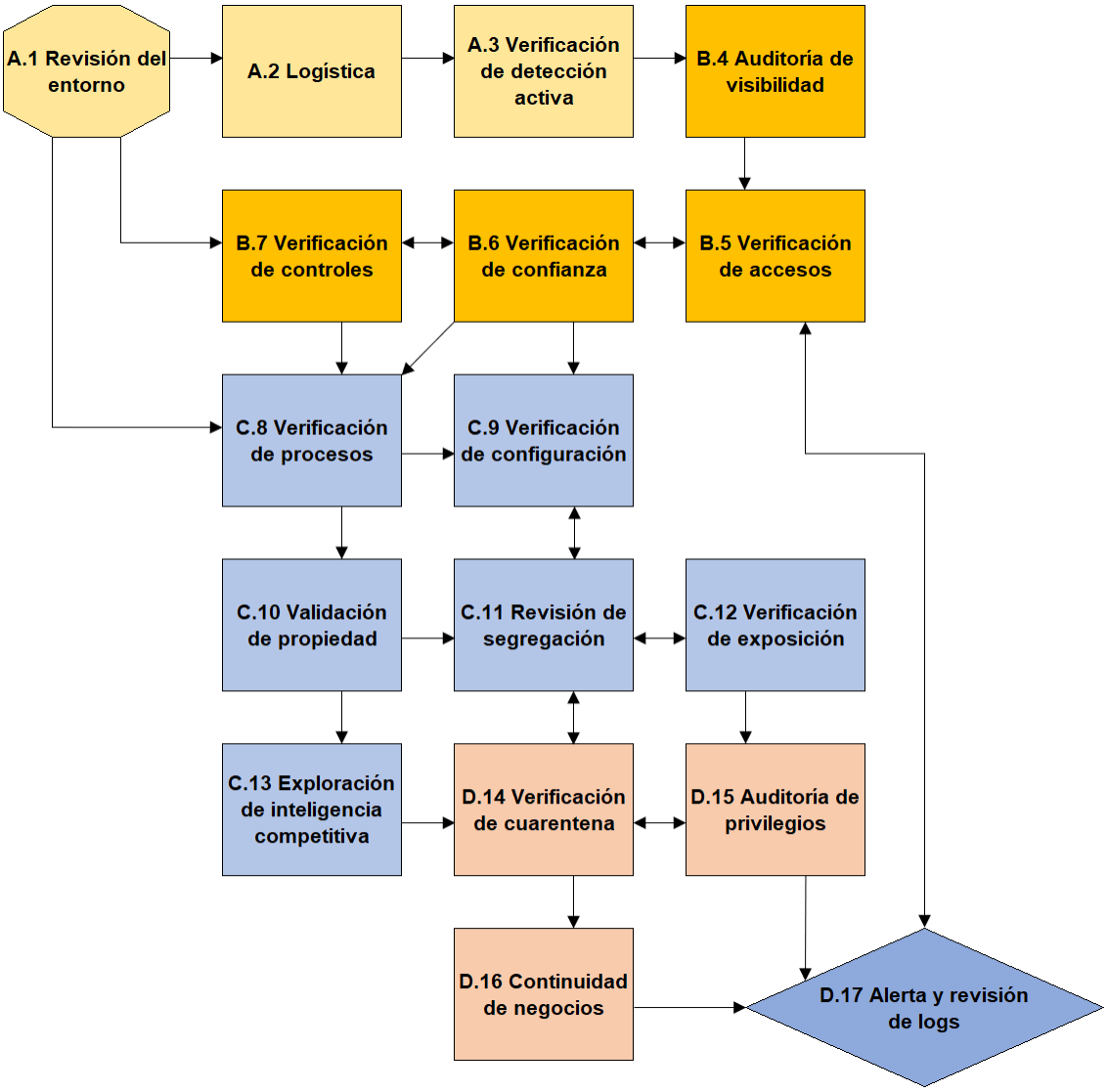


Ilustración 10: Metodología de comprobación de seguridad [13]

8- CANALES

Un análisis completo de seguridad requiere una evaluación de los canales humano, físico, medios inalámbricos, telecomunicaciones y redes de datos. En la práctica el analista de seguridad puede abarcar sólo algunos canales.

Un objetivo de cumplimiento en las pruebas de seguridad en los distintos canales es la medición de brechas con el estándar de seguridad requerido descrito en la política de la empresa, las regulaciones del sector o la legislación regional.

Es preciso que el Analista cuente con múltiples herramientas y métodos para la ejecución de algunas tareas a fin de garantizar que no se levanten sospechas entre el personal y que las pruebas no se invaliden debido a un descubrimiento temprano. También sería pertinente limitar las personas de prueba a uno por departamento u otro límite adecuado para no levantar sospechas.

Los analistas ejecutores de las pruebas precisan habilidades de pensamiento crítico para garantizar que la recopilación de datos reales genere resultados reales a través de la correlación y el análisis.

8.1- Prueba de seguridad humana

La seguridad humana es un componente de la seguridad física e incluye las operaciones psicológicas. Para probar este canal requiere la interacción con personas en posiciones de control de activos.

Este canal abarca la participación de las personas, principalmente el personal operativo dentro del alcance. Se puede llegar a considerar esta prueba como ingeniería social, pero el objetivo de cumplimiento de las pruebas de seguridad en este canal es la prueba de conciencia de seguridad del personal.

Los analistas competentes requerirán habilidades de personas diligentes.

8.2- Prueba de seguridad física

La seguridad física es una clasificación para la seguridad material dentro del ámbito físico que se encuentra dentro de los límites del espacio 3D interactivo con humanos. Probar este canal requiere una interacción no comunicativa con barreras y humanos en posiciones de control de activos.

Este canal cubre la interacción del Analista en la proximidad de los objetivos. Si bien algunos servicios consideran esto simplemente como "irrumpir y entrar", el verdadero objetivo de cumplimiento de las pruebas de seguridad en este canal es la prueba de barreras físicas y lógicas.

Los analistas también deberán estar preparados para la posibilidad de daños corporales accidentales causados por barreras y armas convencionales, interacciones con animales, sujeción a bacterias, virus y hongos dañinos, exposición a radiación electromagnética y de microondas, especialmente aquellas que pueden dañar permanentemente la vista o la audición, y agentes químicos venenosos o corrosivos en cualquier forma.

Los analistas competentes requerirán fuerza física, resistencia, y agilidad.

8.3- Prueba de seguridad inalámbrica

La seguridad del espectro es la clasificación de seguridad que incluye la seguridad electrónica, la seguridad de señales y la seguridad de las emanaciones. La seguridad electrónica es para denegar el acceso no autorizado a información derivada de la interceptación y análisis de radiaciones electromagnéticas ajenas a las comunicaciones. La seguridad de señales es para proteger las comunicaciones inalámbricas del acceso no autorizado y las interferencias. La seguridad de emanación es para prevenir las emanaciones

de la máquina que, de ser interceptadas y analizadas, revelarían la información transmitida, recibida, manejada o procesada de otra manera por equipos de sistemas de información. La prueba de este canal requiere la interacción con las barreras de los activos sobre las frecuencias electromagnéticas y de microondas.

Este canal cubre la interacción del Analista dentro del rango de proximidad de los objetivos. Si bien algunos servicios consideran esto simplemente como escaneo, el verdadero objetivo de cumplimiento de la prueba de seguridad en este canal es la prueba de barrera física y lógica.

Se requerirá que el Analista tenga la protección adecuada contra fuentes de energía electromagnética y otras formas de radiación. Los analistas también deberán estar preparados para la posibilidad de daños corporales accidentales por exposición a radiación electromagnética y de microondas, especialmente aquella que puede dañar permanentemente la vista o la audición. El equipo adecuado debe advertir cuando se encuentre dentro del rango de radiación electromagnética y de microondas de -12dB y más. Las frecuencias específicas pueden afectar negativamente a los dispositivos médicos implantados, causar vértigo, dolores de cabeza, calambres estomacales, diarrea y otras molestias tanto a nivel emocional como físico.

Los analistas competentes requerirán un conocimiento suficiente de la radiación electromagnética y microondas.

