

*Toth Gastón
Sznek Jorge*

Implementación de la guía NIST SP800-30 mediante la utilización de OSSTMM



Universidad Nacional del Comahue
Facultad de Informática

PÁGINA PARA LOS EVALUADORES

Calificación:

Comentarios:

.....

.....

.....

.....

Lugar y fecha de evaluación

DEDICATORIA

A mis padres, por ser mis guías, por apoyarnos a mi hermana y a mí en cada momento, por habernos educado de la forma que lo hicieron, por habernos brindado todo lo que está a su alcance para vernos crecer siendo felices. Les agradezco por estar siempre detrás nuestro, brindándonos el soporte necesario para afrontar la vida con mucha fuerza y confianza. Agradezco sus constantes enseñanzas sobre moral y valores, no solo con sus palabras, sino también con sus actos, demostrando total entereza en todo momento. Es mi mayor deseo poder criar a mi hija de la misma forma que ellos lo han hecho conmigo.

A mi señora, mi compañera de cada día. Agradezco su empuje para que este trabajo haya sido posible, sacrificando una buena parte de su tiempo para permitirme el espacio necesario para estudiar y trabajar en este proyecto. Te agradezco por la paciencia y por prestarme tanta atención cada vez que se me ocurría contarte los detalles de este proyecto.

Gracias por compartir conmigo cada momento, por estar junto a mi lado en las buenas y en las malas, por formar esta familia de la cual estoy orgulloso.

A mi hija adorada, quien me hace ver día a día cuales son las cosas que realmente importan en la vida. Porque está llena de buenos sentimientos que demuestra con toda su dulzura. Gracias hija por divertirnos con todas tus monerías y tus ocurrencias. Siento un orgullo enorme de poder acompañarte en cada uno de tus logros, dejándome enseñarte las cosas que están a mi alcance y enseñándome vos a mi como ser una mejor persona.

A mis amigos, por todos los buenos momentos y por todo el apoyo en momentos difíciles. Porque luego de tantos años de amistad, todavía seguimos compartiendo estudio, trabajo y diversión.

PREFACIO

Esta tesis es presentada como parte de los requisitos para optar al grado académico *Licenciado en Ciencias de la Computación*, de la Universidad Nacional del Comahue y no ha sido presentada previamente para la obtención de otro título en esta Universidad u otras. La misma es el resultado del estudio y la investigación llevada a cabo en el *Departamento de Ciencias de la Computación* en el período comprendido entre los años 2013 y 2014, bajo la dirección del profesor Jorge Sznek. Para conocer detalles sobre el desarrollo, descarga del material en formato digital, descarga de documentación complementaria y demás información puede visitar la página <http://tesis-toth.com.ar>.

Gastón Alejandro Toth
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD NACIONAL DEL COMAHUE
Neuquén, 31 de marzo de 2014

AGRADECIMIENTOS

A los profesores que durante el transcurso de la carrera fomentaron el continuo aprendizaje y el compartimiento de los conocimientos como una filosofía de vida.

A Jorge Sznek por haberme permitido desarrollar este trabajo, el cual me ha servido para conocer diversas metodologías que abren nuevas puertas dentro del ámbito laboral.

A Diego Massaro, el autor de las caricaturas, realmente un excelente artista.

A Pete Herzog por detenerse a explicarme detalles de la metodología que me resultaron difíciles de comprender. También por tomarse el tiempo de escribir un texto, dedicado a los estudiantes de la Facultad del Comahue, con el fin de promover estudio de OSSTMM, y de la Seguridad Informática en general.

RESUMEN

Con las ventajas que brinda la tecnología en la actualidad para el almacenamiento de los datos, su procesamiento y transporte, las organizaciones han llevado la mayor parte de la información que manejan a medios informáticos; y esa información se ha transformado en uno de los activos más valiosos. Es por ello que se presenta como una necesidad creciente la implementación de prácticas que permitan que dicha información se encuentre correctamente protegida. Han surgido diversas metodologías, guías y normativas, que sirven de apoyo para este propósito.

Dentro de las metodologías relacionadas con la evaluación de la seguridad se encuentra un desarrollo muy interesante llevado a cabo por ISECOM (Institute for Security and Open Methodologies) denominado OSSTMM (Open Source Security Testing Methodology Manual). Esta metodología ha sido creada por ISECOM y una gran comunidad de colaboradores con el objetivo de encontrar un estándar a la hora de llevar a cabo la evaluación de la seguridad de la información. Varias características hacen que este manual sea el elegido por muchos profesionales como el estándar de facto. OSSTMM es una metodología, no para el análisis de riesgos, sino para la evaluación de la seguridad, que no tiene en cuenta la subjetividad que se encuentra en la valoración de los activos y los riesgos.

En el presente trabajo se pretende lograr una metodología de análisis de riesgos basada en el estándar NIST SP 800-30 en el cual las distintas fases sean implementadas por la metodología OSSTMM .

ABSTRACT

Given the advantages technology offers for storage, processing and transport of data, organizations have taken their managed information to computer media and such information has become one of their most valuable assets. That is why the implementation of practices that make such information be properly protected is a growing need.

Various methodologies, guides and regulations have emerged, which serve as a support for this purpose. Among the methodologies related to security assessment there is a very interesting development carried out by ISECOM (Institute for Security and Open Methodologies) called OSSTMM (Open Source Security Testing Methodology Manual).

This methodology has been developed by the Institute for Security and Open Methodologies together with a large community of contributors with the aim of finding a standard to carry out the evaluation of information security. Several features make this manual the preferred choice for many professionals.

OSSTMM is not a risk analysis methodology, but a methodology to test operational security without taking into account the subjectivity found the valuation of assets and risks. The present work aims to achieve a risk analysis methodology based on the standard NIST SP 800-30 in which the different phases are implemented by the OSSTMM methodology.

WHY OSSTMM

“Security doesn’t have to last forever; just longer than everything else that might notice it’s gone.”

– Open Source Security Testing Methodology Manual 3.0

Security is a product of risk. Unfortunately, risk is a product of our being human. It is a feeling and an idea which varies from person to person and entirely on the situation. Therefore, using risk to design or analyze security is to bundle it up with every human weakness, failing, worry, dream, and phobia of the people involved.

This humanizing of security makes setting a guideline of acceptable levels of risk no more than a collection of what some people find to be of risk and therefore secured. These are best practices. And best practices are a fairytale. Best practices are like trying to keep a kingdom safe from dragons by implementing what other kings do about their dragon problem (but not whether the problem really goes away or if the villagers, especially the chosen virgins, benefit from the results). Best practices is not the best scientific research. It's also not necessarily the best solution. Despite its name, it's collecting practices that some people feel is effective and then sufficiently watering them down to the least common denominator where all the practices agree. And also, incidentally, where their weaknesses, failings, worries, dreams, and phobias coalesce.

Best practices might get you by for a while but it doesn't compare to being able to thoroughly analyze the environment and make exact measurements as to how security should fit for required functions. That requires science. And that's what you get with the OSSTMM, a security methodology researched and developed under the scientific method.

But it's not easy. It is always more work to design something to fit. It is always more work to test something thoroughly. And it is always more work to analyze something that is running and currently in operation, changing as you study it. But there is also a reason why everyone in every culture has heard before, “It is better to do something right the first time”.

What you do right the first time you save on correction, maintenance, and loss. And unfortunately although people know this when it comes to mopping floors, grocery shopping, and car washing, people do NOT intrinsically know this about safety or security. If they did, the Internet wouldn't be full of videos about people getting hurt in stupid ways because they didn't study basic physics before doing something with painful consequences. People, by default, underestimate the consequences of doing something quickly (and poorly) now and the length of trauma, loss, and damages they will have to make up for later.

Of course the business world is full of examples of releasing poor work now to reap the benefits early and worry later about long-term costs. Just look at how software releases are managed. However, the business world is also full of failure and loss because of it.

And you are in security. Maybe today it's websites that you're protecting. Maybe tomorrow it's high frequency microprocessors controlling the acceleration in cars. Maybe it's locking

down hospital devices. I don't know. And neither do you. We are all interconnected and you not doing security right the first time effects others. Possibly many and in tragic ways.

And this brings me to why the OSSTMM. It was made as a way for others to do security the right way the first time. It's a methodology created from facts researched now. And it was done because we all need each other to not take short-cuts in security and safety. We need security to be done the right way the first time. Because we NEED to care.

This isn't a sales pitch. It's also nothing you haven't heard before. But it does explain why I created the OSSTMM which has nothing to do with the purity of open source and scientific methods. It's actually about caring about what matters. Security matters. If not to you then to someone, somewhere, and it's your responsibility to do it right.

I strongly recommend that the students at UNCOMA University get familiar with the science of security and let the OSSTMM be your starting point.

Pete Herzog,
Managing Director,
ISECOM
www.isecom.org
www.osstmm.org

INDICE

Portada.....	i
Página para los evaluadores.....	iii
Dedicatoria.....	v
Prefacio.....	vii
Agradecimientos.....	ix
Resumen.....	xi
Abstract.....	xii
Why OSSTMM.....	xiii
Parte 1.....	23
Capítulo 1. Introducción.....	25
Seguridad de la información.....	26
Confidencialidad.....	28
Integridad.....	28
Disponibilidad.....	28
Conceptos generales.....	29
Activos.....	29
Amenazas.....	29
Amenazas intencionales.....	29
Amenazas no intencionales.....	30
Controles.....	31
Riesgos.....	31
Vulnerabilidades.....	31
Evolución histórica.....	31
Situación actual.....	32
Capítulo 2. Análisis y gestión de riesgos.....	35
Análisis de riesgos.....	35
Metodologías, guías y normas existentes.....	36
Guías y modelos.....	36
NIST SP 800-30.....	36
Octave.....	38
Normas y estándares.....	38
AS/NZS 4360:2004 Gestión de riesgos.....	38
ISO/IEC 27005:2008.....	39
Basilea II.....	40
FAIR.....	40
Metodologías.....	40
OSSTMM.....	40
MAGERIT.....	40
CRAMM.....	41
IRAM.....	41
CORAS.....	41
Mehari.....	42
Diferentes aproximaciones al análisis de riesgos.....	42
Análisis cuantitativo.....	42

Análisis cualitativo.....	44
Gestión del riesgo.....	45
Parte 2.....	47
Capítulo 3. Elementos del modelo.....	49
Seguridad y protección.....	50
Controles.....	50
La tríada CIA y los controles.....	51
Limitaciones.....	53
Ejemplos de limitaciones.....	54
Relación con los diferentes elementos.....	54
Seguridad Real.....	55
Caracterización del sistema.....	55
Definición del alcance.....	56
Canales.....	56
Capítulo 4. Identificación de amenazas, controles y limitaciones.....	59
Proceso de cuatro puntos.....	60
Inducción.....	61
Interacción.....	61
Investigación.....	61
Intervención.....	62
Diagrama de flujo.....	62
Seguridad operacional.....	63
Visibilidad.....	63
Accesos.....	64
Confianza.....	64
Controles.....	64
Autenticación.....	64
Indemnización.....	64
Resistencia.....	64
Subyugación.....	64
Continuidad.....	65
No repudio.....	65
Confidencialidad.....	65
Privacidad.....	65
Integridad.....	65
Alarma.....	65
Limitaciones.....	65
Vulnerabilidad.....	65
Debilidad.....	66
Preocupación.....	66
Exposición.....	66
Anomalía.....	66
Capítulo 5. Determinación del riesgo.....	67
Fórmulas para la seguridad real.....	68
Porosidad.....	69
Controles.....	69
Controles faltantes.....	69
Controles reales.....	70
Porcentaje real de cobertura.....	70

Controles completos.....	70
Limitaciones.....	71
Seguridad real.....	72
Ejemplo.....	73
Seguridad operacional.....	73
Accesos.....	73
Visibilidad.....	74
Confianza.....	74
Controles.....	74
Controles en el servidor HTTPS.....	74
Controles en el servidor de base de datos.....	74
Limitaciones.....	75
Resultados.....	75
Seguridad operacional.....	75
Controles.....	75
Limitaciones.....	75
Seguridad.....	76
Capítulo 6. Recomendaciones y documentación.....	79
Recomendaciones de control.....	79
Resultado y documentación.....	80
Aspectos a considerar en los reportes.....	81
Reportes con STAR.....	81
Conclusiones.....	83
Glosario.....	85
Referencias.....	89

ÍNDICE DE FIGURAS

Figura 1: Elementos de una metodología de análisis de riesgos.....	26
Figura 2: Seguridad de la información.....	27
Figura 3: Tríada CIA.....	28
Figura 4: Pasos de una metodología propuesta la guía NIST SP-800.....	37
Figura 5: Fases del proceso OCTAVE.....	38
Figura 6: AS/NZS 4360:2004 - Proceso de análisis de riesgos.....	39
Figura 7: Modelo MAGERIT.....	41
Figura 8: Relación entre la tríada CIA y los controles operacionales.....	52
Figura 9: Interacciones dentro del proceso de 4 puntos.....	60
Figura 10: Diagrama de flujo OSSTMM.....	63
Figura 11: Ejemplo infraestructura simple.....	73

ÍNDICE DE TABLAS

Tabla 1: Ejemplo de análisis cuantitativo.....	43
Tabla 2: Tabla de impacto en un análisis cualitativo.....	44
Tabla 3: Equivalencias entre los elementos de los diferentes modelos.....	45
Tabla 4: Controles de interacción.....	51
Tabla 5: Controles de proceso.....	51
Tabla 6: Relación: Confidencialidad - Controles.....	52
Tabla 7: Relación: Integridad - Controles.....	53
Tabla 8: Relación: Disponibilidad - Controles.....	53
Tabla 9: Limitaciones.....	54
Tabla 10: Relación entre los elementos de la seguridad.....	55
Tabla 11: Relación entre clases y canales.....	57
Tabla 12: Categorías para las entradas de datos.....	68
Tabla 13: Valores auxiliares para el cálculo de las limitaciones.....	71

PARTE 1

Esta parte tiene como principal objetivo presentar al lector el contexto en el cual se realizó este trabajo. El primero de los dos capítulos que componen esta sección se centra en la definición del contexto, su motivación y una breve descripción de la evolución histórica de la problemática relacionada con la seguridad de la información; así como también define varios conceptos que son de uso corriente en la materia. El segundo capítulo se refiere más específicamente a las metodologías, guías y normativas de análisis de riesgos y sus diferentes aproximaciones, y se presentan aquellas que son predominantes en cuanto a su uso a nivel mundial.

En esta parte también se hace referencia a dos conceptos que, aunque se encuentren en estrecha relación, son diferentes: seguridad informática y seguridad de la información.





CAPITULO 1.

INTRODUCCIÓN

Hoy en día la información se ha transformado en el activo más importante de toda organización, siendo una pieza fundamental para el logro de los objetivos. La necesidad de protección ha impulsado el desarrollo de estándares, métodos, procedimientos y políticas cuyo propósito es obtener información que sea confiable, cuya distribución esté controlada y que esté disponible en el momento en que se la requiera.

Debido a que asegurar la información no es una tarea sencilla, se han desarrollado metodologías con el objetivo de identificar, clasificar y valorar los activos, así también como las amenazas y los controles existentes, buscando alcanzar el grado de conocimiento necesario para tomar las decisiones más oportunas en cada ocasión.

Conocidas como “metodologías de análisis y gestión de riesgos”, tienen como objetivo reducir el impacto que pueden producir las diferentes amenazas sobre los activos de información, llegando a un nivel tolerable y manejable por la organización (*figura 1*).

Actualmente se pueden encontrar diferentes metodologías relacionadas con la gestión de riesgos y, aunque cada una tiene sus particularidades, comparten una estructura bastante similar. El Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) ha producido una serie de publicaciones especiales dedicadas a la seguridad de la información, la serie SP 800. Dentro de esta serie se encuentra la publicación SP 800-30, que describe una guía para el análisis y gestión de riesgos, la cual definirá el marco para la metodología que se desarrollará en este documento.