8.4- Pruebas de seguridad de telecomunicaciones

La Seguridad de Telecomunicaciones es una clasificación para la seguridad material dentro del ámbito de seguridad electrónica que está dentro de los límites de las telecomunicaciones por cables.

Este canal cubre la interacción del Analista con los objetivos. Si bien algunos servicios consideran esto simplemente como *phreaking*[15], el verdadero objetivo de cumplimiento de las pruebas de seguridad en este canal es la prueba de barreras lógicas.

Se requerirá que el Analista evite sospechas entre el personal por el timbre continuo y secuencial de los teléfonos. Los analistas también deberán estar preparados para trabajar con equipos de telecomunicaciones digitales y analógicos, analizadores de frecuencia de sonido y dentro de redes de información que brinden contenido regional a través de proveedores de telefonía local.

Los analistas competentes requerirán experiencia en electrónica tanto en telefonía analógica como digital.

[15] El Phreaking o crackin telefónico, es la actividad por medio de la cual algunas personas con ciertos conocimientos y herramientas de *hardware* y *software* pueden engañar a las compañías telefónicas para que éstas no cobren las llamadas que se hacen. [39]

8.5- Pruebas de seguridad de redes de datos

Las pruebas para el canal de Seguridad de Redes de Datos requieren interacciones con las protecciones operativas de la red de comunicación de datos existente que se utilizan para controlar el acceso a la propiedad.

Este canal cubre la participación de los sistemas informáticos, principalmente las redes operativas dentro del alcance o marco objetivo. Si bien algunas organizaciones consideran esto simplemente como pruebas de penetración, el verdadero objetivo de cumplimiento de las pruebas de seguridad en este canal es la interacción del sistema y las pruebas de calidad operativa.

Durante las pruebas, los operadores finales y la inteligencia artificial pueden reconocer los ataques en curso tanto por proceso como por firma. Por esta razón, se requerirá que el Analista tenga una variedad suficiente de métodos para evitar la divulgación de las pruebas o trabajar con los operadores para asegurarse de que se revele dónde falla la seguridad y dónde tiene éxito. Las pruebas que se centran solo en el descubrimiento de nuevos problemas solo dejan espacio para correcciones y no diseños para mejoras futuras.

Los analistas requerirán conocimientos adecuados de redes, habilidades de prueba de seguridad diligentes.

9- Cumplimiento

El cumplimiento es la alineación con un conjunto de políticas generales, donde el tipo de cumplimiento requerido depende de la región y el gobierno actual, la industria y los tipos de negocios y la legislación de respaldo.

El OSSTMM reconoce tres tipos de cumplimiento:

a- Legislativo:

   El cumplimiento de la legislación está de acuerdo con la región donde se puede hacerse cumplir la legislación. El incumplimiento de la legislación puede dar lugar a cargos penales. Algunos ejemplos son Sarbanes-Oxley, HIPAA y las diversas leyes de protección de datos y privacidad.

b- Contractual:

   El cumplimiento de los requisitos contractuales está de acuerdo con la industria o dentro del grupo que requiere el contrato y puede tomar medidas para hacerse respetar el cumplimiento. El incumplimiento de los requisitos contractuales a menudo conduce al despido del grupo, pérdida de privilegios, pérdida de reputación, cargos civiles y, en algunos casos donde existe legislación para respaldar al organismo regulador, cargos penales. Un ejemplo es el estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS[16]).

c- Basado en estándares:

[16] *Payment Card Industry Data Security Standard*: Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago.

El cumplimiento de los estándares está de acuerdo con la empresa u organización donde el cumplimiento de los estándares se impone como política. El incumplimiento de los estándares conduce al despido en la organización, la pérdida de privilegios, la pérdida de reputación o confianza en la marca, cargos civiles y, en algunos casos donde existe legislación para apoyar a los responsables políticos, cargos penales. Algunos ejemplos son OSSTMM, ISO 27001[17] e ITIL[18].

El OSSTMM se desarrolla teniendo en cuenta la legislación necesaria, los requisitos contractuales y el cumplimiento de las normas. El enfoque principal del OSSTMM, sobre los objetivos de cumplimiento creados, es la seguridad. Las medidas de cumplimiento que requieren productos o servicios específicos, comerciales o de otro tipo, a menudo a través de esfuerzos especialmente presionados, puede que haya buenas intenciones; sin embargo, en realidad puede ser un desperdicio de recursos o una versión de seguridad menor que la deseada.

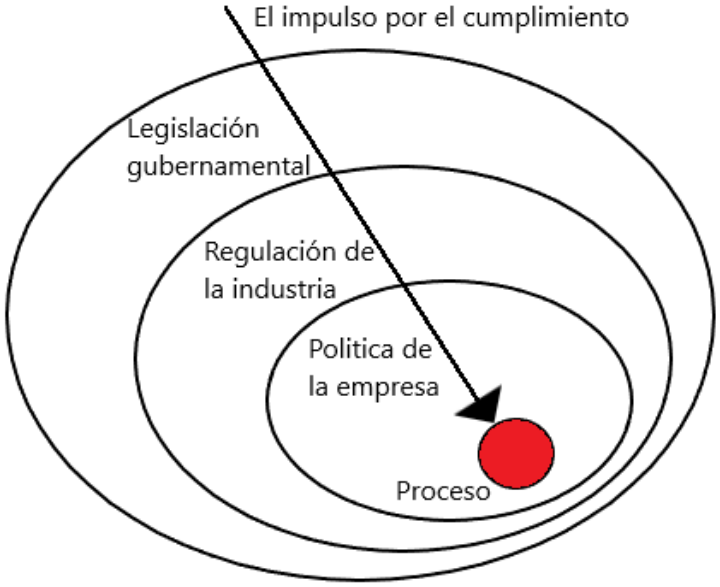


Ilustración 11: Cumplimiento en base a OSSTMM [17]

10- Informe con el reporte STAR

STAR es el informe de auditoría de pruebas de seguridad. Hace referencia a las palabras en inglés *Security Test Audit Report*. Su propósito es presentarse como un resumen ejecutivo el cálculo preciso que indique la superficie de ataque de los objetivos probados dentro de un alcance particular.

[17] ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. [40]

[18] ITIL corresponde a una metodología de gestión que propone una serie de prácticas estandarizadas que nos ayudan a mejorar la prestación de un servicio, reorganizando la manera que tiene la empresa de trabajar y en particular, la del departamento de tecnología de la información. [41]

La plantilla proporcionada debe completarse totalmente y debe ser firmada por el Analista. Posteriormente, se proporciona a ISECOM con el permiso explícito del propietario del alcance junto con el informe de prueba de seguridad completo.

Al proveer el STAR a ISECOM para la verificación, se imprime, firma el auditor de verificación y es sellado por ISECOM. Se proporciona un certificado para todas las pruebas que indican que el alcance ha sido comprobado y verificado. No hay aprobación ni falla, ya que no existe un valor de RAV de superficie de ataque particular que exista para todos los ámbitos como el límite entre uno que pasa y uno que falla.

Desde el sitio de ISECOM es posible obtener la plantilla para realizar un reporte del tipo STAR. URL: https://www.isecom.org/STAR.3.pdf [18]

La portada del reporte STAR se podrá encontrar en el anexo Reporte STAR del presente Trabajo Final de Especialización.

11- Caso de estudio: prueba de seguridad en la infraestructura

A continuación, se mostrará un ejemplo simple donde se analizará la seguridad desde el punto de vista de la infraestructura. [12]

El esquema del ejemplo es como sigue:

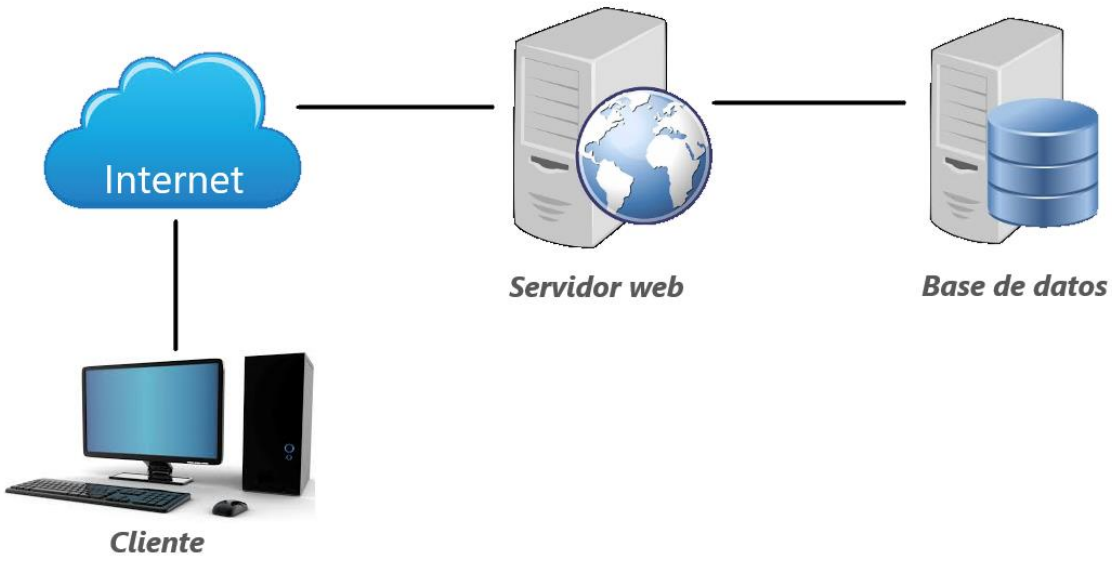


Ilustración 12: Ejemplo infraestructura simple [12]

La estructura consta de las siguientes partes:

- Un servidor web corriendo una aplicación que puede ser accedida a través de Internet.
  - Servidor Apache
  - Soporte para PHP
  - Sólo permite conexiones HTTPS

- El servidor responde mensajes ICMP echo request/reply (ping)
    - Una base de datos que contiene la información de la aplicación.
    - Servidor MySQL
    - Sólo tiene en escucha al puerto 3306
    - No responde pings.

11.1- Seguridad operacional

El análisis será sobre la infraestructura y no sobre las posibles interacciones de la aplicación web que pueda estar corriendo sobre el servidor.

a- Acceso

Contar todos los puntos de acceso por cada lugar de interacción.
Con las herramientas NMAP y Ping es posible determinar los puertos abiertos del servidor expuesto a internet y la respuesta a ICMP echo request/reply.

Comando 1: ping servidorweb
Resultado: Host activo

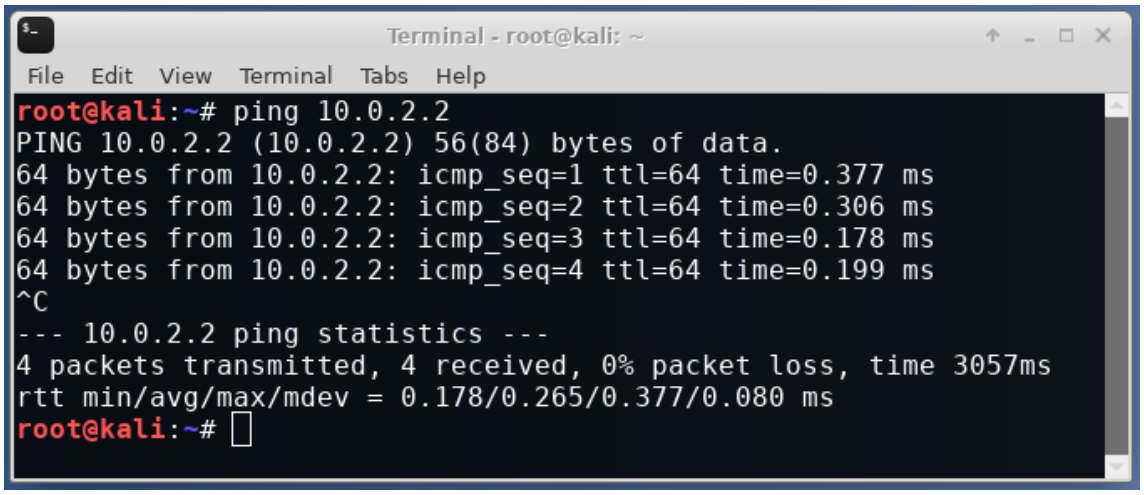


Ilustración 13 Comando ping

Comando 2: nmap -Pp servidorweb -sS -T4
Resultado: Puerto abierto 443, el resto de los puertos están cerrados.

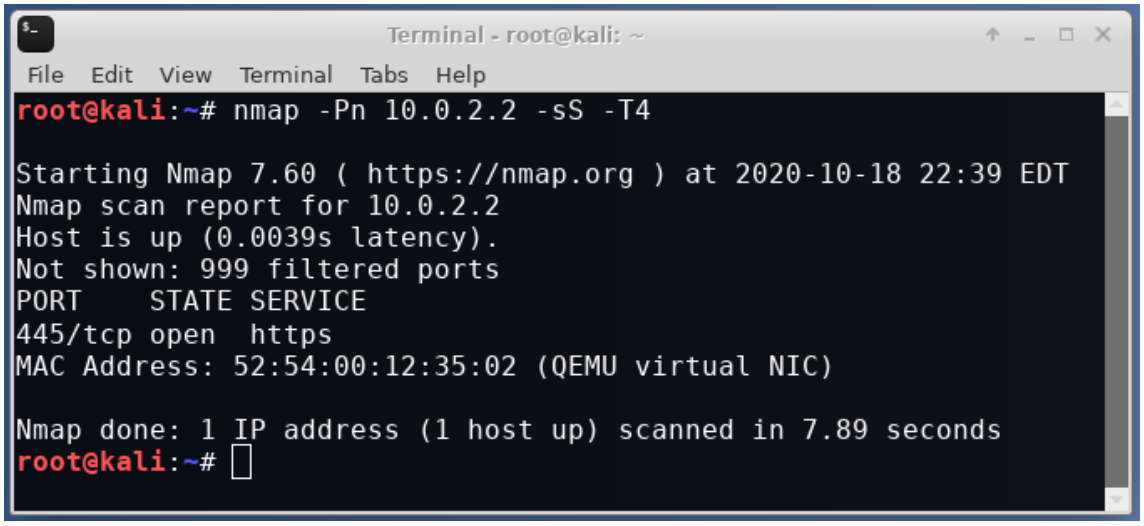


Ilustración 14 Herramienta NMAP

Accesos: 2 → puerto 443 y respuesta a ping

b- Visibilidad

Contar todos los puntos visibles dentro del objetivo.
Existe un solo host visible desde internet y es el que está directamente expuesto a la web.
Pero como existe la posibilidad de interactuar con la base de datos a través del servidor web se puede determinar claramente que existe un servidor de base de datos, por lo tanto, la visibilidad cuenta como 2.

Visibilidad: 2 → servidor web y servidor de base de datos

c- Confianza

Contar cada punto de confianza por cada lugar de interacción.
El único punto de confianza que existe es la comunicación entre el servidor de base de datos y el servidor web.

Confianza: 1 → comunicación entre el servidor de base de datos y el servidor web

11.2- Controles

Controles en el servidor HTTPS

a- Confidencialidad: El protocolo https provee confidencialidad debido a que la información que es transmitida entre el cliente y el servidor se encuentra encriptada. El control de privacidad no se aplica, debido a que no se protege el método de comunicación; es decir, un atacante puede saber que el protocolo usado es https, aunque no pueda determinar el contenido.

Suma 1 a los controles.

b- Integridad: El protocolo https provee integridad ya que una modificación no autorizada en los datos sería detectada por el mismo.

Suma 1 a los controles.

c- Subyugación: El hecho que la comunicación sea únicamente bajo el protocolo https indica que el control de subyugación es aplicado correctamente. No se permite al cliente elegir la forma de comunicación, el servidor determina que el intercambio de datos se hace bajo https.

Suma 1 a los controles.

d- No repudio: El sistema de logs provisto por Apache provee el control de no repudio.

Suma 1 a los controles.

Controles en el servidor de base de datos

e- Autenticación: El acceso a la base de datos requiere credenciales válidas, por lo tanto, el control de autenticación está siendo aplicado.

Suma 1 a los controles.

f- Subyugación: El acceso está únicamente permitido entre el servidor web y la base de datos, cualquier otro intento de conexión que no sea por ese medio será denegado.

Suma 1 a los controles.