Esta guía consta de nueve pasos básicos:

1. Caracterización del sistema.
2. Identificación de amenazas.
3. Identificación de vulnerabilidades.
4. Análisis de controles.
5. Determinación de probabilidades.
6. Análisis de impacto.

7. Determinación del riesgo.
8. Recomendaciones de control.
9. Resultado y documentación.



Figura 1: Elementos de una metodología de análisis de riesgos

Las distintas etapas propuestas por la guía NIST serán implementadas por el manual OSSTMM. El acrónimo OSSTMM proviene de las palabras en inglés “Open Source Security Testing Methodology Manual”, en castellano, manual de metodología abierta de pruebas de seguridad. Es uno de los manuales más completos en lo que respecta a chequeos de seguridad, creado por Pete Herzog, director de ISECOM¹, y una gran comunidad de colaboradores. Este manual se enfoca en los análisis de seguridad desde un punto de vista científico, intentando evitar las subjetividades del profesional y buscando una metodología consistente y repetible. Actualmente se encuentra en vigencia la versión 3 y puede descargarse desde el sitio web de esta organización².

Seguridad de la información

En primer lugar, y debido a que es el objetivo central de la realización de esta metodología, se definirá el significado de *Seguridad de la información*.

Es común hablar de seguridad informática y de seguridad de la información como si fueran la misma cosa y, a primera vista, pareciera ser, sobre todo si se tiene en cuenta que en la actualidad, gracias al constante desarrollo tecnológico, se tiende a digitalizar todo tipo de información y manejarla a través de un sistema informático. Sin embargo, aunque tengan la

1 ISECOM (Institute for Security and Open Methodologies) es una organización abierta y sin fines de lucro cuyo objetivo es investigar y mejorar la forma en la que se llevan a cabo los análisis de seguridad.

2 OSSTMM v3 está disponible en <http://www.isecom.org/mirror/OSSTMM.3.pdf>

necesidad de trabajar en armonía, cada uno de estos aspectos tiene objetivos y actividades diferentes.

Por seguridad informática se entiende al conjunto de políticas, reglas, estándares, métodos y protocolos que se utilizan para la protección de la infraestructura de computadoras y toda la información contenida o administrada por ella. Esta información debe ser protegida de la posible destrucción, modificación, difusión o utilización indebida. No sólo se debe prestar atención a los ataques intencionales, sino también a posibles fallas de software o hardware que atenten contra la seguridad.

Por otra parte, seguridad de la información se refiere a todas aquellas medidas que procuren resguardar la información ante cualquier irregularidad. La principal diferencia entre seguridad informática y seguridad de la información es que la primera se encarga de la seguridad en un medio informático y la segunda se interesa en la información en general (*figura 2*), pudiendo ésta estar almacenada tanto en un medio informático como en cualquier otro. Por ejemplo, un manual de procedimientos escrito en papel, el conocimiento que poseen las personas, escrituras en pizarras y papeles que se descartan, son fuentes importantes de información.



Figura 2: Seguridad de la información

Durante mucho tiempo se ha declarado que la seguridad de la información se basa en tres principios fundamentales: confidencialidad, integridad y disponibilidad, comúnmente conocidos como la tríada CIA (*figura 3*) por sus iniciales en el idioma inglés (Confidentiality, Integrity y Availability).

En una organización es de vital importancia establecer normas, políticas y protocolos de seguridad que tengan como objetivo la preservación de cada una de las características nombradas en el párrafo anterior. La seguridad se debe lograr mediante un proceso continuo; debe ser concebida desde el inicio de cada proyecto y no luego de haberse consolidado, siempre teniendo en cuenta los posibles riesgos, la probabilidad de ocurrencia y el impacto que puedan tener. Luego, es posible tomar decisiones acertadas, basadas en el conocimiento obtenido.

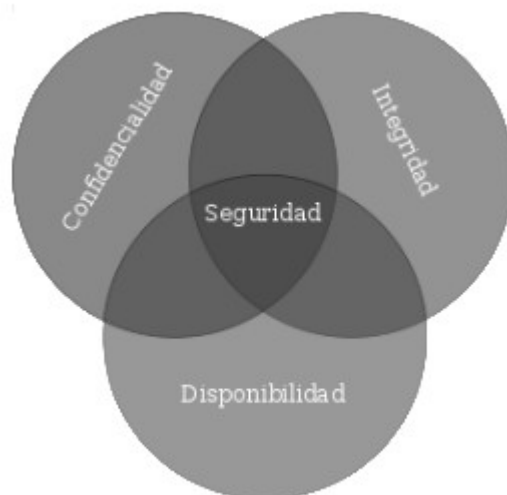


Figura 3: Tríada CIA

Confidencialidad

Es la propiedad que garantiza que la información sea accedida solo por personas o procesos autorizados. Según la definición de la Organización Internacional de Estandarización, la confidencialidad se refiere a “garantizar que la información es accesible solo para aquellos que han sido autorizados” [ISO/IEC 13335-1:2004].

En un sistema donde se garantice la confidencialidad, si un tercero es capaz de interceptar una comunicación entre el remitente y el destinatario, éste no podrá visualizar ningún tipo de información inteligible.

Integridad

Se refiere a la cualidad que busca asegurar que los datos permanezcan inalterados por procesos o personas no autorizadas. Cuando un sistema asegura la integridad y hay un tercero interfiriendo una comunicación, éste no podrá cambiar la información o, en si lo hiciera, deben existir mecanismos que permitan ponerlo en conocimiento. Esto es, se accede a los datos en su totalidad, tal cual como fueron enviados, o directamente pasan a ser inválidos.

En algunos casos se puede permitir prescindir de dicha característica, dependiendo de los requisitos de seguridad de la aplicación. Por ejemplo, en una transmisión de video se permiten ciertos márgenes de error, producidos por pérdida de paquetes o ruido en la línea, donde la calidad final no se ve afectada. Pero en el caso de que alguien hubiese interceptado la comunicación, sería necesario evitar que pudiera cambiar el contenido de tal manera que los datos no representen lo que el remitente quiso transmitir.

Por lo general se envían datos complementarios al mensaje original para asegurar la integridad.

Disponibilidad

La disponibilidad es la característica de la información de encontrarse a disposición en el momento en que sea requerida por las personas o procesos autorizados.

Un sistema que asegura la disponibilidad debe ser capaz de proveer los datos solicitados independientemente de los inconvenientes que puedan surgir. Por ejemplo, los sistemas pueden replicar la información en diferentes lugares geográficos para evitar que algún desastre natural, un incendio, robo o cualquier otro incidente imposibiliten el servicio.

Conceptos generales

Antes de continuar con el desarrollo de este trabajo, es necesario definir ciertos términos que serán de uso frecuente en los próximos capítulos.

Activos

Son todos los elementos físicos o lógicos que posean algún valor para la organización. Su valor depende de cada organización, por lo cual es necesario identificarlos, clasificarlos y determinar su nivel de importancia, para poder definir el tiempo, costo y esfuerzo que se utilizará para protegerlos.

Los activos pueden ser clasificados en diferentes categorías:

- Activos de datos: archivos, bases de datos, manuales de usuario, planes de contingencia, procedimientos.
- Activos de software: software de sistema, software de aplicación, herramientas.
- Activos físicos: equipos de comunicación, computadoras, servidores, impresoras, medios de almacenamiento, equipos de refrigeración o calefacción, muebles, edificios, cableado.
- Servicios: calefacción, alumbrado, energía, comunicaciones.
- Servicios informáticos: conexiones inalámbricas, servicios de autenticación, servicio de transferencia de archivos, correo electrónico, servicio web.
- Activos humanos: personal de la organización, proveedores, personal externo.

Amenazas

Una amenaza puede definirse como cualquier acción o elemento que atente contra alguno de los requerimientos de seguridad del sistema de información. Dicho de otra manera, es una circunstancia que tiene el potencial de causar algún daño, pérdida o difusión no autorizada de información.

Por lo general se asocia el término “amenaza” con la idea de hackers, virus informáticos, troyanos, robo de información y accesos no autorizados a los datos. Pero hay que tener en cuenta que las amenazas pueden ser tanto de carácter intencional (como las mencionadas anteriormente) como no intencional, y ambas deben ser tratadas con el mismo nivel de atención.

Amenazas intencionales

- Fraude: es un delito informático realizado con la intención de engañar o perjudicar a una persona u organización con el fin de obtener un beneficio propio.
- Sabotaje: se refiere a cualquier acción premeditada que perjudique el normal funcionamiento de la organización.

- Fuga de información: se trata de la divulgación no autorizada de datos reservados. Muchas veces se utiliza como una forma de espionaje y competencia desleal.
- Acceso no autorizado: es el acceso a información restringida; puede provenir tanto desde usuarios dentro de la misma organización como desde el exterior de la misma.
- Robo de equipamiento: muchas veces el robo de equipos informáticos es llevado a cabo con el fin de extraer la información que contiene y no por el valor del equipo en sí mismo. Computadoras, teléfonos celulares, cintas con copias de seguridad, discos ópticos, entre otros, pueden contener información de vital importancia para una organización.
- Programas maliciosos: dentro de este grupo se encuentran los virus informáticos, troyanos, gusanos, bombas lógicas, programas espía, etc. Son programas que se ejecutan dentro de la computadora con el fin de extraer o dañar la información. Se dividen en diferentes grupos según su comportamiento.

Virus: se adjuntan a un archivo o programa, de tal manera que la ejecución del archivo original dispare la ejecución del código malicioso. Este código puede realizar acciones inofensivas, como mostrar algún mensaje por pantalla, o puede ejecutar tareas que afecten a la seguridad del sistema, comprometiendo la confidencialidad, integridad o disponibilidad.

Troyanos: entran al sistema como una aplicación inofensiva y buscan tentar al usuario para que las ejecute. Cuando esto sucede, el troyano realiza las tareas para el cual fue diseñado. A diferencia de otros tipos de virus, un troyano no se replica por sí mismo.

Gusanos: son una subclase de virus con la capacidad de propagarse sin la intervención de los usuarios. Utilizan vulnerabilidades de los sistemas para reproducirse de manera automática.

Bombas lógicas: se activan en algún momento predeterminado o por algún evento del sistema.

Programas espía: su función es ejecutarse de manera oculta en el sistema e ir recopilando información que podrá ser utilizada para obtener datos de acceso como usuarios y contraseñas, facilitando un futuro acceso no autorizado al sistema.

Amenazas no intencionales

- Incendios o inundaciones: cualquiera de estos incidentes derivaría en la pérdida de información debido al daño que sufrirían los equipos que la contienen. Muchas medidas pueden adoptarse para mitigar esta amenaza. Algunas de ellas apuntan a la prevención y otras a la recuperación de los datos una vez que el daño ya fue causado. Una práctica tan sencilla como almacenar las copias de seguridad en otro edificio, soluciona en gran medida esta problemática.
- Desastres naturales: caso similar al anterior pero con el agravante de que los desastres naturales abarcan un área mayor, pudiendo afectar al dato original y también a la copia de seguridad. Para afrontar esta situación es necesario evaluar la posibilidad de almacenar copias en diferentes regiones geográficas.
- Descuidos de usuarios: la modificación o eliminación de información por error puede ser un gran riesgo de seguridad. En diversas ocasiones un usuario puede comprometer la seguridad de la información de manera no intencional si ejecuta una acción y no se controla de manera correcta.

Con frecuencia se observan contraseñas de usuarios anotadas en etiquetas pegadas en el monitor. Este es un error muy común que puede tener un fuerte impacto en la seguridad.

Existen muchas formas por las cuales un usuario puede poner en riesgo la confidencialidad, integridad o disponibilidad. Para minimizar los impactos es necesario contar con políticas de seguridad y asegurar su cumplimiento.

Controles

Por controles se entiende al conjunto de elementos, acciones, eventos, políticas y procedimientos que se aplican con el fin de reducir o evitar el impacto de amenazas sobre los activos. Por ejemplo, la forma en la que se determina el acceso a los recursos por parte de los diferentes usuarios viene definida por un tipo de control. Otro control puede venir asociado a las copias de seguridad; en este caso no se previene el daño en los datos, pero se tiene un mecanismo de recuperación en caso de fallas.

Riesgos

El riesgo es la posibilidad de que una amenaza se produzca. El riesgo supone una exposición potencial a un impacto negativo para el cumplimiento de los objetivos de una organización. Sin embargo, el riesgo es una característica inherente a cualquier actividad, por lo que no se puede considerar un factor negativo, sino un factor que conviene conocer y gestionar. El riesgo puede convertirse en una ventaja competitiva para las organizaciones que sean capaces de gestionarlo adecuadamente.

Vulnerabilidades

Una vulnerabilidad es una debilidad en un proceso, en una pieza de hardware o en un programa que puede dar lugar al compromiso de la seguridad en un sistema informático. Una vulnerabilidad puede ser una red inalámbrica sin protección, un puerto abierto en un firewall, aplicaciones sin sus actualizaciones de seguridad o fallas en los controles de acceso del personal a las salas de servidores.

Evolución histórica

En los comienzos de la era informática, las computadoras ocupaban habitaciones enteras y los científicos interactuaban con ellas rediseñando sus circuitos para que realicen diferentes tareas. A medida que fueron pasando los años, se fue sofisticando la manera de programar estos equipos, así también como los métodos de almacenamiento. Las redes de computadoras no existían para esa época. Cada equipo se encontraba aislado del resto y la única forma de compartir información consistía en el envío de cintas magnéticas que almacenaban los datos contenidos en ellas. Para ese momento, la seguridad informática estaba basada en aspectos físicos, es decir, proteger el equipamiento y los medios de almacenamiento para que no fueran robados, dañados o modificados.

En el transcurso de los años 60, más y más computadoras comenzaron a funcionar, mayormente en apoyo a la expansión militar llevada a cabo por la Guerra Fría. El trabajo realizado por estas computadoras pasó a ser crucial para ganar tiempo debido a que eran capaces de realizar gran cantidad de operaciones matemáticas en un tiempo relativamente corto.

La comunicación a través de cintas magnéticas dejó de ser suficiente y fue allí cuando la Agencia de Proyectos de Investigación Avanzada (ARPA³) del Departamento de Defensa de los Estados Unidos fundó el proyecto llamado ARPANET, cuya meta era producir una red redundante y confiable de computadoras que pudieran comunicarse entre sí. ARPANET permitió a los usuarios trabajar con procesos y datos almacenados en forma remota, por primera vez en la historia.

El acceso remoto a la información marcó el fin de la seguridad física como única medida de protección. A medida que ARPANET crecía, se hacían evidentes varios inconvenientes de seguridad; las políticas no eran consistentes y a veces, directamente no existían. Las contraseñas se podían descifrar de manera sencilla gracias a los formatos débiles que se habían implementado. Los ataques informáticos empezaron a ser algo más común, incluyendo dos, muy publicitados, a comienzos de los 80, correspondientes al ingreso no autorizado al sistema del Departamento de Defensa y a la corporación AT&T⁴. Uno de los ataques más grandes hasta ese momento fue un gusano que aprovechaba un agujero de seguridad en UNIX para replicarse en las computadoras conectadas. Llegó a infectar seis mil computadoras, que representaban un diez por ciento del total de equipos de la red.

Para esa época el Departamento de Defensa contaba con un trabajo denominado “Controles de seguridad para sistemas de computadoras”, también conocido como Rand Report R-609, considerado por muchos como el trabajo que dio inicio al estudio de la seguridad informática. Este documento fue clasificado como confidencial por diez años y finalmente desclasificado como tal, en 1975.

El incremento del uso de computadoras personales en los años 80 hizo de la seguridad un asunto aún más importante. Comenzaron a utilizarse computadoras en las oficinas e inclusive en los hogares, las cuales fueron formando parte de pequeñas redes que, a su vez se unieron a una red de redes, hoy conocida como Internet. Las vulnerabilidades se volvieron más fáciles de explotar debido a que el acceso a los diferentes recursos se facilitó enormemente.

Internet se hizo disponible para el público en general en los 90, siendo anteriormente dominio del gobierno y universidades. Trajo la posibilidad de conexión a todos los equipos que pudieran tener acceso a una línea telefónica o a una red local conectada a Internet.

La protección de la información no era el tema principal al momento del despliegue inicial de Internet; es por ello que varios de los problemas que hay hoy en día son el reflejo del desarrollo no orientado a la seguridad de ese momento.

Situación actual

En la actualidad existe un mayor grado de consciencia entre los desarrolladores de hardware y software sobre esta problemática, y es posible observar que, en muchos proyectos, se incluyen temas relacionados con la seguridad informática desde su concepción. Numerosas organizaciones dedican parte de su tiempo y de su presupuesto a la investigación, desarrollo y adquisición de productos y servicios, con el fin de mantener sus datos bien resguardados.

Día a día se conocen nuevas vulnerabilidades en los sistemas y se publican herramientas que explotan estos fallos; esta información es fácilmente accesible desde la web, haciendo posible que haya un creciente número de atacantes potenciales, que no tienen que ser necesariamente

3 ARPA es el acrónimo de las palabras en inglés Advanced Research Project Agency (Agencia de Proyectos de Investigación Avanzada)

4 AT&T, American Telephone and Telegraph; es una compañía estadounidense de telecomunicaciones de larga trayectoria y, en ocasiones, ha sido la compañía de comunicaciones más grande a nivel mundial.

expertos en la materia, debido a que también se publican manuales que explican paso a paso cómo utilizar cada uno de los recursos ofrecidos. Por otra parte, los dueños de la información se ven obligados a capacitarse constantemente para poder estar un paso adelante y resguardar los datos ante cualquier incidente posible.

Hoy en día es de vital importancia para las organizaciones comprender cuáles son los riesgos a los que se expone la información para lograr una correcta gestión y así minimizar el impacto ante las diferentes amenazas.



CAPITULO 2.

ANÁLISIS Y GESTIÓN DE RIESGOS

La disciplina “Seguridad de la Información” se encuentra en constante evolución, y sobre todo en las organizaciones, donde se plantea como un problema de negocio. Aquí toma un enfoque más global, teniendo en cuenta no sólo el aspecto tecnológico sino que también abarca cuestiones legales, organizativas y culturales. Este enfoque ampliado requiere herramientas de gestión que faciliten la obtención de los datos necesarios para poder tomar las decisiones más acertadas en cada situación.

La gestión de la seguridad de la información es el proceso por el cual la organización define, alcanza y mantiene los niveles apropiados de confidencialidad, integridad y disponibilidad.

Este proceso incluye los siguientes puntos principales:

- Determinar los objetivos, estrategias y políticas de seguridad de la información.
- Determinar los activos y su respectivo valor para la organización.
- Determinar los requerimientos de seguridad.
- Identificar las amenazas y vulnerabilidades.
- Identificar los riesgos.
- Especificar los controles considerando las amenazas, vulnerabilidades y riesgos.
- Supervisar la implementación y funcionamiento de los controles.
- Concientizar al personal de la organización en materia de seguridad.
- Detectar los incidentes de seguridad y actuar en consecuencia.

Análisis de riesgos

Son infinitos los posibles eventos que pueden afectar de forma negativa al cumplimiento de los objetivos establecidos por una organización. Estos pueden tener origen interno o externo, ser accidentales o intencionales, y su naturaleza puede variar, dando lugar a un riesgo financiero, operativo, tecnológico, de mercado, legal, etc. Incontables son las medidas de

protección que pueden tomarse ante dichos eventos, pero lógicamente es recomendable efectuar un análisis para determinar un costo de implementación proporcional al valor del activo.

El análisis de riesgos es una herramienta que posibilita la identificación, clasificación y valoración de los sucesos que amenazan la realización de los objetivos de la organización y permite establecer las medidas oportunas para reducir el impacto hasta un nivel tolerable. Tiene cuatro objetivos principales:

- Identificar los activos y su valor para la organización.
- Identificar vulnerabilidades y amenazas.
- Cuantificar la probabilidad y el impacto de estas amenazas potenciales.
- Proveer un balance económico entre el impacto de una amenaza y el costo de la contramedida.

Metodologías, guías y normas existentes

La industria cuenta con diferentes metodologías, guías y normas en lo que respecta al análisis de riesgos. Cada una de ellas tiene sus particularidades pero en general respetan un núcleo común (identificación de activos, vulnerabilidades, amenazas, controles y cálculo del riesgo). Dependiendo de las necesidades de cada organización será conveniente optar por una o por otra. A continuación se mostrará una breve introducción a las más reconocidas y mayormente utilizadas.

Guías y modelos

NIST SP 800-30

La publicación especial SP 800-30 de NIST⁵, llamada “Guía de gestión de riesgos para sistemas de tecnología de la información”, será la que se utilizará como guía para el desarrollo de este trabajo y será explicada con más detalle en los próximos capítulos. Es considerada como un estándar en el gobierno federal de los Estados Unidos.

La siguiente figura muestra los nueve pasos de la metodología con sus entradas y salidas.

5 NIST es el Instituto Nacional de Estándares y Tecnología, en inglés: “National Institute of Standards and Technology”. El sitio oficial puede ser accedido a través de la url: <http://www.nist.gov>

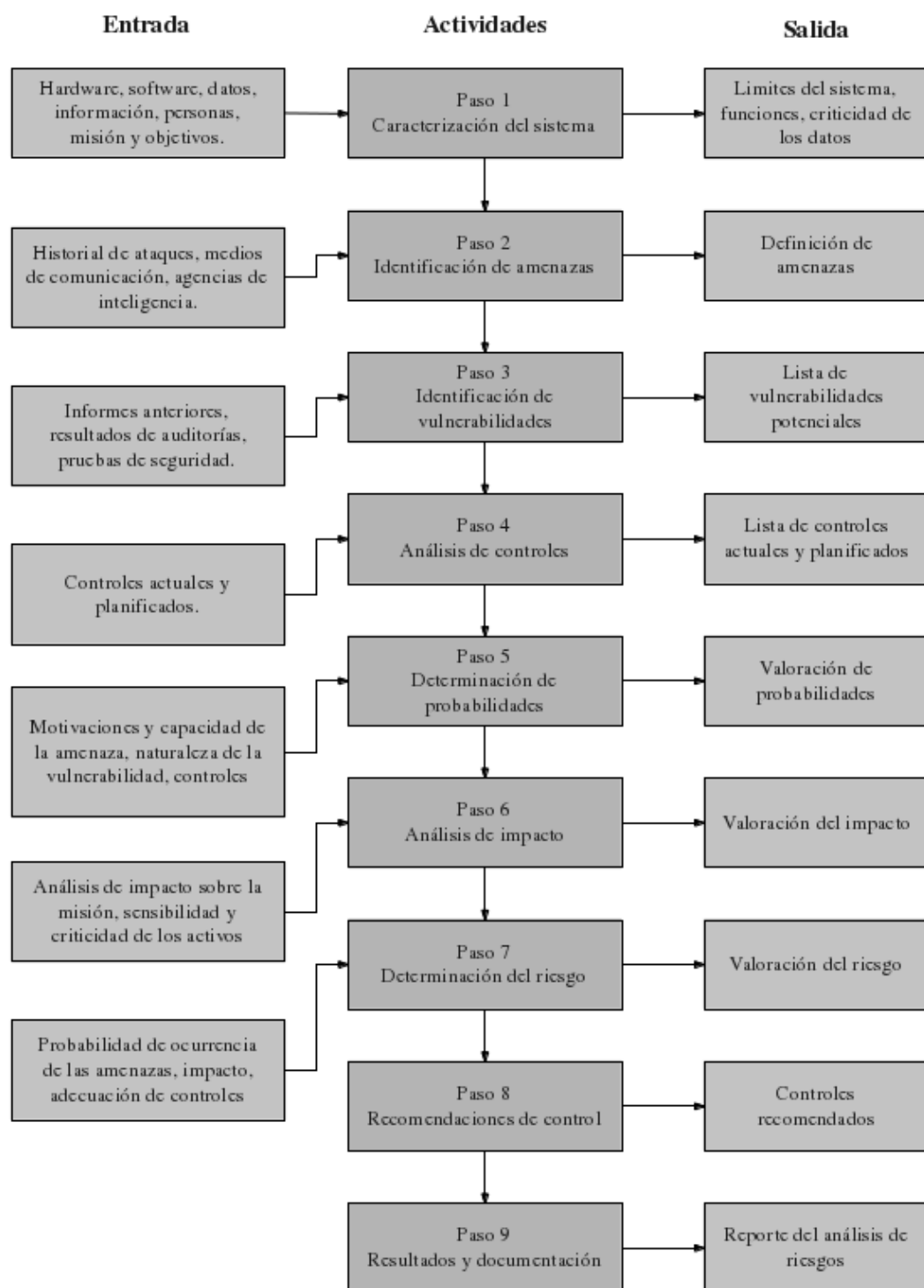


Figura 4: Pasos de una metodología propuesta la guía NIST SP-800

Octave

OCTAVE, acrónimo de las palabras en inglés “Operationally Critical Threat, Asset and Vulnerability Evaluation”, es un modelo para la creación de metodologías de análisis de riesgos desarrollado por la Universidad de Carnegie Mellon.

Cualquier metodología que aplique los criterios definidos por OCTAVE puede considerarse compatible con este modelo. Se han publicado tres versiones diferentes:

- OCTAVE: La metodología original, definida para grandes organizaciones.
- OCTAVE-S: Metodología definida para pequeñas organizaciones.
- OCTAVE Allegro: Metodología definida para analizar riesgos con un mayor enfoque en los activos de información, en oposición al enfoque en los recursos de información.

El proceso puede ser explicado mediante la siguiente figura:

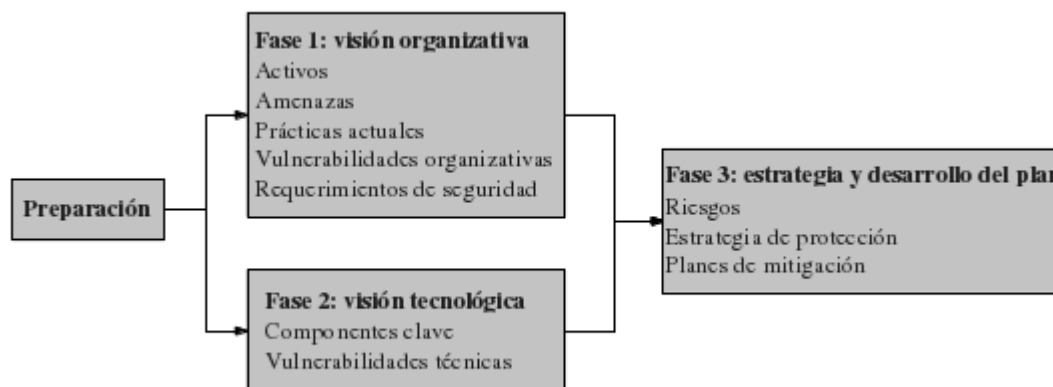


Figura 5: Fases del proceso OCTAVE

Normas y estándares

AS/NZS 4360:2004 Gestión de riesgos

Al momento de la publicación de las normas ISO/IEC 27001:2005 e ISO/IEC 27002:2005 la norma australiana AS/NZS 4360:2004 era la única de carácter internacional para la realización de análisis de riesgos de seguridad de la información, y por ello fue la norma dominante, soportando la implantación de SGSI⁶.

La norma AS/NZS 4360 suministra orientaciones genéricas para la gestión de riesgos. Puede aplicarse, además de la seguridad de información, a una gran variedad de actividades dentro cualquier organización.

El proceso que propone esta norma se define mediante el siguiente esquema:

⁶ SGSI es la forma abreviada de “Sistema de Gestión de Seguridad de la Información”

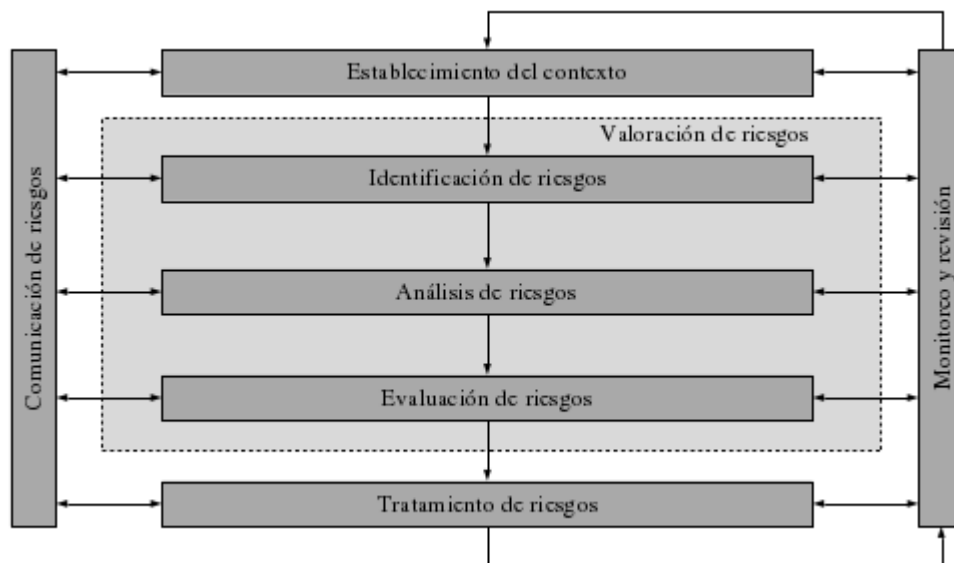


Figura 6: AS/NZS 4360:2004 - Proceso de análisis de riesgos

ISO/IEC 27005:2008

La serie de estándares ISO/IEC 27000⁷, desarrollados por ISO⁸ e IEC⁹, proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización.

Dentro de este conjunto está la norma ISO/IEC 27005:2008, la cual contiene las directrices generales para la gestión de riesgos en sistemas de información. Es compatible con los conceptos especificados en la norma ISO/IEC 27001 y permite aplicar de manera satisfactoria un SGSI basado en un enfoque de gestión de riesgos. Fue publicada por primera vez en junio de 2008 y mejorada en el año 2011.

Cabe señalar que esta norma no proporciona una metodología concreta de análisis, sino que define los elementos que debe incluir toda buena metodología de análisis de riesgos. Describe a través de sus cláusulas el proceso recomendado, incluyendo las fases que lo conforman.

El proceso de gestión de riesgos se describe en los siguientes pasos:

- Clausula 7: Establecimiento del contexto.
- Clausula 8: Valoración del riesgo.
- Clausula 9: Tratamiento del riesgo.
- Clausula 10: Aceptación del riesgo.
- Clausula 11: Comunicación del riesgo.
- Clausula 12: Monitorización y revisión del riesgo.

Además, el estándar incluye seis anexos de carácter informativo con orientaciones que van desde la identificación de activos, ejemplos de vulnerabilidades y amenazas asociadas, hasta

7 Se puede encontrar información detallada (en idioma español) de la serie 27000 en el sitio web: <http://www.iso27000.es>

8 ISO es acrónimo de International Organization for Standardization, en español, Organización Internacional de Normalización.

9 IEC, International Electrotechnical Commission (Comisión Electrotécnica Internacional)

distintas aproximaciones para el análisis, distinguiendo entre análisis de riesgos de alto nivel y análisis detallado.

Basilea II

Estándar internacional que sirve de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

FAIR

Factor Analysis of Information Risk. Desarrollada por Risk Management Insight (RMI) para mejorar la utilización de los modelos actuales para la realización de análisis de riesgos. Brinda un marco para la realización de análisis de riesgos.