11.3- Limitaciones

a- Preocupación: El servidor web acepta cifrado de 56 bit, que son considerados como débiles.

Suma 1 a las limitaciones.

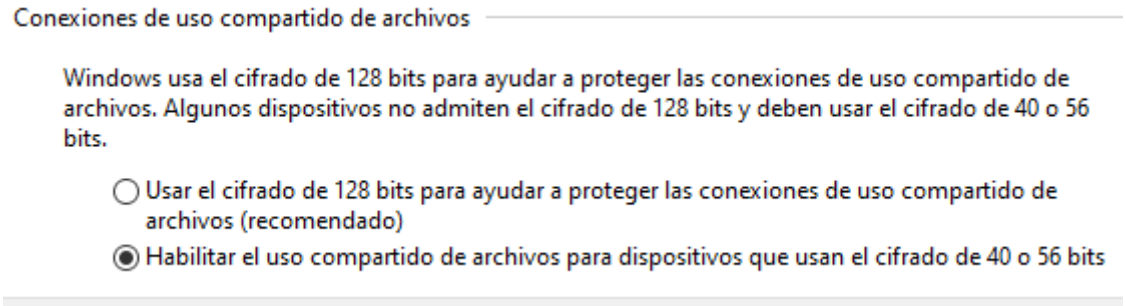


Ilustración 15 Configuración de uso compartido en 56 bit

b- Exposición: El banner obtenido a través de una conexión al servidor https brinda información.

Suma 1 a las limitaciones.

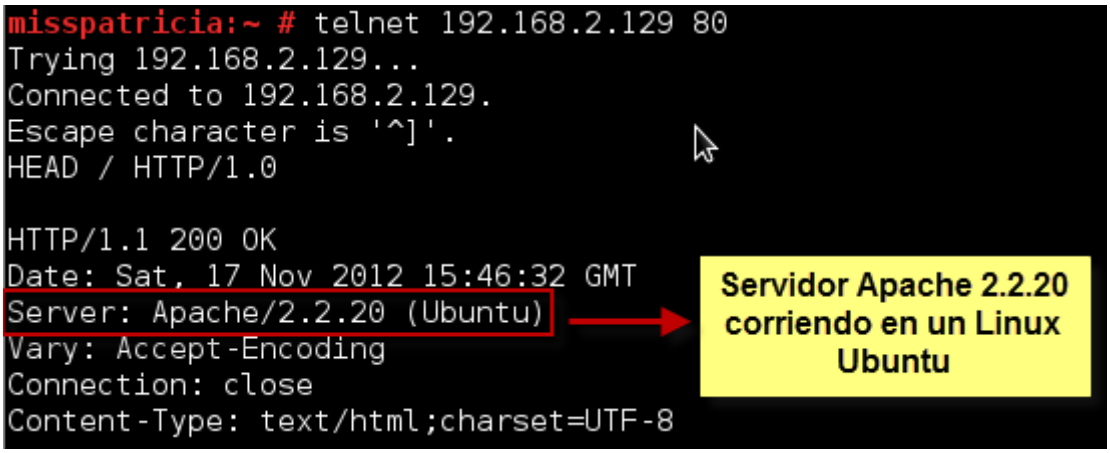


Ilustración 16 Ejemplo de Banner [19]

11.4- Calculadora de RAVs de OSSTMM

Posterior a la obtención de los valores, se procede a cargar estos valores de entrada en la planilla que provee ISECOM para el cálculo de RAVs. Los resultados son calculados automáticamente.

Attack Surface Security Metrics

OSSTMM version 3.0

OPSEC	
Visibility	2
Access	2
Trust	1
Total (Porosity)	5

CONTROLS		
Class A		Missing
Authentication	1	4
Indemnification	0	5
Resilience	0	5
Subjugation	2	3
Continuity	0	5
Total Class A	3	22

Class B		Missing
Non-Repudiation	1	4
Confidentiality	1	4
Privacy	0	5
Integrity	1	4
Alarm	0	5
Total Class B	3	22

		True Missing
All Controls Total	6	44
Whole Coverage	12,00%	88,00%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	0	9,800000	0,000000
Weaknesses	0	5,400000	0,000000
Concerns	1	5,400000	5,400000
Exposures	1	0,904000	0,904000
Anomalies	0	0,376000	0,000000
Total # Limitations	2		6,3040

True Controls	3,187403
Full Controls	3,187403
True Coverage A	12,00%
True Coverage B	12,00%
Total True Coverage	12,00%
Security Δ	-11,94
True Protection	88,06

Actual Security: 88,15 ravs

Ilustración 17: RAV - Attack Surface Security Metrics. [12]

11.5- 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 ilustración 12 marcada de color rojo, cual muestra el equilibrio que existe entre los valores numéricos de la porosidad, los controles y las limitaciones, por lo tanto, 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.

La otra expresión permite analizar el riesgo de la superficie de ataque es la Seguridad Actual, en donde para el canal auditado posee un valor numérico de 88,15 RAVs, lo que se traduce en una deficiencia del alcance de aproximadamente un 12%; y por tanto se puede asegurar que existe un porcentaje de vulnerabilidades dentro del sistema de seguridad que se maneja dentro de la organización.

12- Beneficios de la metodología OSSTMM

Este estándar cuenta con licencia de metodología abierta, por esta razón todos lo pueden utilizar, pero es importante saber cómo utilizarlo.

Es comprensible, lógica, rigurosa y basada en la ética.

Existen certificaciones asociadas al uso de este estándar, hay dos principalmente, la OPST[19] es del profesional *pentester*, el que debe ejecutar la prueba, luego se encuentra el OPSA[20] que es un nivel menor, con el perfil para el analista que interpreta el informe que se entrega a OSSTMM.

Representa el estándar de facto[21], ordenado, modular y de calidad profesional. Además, permite cumplir con estándares internacionales.

En los módulos se puede observar las distintas dimensiones de la seguridad, con descripción de las tareas a llevar a cabo. Aquí se evalúan desde procesos, personas, y tecnología.

No solo aborda temas técnicos, también se encarga de la forma en que la metodología debe ser comercializado, la forma en que los resultados deben ser presentados, normas éticas y legales que deben ser consideradas, tiempos que deberían ser consideradas para cada tarea.

Que sea estándar por las métricas permite realizar el análisis de manera repetible, siguiendo siempre los mismos pasos y que se trate de aplicar el menor criterio personal posible del auditor. [16]

---

[19] OPST: *OSSTMM Professional Security Tester*
[20] OPSA: *OSSTMM Professional Security Analyst*
[21] Los estándares de facto son normas que se caracterizan por no haber sido legitimadas por un organismo de estandarización, generalmente son aceptados y ampliamente utilizados por iniciativa propia de un gran número de interesados. [42]

Se obtiene el RAV el cual permite una medición cuantitativa del nivel de riesgo, un reporte preciso. El RAV habilita el cálculo de ROI[22] de las medidas de seguridad, por lo tanto, permite justificar las inversiones en seguridad tecnología de la información. [20]

13- Conclusiones

En la actualidad la información representa el activo más valioso de toda organización. Con la implementación de tecnologías para una eficiente comunicación y manipulación de información en sistemas, trae consigo amenazas de seguridad de un amplio rango de fuentes incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o negación de ataques de servicio se hacen cada vez más comunes, y más ambiciosas.

Se debe tener en cuenta que los avances tecnológicos avanzan velozmente al igual que los delitos dirigido a la información, con lo que es necesario tomar acciones para contar con procesos y políticas de parches, actualizaciones de software, adquisición de nuevos productos tanto en software como hardware, lo cual debe demostrar que la protección de estos activos es adecuado y eficiente. [21]

Esta protección también debe contar con evaluaciones periódicas para corroborar que sean adecuadas y suficientes, o en lo contrario podrían afectar a las tareas y procesos cotidianos de la organización.

Las razones de tiempo o económicas no deben evitar la aplicación de análisis y evaluación a los procesos y el analista no debe ser protagonista de adquirir restricciones sin una razón válida para ello.

De acuerdo con lo que se necesite y como se necesite evaluar los procesos, existen varios tipos de evaluaciones y metodologías para comprobar la calidad de la seguridad de la información implantada.