Metodologías

OSSTMM

OSSTMM es un manual de metodologías para pruebas y análisis de seguridad. Se encuentra publicado bajo la licencia Creative Commons 3.0, permitiendo la libre utilización y distribución. Como proyecto de Software Libre, está abierto para que cualquier analista de seguridad pueda contribuir a la mejora del manual. El manual está realizado por ISECOM (Institute for Security and Open Methodologies), bajo la dirección de Pete Herzog.

La primera versión fue publicada en diciembre del 2000. Más tarde, en el año 2003, se publicó la 2.1, la cual cuenta con una versión en el idioma español. Actualmente se encuentra en vigencia la versión 3 de este documento.

Esta metodología busca establecer un método científico para el análisis de la seguridad, evitando basarse en la experiencia y subjetividades del analista.

Se trata de realizar una medición del estado de la seguridad en un ambiente operativo, teniendo en cuenta los controles (medidas de seguridad) en las interacciones y las limitaciones (debilidades o vulnerabilidades) que éstos puedan presentar. Se define el concepto de seguridad operacional como una combinación entre separación y controles, donde la separación de una amenaza y el activo representa la seguridad total, y en caso de no poder separar la amenaza del activo, es posible establecer controles para ofrecer protección. OSSTMM define diez tipos de controles (que abarcan todas las medidas de protección posibles) y también propone el análisis de las limitaciones que pueden encontrarse en dichos controles.

En pocas palabras, la separación ofrece seguridad total, y en los casos que no se pueda brindar separación, se aplican controles para aumentar la protección. A su vez, éstos cuentan con limitaciones, que disminuyen dicha protección. Cada una de estas características es medida de tal forma que se obtiene un valor que indica el estado de la seguridad operacional¹⁰ en un instante dado.

Actualmente se está considerando OSSTMM como un nuevo estándar ISO.

MAGERIT

La primera versión de MAGERIT (Metodología de Análisis y Gestión de Riesgos IT) fue publicada en el año 1997 por el Ministerio de Administración Pública de España. Se trata de

¹⁰ Cada uno de estos conceptos (separación, controles, limitaciones, seguridad operacional) serán explicados con mayor detalle en los capítulos siguientes.

una metodología abierta de uso muy extendido en el ámbito español y su uso es obligatorio en la administración pública de dicho país. Dispone de una herramienta de soporte, PILAR (Proceso Informático-Lógico para el Análisis y la gestión de Riesgos), de uso gratuito para la Administración Pública española y comercial para organizaciones privadas.

Está compuesta por tres volúmenes:

- Volumen I – Método. Explica detalladamente la metodología.
- Volumen II – Catálogo de elementos. Complementa el volumen principal proporcionando diversos inventarios de utilidad en la aplicación de la metodología.
- Volumen III – Guía de técnicas. Complementa el volumen principal proporcionando la introducción de algunas de las técnicas a utilizar en las distintas fases del análisis de riesgos.

Esta metodología puede describirse de forma gráfica mediante la figura a continuación:

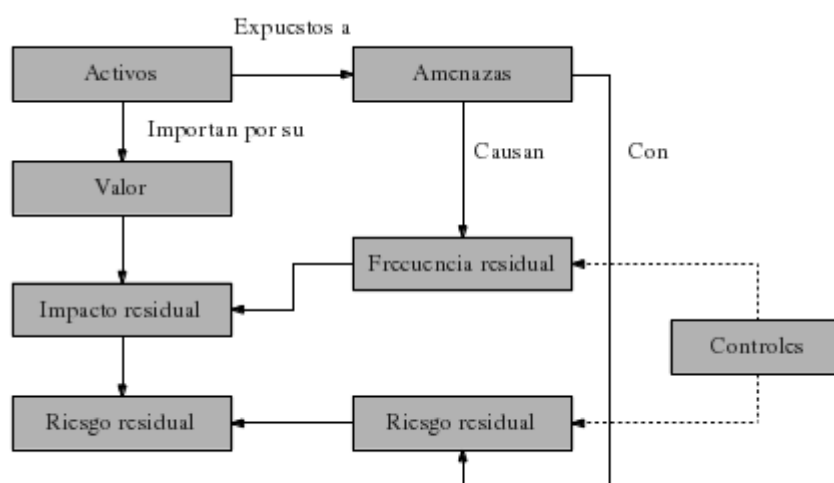


Figura 7: Modelo MAGERIT

CRAMM

CCTA Risk Analysis and Management Method. Es una metodología de análisis de riesgos desarrollada en el Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones (CCTA). Es el método de análisis de riesgos preferido en la Administración Pública británica.

IRAM

Information Risk Analysis Methodologies. El ISF (Information Security Forum) es una organización sin fines de lucro que desarrolla de forma colaborativa recomendaciones y herramientas de seguridad para sus miembros. Entre las tareas desarrolladas se encuentra la metodología de análisis de riesgos IRAM, que es el trabajo más actual de esta organización.

CORAS

Construct a Platform for Risk Analysis of Security critical systems. Desarrollado a partir de 2001 por SINTEF, un grupo de investigación noruego financiado por organizaciones del sector público y privado.

Mehari

Es la metodología de análisis y gestión de riesgos desarrollada por CLUSIF (CLUB de la Sécurité de l'Information Français) en 1995, y deriva de las metodologías previas Melissa y Marion. La metodología ha evolucionado proporcionando una guía de implantación de la seguridad en una entidad a lo largo del ciclo de vida. Del mismo modo, evalúa riesgos en base a los criterios de disponibilidad, integridad y confidencialidad.

Diferentes aproximaciones al análisis de riesgos

Dentro de las diferentes metodologías se destacan dos aproximaciones principales, **cuantitativa** y **cualitativa**. Un análisis de riesgo cuantitativo se utiliza para asignar valores numéricos y monetarios a todos los elementos en el proceso de análisis. Cada elemento dentro del análisis (valor del activo, frecuencia de amenazas, severidad de la vulnerabilidad, impactos, costo y efectividad de los controles) es cuantificado e introducido en ecuaciones con el objetivo de determinar los riesgos. Por otro lado, un análisis cualitativo no asigna valores numéricos; en su lugar, se califica a los elementos dentro de ciertos grupos, es decir, el valor de un activo puede ser bajo, medio o alto; la frecuencia de amenazas puede ser baja, media o alta, y así sucesivamente con el resto de los elementos. Al finalizar el análisis tendremos el valor del riesgo situado dentro de alguno de estos grupos. Cabe aclarar que la clasificación “bajo, medio, alto” es sólo una entre tantas. Otros ejemplos utilizados en diferentes metodologías son la clasificación por colores (verde, amarillo y rojo) y la clasificación numérica, donde a cada elemento se le asigna un valor de una escala prefijada. Dentro de los resultados de un análisis cuantitativo se podría ver algo como: “...el riesgo de pérdidas es de \$500.000 en caso de que la base de datos sea comprometida...”, en cambio un análisis cualitativo arrojaría un resultado como: “...el riesgo de pérdida de información por accesos no autorizados al sistema es bajo...”.

Análisis cuantitativo

Una vez que se han identificado los activos, se les ha asignado un valor y se han identificado las vulnerabilidades y amenazas, se puede continuar con la sección que corresponde al análisis propiamente dicho.

En caso de haber optado por un análisis cuantitativo, se utilizarán fórmulas matemáticas para el proceso de determinación del riesgo. Las ecuaciones más usadas para este propósito son SLE (Single Loss Expectancy) y ALE (Annual Loss Expectancy).

SLE podría traducirse al español como “pérdida individual esperada” y se refiere a un valor que representa la potencial pérdida de dinero si una amenaza se hace efectiva. La ecuación es la siguiente:

$$\text{SLE} = \text{Valor del activo (AV)} * \text{Factor de exposición (EF)}$$

El factor de exposición representa el porcentaje de pérdida que una amenaza puede producir en un activo. Por ejemplo, si un servidor de archivos tiene un valor de \$40.000 y el daño estimado por la entrada de un virus es del 30%, entonces la expectativa de pérdida es de \$12.000:

$$\text{SLE} = \text{Valor del activo } (\$40.000) * \text{Factor de exposición } (0.30) = \$12.000$$

Esto indica que la organización perdería \$12.000 en el caso que un virus ingrese al sistema. Pero como los presupuestos se hacen generalmente de forma anual, es necesario calcular la expectativa de pérdida anual (ALE). La ecuación se muestra a continuación:

$$\text{ALE} = \text{SLE} * \text{Annualized Rate of Occurrence (ARO)}$$

La tasa anual de ocurrencia es el valor que representa la frecuencia estimada de ocurrencia de una amenaza en el transcurso de un año. Este valor puede ir desde 0 (nunca) en adelante, siendo, por ejemplo, 1.0 una ocurrencia al año y 0.2 una ocurrencia cada 5 años. Por ejemplo si la probabilidad de entrada de virus al servidor de archivos es de dos veces cada año, el valor de ARO será 2.0. Continuando con el caso anterior:

$$\text{ALE} = \text{SLE } (\$12.000) * \text{ARO } (2.0) = \$24.000$$

El valor de ALE indica a la gerencia de la organización que la pérdida anual por infección de virus en el servidor de archivos es de \$24.000 y por lo tanto el costo de los controles que se deseen aplicar para mitigar esta amenaza no deben superar ese valor. En caso contrario se estaría gastando más dinero en controles de lo que se perdería si la amenaza se hace efectiva. La tabla 1 muestra un ejemplo de los resultados de un análisis de riesgos cuantitativo. Con esta información una compañía puede tomar decisiones sobre cuáles amenazas serán tratadas y cuánto dinero se invertirá, dependiendo de la severidad de la amenaza, la frecuencia de ocurrencia y el valor del activo.

Activo	Amenaza	SLE	ARO	ALE
Base de datos	Fallo	\$20.000	0.1	\$2.000
Servidor de archivos	Virus	\$12.000	2	\$24.000
Datos de tarjetas de créditos de clientes	Robo	\$50.000	3	\$150.000

Tabla 1: Ejemplo de análisis cuantitativo

Luego de obtener los valores esperados de pérdidas, es necesario evaluar los controles que se aplicarán. Hay que tomar en consideración que el costo de un control nunca debería superar el valor que se perdería en caso de no aplicarlo, es decir, hay que hacer un análisis de costo-beneficio. Un cálculo comúnmente utilizado para determinar el costo-beneficio es:

$$(\text{ALE antes de aplicar el control}) - (\text{ALE luego de aplicar el control}) - (\text{costo anual del control}) = \text{Ahorro por la aplicación del control}$$

Por ejemplo, si la pérdida anual esperada por intrusiones en el servidor web es de \$10.000, y luego de la implementación de un firewall el ALE es de \$2.000, con un costo anual de instalación y mantenimiento de \$400, entonces el ahorro obtenido es de \$7.600 (\$10.000 - \$2.000 - \$400). Por lo tanto, es muy recomendable su implementación.

Cuando se trata de un análisis cuantitativo muchas veces se piensa que el proceso es puramente objetivo y científico porque los datos son presentados como valores numéricos. Pero un análisis cuantitativo puro es muy difícil de lograr debido a la subjetividad de los datos. Resulta casi imposible determinar cuándo va a ocurrir un incendio, cuándo va a ingresar un virus al sistema o cuándo alguien va a robar información de tarjetas de crédito. Es por ello que los datos se extraen de la experiencia y de información histórica. Como resultado se debería obtener una lista de valores, tan aproximados a la realidad como sea posible, que ayuden a los directivos a tomar decisiones. Entre los resultados esperados se encuentran:

- Valor monetario asociado a cada activo
- Listado de amenazas significativas
- Probabilidad de ocurrencia de cada amenaza
- Pérdidas que la organización puede soportar en el lapso de un año
- Controles recomendados

Análisis cualitativo

El otro enfoque es el análisis cualitativo, el cual no asigna valores numéricos a los componentes. En su lugar, este método se basa en el análisis de diversos escenarios donde se evalúa la severidad de las amenazas, la probabilidad de ocurrencia y la validez de los controles de una manera más subjetiva. Los análisis cualitativos incluyen buenas prácticas, intuición y experiencia. Algunos ejemplos de técnicas cualitativas para recolectar información son las encuestas, los cuestionarios, las reuniones, las presentaciones y las entrevistas.

Se definen categorías dentro de las cuales serán clasificados los diferentes elementos del modelo. Por ejemplo, el valor de cada activo podría clasificarse como bajo, medio o alto; así también como la probabilidad de ocurrencia de una amenaza o el impacto que esta tendría en caso de que se haga efectiva.

Se reemplaza el uso de fórmulas matemáticas por tablas que representan un orden de magnitud, facilitando en gran medida el desarrollo del análisis aunque teniendo como desventaja cierta pérdida de precisión.

Una matriz típica de un análisis cualitativo se vería de la siguiente forma:

		Degradación		
Impacto		Baja	Media	Alta
Valor	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto

Tabla 2: Tabla de impacto en un análisis cualitativo

Aquí se muestra cómo el impacto se ve directamente influenciado por el valor del activo y la degradación que se produce por la amenaza. Donde un activo de alto valor, combinado con una degradación alta producen un impacto clasificado como “Alto” y, en el otro extremo, un activo de escaso valor conjugado con una baja degradación generan un impacto de clasificación “Baja”.

Esta tabla es análoga al valor de SLE presentado anteriormente, donde sería posible definir las siguientes equivalencias:

Método cuantitativo	Método cualitativo
SLE	Impacto
Valor del activo	Valor del activo
Factor de exposición	Degradación
$SLE = AV * EF$	$Impacto = AV * Degradación$

Tabla 3: Equivalencias entre los elementos de los diferentes modelos

Gestión del riesgo

Finalizado el proceso de análisis de riesgos, sea por el método que fuere, se debe gestionar de alguna manera. Para ello es necesario conocer la diferencia que existe entre el “riesgo total” y el “riesgo residual”, el primero es el valor que se obtiene considerando el valor de los activos, las vulnerabilidades, las amenazas, el impacto y la probabilidad de ocurrencia; por otra parte, el riesgo residual se refiere al riesgo remanente luego de la aplicación de los controles. Debido a que ninguna organización es capaz de eliminar todas las amenazas, siempre existirá riesgo residual. La cuestión es determinar la forma en que será gestionado.

Básicamente existen cuatro formas de tratar el riesgo:

- Transferirlo: ante ciertos riesgos, difíciles de gestionar o de baja ocurrencia, se puede optar por transferir el riesgo a otra compañía, tal como las aseguradoras.
- Evitarlo: si la prestación de un servicio supone un gran riesgo, la organización puede elegir dejar de prestar dicho servicio. Por ejemplo, si el uso de mensajería instantánea introduce riesgo a la organización, y este servicio no es relevante para el normal funcionamiento, una opción sería prescindir del servicio, evitando el riesgo.
- Reducirlo: es la forma en la que una organización lleva el riesgo a un nivel aceptable para lograr un normal funcionamiento. La implementación de firewalls, antivirus, copias de seguridad y capacitación del personal son claros ejemplos de reducción de riesgos.
- Aceptarlo: se acepta el riesgo potencial sin tomar medidas. Esta opción es generalmente adoptada cuando la probabilidad de ocurrencia es mínima o nula y los costos de aplicar controles son superiores al posible impacto que se produciría al concretarse la amenaza.

PARTE 2

Los capítulos que conforman la segunda parte de este trabajo representan el desarrollo de una metodología de análisis de riesgos que cumple con los pasos propuestos por la guía NIST SP 800-30, pasos que son implementados mediante la metodología OSSTMM. A pesar de que esta última no es utilizada para la determinación de riesgos, se puede obtener un valor que representa el estado actual de la seguridad en un sistema de información, con la ventaja de no contar con valoraciones de activos que hayan sido definidas de manera subjetiva por el analista, sino que se busca un método objetivo y repetible para la obtención del resultado.