Hoy en día las metodologías de pruebas son necesarias para asegurar un mínimo de calidad en la seguridad de cualquier producto. La mala gestión en la evaluación de seguridad puede resultar en valores elevados a la larga y daño en la imagen y reputación de la organización. [16]

Una vez empleada la metodología de evaluación debe ser capaz de devolver métricas para confirmar que se ha llevado a cabo adecuadamente y para comprender el resultado de la aplicación de esta.

La metodología OSSTMM se ha convertido en una autentica referencia para los organismos que quieren desarrollar una comprobación de calidad, ordenado y eficiente. Es uno de los estándares profesionales más completos y comúnmente utilizados a la hora de revisar la seguridad de los sistemas. El

[22] El ROI (*Return On Investment*) o Retorno de Inversión es el indicador de las ganancias que se han obtenido tras llevar a cabo determinadas acciones. [43]

cual permite brindar seguridad en el manejo de la información en las organizaciones. [22]

OSSTMM puede ser integrada fácilmente con las normas existentes en la organización para asegurar una auditoría de seguridad completa a través de todos los canales.

Se ha desarrollado principalmente como una metodología de auditoría de seguridad que evalúa en función de los requisitos normativos y de la industria. La ayuda que brinda es que sea una base para desarrollar una que se adapte a los reglamentos y marcos según la necesidad de la organización. [23]

El manual OSSTMM incluye información para planificar el proyecto de evaluación, cuantificar resultados, y las reglas del contrato para realizar auditorías de seguridad.

La metodología tiene la propiedad de ser fácilmente integrada con leyes y política existentes para asegurar una auditoría exhaustiva a través de todos los canales, como ser la interacción humana, física, o telecomunicaciones. [24]

Es elemental que cada una de las acciones planificadas dentro de la evaluación se prevea no violar la ley, reglamento o política, y además cada una de las actividades deben ser coordinadas con la organización que requiere la implementación de este tipo de pruebas a su seguridad. [25]

El hecho de que la metodología separe en canales las pruebas que se deben realizar es bueno, no solo para el analista; sino también para la organización porque permite conocer con precisión en que parte de la infraestructura del sistema de seguridad se encuentra el mayor número de vulnerabilidades y así poder aplicar las correcciones necesarias en el canal que se necesite. [14]

STAR es la plantilla de evaluación de OSSTMM que proporciona una evidencia de la comprobación de seguridad, además es un proceso de formalización de la evaluación. Brinda una apropiada visión general del estado de seguridad real de la organización. [26] Además, es un resumen ejecutivo preciso que indica la superficie de ataque de los objetivos probados dentro de un alcance particular.

La metodología OSSTMM proporciona métricas a través del RAV, se utiliza para la superficie de ataque de un objetivo o alcance, abarca a lo que se encuentra expuesto. Su utilización a lo largo del tiempo proporciona una representación gráfica y de los cambios en el estado. Esta métrica es precisa para medir la susceptibilidad a los ataques.

La función básica del RAV es analizar los resultados de las pruebas y medir el valor actual de la seguridad basado en tres factores, seguridad operacional, controles y limitaciones. El RAV ayuda a optimizar y justificar las inversiones en medidas de seguridad.

Lo que se obtiene del uso de OSSTMM es adquirir una comprensión de la interconexión de las personas, los procesos, los sistemas y el software. Cuando probamos las operaciones, se obtiene el panorama general de las

relaciones. Podemos ver la interconexión de las operaciones con gran detalle. Es posible trazar un mapa de cómo las personas, los negocios y las operaciones subsisten y prosperan entre sí.

14- Anexo

14.1- Reglas de compromiso

Estas reglas definen las pautas operativas de las prácticas aceptables en las pruebas de marketing y venta, la realización de trabajos de prueba y el manejo de los resultados de las pruebas. [13]

A. Ventas y marketing
   1) El uso del miedo, la incertidumbre, la duda y el engaño no se puede utilizar en las presentaciones de ventas o marketing, sitios web, materiales de apoyo, informes o discusión de pruebas de seguridad con el propósito de vender o proporcionar pruebas de seguridad. Esto incluye destacar delitos, hechos, perfiles de delincuentes o piratas informáticos glorificados y estadísticas para motivar las ventas, entre otros.
   2) Está prohibido ofrecer servicios gratuitos por no penetrar en el objetivo.
   3) Están prohibidos los concursos públicos de craqueo, piratería y allanamiento para promover la garantía de seguridad para las ventas o el marketing de pruebas de seguridad o productos de seguridad.
   4) Solo se permite nombrar clientes pasados o presentes en el marketing o ventas para clientes potenciales si el trabajo para el cliente fue específicamente el mismo que se comercializó o vendió y el cliente designado ha proporcionado un permiso por escrito para hacerlo.
   5) Se requiere que los clientes sean informados de manera veraz y objetiva con respecto a sus medidas de seguridad y protección. La ignorancia no es una excusa para una consultoría deshonesta.

B. Evaluación / Entrega estimada
   6) Está estrictamente prohibido realizar pruebas de seguridad en cualquier ámbito sin el permiso explícito por escrito del propietario del objetivo o la autoridad correspondiente.
   7) Las pruebas de seguridad de sistemas, ubicaciones y procesos obviamente altamente inseguros e inestables están prohibidas hasta que se haya implementado la infraestructura de seguridad adecuada.

C. Contratos y Negociaciones
   8) Con o sin un contrato de Acuerdo de Confidencialidad, el Analista de Seguridad debe proporcionar confidencialidad y no divulgación de la información del cliente y los resultados de las pruebas.
   9) Los contratos deben limitar la responsabilidad al costo del trabajo, a menos que se haya demostrado una actividad maliciosa.
   10) Los contratos deben explicar claramente los límites y peligros de la prueba de seguridad como parte de la declaración de trabajo.
   11) En el caso de pruebas remotas, el contrato debe incluir el origen de los Analistas por dirección, número de teléfono o dirección IP.
   12) El cliente debe proporcionar una declaración firmada que proporcione permiso de prueba que exima a los Analistas de la intrusión dentro del alcance y la responsabilidad por daños al costo del servicio de auditoría, con la excepción de que se haya demostrado actividad maliciosa.
   13) Los contratos deben contener nombres y números de teléfono de los contactos de emergencia.
   14) El contrato debe incluir permisos claros y específicos para pruebas que involucren fallas de supervivencia, denegación de servicio, pruebas de procesos e ingeniería social.
   15) Los contratos deben contener el proceso para futuros cambios de contrato y declaración de trabajo.

16) Los contratos deben contener conflictos de interés verificados para una prueba e informe de seguridad real.

D. Definición del alcance
   17) El alcance debe estar claramente definido contractualmente antes de verificar los servicios vulnerables.
   18) La auditoría debe explicar claramente los límites de cualquier prueba de seguridad según el alcance.

E. Plan de prueba
   19) El plan de prueba no puede contener planes, procesos, técnicas o procedimientos que estén fuera del área de experiencia o nivel de competencia del Analista.

F. Proceso de prueba
   20) El Analista debe respetar y mantener la seguridad, la salud, el bienestar y la privacidad del público tanto dentro como fuera del alcance.
   21) El Analista siempre debe operar dentro de la ley de la ubicación física de los objetivos, además de las reglas o leyes que rigen la ubicación de prueba del Analista.
   22) Para evitar aumentos temporales de la seguridad durante la prueba, solo notifique a las personas clave sobre la prueba. Es el juicio del cliente el que discierne quiénes son las personas clave; sin embargo, se supone que serán los guardianes de la información y las políticas, los administradores de los procesos de seguridad, el personal de respuesta a incidentes y el personal de operaciones de seguridad.
   23) Si es necesario para las pruebas con privilegios, el cliente debe proporcionar dos tokens de acceso separados, ya sean contraseñas, certificados, números de identificación seguros, insignias, etc. y deben ser típicos para los usuarios de los privilegios que se están probando en lugar de estar especialmente vacíos o seguros. accesos.
   24) Cuando las pruebas incluyen privilegios conocidos, el analista debe probar primero sin privilegios (como en un entorno de caja negra) antes de volver a probar con privilegios.
   25) Se requiere que los Analistas conozcan sus herramientas, de dónde provienen, cómo funcionan las herramientas y que las prueben en un área de prueba restringida antes de usar las herramientas en la organización del cliente.
   26) La realización de pruebas que están destinadas explícitamente a probar la denegación de un servicio o proceso o la capacidad de supervivencia solo se pueden realizar con permiso explícito y solo en el alcance donde no se produzcan daños fuera del alcance o la comunidad en la que reside el alcance.
   27) Las pruebas que involucren a personas solo se pueden realizar en aquellas identificadas en el alcance y no pueden incluir a personas privadas, clientes, socios, asociados u otras entidades externas sin el permiso por escrito de esas entidades.
   28) Las limitaciones verificadas, como infracciones descubiertas, vulnerabilidades con tasas de explotación conocidas o altas, vulnerabilidades que se pueden explotar para un acceso completo, no supervisado o imposible de rastrear, o que pueden poner inmediatamente en peligro vidas, descubiertas durante las pruebas, deben informarse al cliente con una solución práctica lo antes posible de cómo se encuentran.
   29) Cualquier forma de prueba de desbordamiento en la que un osciloscopio sea desbordado por una fuente más grande y fuerte está prohibida en canales que no sean de propiedad privada.
   30) El Analista no puede dejar el alcance en una posición de menor seguridad real que cuando se proporcionó.