CAPITULO 3.

ELEMENTOS DEL MODELO

En la sección anterior se explicaron ideas generales que permiten al lector comprender el contexto de este trabajo; de aquí en adelante se desarrollará la metodología propuesta y, en este capítulo en particular, se definirán los elementos que la componen.

Cabe aclarar que este estudio está basado en la seguridad operacional, esto significa que no se hacen asunciones de cómo debe funcionar una solución de seguridad; en su lugar se observa cómo se comporta realmente. Es importante esta aclaración debido a que los sistemas en general son diseñados para funcionar de alguna manera específica, pero al momento de su implementación existen incontables motivos por los cuales el comportamiento puede no ser el que se espera. Es por ello que se hace hincapié en el término *operacional*, ya que lo que se desea realmente es analizar un ambiente real y no una definición teórica.

La seguridad operacional se obtiene mediante una combinación de separación y controles. Para que una amenaza sea efectiva debe interactuar directa o indirectamente con un activo. Si se quiere obtener seguridad total entonces se debe separar la amenaza del activo evitando cualquier interacción posible. En caso de no ser factible una separación completa, lo que se puede hacer es aplicar controles en las interacciones, obteniendo así cierto grado de protección. De aquí se obtienen estos dos conceptos fundamentales:

- **Seguridad:** separación del activo y la amenaza ante cualquier interacción. Esto puede incluir la eliminación tanto del activo como de la amenaza.
- **Protección:** es una forma de controlar el impacto de una amenaza. Se aplican controles para reducir los efectos de una amenaza, llevándolas a un nivel aceptable.

Seguridad y protección

La seguridad está directamente relacionada con la separación entre las amenazas y los activos. Cuando se analiza el estado de seguridad se puede observar en qué lugares existen posibilidades de interacción y en cuáles no, muchas de estas interacciones son requeridas para llevar adelante las operaciones y otras podrían evitarse. Por ejemplo, un servidor web que escucha conexiones en el puerto 80, tiene un punto de interacción que es totalmente necesario para que pueda ser accedido por los clientes. En este caso las amenazas no pueden separarse totalmente del activo pero sí pueden ser controladas mediante diferentes estrategias tal como un firewall de aplicación¹¹.

Al momento de realizar las pruebas, el analista podría no conocer la justificación de negocio de ese punto de interacción, pero lo que sí sabe es que ese punto reduce la separación entre las amenazas y los activos, incrementando la *porosidad*¹². Cada punto de interacción disminuye la separación debajo del 100%, donde el 100% representa una separación total.

La porosidad puede ser catalogada dentro de las siguientes categorías:

- **Visibilidad:** es un objetivo dentro del alcance visible para el analista. Continuando con el ejemplo anterior, si el analista comprueba que hay un firewall de aplicación y detrás hay un servidor web, entonces tendrá una visibilidad de 2.
- **Accesos:** son calculados mediante la cantidad de lugares por donde pueden ocurrir las interacciones. En el caso de un análisis de seguridad física, una puerta, por ejemplo, cuenta como un acceso.
- **Confianza:** es una interacción que no requiere autenticación entre dos elementos dentro del alcance. Por ejemplo, un proxy que redirige todo el tráfico de entrada a un equipo que procesa la petición sin verificar el origen, representaría una confianza.

Tomando como base las interacciones, se puede definir *confianza* como una interacción entre objetos dentro del alcance, *acceso* como una interacción entre objetos dentro y fuera del alcance, y *visibilidad* como una interacción que solo expone el contenido del alcance.

La suma de estos tres elementos determina la porosidad; y el aumento de la porosidad reduce la separación afectando negativamente a la seguridad.

Controles

Cuando las interacciones deben estar presentes entonces existen los controles para proveer protección a las operaciones. El objetivo principal es reducir el impacto de las amenazas sobre los activos.

Existen diez tipos de controles divididos en dos clases:

- Controles de interacción (Clase A): estos controles afectan directamente a la visibilidad, accesos o confianza.

11 Firewall de aplicación: WAF por sus siglas en inglés (WEB Application Firewall), es un dispositivo de software o hardware que analiza y filtra el tráfico entre un servidor web y los clientes. Dentro del modelo TCP/IP los WAF trabajan sobre la capa de aplicación analizando ataques como por ejemplo inyecciones SQL, XSS o LFI.

12 Porosidad es el término utilizado por OSSTMM para representar los puntos de interacción. Son puntos que reducen la separación entre amenazas y activos.

- Controles de proceso (Clase B): se utilizan para crear procesos defensivos. No afectan a las interacciones sino que proporcionan seguridad cuando la amenaza está presente.

Controles de interacción	
Autenticación	Se basa en el intercambio y validación de credenciales, donde se hacen presentes mecanismos de identificación y autorización.
Indemnización	Es un compromiso entre el propietario del activo y la parte que interactúa. Puede ser un aviso legal para el caso en que una de las partes no cumpla con las reglas prefijadas; o puede ser un seguro contratado a terceros para el caso que se produzcan fallas o pérdidas de algún tipo.
Resistencia	Es el mecanismo que brinda protección a los activos en caso que las interacciones sufran alguna falla.
Subyugación	Define las condiciones en las cuales ocurrirán las interacciones. Esto quita libertad en la forma de interacción pero disminuye los riesgos.
Continuidad	Permite mantener la interacción con los activos aún en caso de fallas.

Tabla 4: Controles de interacción

Controles de proceso	
No repudio	Impide que las partes que interactúan nieguen su participación en la interacción.
Confidencialidad	Impide que la información que circula entre dos partes sea conocida por terceros no autorizados.
Privacidad	Evita que un tercero conozca la forma en la cual es accedido, mostrado o intercambiado un activo.
Integridad	Permite identificar cuando un activo ha sido modificado por alguien ajeno a la interacción en curso.
Alarma	Es un aviso de que ha ocurrido una interacción o que la misma está en curso.

Tabla 5: Controles de proceso

Los controles tienen una influencia positiva en la seguridad debido a que permiten minimizar la superficie de ataque, pero también ellos pueden ampliarla en el caso de que dichos controles posean limitaciones.

La tríada CIA y los controles

Para comprender mejor la función de los controles operacionales, pueden ser relacionados con los elementos de la tríada CIA mencionada en el primer capítulo. El mapeo no es uno a uno exactamente pero sirve para entender cómo son utilizados los controles para cumplir con cada uno de estos objetivos (*figura 8*).

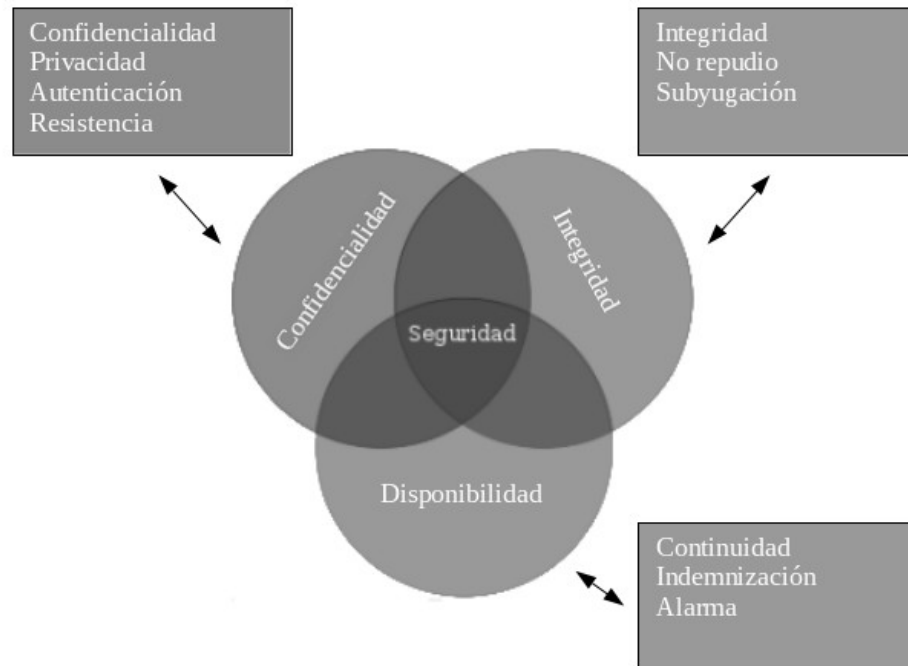


Figura 8: Relación entre la tríada CIA y los controles operacionales

A continuación se muestran tres tablas que ejemplifican la forma en la que se relacionan estos conceptos.

Confidencialidad	
Confidencialidad	La información no puede ser accedida por terceros no autorizados. <i>Confidencialidad respecto a los activos.</i>
Privacidad	La forma en que se accede a los activos es secreta. <i>Confidencialidad respecto a la forma de interacción.</i>
Autenticación	Los miembros que hayan proporcionado las credenciales correctas tendrán acceso a los activos. <i>Brinda un modo de discernir entre quién puede tener acceso y quién no a la información confidencial.</i>
Resistencia	Un fallo en algún proceso o interacción no deja al descubierto los activos. <i>Confidencialidad respecto a los activos en caso de fallas.</i>

Tabla 6: Relación: Confidencialidad - Controles

Integridad	
Integridad	Es posible identificar cuando la información es modificada por un tercero. <i>Integridad respecto a los activos.</i>
No repudio	Es posible identificar las partes que intervienen en la comunicación. <i>Integridad respecto a los participantes de la comunicación.</i>
Subyugación	Se define la forma en la que se llevará a cabo la comunicación. <i>Integridad en la forma de comunicación. Sólo se realiza si respeta el modo establecido.</i>

Tabla 7: Relación: Integridad - Controles

Disponibilidad	
Continuidad	Las interacciones no se interrumpen en caso de fallas. <i>Disponibilidad de servicio aun cuando existen cortes o desperfectos.</i>
Indemnización	En caso de pérdida de datos, es posible recuperar la información (o una copia de la misma). <i>Disponibilidad luego de una pérdida de datos.</i>
Alarma	En caso de fallas, una alarma sonora, un correo electrónico o un mensaje de texto pueden dar aviso sobre un corte en el servicio. <i>Aviso sobre cortes en la disponibilidad para que los responsables puedan tomar medidas.</i>

Tabla 8: Relación: Disponibilidad - Controles

Limitaciones

La incapacidad de un mecanismo de protección de funcionar como se espera de él, se conoce como *limitación*. Dicho de otra manera, las limitaciones son los inconvenientes que presentan los controles para mantener la separación entre los activos y las amenazas.

Es posible clasificar las limitaciones dentro de cinco categorías:

- Vulnerabilidad
- Debilidad
- Preocupación
- Exposición
- Anomalía

Limitaciones	
Vulnerabilidad	Es una falla que puede permitir el acceso no autorizado a un activo o puede denegar dicho acceso a alguien que sí esté autorizado.
Debilidad	Es una falla que reduce o anula los efectos de los controles de interacción.
Preocupación	Es una falla que reduce los efectos de los controles de proceso.
Exposición	Es una acción injustificada que permite dejar visible, ya sea de forma directa o indirecta, a un activo.
Anomalía	Es un elemento desconocido y no se encuentra dentro de las operaciones normales. Por lo general es síntoma de algún fallo pero que todavía no se comprende.

Tabla 9: Limitaciones

Ejemplos de limitaciones

Vulnerabilidad

- Una puerta de vidrio o de metal corroído.
- Una lectora de CD booteable en una computadora.
- Falta de entrenamiento al personal para que no revele información sensible.
- Una falla en el software que permite sobrescribir áreas de memoria no autorizadas.
- Una impresora que permita reimprimir lo último que se envió.

Debilidad

- Un generador sin combustible.
- Una pantalla de ingreso de credenciales que no posea limite de intentos.
- Un router con usuario y contraseña por defecto.
- Un access point que autentique a los usuarios sólo por la dirección MAC.

Preocupación

- Una alarma de incendios que no suene lo suficientemente fuerte.
- Un archivo de log que no almacena información completa.
- Un access point con cifrado débil.

Exposición

- Una ventana que permite visualizar los activos.
- Errores de una aplicación web que brindan mucha información.
- Respuestas ICMP.

Anomalía

- Una respuesta ICMP de una computadora que no está en la red.
- Aves en los equipos de comunicación.

Relación con los diferentes elementos

A continuación se presenta una tabla que muestra la relación entre las limitaciones y los diferentes elementos del modelo.

Categoría		Elementos	Limitaciones
Porosidad		Visibilidad	Exposición
		Acceso	Vulnerabilidad
		Confianza	
Controles	Clase A – De interacción	Autenticación	Debilidad
		Indemnización	
		Resistencia	
		Subyugación	
		Continuidad	
	Clase B – De proceso	No repudio	Preocupación
		Confidencialidad	
		Privacidad	
		Integridad	
		Alarma	
Anomalías			

Tabla 10: Relación entre los elementos de la seguridad

Seguridad Real

El rol de los controles es reducir y manejar la porosidad. Por cada poro existen diez tipos de controles que pueden ser aplicados y buscan llevar a la seguridad al 100%. Inclusive hay veces en que se puede superar este porcentaje, indicando que se han aplicado controles excesivos, aumentando los costos de manera innecesaria. Luego, las limitaciones reducen la efectividad de los controles. El término *seguridad real* hace referencia a una instantánea de la superficie de ataque en un ambiente operacional.

Caracterización del sistema

Este es el primer paso de la metodología propiamente dicha. Recordando los nueve pasos de la publicación SP 800-30 de NIST:

1. Caracterización del sistema.
2. Identificación de amenazas.
3. Identificación de vulnerabilidades.
4. Análisis de controles.
5. Determinación de probabilidades.
6. Análisis de impacto.
7. Determinación del riesgo.

8. Recomendaciones de control.
9. Resultado y documentación.

Según la guía NIST SP 800-30, esta etapa inicial es donde se definen los activos que van a ser analizados, el alcance de las pruebas y el esfuerzo que se dedicará en cada una de ellas. En la sección siguiente se detallan las tareas definidas en OSSTMM que sirven para implementar la primera de las nueve fases.

Definición del alcance

- Definir los **activos** que quieren protegerse.
- Identificar el área alrededor de los activos, la cual incluye los mecanismos de protección y los procesos o servicios en torno a los activos. Esta es la **zona de compromiso**.
- Definir todo aquello que se encuentre fuera de la zona de compromiso y sea necesario para mantener operacionales a los activos. Esto incluye a la electricidad, agua, información, leyes, contratos, socios, procesos, protocolos, recursos, etc. Esto es el **alcance**.
- Definir cómo el alcance interactúa consigo mismo y con el exterior. Caracterizar la dirección de las interacciones, es decir, de adentro hacia adentro, de adentro hacia afuera, de afuera hacia adentro. Estos son los **vectores**.
- Dentro de cada vector las interacciones pueden ocurrir en varios niveles o **canales**. Se clasifican en: humanos, físicos, medios inalámbricos, telecomunicaciones y redes de datos. Se deben definir las herramientas que se necesitarán para los análisis que se lleven a cabo en los diferentes canales.
- Se debe definir el **tipo de test** que se realizará. El tipo de test depende del conocimiento que se tenga del entorno. De esta forma se pueden encontrar tres grandes categorías: *black box* (sin conocimiento), *gray box* (conocimiento incompleto) y *white box* (conocimiento total).
- Verificar que el análisis se encuentra definido dentro de las **reglas de compromiso**¹³ asegurando que los procesos ejecutados no generan malentendidos ni falsas expectativas.

Canales

El alcance es el ambiente operativo donde producen las interacciones con los activos. Se divide en tres clases, utilizadas actualmente en la industria de la seguridad, y son: PHYSSEC, SPECSEC y COMSEC. A su vez se subdividen en cinco canales como se muestra en la tabla que sigue.

¹³ Las reglas de compromiso son directivas que definen los límites de las pruebas que serán realizadas. Es un contrato entre el cliente y el analista, donde se determina cuáles actividades pueden realizarse y cuáles no.

Clase	Canal	Descripción
PHYSSEC Seguridad física	Humano	Involucra la interacción entre personas.
	Físico	Hace referencia a los elementos tangibles tales como el hardware, maquinaria, puertas, ventanas, pizarras, escritos, etc.
SPECSEC Seguridad inalámbrica	Medios inalámbricos	Son las comunicaciones, señales y emanaciones que tienen lugar dentro del espectro electromagnético.
COMSEC Seguridad en las comunicaciones	Telecomunicaciones	Redes de comunicación donde la interacción se produce sobre líneas del tipo telefónico.
	Redes de datos	Establecidas sobre redes de datos cableadas.

Tabla 11: Relación entre clases y canales

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 acotados, abarcando sólo algunos canales.

The background of the page features a series of overlapping, semi-transparent blue squares and rectangles of various sizes, creating a modern, layered effect. Some shapes have white outlines, and they are arranged in a way that suggests depth and movement.

CAPITULO 4.

IDENTIFICACIÓN DE AMENAZAS, CONTROLES Y LIMITACIONES

En el capítulo anterior se definieron los elementos que forman parte del modelo, así como también se describió el primer paso de esta metodología, del cual se obtienen los activos a ser analizados, los canales y la dirección de las comunicaciones.

En el capítulo actual se verán los tres puntos que siguen en la guía NIST SP 800-30 relativos a la identificación y análisis de amenazas, vulnerabilidades y controles.

1. Caracterización del sistema.
- 2. Identificación de amenazas.**
- 3. Identificación de vulnerabilidades.**
- 4. Análisis de controles.**
5. Determinación de probabilidades.
6. Análisis de impacto.
7. Determinación del riesgo.
8. Recomendaciones de control.
9. Resultado y documentación.

Los pasos 2, 3 y 4 de esta guía hacen referencia a la identificación de amenazas y vulnerabilidades, así como también al análisis de los controles. Para poder implementarlo utilizando OSSTMM, primero se definirá un proceso que permite analizar los puntos de

interacción con el objetivo; luego se analizarán los controles que se aplican sobre cada punto, y por último, las limitaciones o vulnerabilidades que presentan dichos controles.

Como resultado de este capítulo se obtendrá una metodología de análisis que relaciona los cuatro primeros puntos de esta guía de tal forma que permita al auditor recolectar los datos necesarios para que puedan ser ingresados como entradas a una serie de cálculos que determinarán el estado de la seguridad actual.

Proceso de cuatro puntos

Muchas veces se considera a la seguridad como una estrategia defensiva donde se aplican ciertas recomendaciones y prácticas para proteger al sistema y se supone que todo se comporta como ha sido configurado. Por lo general, esto no es así y, si bien es necesario corroborar las configuraciones para un mejor análisis, también debe probarse el sistema en funcionamiento. Muchas son las variables que intervienen en las operaciones cotidianas, y deben ser tenidas en cuenta al momento de decidir si todo se comporta como se espera.

Es por ello que, para un análisis completo, se necesita evaluar la información que provenga de todas las fuentes posibles. 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.

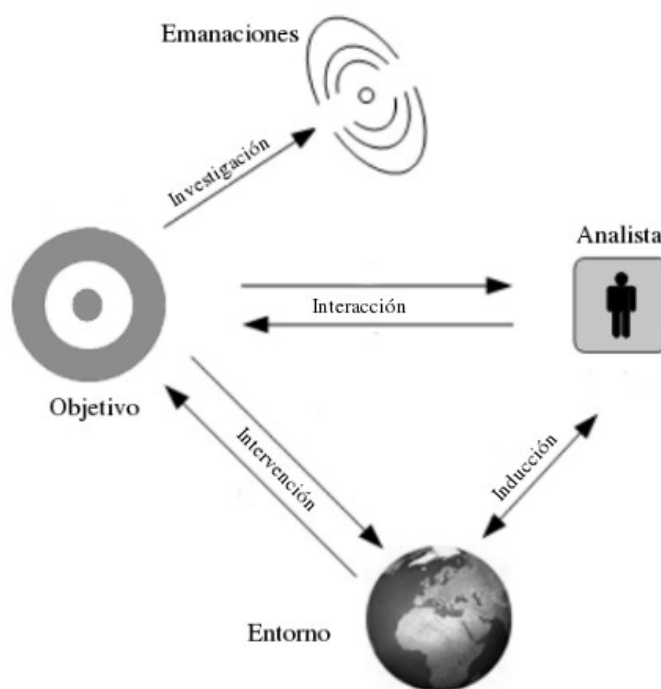


Figura 9: Interacciones dentro del proceso de 4 puntos

1. **Inducción:** Estudiar el entorno donde reside el objetivo, debido a que de una manera u otra condiciona su comportamiento y muchas veces dicho comportamiento deriva directamente de la influencia que recibe del ambiente.
2. **Interacción:** Interactuar directamente con el objetivo y observar las respuestas obtenidas.

3. **Investigación:** Analizar las emanaciones que provengan del objetivo, así también como cualquier pista o indicador de las emanaciones mencionadas.
4. **Intervención:** 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.

Inducción

- Revisión del entorno: Conocer las normas, leyes, políticas y cultura organizacional que influyen en los requerimientos de seguridad dentro de la empresa o institución.
- 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.
- Verificación de detección activa: Averiguar si existen controles que detecten intrusiones que puedan filtrar o bloquear intentos de análisis, obteniendo falsos negativos como resultado.

Interacción

- Auditoría de visibilidad: Enumerar los objetivos visibles dentro del alcance. Conocer los puntos donde la interacción sería posible.
- 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.
- Verificación de confianza: Verificar las relaciones de confianza entre los objetivos, donde exista acceso a la información sin necesidad de autenticación.
- 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.

Investigación

- 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.
- 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.
- 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.
- 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.

- 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.
- 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.

Intervención

- 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.
- 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.
- 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.
- 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.

Diagrama de flujo

Juntando los módulos que derivan del proceso de cuatro puntos se obtiene un diagrama de flujo que define una metodología aplicable a cualquier tipo de test y sobre cualquier canal.

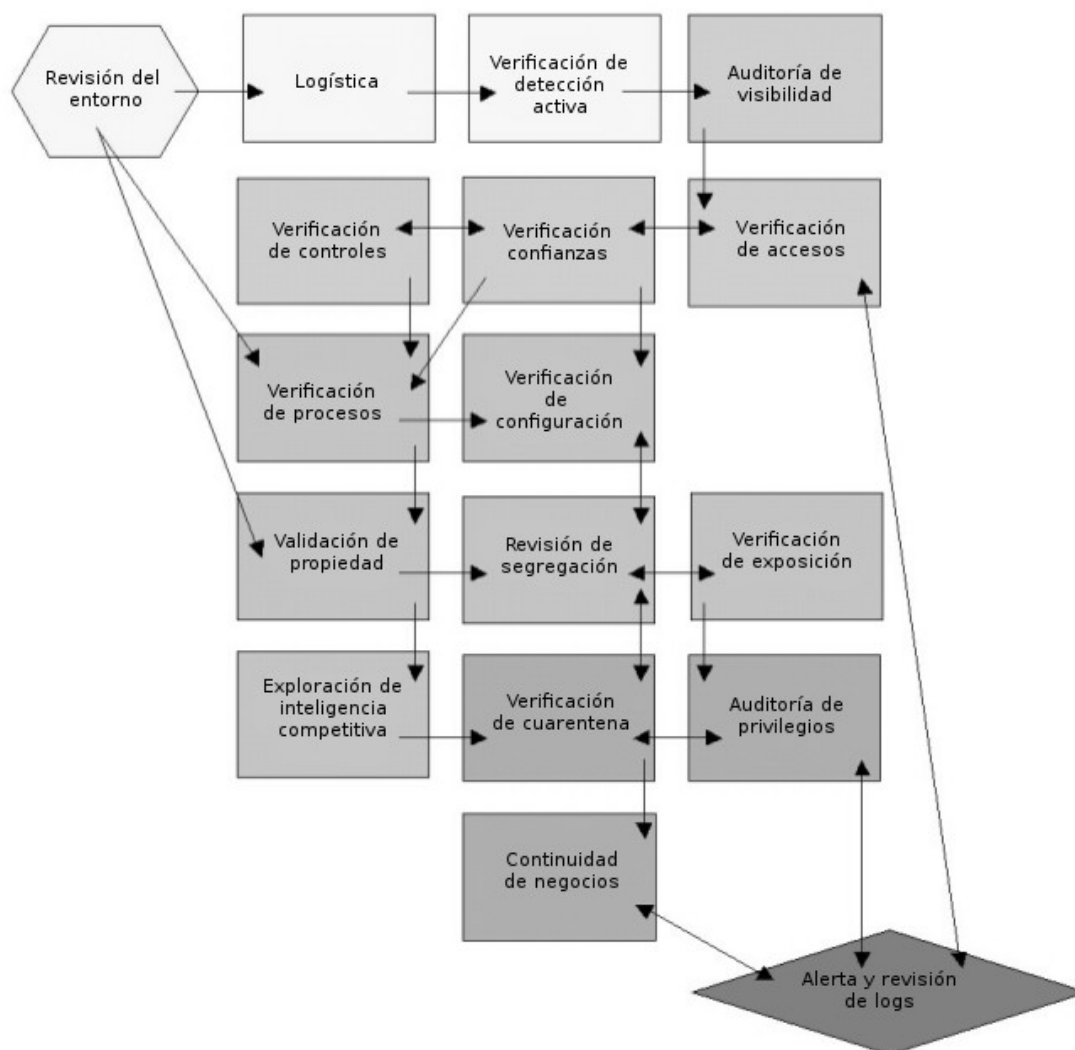


Figura 10: Diagrama de flujo OSSTMM

Siguiendo el diagrama anterior es posible obtener los datos que se requieren como entrada para determinar el estado de la seguridad en un momento determinado. Previamente es necesario clasificar la información obtenida según las indicaciones de las secciones siguientes.

Seguridad operacional

La medición de la superficie de ataque requiere la cuantificación de los *accesos*, *visibilidad* y *confianza*. Para llevar a cabo esta tarea deben seguirse los puntos que se indican a continuación.

Visibilidad

Contar el número de objetivos dentro del alcance. Por ejemplo si en una organización hay 100 empleados pero sólo 40 interactúan dentro de un canal específico, entonces se tiene una visibilidad de 40. Por cada canal se hacen diferentes auditorías para determinar la visibilidad.

Accesos

Contar todos los puntos de acceso por cada lugar de interacción.

En el caso del canal físico, si dentro de un edificio hay 3 puertas y 5 ventanas, se obtiene un acceso de 8. En el caso que se encuentren selladas, el acceso es 0.

En el caso de las redes de datos, si hay una ip activa dentro de la red y para esa ip hay 2 puertos abiertos, se cuenta un acceso equivalente a 3 (1 ip activa + 2 puertos abiertos).

Es más sencillo de analizar cuando se trata del canal humano: si la persona responde a cualquier pregunta cuenta como un acceso, si no responde no cuenta como acceso.

Confianza

Contar cada punto de confianza por cada lugar de interacción.

Por ejemplo, en el canal de las redes de datos, cada redirección de puertos cuenta como 1 punto de confianza.

En el canal humano, cada persona que actúa como intermediario se cuenta como 1.

Controles

En el próximo paso se deben contar los controles, los mecanismos de protección.

Autenticación

Contar cada instancia de autenticación requerida para obtener acceso.

Por ejemplo, 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.

Indemnización

Contar todas las instancias de métodos utilizados para la compensación por pérdidas referidas a los activos.

Por ejemplo, un seguro que cubre el robo de 30 equipos de computación cuenta como 30.

Resistencia

Contar cada instancia de acceso o confianza donde una falla en el sistema de seguridad no provea un nuevo acceso.

Suponiendo que existe un webservice 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 debería validar ninguna credencial hasta la restauración de la conexión. En caso de rechazar las credenciales, cuenta como 1 el valor de resistencia (este sería el caso ideal). Existe la posibilidad de que el servicio no esté correctamente diseñado y cuando pierde la conexión comience a validar todas las credenciales, inclusive las que no son correctas; en ese caso la resistencia es 0.

Subyugación

Contar todos los puntos de acceso o confianza donde la interacción deba cumplir condiciones preestablecidas.

Por ejemplo el uso de PKI para las comunicaciones entre un cliente y un servidor cuenta como 1 ya que la comunicación sólo puede establecerse si cumplen esa condición.

Continuidad

Contar 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.

No repudio

Contar 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.

Confidencialidad

Contar 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.

Privacidad

Contar 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.

Integridad

Contar 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 puede usarse para proveer integridad.

Alarma

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

Limitaciones

Finalmente las limitaciones, que son las fallas que presentan los controles para mantener la separación entre los activos y las amenazas.

Vulnerabilidad

Contar 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.

Debilidad

Contar 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.

Preocupación

Contar 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.

Exposición

Contar 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.

Anomalía

Contar 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 proveniente de una dirección IP inexistente.



CAPITULO 5.

DETERMINACIÓN DEL RIESGO

Este capítulo describirá la etapa de análisis de riesgos vista desde el enfoque propuesto por OSSTMM.

1. Caracterización del sistema.
2. Identificación de amenazas.
3. Identificación de vulnerabilidades.
4. Análisis de controles.
- 5. Determinación de probabilidades.**
- 6. Análisis de impacto.**
- 7. Determinación del riesgo.**
8. Recomendaciones de control.
9. Resultado y documentación.

Según la guía NIST el quinto, sexto y séptimo paso definen el riesgo existente luego del análisis de los puntos vistos en el capítulo anterior. Cualquier método, ya sea cualitativo o cuantitativo, puede ser utilizado en estas etapas; pero debido a que el enfoque de OSSTMM es algo diferente ya que intenta eliminar subjetividades, el riesgo se medirá como la superficie desprotegida dentro del ambiente operacional.

En las secciones siguientes se verán una serie de fórmulas que relacionan la porosidad, los controles y las limitaciones de tal forma que, al final del análisis, se obtenga el resultado de la *seguridad real*.

Fórmulas para la seguridad real

Dentro de OSSTMM, los RAVs¹⁴ (Risk Assessment Values) representan la percepción de la seguridad de forma similar a un valor porcentual. Donde un rav de 100 representa el balance perfecto entre las operaciones, controles y limitaciones.

Los ravs derivan de tres categorías definidas dentro del objetivo: seguridad operacional, controles y limitaciones. En primera instancia se debe asociar la información obtenida en los pasos anteriores a la categoría apropiada.

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

Tabla 12: Categorías para las entradas de datos

Luego de haber obtenido los valores que corresponden a cada categoría, OSSTMM define una serie de fórmulas que determinan un hash que lleva el nombre de “Seguridad real”. ISECOM ha optado por representar este valor de tal forma que se logre un número consistente con la percepción respecto al estado de seguridad de un sistema, donde un valor de 100 ravs representa el balance perfecto entre los distintos elementos, más de 100 significa que hay controles excesivos y un valor menor a 100 indica que faltan controles. Esto no es un valor porcentual, pero debido a que resulta cómodo trabajar con porcentajes, se seleccionó el valor de 100 como el balance perfecto y el resto de las combinaciones se distribuyen según una curva logarítmica que representa de forma aproximada y consistente la percepción de seguridad definida en todos los estándares de seguridad.

¹⁴ Dentro del sitio web de ISECOM (<http://www.isecom.org/research/ravs.html>) se puede descargar una planilla de cálculo en la cual el analista ingresa los datos obtenidos de la auditoría y automáticamente se obtiene el valor del rav, indicando el nivel de seguridad del sistema.

Este valor puede utilizarse para comparar los resultados que derivan de diversas entradas y de esa forma permite analizar la evolución lograda luego de la aplicación de diferentes mecanismos de control.

A continuación se detallan los valores auxiliares que se utilizarán para llegar al resultado final.

Porosidad

La seguridad operacional, también conocida como *porosidad*, es el primero de los tres factores de la seguridad real que debe ser determinado. Inicialmente se determina como la suma de la visibilidad (P_v), accesos (P_a) y confianza (P_t).

$$OpSec_{sum} = P_v + P_a + P_t$$

Para calcular el rav es necesario determinar el valor base de la seguridad operacional, $OpSec_{base}$, que está dado por la ecuación:

$$OpSec_{base} = \log^2(1 + 100 * OpSec_{sum})$$

En el caso que la sumatoria de $OpSec_{sum}$ sea 0, es decir, que no existen interacciones, la fórmula es equivalente a $\log^2(1)$ cuyo resultado es 0. Cuando se da esta condición el resultado final del rav será 100, que se traduce a: *Seguridad Perfecta*.

Controles

El próximo paso para el cálculo es determinar la suma de los controles (LC_{sum}).

- Autenticación (LC_{Au})
- Indemnización (LC_{Id})
- Resistencia (LC_{Re})
- Subyugación (LC_{Su})
- Continuidad (LC_{Ci})
- No repudio (LC_{NR})
- Confidencialidad (LC_{Cf})
- Privacidad (LC_{Pr})
- Integridad (LC_{It})
- Alarma (LC_{Al})

$$LC_{sum} = LC_{Au} + LC_{Id} + LC_{Re} + LC_{Su} + LC_{Ci} + LC_{NR} + LC_{Cf} + LC_{Pr} + LC_{It} + LC_{Al}$$

Controles faltantes

Por cada categoría se debe calcular el valor de los controles faltantes. Se debe tener en cuenta que este valor nunca puede ser menor a 0. Entonces el algoritmo para cada categoría es el siguiente:

$$\begin{aligned} &\text{SI } OpSec_{sum} - LC_x < 0 \\ &\text{ENTONCES } MC_x = 0 \\ &\text{SINO } MC_x = OpSec_{sum} - LC_x \end{aligned}$$

Luego se suman los controles faltantes de todas las categorías para obtener el valor de MC_{sum} .

$$MC_{sum} = MC_{Au} + MC_{Id} + MC_{Re} + MC_{Su} + MC_{Ci} + MC_{NR} + MC_{Cf} + MC_{Pr} + MC_{It} + MC_{Al}$$

Controles reales

Los controles reales (TC_{sum}) son la inversa de los controles faltantes. Donde cada uno de los elementos se calcula como:

$$TC_x = OpSec_{sum} - MC_x$$

Por lo tanto la suma de los controles reales para los diez tipos de controles queda de la siguiente manera:

$$TC_{sum} = TC_{Au} + TC_{Id} + TC_{Re} + TC_{Su} + TC_{Ci} + TC_{NR} + TC_{Cf} + TC_{Pr} + TC_{It} + TC_{Al}$$

El valor obtenido sirve para medir la ubicación ideal de los controles. El valor base ayuda a eliminar la influencia de ubicaciones desproporcionadas dentro de los controles. El valor base (TC_{base}) se calcula como se muestra a continuación:

$$TC_{base} = \log^2(1 + 100 * (OpSec_{sum} - MC_{sum} * 0.1))$$

Porcentaje real de cobertura

Como se ha visto en los capítulos anteriores, por cada punto de interacción existen diez controles posibles; por lo tanto, si la cantidad de controles es cero, el porcentaje real de cobertura será 0%, y si la cantidad de controles es igual a $OpSec_{sum} * 10$ (contando sólo una vez los controles del mismo tipo), entonces el valor real de cobertura es 100%.

Este valor se puede obtener mediante la siguiente fórmula:

$$(100 * (1 - MC_{sum} / (10 * OpSec_{sum})))$$

Este dato es muy importante ya que determina que es lo que se debe corregir, es decir, los puntos que no cuentan con los controles necesarios.

Controles completos

Este valor tiene en cuenta los controles que se aplican a la misma instancia de visibilidad, acceso o confianza. Sirve, por ejemplo, para medir el valor de la defensa en profundidad.

$$FC_{base} = \log^2(1 + 10 * LC_{sum})$$

Por ejemplo si se aplican cinco controles de autenticación a una instancia de acceso, esto podría derivar en un rav mayor a 100.

Limitaciones

Las limitaciones se miden individualmente y están directamente relacionadas con la *porosidad* y los *controles*. En el caso de una exposición o anomalía también se deben tener en cuenta otras limitaciones relacionadas. Las exposiciones o anomalías no generan inconvenientes por si mismas, a menos que estén relacionadas con alguna otra limitación. Por ejemplo, cuando una exposición no conduce a nada que sea explotable, no afecta a la seguridad; y por lo tanto no se tiene en cuenta en el cálculo del rav.

Los valores de la tabla que se muestra a continuación se utilizan para el cálculo de las limitaciones, donde la primer columna contiene las entradas, la segunda el peso que corresponde a cada una de ellas y la tercera, las variables utilizadas.

Entrada	Valor	Variables
Vulnerabilidad L_V	$(OpSec_{sum} + MC_{sum}) / OpSec_{sum}$	MC_{sum} : Suma de controles faltantes
Debilidad L_W	$(OpSec_{sum} + MC_A) / OpSec_{sum}$	MC_A : Suma de controles faltantes de clase A
Preocupación L_C	$(OpSec_{sum} + MC_B) / OpSec_{sum}$	MC_B : Suma de controles faltantes de clase B
Exposición L_E	$((P_A + P_V) * MC_{vg} + L_V + L_W + L_C) / OpSec_{sum}$	P_V : Suma de visibilidad P_A : Suma de accesos MC_{vg} : Porcentaje de cobertura faltante = $(MC_{sum} * 0.1 / OpSec_{sum})$
Anomalía L_A	$(P_T * MC_{vg} + L_V + L_W + L_C) / OpSec_{sum}$	P_T : Suma de confianza

Tabla 13: Valores auxiliares para el cálculo de las limitaciones

Teniendo las variables de entrada y la ponderación correspondiente se puede obtener la fórmula que determina las limitaciones mediante la suma de sus productos.

$$\begin{aligned} \text{SecLim}_{\text{sum}} = & \\ & (L_V * (\text{OpSec}_{\text{sum}} + \text{MC}_{\text{sum}}) / \text{OpSec}_{\text{sum}}) + \\ & (L_W * (\text{OpSec}_{\text{sum}} + \text{MC}_A) / \text{OpSec}_{\text{sum}}) + \\ & (L_C * (\text{OpSec}_{\text{sum}} + \text{MC}_B) / \text{OpSec}_{\text{sum}}) + \\ & (L_E * ((P_A + P_B) * \text{MC}_{\text{vg}} + L_V + L_W + L_C) / \text{OpSec}_{\text{sum}}) + \\ & (L_A * (P_T * \text{MC}_{\text{vg}} + L_V + L_W + L_C) / \text{OpSec}_{\text{sum}}) \end{aligned}$$

Por último, el valor base está dado por el siguiente cálculo:

$$\text{SecLim}_{\text{base}} = \log^2(1 + 100 * \text{SecLim}_{\text{sum}})$$

Seguridad real

Esta es la parte final en la cual se utilizarán los cálculos definidos previamente para obtener el valor de la seguridad real. Antes de pasar al cálculo final, se utilizará un valor auxiliar (valor delta) que representa el cambio que una solución de seguridad genera en el alcance. El valor delta se calcula mediante la siguiente fórmula:

$$\text{ActSec}_{\Delta} = \text{FC}_{\text{base}} - \text{OpSec}_{\text{base}} - \text{SecLim}_{\text{base}}$$

El cálculo final determinará el estado actual de las operaciones con los controles aplicados y las limitaciones descubiertas.

Como se mencionó anteriormente, el valor que se obtiene no es un porcentaje aunque un rav de 100 determina el balance óptimo en la seguridad. El resultado del rav se calcula según la fórmula que se muestra a continuación:

$$\begin{aligned} \text{ActSec} = & 100 + \text{ActSec}_{\Delta} - \\ & 0.01 * (\text{OpSec}_{\text{base}} * \text{FC}_{\text{base}} - \text{OpSec}_{\text{base}} * \text{SecLim}_{\text{base}} + \text{FC}_{\text{base}} * \text{SecLim}_{\text{base}}) \end{aligned}$$

Si se analizan diferentes entradas de datos utilizando la planilla de cálculo de ravs, se puede observar que, a medida que aumenta el valor de la porosidad, disminuye el valor del rav, es decir, la percepción de seguridad disminuye. Cuando se agregan controles, el valor de la seguridad real sube nuevamente, indicando que la percepción de seguridad ha aumentado. Por otra parte, cuando se consideran las limitaciones de los controles, el resultado del rav vuelve a disminuir porque también disminuye la percepción de seguridad.

Ejemplo

A continuación se desarrollará un ejemplo simple donde se analizará la seguridad desde el punto de vista de la infraestructura. El esquema es el siguiente:

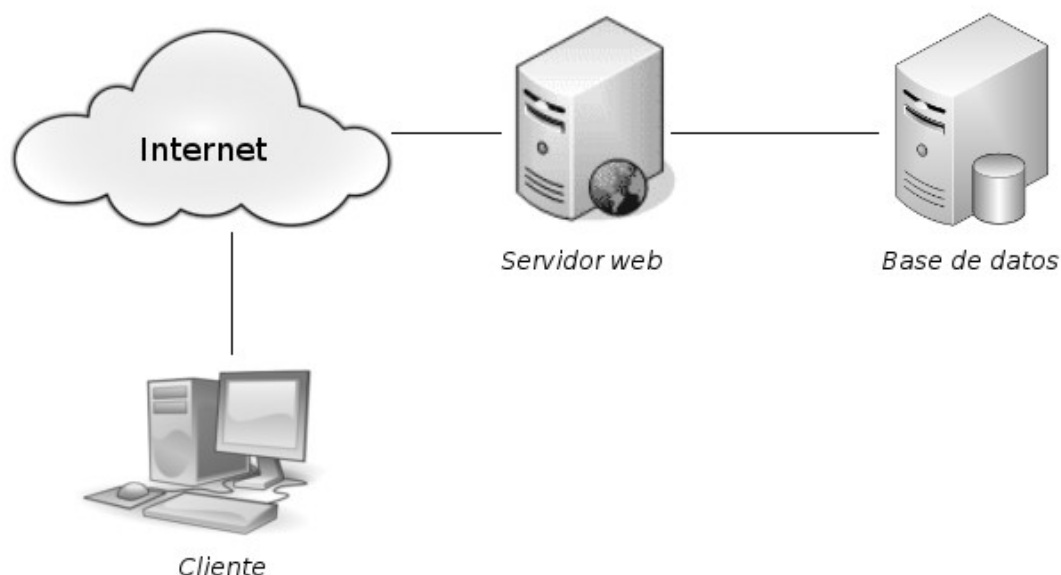


Figura 11: Ejemplo infraestructura simple

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.

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.

Accesos

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

Comando 2: nmap -p 1-65535 servidorweb

Resultado: Puerto abierto 443, el resto de los puertos están cerrados.

Accesos: 2 (puerto 443 y respuesta a ping)

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)

Confianza

Contar cada punto de confianza por cada lugar de interacción.

El único punto de confianza que existe es la comunicación que existe 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)

Controles

Controles en el servidor HTTPS

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.*

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.*

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.*

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

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.*

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.*

Limitaciones

Preocupación: El servidor web acepta cifrado de 56 bit, que son considerados como débiles. *Suma 1 a las limitaciones.*

Exposición: El banner obtenido a través de una conexión al servidor https brinda información. *Suma 1 a las limitaciones.*

Resultados

Seguridad operacional

- Accesos $\rightarrow 2$
- Visibilidad $\rightarrow 2$
- Confianza $\rightarrow 1$

$$Porosidad = OpSec_{sum} = P_A + P_V + P_T = 2 + 2 + 1 = 5$$

$$OpSec_{base} = \log^2(1 + 100 * OpSec_{sum}) = \log^2(1 + 100 * 5) = 7,289124$$

Controles

- Autenticación $\rightarrow 1$ (Controles faltantes $\rightarrow 4$)
- Indemnización $\rightarrow 0$ (Controles faltantes $\rightarrow 5$)
- Resistencia $\rightarrow 0$ (Controles faltantes $\rightarrow 5$)
- Subyugación $\rightarrow 2$ (Controles faltantes $\rightarrow 3$)
- Continuidad $\rightarrow 0$ (Controles faltantes $\rightarrow 5$)
- No repudio $\rightarrow 1$ (Controles faltantes $\rightarrow 4$)
- Confidencialidad $\rightarrow 1$ (Controles faltantes $\rightarrow 4$)
- Privacidad $\rightarrow 0$ (Controles faltantes $\rightarrow 5$)
- Integridad $\rightarrow 1$ (Controles faltantes $\rightarrow 4$)
- Alarma $\rightarrow 0$ (Controles faltantes $\rightarrow 5$)

$$Controles = LC_{sum} = LC_{Au} + LC_{Id} + LC_{Re} + LC_{Su} + LC_{Ct} + LC_{NR} + LC_{Cf} + LC_{Pr} + LC_{It} + LC_{Al} = 6$$

$$Controles\ faltantes = 22\ de\ clase\ A + 22\ de\ clase\ B = 44$$

$$TC_{base} = \log^2(1 + 100 * (OpSec_{sum} - MC_{sum} * 0.1)) = \log^2(1 + 100 * (5 - 44 * 0.1)) = 3,187403$$

$$FC_{base} = \log^2(1 + 10 * LC_{sum}) = \log^2(1 + 10 * 6) = 3,187403$$

Limitaciones

- Preocupación $\rightarrow 1$
- Exposición $\rightarrow 1$

Peso de las limitaciones

$$Mc_{vg} = (MC_{sum} * 0.1 / OpSec_{sum}) = (44 * 0.1) / 5 = 0,88$$

$$Lv \Rightarrow (OpSec_{sum} + MC_{sum}) / OpSec_{sum} = (5 + 44) / 5 = 9,8$$

$$L_W \Rightarrow (\text{OpSec}_{\text{sum}} + \text{MC}_A) / \text{OpSec}_{\text{sum}} = (5 + 22) / 5 = 5,4$$

$$L_C \Rightarrow (\text{OpSec}_{\text{sum}} + \text{MCB}_B) / \text{OpSec}_{\text{sum}} = (5 + 22) / 5 = 5,4$$

$$L_E \Rightarrow ((P_A + P_V) * \text{MC}_{\text{vg}} + L_V + L_W + L_C) / \text{OpSec}_{\text{sum}} = (4 * 0,88 + 0 + 0 + 1) / 5 = 0,904$$

$$L_A \Rightarrow (P_T * \text{MC}_{\text{vg}} + L_V + L_W + L_C) / \text{OpSec}_{\text{sum}} = (1 * 0,88) + 0 + 0 + 1) / 5 = 0,376$$

$$\begin{aligned} \text{SecLim}_{\text{base}} &= \log^2(1 + 100 * \text{SecLim}_{\text{sum}}) \\ &= \log^2(1 + 100 * (0 * 9,8 + 0 * 5,4 + 1 * 5,4 + 1 * 0,904 + 0 * 0,376)) = \\ &= \log^2(1 + 100 * (6,304)) = 7,841706 \end{aligned}$$

Seguridad

$$\text{ActSec}_{\Delta} = \text{FC}_{\text{base}} - \text{OpSec}_{\text{base}} - \text{SecLim}_{\text{base}} = 3,187403 - 7,289124 - 7,841706 = -11,94$$


$$\begin{aligned} \text{ActSec} &= 100 + \text{ActSec}_{\Delta} - 0,01 * (\text{OpSec}_{\text{base}} * \text{FC}_{\text{base}} - \text{OpSec}_{\text{base}} * \text{SecLim}_{\text{base}} + \text{FC}_{\text{base}} * \\ &\text{SecLim}_{\text{base}}) = 88,15 \end{aligned}$$

ActSec = 88,15 ravs

Calculadora de RAVs de OSSTMM

Luego de cargar los valores en la planilla que provee ISECOM para el cálculo de RAVs, se observan los resultados de manera más simplificada. El analista debe cargar los valores de entrada y los resultados de las fórmulas 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		
Actual Security: 88,15 ravs				



INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

True Controls

3,187403

Full Controls

3,187403

True Coverage A

12,00%

True Coverage B

12,00%

Total True Coverage

12,00%



OSSTMM
www.osstmm.org

Security A

-11,94

True Protection

88,06



CAPITULO 6.

RECOMENDACIONES Y DOCUMENTACIÓN

Las dos últimas etapas de la guía NIST SP 800-30 hacen referencia a las recomendaciones de control, resultados y documentación.

1. Caracterización del sistema.
2. Identificación de amenazas.
3. Identificación de vulnerabilidades.
4. Análisis de controles.
5. Determinación de probabilidades.
6. Análisis de impacto.
7. Determinación del riesgo.
- 8. Recomendaciones de control.**
- 9. Resultado y documentación.**

Recomendaciones de control

En esta etapa se puede analizar cómo impactaría el agregado de diversos controles sobre las operaciones. El objetivo es reducir la superficie de ataque sin generar sobrecarga de controles de un mismo tipo por un lado, dejando áreas desprotegidas por otro. Finalmente el analista intentará buscar la combinación de controles que reduzcan el riesgo a un nivel aceptable.

Para llevar a cabo esta tarea es necesario recordar que existen diez tipos de controles diferentes y por ello es de suma importancia reconocer cuáles de ellos están siendo aplicados y cuáles no.

Suponiendo que existe una página web que maneja información sensible y el análisis de la superficie de ataque arrojó un resultado de 50 ravs, entonces existe una gran parte del alcance

que se encuentra desprotegida. En ese caso sería conveniente analizar el agregado de un nuevo control para aumentar el valor de los ravs y reducir la superficie desprotegida. Si el costo de aplicar el control es mayor al valor del activo que protege, entonces deberá ser desestimado para abordar el análisis de un control diferente.

Cuando se requiera analizar el costo-beneficio de aplicar un nuevo control, se tendrá que calcular el valor de la *seguridad real* sin dicho control y luego se podrán repetir los cálculos, pero esta vez se tendrá que contabilizar el cambio aplicado para luego observar la variación que se obtiene.

El control que está siendo analizado debe ser considerado con sus limitaciones debido a que éstas afectan al resultado final. Si no son consideradas correctamente, puede ser que se esté aumentando la superficie de ataque cuando el analista piense que está reduciéndola. Por ejemplo, si se contrata a un guardia de seguridad para proteger la entrada a una zona restringida, y el guardia no es capacitado de forma correcta o no se le dan los elementos que requiere para su buen desempeño, éste puede brindar información confidencial a usuarios malintencionados, y así, poner al descubierto más cantidad de información que antes del nuevo control.

Además del nivel de seguridad que introduce un nuevo control, siempre deben tenerse en cuenta aspectos como el efecto que causa en el rendimiento, la aceptación del usuario, la factibilidad y el costo de implementación, entre otros.

Por lo tanto, las recomendaciones de control deben venir acompañadas del análisis y comparativa de ambas soluciones.

Resultado y documentación

Al finalizar un análisis de seguridad se debe entregar al cliente un documento que contenga el detalle de los resultados obtenidos. Generalmente los reportes de auditorías contienen dos grandes secciones:

- Resumen ejecutivo
- Reporte técnico

El resumen ejecutivo debe ser escrito en términos que un gerente, un directivo o una persona de TI puedan entender, sin detalles técnicos. A un gerente de una gran empresa no le preocupa la versión de SSH que se esté usando, las reglas definidas en el firewall o cómo se gestionan las copias de seguridad; pero lo que sí le resulta de suma importancia es cuánto dinero puede perder si un servidor se ve comprometido de tal forma que no permita realizar ventas por un lapso de tiempo, si la imagen de la empresa se ve degradada debido a un ataque de phishing o si los datos de sus clientes son divulgados generando desconfianza hacia la organización.

Por otra parte se encuentra el reporte técnico, el cual debe contener el detalle de las incidencias, ya en un lenguaje más técnico, donde se indique de manera clara la ubicación del problema y la forma de reproducirlo. En el caso de ser una auditoría en un sitio web, se debe copiar la url vulnerable, y los parámetros utilizados para explotarla, y generalmente se copian capturas de pantalla que prueban lo que se está informando. Esta sección del reporte debe permitir al personal técnico localizar las fallas de una manera rápida y sencilla, así como también comprender el origen del incidente para evitar repetirlo en futuras ocasiones.

Aspectos a considerar en los reportes

Existen ciertos aspectos que deben tenerse en cuenta a la hora de escribir un reporte de auditoría, a continuación se enumeran los más destacados:

- El analista debe respetar la privacidad de todos los individuos.
- Los resultados deben estar escritos en forma estadística, de tal manera que el personal involucrado no sea directamente identificado.
- Siempre que se encuentre una incidencia de carácter grave, debe ser informada de forma inmediata para su corrección y no esperar a la entrega final del reporte.
- El analista no debe firmar un reporte en el cual no estuvo directamente involucrado.
- Los reportes deben contener información objetiva, basada en datos reales.
- Si el reporte incluye soluciones y recomendaciones, éstas deben ser válidas y prácticas.
- Los reportes deben mostrar de manera clara las anomalías y resultados que no pueden ser clasificados por algún motivo en particular.
- Los reportes deben mostrar tanto las vulnerabilidades que fueron explotadas como aquellas que no pudieron serlo.
- El cliente debe ser notificado al momento del envío del reporte, de tal manera que pueda esperar y confirmar la recepción.
- Los canales de comunicación deben mantener la confidencialidad.
- Los resultados de un reporte nunca podrán ser utilizados como muestra para promocionarse comercialmente.

Reportes con STAR

STAR hace referencia a las palabras en inglés *Security Test Audit Report*, o en español *Reporte de Auditoría de Pruebas de Seguridad*. El propósito de este reporte es ofrecer soporte a un informe ejecutivo brindando un cálculo preciso de la superficie de ataque de los objetivos bajo análisis.

Desde el sitio de ISECOM se puede descargar la plantilla para realizar un reporte del tipo STAR. URL: <http://www.isecom.org/mirror/STAR.3.pdf>

Esta plantilla debe ser completada y firmada por el analista y debe contener la siguiente información:

- Fecha del análisis
- Duración
- Nombre del auditor
- Tipo de test
- Alcance de las pruebas
- Canales analizados
- Vectores analizados
- Valores de seguridad operacional
- Controles
- Limitaciones
- Métricas resultantes de los cálculos
- Cuáles pruebas fueron completadas, cuáles no y hasta qué punto
- Cualquier observación sobre la validez de los resultados
- Anomalías y detalles desconocidos

CONCLUSIONES

Actualmente la información se ha transformado en uno de los activos más importantes dentro de una organización. Nuestro deber como profesionales de la informática es buscar que dicha información esté debidamente protegida, que esté disponible para cuando algún usuario autorizado la requiera, y que sólo sea modificada por aquellos que posean los permisos necesarios para hacerlo.

La seguridad se debe ser concebida desde el comienzo de cada proyecto y no cuando éste se encuentre en las etapas finales. Generalmente este último enfoque deriva en soluciones improvisadas que no atacan el problema de fondo. En el caso del desarrollo de software, la seguridad debe formar parte del diseño y debe ser implementada durante todo el proceso. Por otra parte, la gente que se encarga de administrar los sistemas y las redes de datos debe ocuparse de mantener los servidores actualizados, así como también definir diversas políticas que lleven a un ambiente más protegido. El personal que no pertenece al área de informática debe ser capacitado para cumplir con las políticas implementadas, ya que no sólo es importante la información que circula por la red sino que los documentos escritos o respuestas verbales pueden dar lugar al compromiso del sistema o a una violación de la confidencialidad de los datos. Tener en cuenta que incendios e inundaciones, entre otros, pueden afectar en gran medida a la seguridad de los datos.

Éstos son sólo algunos de los temas que deben considerarse cuando se trata de seguridad de la información. El personal de la alta gerencia debe apoyar esta visión, ya que de eso dependerá el cumplimiento de las políticas establecidas, los fondos disponibles para proteger la información, la toma de decisiones y la determinación de prioridades.

Como se vio en los capítulos anteriores, la seguridad puede verse comprometida desde diferentes canales y puede ser de manera intencional como no intencional. Es por ello que debe analizarse de manera integral, cubriendo todos los aspectos posibles de forma organizada, cuantificable y repetible. El objetivo de este trabajo fue combinar la guía propuesta por NIST para el análisis de riesgos y la metodología de pruebas de seguridad propuesta por ISECOM, logrando una metodología de análisis objetiva, cuantificable, repetible y que además cumple con todos los pasos que se indican en la publicación especial de NIST SP 800-30.

GLOSARIO

Acceso: Es un punto donde se producen las interacciones. Por ejemplo, un servidor web sería un ejemplo de *acceso*. Es uno de los tres elementos que componen la porosidad.

Activo: Son todos los elementos físicos o lógicos que posean algún valor para la organización.

Alarma: Es un aviso de que ha ocurrido un evento o interacción. Es uno de los cinco controles de proceso.

Alcance: Es el ambiente operativo donde producen las interacciones con los activos.

Amenaza: Es una circunstancia que tiene el potencial de causar algún daño, pérdida o difusión no autorizada de información.

Anomalía: Es un elemento desconocido y no se encuentra dentro de las operaciones normales. Es una de las categorías en las que se dividen las limitaciones.

Autenticación: Es la combinación entre los mecanismos de identificación y autorización. Es uno de los cinco controles de interacción.

Canales: Son todos los medios por los cuales se pueden llevar a cabo las interacciones. Existen cinco canales definidos por OSSTMM: humano, físico, medios inalámbricos, telecomunicaciones y redes de datos.

Confianza: Es una interacción que no requiere autenticación entre dos elementos dentro del alcance. Es uno de los tres elementos que componen la porosidad.

Confidencialidad: Es el control de proceso que impide que la información que circula entre dos partes sea conocida por terceros no autorizados.

Continuidad: Es el control de interacción que permite mantener la interacción con los activos aún en caso de fallas.

Controles: Son los mecanismos que brindan protección a las operaciones cuando no es posible separar la amenaza del activo. Existen diez tipos de controles, se dividen en cinco controles de proceso y cinco de interacción.

Debilidad: Es una falla que reduce o anula los efectos de los controles de interacción.

Exposición: Es una acción injustificada que permite dejar visible, ya sea de forma directa o indirecta, a un activo.

Indemnización: Es un compromiso entre el propietario del activo y la parte que interactúa donde existe un resarcimiento previamente pactado en caso de pérdidas.

Inducción: Es uno de los elementos del proceso de cuatro puntos cuyo objetivo es el estudio del entorno donde reside el objetivo para observar de qué manera condiciona su comportamiento.

Integridad: Es el control de proceso que permite identificar cuando un activo ha sido modificado por alguien ajeno a la interacción en curso.

Interacción: Dentro del proceso de cuatro puntos, *interacción* se refiere a la comunicación directa con el objetivo para analizar las respuestas obtenidas.

Intervención: Es el análisis de las respuestas del objetivo ante la modificación de los recursos del entorno. Es una de las fases del proceso de cuatro puntos.

Investigación: Es la fase del proceso de cuatro puntos donde se analizan las emanaciones que provengan del objetivo, así también como cualquier pista o indicador de las emanaciones mencionadas.

ISECOM: Instituto para la Seguridad y las Metodologías Abiertas.

Limitaciones: Son los inconvenientes que presentan los controles para mantener la protección de los activos ante las amenazas.

Nist SP 800-30: Es una publicación especial del instituto NIST que describe una guía de gestión de riesgos para sistemas de Tecnología de la Información.

No repudio: Es el control de proceso que impide que las partes que interactúan en una comunicación nieguen su participación.

OSSTMM: Es una metodología creada por ISECOM, que busca establecer un método científico para el análisis de la seguridad.

Porosidad: Es el término utilizado para representar los puntos de interacción. Son puntos que reducen la separación entre amenazas y activos.

Preocupación: Es una falla que reduce los efectos de los controles de proceso.

Privacidad: Es el control de proceso que evita que un tercero conozca la forma en la cual es accedido, mostrado o intercambiado un activo.

Proceso de cuatro puntos: Es el proceso que se debe llevar a cabo para realizar un análisis completo de seguridad. Se contemplan: el análisis del entorno, la interacción directa, las emanaciones del objetivo y la modificación del ambiente, asegurando una revisión integral.

Rav: Es un valor que combina la porosidad, controles y limitaciones para obtener el porcentaje de la superficie protegida.

Resistencia: Es el mecanismo que brinda protección a los activos en caso que las interacciones sufran alguna falla.

Seguridad operacional: Es la medida de la visibilidad, accesos y confianza dentro del alcance. Véase *porosidad*.

Seguridad real: Es el resultado que se obtiene luego de analizar la seguridad operacional, los controles y sus limitaciones.

Separación: Es la acción de aislar al activo de la amenaza. Cuando existe separación, el activo está completamente seguro, en cambio cuando existe la necesidad de interacción, se deben agregar controles para brindar protección.

SGSI: Sistema de gestión de la seguridad de la información.

Subyugación: Es el control que define las condiciones en las cuales ocurrirán las interacciones.

Visibilidad: Representa a los objetivos observables dentro del alcance.

Vulnerabilidad: Es una falla que puede permitir el acceso no autorizado a un activo o puede denegar dicho acceso a alguien que sí esté autorizado.

REFERENCIAS

- [1] Herzog P, et al. (2010). Open Source Security Testing Methodology Manual v3.
- [2] Harris S. (2013). CISSP Exam Guide (*Sexta edición*), Mc Graw Hill.
- [3] EC-Council. (2010). Ethical Hacking and Countermeasures (*Versión 6.1*).
- [4] NIST. (2002). Risk Management Guide for Information Technology Systems (*NIST SP 800-30*).
- [5] ISO/IEC 27001:2005. (2005). Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. (*ISO 27000 Series*).
- [6] Endres Pablo. (2012). Do Reverse Proxies provide real security?
- [7] Matalobos Veiga Juan Manuel. (2009) Análisis de riesgos de seguridad de la información.
- [8] Lewis University. A Brief History of Information Security. Recuperado de <http://www.lewisu.edu/academics/msinfosec/history.htm>.
- [9] Borghello Cristian F. (2009). Metodologías de Análisis de Riesgo. Recuperado de <http://seguinfo.wordpress.com/2009/03/05/metodologias-de-analisis-de-riesgo-2/>.
- [10] Academia Latinoamericana de Seguridad Informática. Concepto de análisis de riesgos. Recuperado de <http://arcadia.inf.udec.cl/~psi/documentos/riesgos/analisis-riesgos.ppt>.
- [11] Análisis de Riesgos: ISO 27005 vs magerit y otras metodologías. Recuperado de <http://www.delitosinformaticos.com/10/2009/proteccion-de-datos/analisis-de-riesgos-iso-27005-vs-magerit-y-otras-metodologias#.URyUxjSldc0>.
- [12] Introducción al análisis de riesgos. (2012) Recuperado de <http://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93%93-metodologias-ii/>.
- [13] Florencio Cano. (2012). Análisis de "riesgos" sin usar probabilidades según OSSTMM 3. Recuperado de <http://www.seinhe.com/blog/90-analisis-de-riesgos-sin-usar-probabilidades-segun-osstm-m-3>.