G. Reportando
   31) El Analista debe respetar la privacidad de todas las personas y mantener su privacidad para todos los resultados.
   32) Los resultados que involucren a personas no capacitadas en seguridad o personal que no es de seguridad solo pueden informarse por medios no identificativos o estadísticos.
   33) El Analista no puede firmar los resultados de las pruebas ni los informes de auditoría en los que no haya participado directamente.
   34) Los informes deben ser objetivos y sin falsedades ni malicia dirigida personalmente.

35) Se requieren notificaciones al cliente cada vez que el analista cambia el plan de prueba, cambia el lugar de prueba de origen, tiene hallazgos de baja confianza o se ha producido algún problema de prueba. Se deben proporcionar notificaciones antes de ejecutar pruebas nuevas, peligrosas o de alto tráfico, y se requieren actualizaciones de progreso regulares.
36) Cuando se incluyan soluciones y recomendaciones en el informe, deben ser válidas y prácticas.
37) Los informes deben marcar claramente todas las incógnitas y anomalías.
38) Los informes deben indicar claramente tanto las medidas de seguridad exitosas como las fallidas descubiertas y los controles de pérdidas.
39) Los informes deben utilizar únicamente métricas cuantitativas para medir la seguridad. Estas métricas deben basarse en hechos y carecer de interpretaciones subjetivas.
40) El cliente debe ser notificado cuando se envía el informe como esperar su llegada y confirmar la recepción de la entrega.
41) Todos los canales de comunicación para la entrega del informe deben ser confidenciales de punta a punta.
42) Los resultados y los informes nunca se pueden utilizar para obtener beneficios comerciales más allá de la interacción con el cliente.

(Volver a: Reglas de compromiso)

14.2- Las diez propiedades de confianza

Las diez propiedades de confianza para realizar un análisis de confianza adecuado son [13]:

#	Propiedad de confianza		Descripción
1		Tamaño	La cantidad de confianza. ¿Debe la confianza extenderse a solo uno o a muchos? ¿El grupo debe ser de confianza y está destinado a tomar decisiones colectivas?
2		Simetría	El vector (dirección) de la confianza. La confianza puede ser unidireccional (asimétrica) y se define en cuanto a qué dirección debe viajar la confianza o en ambos sentidos (simétrica). Una persona que también debe confiar en ti debe considerar la reciprocidad de romper la confianza.
3		Visibilidad	El nivel de transparencia de todas las partes y procesos operativos del objetivo y su entorno.
4		Subyugación	También llamado control, la cantidad de influencia sobre el alcance por parte del operador.
5		Consistencia	La evidencia histórica de compromiso o corrupción del objetivo.
6		Integridad	La cantidad y el aviso correspondiente de cambio dentro del objetivo.
7		Compensaciones	Las compensaciones de una garantía suficiente son una compensación para el que confía o un castigo para el que rompe la confianza. Es un valor que se deposita en la confianza con el objetivo.
8		Valor	La compensación financiera por riesgo, la cantidad de ganancia o ganancia por la cual el riesgo de depositar la confianza en el objetivo es suficiente para compensar el riesgo de falla en la confianza.
9		Componentes	El número de otros elementos que actualmente proporcionan recursos para el objetivo ya sea a través de interacciones directas o indirectas, similar a la Intervención del proceso de cuatro puntos.
10		Porosidad	La cantidad de separación entre el objetivo y el entorno externo.

Tabla 5: Las diez propiedades de confianza [13]

(Volver a: Las diez propiedades de confianza)

14.3- Proceso de cuatro puntos

Cada una de estas fases se divide en diferentes etapas que llevan el análisis a distintos niveles de profundidad, sin embargo, ninguna de ellas es ni más ni menos importante que la otra. [12]

#	Fase	#	Módulo	Descripción
A	**Inducción**	A.1	Revisión del entorno	Conocer las normas, leyes, políticas y cultura organizacional que influyen en los requerimientos de seguridad dentro de la empresa o institución.
		A.2	Logística	Obtener detalles del canal de análisis para evitar falsos positivos o falsos negativos; por ejemplo, en el canal humano, es necesario conocer los horarios de atención del personal, ya que una auditoría brindaría resultados incompletos cuando la organización está en inactividad. Es decir, en los horarios donde no hay atención al público, la interacción sería nula, y un análisis en ese horario no reflejaría la realidad de manera completa. Por lo tanto, es necesario definir los horarios, lugares y tipos de análisis para lograr resultados más precisos.
		A.3	Verificación de detección activa	Averiguar si existen controles que detecten intrusiones que puedan filtrar o bloquear intentos de análisis, obteniendo falsos negativos como resultado.
B	**Interacción**	B.4	Auditoría de visibilidad	Enumerar los objetivos visibles dentro del alcance. Conocer los puntos donde la interacción sería posible.
		B.5	Verificación de accesos	Determinar los puntos de acceso, la forma de interacción y el propósito de su existencia. En el caso del canal “redes de datos”, el ejemplo más claro es la verificación de puertos.
		B.6	Verificación de confianza	Verificar las relaciones de confianza entre los objetivos, donde exista acceso a la información sin necesidad de autenticación.
		B.7	Verificación de controles	Verificar la efectividad de controles de proceso (clase B): no repudio, confidencialidad, privacidad e integridad; el control de alarma se verifica al final de esta metodología.
C	**Investigación**	C.8	Verificación de procesos	Comprobar el mantenimiento y efectividad de los niveles de seguridad en los procesos establecidos. Además, se debe verificar el cumplimiento de las normas, leyes, regulaciones y políticas que se investigaron en el primer punto.
		C.9	Verificación de la configuración	Revisar el funcionamiento de los procesos en condiciones normales, para identificar cuál es su objetivo y así comprender la justificación de negocio de esa pieza de información.
		C.10	Validación de propiedad	Revisar la procedencia de los datos, información, sistemas, etc., con el fin de identificar falsificaciones, fraudes, faltas de licencias o violaciones a los derechos de autor.
		C.11	Revisión de segregación	Revisar los controles que aseguran separación entre la información personal y organizacional. Éste es un punto focal dentro de la ética y la legalidad en el almacenamiento y transmisión de los datos.

#	Fase	#	Módulo	Descripción
		C.12	Verificación de exposición	Buscar información, disponible de manera abierta, que permita conocer detalles del objetivo. Normalmente se puede obtener una gran cantidad de información en las redes sociales, buscadores, folletos impresos, entre otros, que permite armar un perfil de la organización y que puede ser de vital importancia en las futuras etapas del análisis.
		C.13	Exploración de inteligencia de negocios	Verificar la existencia de fuentes de información que contengan datos de negocio que debieran ser confidenciales y que, en caso de ser revelados, puedan brindar ventajas competitivas a otras organizaciones.
D	**Intervención**	D.14	Verificación de cuarentena	Verificar la efectiva separación de elementos hostiles. Un ejemplo sencillo de esta etapa es cuando una pieza de software no se comporta dentro de los patrones permitidos, y es aislada para evitar afectar a otros sistemas.
		D.15	Auditoría de privilegios	Analizar el correcto uso de los sistemas de autenticación y autorización. Analizar la posibilidad de ingresos no autorizados y escaladas de privilegios.
		D.16	Continuidad de negocio	Analizar la efectividad de los controles de resistencia y continuidad. Esto puede ser realizado mediante intentos de denegación de servicio o denegación de interacciones.
		D.17	Alerta y revisión de logs	Verificar la correctitud en la relación entre las actividades realizadas y los registros almacenados. Además, se deben verificar los mecanismos que proporcionan una forma de alarma ante eventos no deseados.

Tabla 6: Proceso de cuatro puntos [12]

(Volver a: OSSTMM como una metodología)

14.4- Reporte STAR

Security Test Audit Report

OSSTMM 3.0 Security Verification Certification

OSSTMM.ORG - ISECOM.ORG

Report ID		**Date**	
Lead Auditor		**Test Date Duration**	
Scope and Index		**Vectors**	
Channels		**Test Type**	

I am responsible for the information within this report and have personally verified that all information herein is factual and true.

SIGNATURE	**COMPANY STAMP/SEAL**
ISECOM Certification #	**ISECOM Certification #**

OPERATIONAL SECURITY VALUES		**CONTROLS VALUES**	
Visibility		Authentication	
Access		Indemnification	
Trust		Resilience	
		Subjugation	
LIMITATIONS VALUES		Continuity	
Vulnerability		Non-Repudiation	
Weakness		Confidentiality	
Concern		Privacy	
Exposure		Integrity	
Anomaly		Alarm	
OpSec		**True Controls**	
Limitations		**Security Δ**	

True Protection		**Actual Security**	

Ilustración 18: Reporte STAR [18]

(Volver a: Informe con el reporte STAR)

15- Bibliografía específica

[1] G. M. Adorno Morán y V. J. Morán Maldonado, *Automatización de un sistema de análisis de vulnerabilidad para portales web del gobierno,* San Lorenzo, Paraguay: Facultad Politécnica, Universidad Nacional de Asunción, 2015.

[2] *Tecnología de la Información. Técnicas de seguridad. Código para la práctica de la gestión de la seguridad de la información.,* Estándar Internacional ISO/IEC 17799, 2005.

[3] ESET, «ESET Security Report 2020,» ESET, Latinoamérica, 2020.

[4] ESET, «ESET Security Report 2019,» ESET, Latinoamética, 2019.

[5] R. López Santoyo, *Propuesta de implementación de una metodología de auditoría de seguridad informática,* Madrid, España: Escuela Politécnica Superior, Universidad Autónoma de Madrid, 2015.

[6] D. O. Pinos Solano, *Análisis de vulnerabilidades y acciones correctivas sobre un sistema web,* Guayaquil, Ecuador: Escuela Superior Politécnica del Litoral, 2017.

[7] R. Pillay, Learn Penetration Testing, Birmingham - Mumbai: Packt Publishing Ltd, 2019.

[8] K. Scarfone, M. Souppaya, A. Cody y A. Orebaugh, *Technical Guide to Information Security Testing and Assessment,* USA: U.S. Department of Commerce, National Institute of Standards and Technology, 2008.

[9] L. C. Pinzón G., M. Talero M. y J. A. Bohada, «Pruebas de Intrusión y Metodologías Abiertas,» *Revista Ciencia, Innovación y Tecnología (RCIYT),* vol. 1, pp. 25-38, 2013.

[10] Y. d. l. N. C. Gavilánez, *Metodología OSSTMM para la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 bits a nivel de usuario final,* Riobamba, Ecuador: Escuela Superior Politécnica de Chimborazo, 2016.

[11] H. M. Deitel, Introducción a los Sistemas Operativos, México: Addison-Wesley Iberoamericana, 1987.

[12] G. A. Toth, *Implementación de la guía NIST SP800-30 mediante la utilización de OSSTMM,* Neuquén, Argentina: Facultad de Informática, Universidad Nacional del Comahue, 2014.

[13] P. Herzog, Open Source Security Testing Methodology Manual, ISECOM, 2010.

[14] C. L. Bracho y F. G. Cuzme, *Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio.,* Ibarra, Ecuador: Universidad Técnica del Norte, 2017.

[15] K. Rodriguez Lago, «Metodologías para la auditoria de la seguridad,» Linkedin, 11 12 2017. [En línea]. Available: https://www.linkedin.com/pulse/metodolog%C3%ADas-para-la-auditoria-de-seguridad-kevin-rodriguez-lago/. [Último acceso: 30 09 2020].

[16] G. Bergel, «Metodologías de testing de seguridad,» ElevenPaths Talks, 7 04 2016. [En línea]. Available: https://www.elevenpaths.com/es/noticias-y-eventos/elevenpaths-talks/metodologias-de-testing-de-seguridad/index.html. [Último acceso: 22 09 2020].

[17] F. Rathod, «SlideShare,» Open Source Security Testing Methodology Manual - OSSTMM, 5 03 2016. [En línea]. Available: https://www.slideshare.net/falgun911/open-source-security-testing-methodology-manual-osstmm-by-falgun-rathod. [Último acceso: 12 10 2020].

[18] P. Herzog, «STAR - ISECOM,» 2010. [En línea]. Available: https://www.isecom.org/STAR.3.pdf. [Último acceso: 06 10 2020].

[19] F. Catoira, «Penetration Test, ¿en qué consiste?,» ESET, 24 07 2012. [En línea]. Available: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/. [Último acceso: 17 10 2020].

[20] Dreamlab Chile, «OSSTMM OPST,» Emagister, [En línea]. Available: https://www.emagister.cl/osstmm-opst-cursos-2778380.htm. [Último acceso: 12 10 2020].

[21] Á. Bahamontes Gómez, «Auditoría de seguridad informática,» Perito y Tasador, 05 06 2012. [En línea]. Available: http://www.peritoytasador.es/auditoria-de-seguridad-informatica/. [Último acceso: 21 09 2020].

[22] L. M. Escobar Castro, «Metodología OSSTMM 3.0,» Prezi, 05 12 2018. [En línea]. Available: https://prezi.com/p/ybrqxc_ckpbj/osstmm-30/. [Último acceso: 22 09 2020].

[23] E. e. Nomada, «Metodologia OSSTMM para PenTesting,» YouTube, 28 09 2019. [En línea]. Available: https://www.youtube.com/watch?v=Ym2fM9vTZ1A. [Último acceso: 21 09 2020].

[24] A. E. Caballero Quezada, «Introducción a OSSTMM (Open Source Security Testing Methodology Manual),» ReYDeS, 17 11 2015. [En línea]. Available: http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual. [Último acceso: 22 09 2020].

[25] J. R. López, *Desarrollo de un esquema de análisis de vulnerabilidades y pruebas de penetración en sistemas operativos para una organización de la administración pública federal,* México: Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánica y Eléctrica, 2009.

[26] J. R. Anabalón, «Deoxy-Trichotecene "OSSTMM",» 07 12 2006. [En línea]. Available: http://www.geocities.ws/trichotecene/doc/papers/osstmm. [Último acceso: 14 09 2020].

[27] A. Reyes Plata, «Ethical Hacking,» Universidad Nacional Autónoma de México, 22 10 2010. [En línea]. Available: https://www.seguridad.unam.mx/ethical-hacking#Ethical. [Último acceso: 17 10 2020].

[28] Support Google, «Proteger sitios web con el protocolo HTTPS,» Google, [En línea]. Available: https://support.google.com/webmasters/answer/6073543?hl=es. [Último acceso: 17 10 2020].

[29] E. J. Sandoval Castellanos, «Ingeniería Social: Corrompiendo la mente humana,» Revista Seguridad, 04 05 2011. [En línea]. Available: https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana. [Último acceso: 17 10 2020].

[30] G. B., «¿Qué es MySQL?,» Hostinger Tutoriales, 13 05 2019. [En línea]. Available: https://www.hostinger.es/tutoriales/que-es-mysql/#Que-es-MySQL. [Último acceso: 17 10 2020].

[31] J. Marin de la Fuente, «¿Qué es Nmap? Por qué necesitas este mapeador de red,» Marin de la Fuente, 29 04 2019. [En línea]. Available: https://www.marindelafuente.com.ar/que-es-nmap-por-que-necesitas-este-mapeador-de-red/. [Último acceso: 17 10 2020].

[32] PHP.Net, «¿Qué es PHP?,» PHP.Net, [En línea]. Available: https://www.php.net/manual/es/intro-whatis.php. [Último acceso: 17 10 2020].

[33] McAfee, «Centro de conocimiento: Cómo reconocer el malware y protegerse,» McAfee, [En línea]. Available: https://service.mcafee.com/webcenter/portal/cp/home/articleview?locale=es_MX&articleId=TS102449. [Último acceso: 16 10 2020].

[34] CISCO, «¿Qué es un firewall?,» CISCO, [En línea]. Available: https://www.cisco.com/c/es_es/products/security/firewalls/what-is-a-firewall.html. [Último acceso: 16 10 2020].

[35] Culturación, «¿Qué es y para qué sirve un web service?,» Culturación, [En línea]. Available: https://culturacion.com/que-es-y-para-que-sirve-un-web-service/. [Último acceso: 16 10 2020].

[36] Infosegur, «PKI: Public Key Infrastructure,» infosegur, [En línea]. Available: https://infosegur.wordpress.com/unidad-4/pki-public-key-infrastructure/. [Último acceso: 16 10 2020].

[37] B. Donohue, «¿Qué Es Un Hash Y Cómo Funciona?,» Kaspersky, 10 04 2014. [En línea]. Available: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/. [Último acceso: 16 10 2020].

[38] Redes Locales y Globales, «Protocolo ICMP (Internet Control Messaging Protocol),» Redes Locales y Globales, [En línea]. Available: https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/9-protocolos-tcp-ip/protocolos-de-nivel-de-red/protocolo-icmp. [Último acceso: 16 10 2020].

[39] Facultad de Informática de la Universidad Complutense de Madrid, «Cracking,» Wiki de la asignatura Ética, Legislación y Profesión (ELP), 18 12 2017. [En línea]. Available: https://wikis.fdi.ucm.es/ELP/Cracking. [Último acceso: 16 10 2020].

[40] ISO Tools Excellence, «¿Qué es la ISO 27001?,» Software ISO Riesgos y Seguridad, [En línea]. Available: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/. [Último acceso: 16 10 2020].

[41] Emagister, «¿Qué es ITIL, para qué sirve y qué tipos de certificados existen?,» Emagister, 27 09 2019. [En línea]. Available: https://www.emagister.com/blog/que-es-itil/. [Último acceso: 16 10 2020].

[42] ICC LICENCIATURA, «Instituto Consorcio Clavijero - Clasificacion de Normas,» [En línea]. Available: https://cursos.clavijero.edu.mx/cursos/058_rtl/modulo2/contenidos/documentos/clasificacionNormas.pdf. [Último acceso: 12 10 2020].

[43] M. Estaún, «Qué es y cómo se calcula el ROI o Retorno de Inversión,» IEBS, 17 01 2019. [En línea]. Available: https://www.iebschool.com/blog/que-es-como-calcula-roi-marketing-estrategico/. [Último acceso: 12 10 2020].

[44] Red Hat, «Internet of Things (IoT) ¿Qué es el Internet de las cosas?,» Red Hat, [En línea]. Available: https://www.redhat.com/es/topics/internet-

of-things/what-is-iot. [Último acceso: 16 10 2020].

[45] F. Catoira, «Obtener información de servidores web con banner grabbing,» ESET, 21 11 2012. [En línea]. Available: https://www.welivesecurity.com/la-es/2012/11/21/obtener-informacion-de-servidores-web-con-banner-grabbing/. [Último acceso: 20 10 2020].

16- Bibliografía General

- P. Herzog, Open Source Security Testing Methodology Manual, ISECOM, 2010.

- A. Toth, Implementación de la guía NIST SP800-30 mediante la utilización de OSSTMM, Neuquén, Argentina: Facultad de Informática, Universidad Nacional del Comahue, 2014.

17- Glosario

17.1- Glosario específico

COMSEC	*Communications Security,* Seguridad de las Comunicaciones.
Controles	Para reducción de impacto y de pérdida.
ISECOM	Instituto de Seguridad y Metodologías Abiertas es una comunidad de investigación de seguridad abierta que ofrece recursos, herramientas y certificaciones originales en el campo de la seguridad.
Limitaciones	Estado actual de los límites percibidos y conocidos para canales, operaciones y controles, tal como se verifica en la auditoría.
Objetivo	Propósito del ataque, compuesto por el activo y las protecciones que pueda tener el activo.
Operaciones	Asumir la ausencia de seguridad para ser interactivo, útil, público, abierto o disponible.
OSSTMM	*Open Source Security Testing Methodology Manual*, Manual de la Metodología Abierta de Comprobación de la Seguridad.
PHYSSEC	*Physical Security*, Seguridad Física.

Porosidad	Todos los puntos interactivos, operaciones, que se clasifican como Visibilidad, Acceso o Confianza.
RAV	*Risk Assessment Values*, es la dimensión de una superficie de ataque, la cantidad de interacciones no controladas con un objetivo, que se calcula mediante el equilibrio cuantitativo entre la porosidad, las limitaciones y los controles.
Seguridad (*Safety*)	Forma de protección donde la amenaza o sus efectos se encuentran controlados.
Seguridad (*Security*)	Forma de protección donde se logra una separación entre los activos y la amenaza.
Seguridad perfecta	Equilibrio exacto de seguridad y controles con operaciones y limitaciones.
SPECSEC	*Spectrum Security*, Seguridad del espectro.
Superficie de ataque	Falta de separación específica, y controles funcionales que existen para un vector.
Vector	Dirección de una interacción.
Vector de ataque	Alcance de un vector generado para abordar las pruebas de seguridad de una manera organizada.
Vulnerabilidad	Punto donde una persona o proceso puede acceder, denegar el acceso a otros o esconderse a sí mismo o a los activos dentro del alcance.

17.2- Glosario general

Ethical Hacking	Explotar las vulnerabilidades existentes en el sistema de "interés" valiéndose de prueba de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc. [27]
Firewall	Es un dispositivo de seguridad de la red que monitoriza el tráfico entrante y saliente y decide si debe permitir o bloquear un tráfico específico en función de un conjunto de restricciones de seguridad ya definidas.
Hash	Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.

HTTPS	*HyperText Transfer Protocol Secure*, Protocolo de transferencia de hipertexto es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio web. [28]
ICMP	*Internet Control Messaging Protocol,* Protocolo de mensajes de control de Internet, sirve para informar de sucesos que han ocurrido en la red. Permite a los nodos intermedios enviar mensajes de control a los equipos que enviaron la información.
Ingeniería social	Es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. [29]
IoT	Es la tendencia constante de conectar todo tipo de objetos físicos al Internet.
Malware	Es cualquier aplicación o software destinado a dañar un equipo, dispositivo móvil, sistema informático o red de equipos informáticos, o bien a asumir un control parcial de su funcionamiento, a menudo en un intento de acceder a la información personal.
MySQL	Es un sistema de gestión de bases de datos relacionales de código abierto un modelo cliente-servidor. [30]
NMAP	Abreviatura de Network Mapper, es una herramienta gratuita de código abierto para la exploración de vulnerabilidades y la detección de redes. [31]
PCI DSS	*Payment Card Industry Data Security Standard*, estándar de Seguridad de Datos para la Industria de Tarjeta de Pago.
Pentester	Persona que lleva adelante la auditoría. [19]
PHP	*Hypertext Preprocessor*, es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML. [32]
Phreaking	Es la actividad por medio de la cual algunas personas con ciertos conocimientos y herramientas de hardware y software pueden engañar a las compañías telefónicas para que éstas no cobren las llamadas que se hacen.
PKI	*Public Key Infrastructure*, Infraestructura de Clave Pública, todo lo necesario, tanto de hardware como de software, para las comunicaciones seguras mediante el uso de certificadas digitales y firmas digitales.
Ransomware	Es un tipo específico de software malicioso utilizado para extorsionar.

ROI	*Return On Investment,* Retorno de Inversión es el indicador de las ganancias que se han obtenido tras llevar a cabo determinadas acciones.
Webservice	Conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones.