GUIA PARA LA EVALUACION DE SEGURIDAD EN UN SISTEMA

Luz Marina Santos
Universidad de Pamplona
lsantos@unipamplona.edu.co
Teléfono: 5685303 Ext. 141
Carrera 9 # 5-53 2do. Piso Pamplona

Resumen

Este documento presenta una serie de delineamientos básicos productos de la experiencia e investigación para la evaluación de seguridad en un sistema, con el objeto de articular diversos conceptos y técnicas para la identificación y valoración de riesgos. El artículo se enfoca primordialmente en los métodos de análisis de riesgos, *checklist* y auditoria.

Palabras claves

Riesgo, amenaza, impacto, frecuencia, vulnerabilidad, *checklist*, políticas de seguridad y auditoria.

1. INTRODUCCION

A nivel de investigación y academia diversas metodologías para implantar seguridad en sistemas han sido planteadas: *Metodología de implantación de seguridad en redes* **[ACOS-98]**, "*Metodología para la implantación de seguridad en aplicaciones distribuidas* **[SANT-99]**, etc; también se elaboran otra serie de metodologías por analistas de seguridad que laboran en la empresa privada.

Todas las metodologías llegan a un punto donde se preguntan ¿cómo valorar el impacto que causaría a un sistema la consecución de una amenaza?, la respuesta no es fácil, requiere de un análisis serio por parte del grupo de personas encargado de realizar dicha valoración.

El objetivo del presente es exponer y presentar algunas reflexiones sobre tres métodos tradicionales para evaluar la seguridad de un sistema: análisis de riesgos, listas de chequeo y auditoria.

En áreas donde las pérdidas esperadas y frecuencia de las amenazas están bien definidas, el análisis de riesgos puede ser usado. Donde las pérdidas esperadas y frecuencia de las amenazas no esta claro, se pueden usar inicialmente listas de chequeo para verificar los principios y prácticas de seguridad estándares. Requerimientos de seguridad adicionales pueden ser determinados con métodos de auditoria o evaluaciones de protección de seguridad. **[FIPS-79]**

2. APLICACIÓN DE LOS METODOS DE EVALUACION

No se trata de especificar en qué o cuáles casos se aplica un método u otro, los tres se complementan con el objeto de evaluar la seguridad, lo que si es posible diferenciar es los espacios de tiempo en que se realizan.

Para empezar la evaluación de seguridad en un sistema resulta beneficioso aplicar listas de chequeo, estas no son un sustituto del formal análisis de riesgos, más bien, al

realizarse constituye un punto de partida a éste en aquellos puntos que quedan sujetos a revisión. Además que se pueden tomar medidas correctivas en forma rápida, que no implican mayor costo y esfuerzo.

El proceso de auditoria es planeada para realizarse periódicamente, lo que indica que se llevará a cabo tiempo después que se ha realizado un análisis de riesgos, con el objeto de verificar si se están cumpliendo los controles y políticas de seguridad previstos anteriormente.

Independiente de si existe en la organización o no información estadística de los elementos que determinan los riesgos, es recomendable al grupo evaluador realizar el proceso de análisis de riesgos, así sea en forma cualitativa, con el objeto de crear esta cultura en la organización.

A continuación la tabla 1 presenta los beneficios y dificultades que presentan los métodos tratados en este artículo.

Tabla 1. Pros/Contras

Métodos /	**PROS**	**CONTRAS**
Análisis de Riesgos	-Crea la cultura del riesgo y su manejo en una organización. -Expresa en mejores términos las pérdidas al ocurrir un evento desfavorable. *Metodología cuantitativa* -Las valoraciones son objetivas. -El valor de la información es expresado en términos monetarios. -El presupuesto destinado a la seguridad del sistema esta basado en análisis confiables y bien sustentados. *Metodología cualitativa* -No es necesario determinar el valor monetario de la información, ni la frecuencia de las amenazas, ni el costo de las medidas a tomar y del análisis costo/beneficio.	-Existe resistencia a su aplicación, ya sea por ignorancia, arrogancia o miedo. -Es un proceso que requiere gran cantidad de tiempo y de información disponible. -Proceso costoso. *Metodología cuantitativa* -No es práctico realizar valoraciones cuantitativas sin ayuda de herramientas y bases de conocimiento bien sólidas. -Requieren una cantidad sustancial de información. -No existe un estándar sobre amenazas y sus frecuencias. *Metodología cualitativa* -Toda valoración es esencialmente subjetiva, en procesos y métricas. -La percepción de valores puede no reflejar realmente el actual valor del riesgo.
Listas de chequeo (Check-list)	-Existen en forma abundante y libre. (Listas de chequeo técnicas) -Fácil de aplicar, resumir y comparar. -Flexibles -Su análisis es rápido, consiste en verificar si existe o no existe un control que es aplicable al sistema en análisis. -Se pueden aplicar medidas correctivas de inmediato.	-Arbitrario y subjetivo -Necesitan actualizarse constantemente, en el caso que sean listas de chequeo de tipo técnico. -Pueden no tratar necesidades de un sistema particular.
Auditoria	-Propicia el mejoramiento de procedimientos en el sistema. -Reduce errores organizacionales -Promueve la aplicación de las políticas y estándares de seguridad. -Descubre nuevas amenazas al sistema. (Retroalimenta el análisis de riesgos)	-Aptitud negativa de los encargados de las partes auditadas. -Requiere tiempo y esfuerzo. -Requiere tener pistas de auditoria

3. ANALISIS DE RIESGOS

El proceso de identificar, analizar y valorar, mitigar o transferir el riesgo es generalmente caracterizado como manejo del riesgo **[KRAU-99]**. Hay una serie de preguntas que se hacen en este proceso:

1.¿Que podría ocurrir? (amenaza)
2.¿Sí ocurre, cuánto daño podría causar? (impacto)
3.¿Qué tan a menudo podría ocurrir?
4.¿Qué tan ciertas son las respuestas a las anteriores preguntas?

Una vez respondidas acertadamente las anteriores preguntas, se responden ahora las siguientes:

1.¿Qué puede ser hecho? (mitigación del riesgo)
2.¿Cuál es el costo de la medida? (anual)
3.¿Es la medida efectiva? (análisis costo/beneficio)

El manejo de riesgos compara el costo de implementar medidas de seguridad contra los costos generados al ocurrir un evento desfavorable en el sistema que afecte directa o indirectamente la prestación de servicios.

3.1 ETAPAS DEL ANALISIS DE RIESGOS

El análisis de riesgos busca cuantificar el impacto de las amenazas potenciales sobre un sistema, comprende cuatro subetapas: planeación del análisis de riesgos, identificación de amenazas y vulnerabilidades, valoración del impacto y frecuencia de escenarios recurso/amenazas y tratamiento del riesgo.

3.1.1 Planeación del análisis de riesgos

Si el sistema a evaluar es muy complejo y la organización es muy grande, es conveniente para el analista de seguridad elaborar un análisis de riesgos por subsistemas, lo que facilitará también la presentación y comprensión de informes por parte de los directivos de la empresa. Los siguientes ítem corresponden la parte preliminar de el análisis de riesgos:

a)*La dirección del análisis*: con el objeto de influenciar el estilo de análisis y la información de salida del proceso de valoración del riesgo. Se identifica el proceso de valoración del riesgo, tipo de salida requerida y necesidades críticas.
b)*El alcance*: se determina el alcance del análisis. Cuales recursos del sistema requiere o no el análisis de riesgos. Cuales agentes de amenazas no serán considerados, etc.
c)Los límites: se define en términos de límites físicos y lógicos. El límite físico indica donde termina el sistema y comienza el sistema; indica las características de todas las interfaces con otros sistemas. El límite lógico define la amplitud y profundidad del análisis.
d)Descripción del sistema: requerimientos (o misión) del sistema, concepto de operación, e identificación de la naturaleza de los recursos del sistema. Está descripción provee las bases para posteriores análisis y es prerrequisito para iniciar la valoración de riesgos.
e)Objeto del riesgo y certeza requerida: el objeto ayudará a

determinar si el riesgo está en los límites aceptables. La certeza define el nivel de acierto para la valoración del riesgo, este factor determina el nivel de esfuerzo en el análisis.

3.1.2 Identificación de amenazas y vulnerabilidades

Las amenazas en el sistema provienen del personal encargado, personal externo, daño en equipos, caída de enlaces, etc. Al momento se tiene la información como lo muestra la siguiente tabla.

Tabla 2. Relación recurso/amenazas

Recurso	Amenazas
Recurso 1	Amenaza 1 Amenaza 2 ....
Recurso 2	Amenaza 1 Amenaza 2 ....

Un análisis de vulnerabilidades, por ejemplo puede identificar solo la ausencia de medidas para reducir los riesgos, lo anterior se puede indicar cualitativamente en binario como si o no. Se encuentran las debilidades o vulnerabilidad desde los siguientes puntos de vista.

- Vulnerabilidades de software: errores de aplicaciones, errores de sistemas operativos, rutinas de acceso no autorizados, servicios no autorizados

- Vulnerabilidades de hardware: inapropiada operación, fallas en mantenimiento, inadecuada seguridad física, falta de protección contra desastres naturales

- Vulnerabilidades de datos: inadecuados controles de acceso a personal no autorizado

- Vulnerabilidades administrativas: ausencia de políticas de seguridad, ausencia de cultura de seguridad, ausencia de procedimientos, falta de educación y entrenamiento en seguridad

- Vulnerabilidades de comunicaciones: inadecuados controles de acceso a la red, inadecuados mecanismos para prevenir fallas en comunicaciones

- Vulnerabilidades de personal (empleados): inadecuados controles de acceso físico, inadecuados controles de acceso lógico

Por medio de entrevistas con cuestionarios previamente diseñados que contemplen los principios y prácticas de seguridad generalmente aceptados, se encontrarán las vulnerabilidades que tiene el sistema. A continuación se relacionan una serie de fuentes de información importantes a esta subetapa:

- *National Research Council Report "Computers at Risk"*
- *National Information Infraestructure Task Force (NITF) findings*
- *Presidential National Security and Telecommunications Advisory Council (NSTAC) report*
- *President's Commission on Critical Infraestructure Protection (PCCIP) report*

Para cada una de las amenazas encontradas se define cuales

vulnerabilidades presenta el sistema que pueden llevar a su realización. Se forman escenarios recurso/ amenaza/ vulnerabilidades como lo indica la tabla 3.

Algunas debilidades observadas en el sistema, dan píe a una serie de *recomendaciones de seguridad iniciales* que se pueden poner en práctica de inmediato, por lo general implican bajos costos, como respaldo a estos controles se implanta las correspondientes políticas de seguridad.

Tabla 3. Relación recurso/amenaza/vulnerabilidades

Recurso	Amenaza	Vulnerabilidades
Recurso 1	Amenaza 1	Vulnerabilidad 1 Vulnerabilidad 2 ...
	Amenaza 2	Vulnerabilidad 1 Vulnerabilidad 2 ...
Recurso 2	Amenaza 1	Vulnerabilidad 1 Vulnerabilidad 2 ...

3.1.3 Valoración del impacto y frecuencia de ocurrencia de las amenazas

a)Método cuantitativo: en este punto se hace una revisión de la información que previamente se ha recolectado, la frecuencia esta basada en las diferentes bitácoras, *logs* y reportes de incidentes. El impacto se determina en forma cuantitativa tomando diversos: criterios, pero en últimas todos representan valores económicos: valor del # de operaciones que deja el sistema de procesar por la ocurrencia de un evento. Lo ideal es poder expresar el impacto en términos económicos.

El impacto se determina de la siguiente fórmula: **[KRAU-99]**

$$I = valor\_recurso * factor\_de\_\text{exp}osición$$

Los impactos afectan la confidencialidad, integridad y disponibilidad de los recursos del sistema. El impacto de una amenaza a la integridad de los datos es diferente a sí ocurre modificación o destrucción de los datos. Igual ocurre con el impacto de una amenaza a la disponibilidad, depende del tiempo que el recurso de red permanezca no disponible y la frecuencia con que el sistema requiere los datos. Al final de esta subetapa se genera la tabla 4.

La frecuencia se da en forma anual, por ejemplo, si una amenaza ocurre una vez en 10 años, tiene una frecuencia de 1/10 ó 0.1; una amenaza ocurriendo 50 veces en un año tiene una frecuencia de 50.

Tabla 4. Recurso/Amenaza/Impactos

	Integridad Datos		Confiden-	Disponibilidad		
	Modificac.	Destrucción	cialidad	2hrs	24hrs	72hr
Recurso						
Amen. 1	i f	i f	i f	i f	i f	i f
Amen. 2	i f	i f	i f	i f	i f	i f
.....						

b)Métodos cualitativos: estos métodos valoran de una forma muy subjetiva el riesgo, a los elementos para valorar los riesgos generalmente se le asignan los valores de alto, medio y bajo.

El grupo evaluador tenga o no el impacto expresado en términos económicos puede escoger un nivel de impacto cualitativamente como bajo, medio o alto, teniendo en cuenta rangos de pérdidas económicas.

Algunas métodos utilizan como elemento para valorar los riesgos la posibilidad de ocurrencia de presentarse una amenaza.

3.1.4 Cálculo del riesgo

a)Tener el impacto y frecuencia (cuantitativo). Como en toda disciplina la pérdida es igual al producto de los valores de impacto y frecuencia de ocurrencia (i x f). Para f, el periodo anual es el común tomado como referencia en las metodologías y herramientas para análisis de riesgos. *"Aquí el riesgo indica las pérdidas anuales que genera la amenaza"*. Se genera la relación recurso/amenaza/impacto anual como indica tabla 6.

b)Métodos cualitativos. No se tiene en cuenta la frecuencia para valorar los riesgos. La tabla 5 muestra un claro ejemplo donde se emplea una matriz impacto/posibilidad de ocurrencia de una amenaza para determinar el nivel de riesgo que se tiene. *"Aquí el riesgo indica las pérdidas ante la posibilidad de presentarse la amenaza"*

Tabla 5. Nivel del riesgo

	Posibilidad de ocurrencia		
Impacto	**Alta**	**Media**	**Baja**
Alta	A	A	M
Media	A	M	M
Baja	B	B	B

Las áreas señaladas como A indican que son riesgos que requieren pronta atención, las áreas marcadas como B no es prioritario la toma de medidas

3.1.5 Tratamiento del riesgo

Luego del análisis de riesgos se procede a determinar el tipo de acción a tomar para cada riesgo. Se estudian las amenazas que presentan los recursos del sistema y se determina si es posible la implantación de mecanismos que reduzcan o eliminen el riesgo, en caso contrario las acciones a tomar serían la aceptación o transferencia del riesgo. El costo de proteger las aplicaciones de una amenaza debe ser menor que el costo de la recuperación. Para el tratamiento de

un riesgo se puede seguir las estrategias planteadas en **[HIGU-94]:** aceptar, transferir, eliminar, reducir.

A los anteriores se agrega la estrategia "evaluar", en la cual los controles quedan en un estado de evaluación por desconocerse la forma de llevarlo a cabo, requiere un tratamiento de más investigación y/o consenso con el staff del sistema. Por lo general en este tipo de casos la fecha queda por definir.

Tabla 6. Recurso/Amenaza/Impacto Anual

	Integridad Datos		Confiden cialidad	Disponibilidad			Ries.
	Modificac.	Destrucción		2hrs		24hrs	
Recurso							
Amen. 1	($)	($)	($)	($)	($)	($)	($)
Amen. 2	($)	($)	($)	($)	($)	($)	($)
.....							

3.1.6 Mitigación del riesgo

El proceso de mitigación de riesgos se sigue en caso de que la acción sobre el riesgo sea reducirlo o eliminarlo, incluye como primera medida la identificación de metas, cuyo propósito es describir el estado deseado resultante después de la mitigación del riesgo.

Posteriormente se identifican las estrategias a seguir para mitigar los riesgos. Su propósito es obtener alternativas de solución para cada riesgo. **[SANT-99]**

El diseño de controles es un proceso que requiere de mucho cuidado, se debe tener presente toda

Tabla 7. Relación amenaza/estrategias/costo anual

RECURSO: XXX		
AMENAZA	***ESTRATEGIAS***	***COSTO***
Amenaza n	*Estrategia 1* *Estrategia ...* *Estrategia n*	

la información de seguridad obtenida anteriormente. Se plantean cuestiones como: ¿de qué forma puedo reducir vulnerabilidades y por ende reducir el nivel de vulnerabilidad?, ¿qué mecanismos aunque no reducen el nivel de vulnerabilidad reducen el impacto?, puede un mecanismo determinado eliminar completamente la amenaza, etc.

Las estrategias aquí asignadas deben ser valoradas en términos económicos para realizar un análisis **costo/beneficio,** no se pueden plantear soluciones que excedan el valor del impacto para determinado riesgo.

4. OTROS METODOS DE EVALUACION DE SEGURIDAD

4.1 AUDITORIA

La auditoria examina si el sistema esta cumpliendo con los requerimientos de seguridad incluyendo políticas de la organización y del sistema. Dentro de las técnicas a emplear incluye investigación, observación y pruebas. Una auditoria puede variar ampliamente en alcance, examinar un sistema entero para el proceso de reacreditación o puede investigar un solo evento malicioso.

La auditoria puede ser interna o externa, la diferencia puede radicar en la objetividad con que se realice. La auditoria interna puede tener conflictos de intereses, o al contrario, estar motivado por el deseo de mejorar la seguridad del sistema, además de ser conocedores del sistema pueden encontrar problemas ocultos.

La auditoria toma documentación existente en cuanto a: políticas aplicables, análisis de riesgos, descripción de procesos, lista de controles. La ausencia de algún documento amerita la recomendación de la realización del mismo.

Los procesos de auditoria con el objeto de asegurar el funcionamiento operacional de la seguridad en un sistema es planificada y basada en la revisión de *logs*, por lo que a continuación se presenta la importancia del establecimiento de *logs* y como se aplica este control.

4.1.1 Establecimiento de *logs*. las pistas de auditoria o *logs* mantienen un registro de las actividades que los administradores y usuarios realizan sobre un sistema. Junto con herramientas y procedimientos adecuados, los *logs* pueden ayudar a detectar violaciones de seguridad, problemas de desempeño, etc. Los *logs* son usados como soporte para las operaciones requeridas del sistema y/o medio para asegurar políticas.

Como soporte para operaciones, los *logs* son usados para ayudar a los administradores del sistema que no han sufrido daño por *hackers*, intrusos o problemas técnicos. Los *logs* deberían registrar como mínimo los siguientes eventos:

- Cualquier intento de logearse (exitoso y no exitoso)
- Identidad
- Fecha
- Tiempo de cada intento de entrada
- Fecha y tiempo de salida
- Dispositivos usados
- Las funciones ejecutadas.

Una auditoria podría identificar intentos de *login* fallidos, especialmente si no se limita el número de intentos en el sistema. Algunos sistemas no tienen la función de registrar intentos de acceso fallidos, de esta forma sólo se puede monitorear los intentos de acceso exitosos.

4.1.2 Aplicación del control: dos procesos están involucrados en la aplicación de *logs* : definición e implantación y revisión.

a)Definición e implantación: al implementar *logs* se deben considerar información confidencial y por lo tanto requieren protección contra borrado o modificación no autorizada. Fuertes controles de acceso y encripción pueden ser mecanismos efectivos para preservar la confidencialidad e integridad. El

acceso en línea a *logs* debería estar estrictamente controlado, sólo visible al personal de administración que lo requiera para propósitos de revisión.

b)Revisión: los logs requieren ser revisados ya sea ante la ocurrencia de un incidente de seguridad, automáticamente en tiempo real (monitoreo) o por una evaluación de seguridad planeada. Los administradores del sistema determinarán la longitud de los *logs* que será mantenido. Para el sistema el establecimiento de *logs* ayudará en los aspectos de control de acceso, reconstrucción de eventos y detección de intrusos.

-Control de acceso: los *logs* trabajan en conjunto con los controles de acceso lógico, las cuales restringen el uso de los recursos del sistema. El acceso se concede teniendo en cuenta lo que el usuario del sistema necesite para realizar sus labores. Los logs sirven para analizar las acciones que los usuarios autorizados realizan, siempre que las cuentas y *passwords* de acceso no sean genéricos.

-Reconstrucción de eventos: la operación del sistema no se escapa de la ocurrencia de problemas, estos pueden ser resueltos fácilmente con la revisión de *logs* para hacer seguimiento a las últimas operaciones realizadas y detectar como, cuando y porque se originó el problema. El análisis de los *logs* ayuda a distinguir si los errores fueron inducidos por los operadores o por errores del software. Adicionalmente, sí un problema técnico ocurre (por ejemplo daño de archivos) los *logs* pueden ayudar en el proceso de recuperación.

-Detección de intrusos: los *logs* deben diseñarse e implementarse con la información apropiada que asista en la detección de intrusos. Las intrusiones pueden detectarse en tiempo real o después de ocurrido el evento. Los equipos y sistemas críticos para el sistema podrían tener implementado *logs* como herramientas en línea para monitorear constantemente su estado, teniendo en cuenta no afecte el desempeño del sistema.

4.2 CHECKLIST

La lista de chequeo es considerada como una herramienta de auditoria, es uno de los métodos de evaluación más viejos ampliamente usados, en seguridad informática consiste en revisar si existen controles administrativos, operativos y técnicos, este proceso no evalúa la efectividad de los controles implantados. Además se identifica que se cumplan los principios de seguridad generalmente aceptados (GSSPs).

Controles administrativos: estos controles hacen referencia a la recolección de documentos como: políticas y normatividad general referente a la seguridad del sistema. **[NIST1]**

Controles operativos: estos controles hacen referencia a los procedimientos que sirven para asegurar los requerimientos de seguridad. Ejemplo: planes de contingencia, manejo de incidentes, realización de backups etc.

Controles técnicos: estos controles hacen referencia a cualquier dispositivo de hardware o software que aseguran el cumplimiento de los

requerimientos de seguridad. Ejemplo: control de acceso y autorización, *firewalls*, mecanismos de auditoria de eventos, etc.

A continuación se amplia cada uno de los controles enfocados a un sistema de redes:

Controles Administrativos

- ★ Existe una política especifica del sistema para el manejo de seguridad
- ★ Existen políticas para el manejo de redes, sistemas operativos, aplicaciones, etc.
- ★ Existen políticas para el manejo de Internet
  - Tipo de información que puede ser transmitida
  - Tipos de sistemas que pueden ser conectados a la red
  - Uso de *firewalls* y *gateways* seguros
  - Requerimientos para autenticación de usuarios
- ★ Existen políticas para el manejo de otras redes externas
- ★ Existe un ente encargado de dar solución a incidentes de seguridad
- ★ Las funciones de seguridad están integradas en las funciones del personal

Donde existan políticas los siguientes tópicos son evaluados:

- ★ Define el objetivo?
- ★ Esta respaldada por los directivos?
- ★ Define procedimientos, son claros y entendibles?
- ★ Indica la información, software y hardware a emplear?
- ★ Designa personal responsable?
- ★ Dicta las penalidades y acciones disciplinarias?
- ★ Los procedimientos son actualizados periódicamente?
- ★ Conoce los usuarios y personal adecuado las políticas?

Controles Operacionales

- ★ Análisis de riesgos
- ★ Separación de deberes
- ★ Identificación del personal clave
- ★ Conocimiento y entrenamiento de personal
- ★ Efectiva administración de usuarios
- ★ Registro de intrusos
- ★ Planes de contingencia
- ★ Controles de acceso físico
- ★ Seguridad física contra incendios

Controles Técnicos

- ★ Identificación y autenticación
- ★ Manejo de llaves
- ★ Control de acceso lógico
- ★ Protección a puertos
- ★ *Firewalls*, *gateways* seguros
- ★ Autenticación basada en *hots*
- ★ Auditoria
- ★ Detección de intrusos
- ★ Reconstrucción de eventos
- ★ *Logs*, revisión
- ★ Criptografía
- ★ Firmas electrónicas
- ★ Certificados

Dependiendo del sistema en análisis se establece los seis o más relevantes controles que se identificaran con letras mayúsculas. Los controles pueden tomar uno de cinco posibles estados: implantado (I), en proceso de ser implantado (P), control no existente (N), se desconoce su estado/por verificar (V) ó no aplica (X). Por ejemplo si el recurso1 es un servidor y el control A es “Backups de configuración y datos de equipos” el siguiente cuadro indica que si se encuentra en funcionamiento dicho control.

Tabla 8. Estado de los controles técnicos

Controles Técnicos	Estado de los controles					
	A	**B**	**C**	**D**	**E**	**F**
Sistema						
Recurso1	I	N	P	N	N	N
Recurso2	I	N	P	N	N	N
...						
...						
Recurson	I	N	P	N	N	N

5. CONCLUSIONES

En Colombia las organizaciones y/o empresas no cuentan con registros acerca de los incidentes de seguridad, lo que dificulta la labor de determinar el impacto de los riesgos en términos económicos, necesitando considerarse en la mayoría de los casos una serie de complicadas matrices para determinar el impacto de los riesgos en términos cualitativos de alto, medio o bajo, siendo esto además un proceso bastante polémico y desgastante al interior de las Organizaciones.

Como recomendación de seguridad fundamental a las empresas es importante empezar a llevar registros sobre incidentes de seguridad con el fin de dar mayor confiabilidad y mejorar los resultados en el ciclo de vida del análisis de riesgos.

Es indispensable retroalimentar el procceso de análisis de riesgos que obedecen a los siguientes: realización de cambios en el sistema, incidentes de seguridad y revisiones periódicas**. [ORTI-88]**

Son de vital importancia para el analista de seguridad informática la puesta en práctica de los métodos de checklist y auditoría para determinar controles ausentes en el sistema, ya que estas herramientas se basan en estándares mínimos de seguridad que debe cumplir todo sistema, la ausencia de alguno de ellos implica la recomendación inmediata del cumplimiento de esta.

6. REFERENCIAS

[ACOS-98] Beatríz Acosta. *Metodología de Implantación de Seguridad en Redes*, Tesis de Postgrado en Ingeniería de Sistemas y Computación, Universidad de los Andes, 1998.

[FIPS-79] Federal Information Processing Standards Publications FIPS PUB65 - Guideline for Automatic Data Processing Risk Analysis, 1979.

[HIGU-94] Higuera Ronald, et al., *"An Introduction to team risk management"*, Carnegie Mellon University, Pensilvania, 1.994.

[KRAU-99] Micki Krause and Harold F. Tipton. *"Handbook of Information Security Management*", 1999

[NIST1] NIST Computer Security Handbook.

[ORTI-99] John Carlos Ortíz, *"Metodología para evaluación de seguridad en sistemas distribuidos*", Tesis de Postgrado en Ingeniería de Sistemas y Computación, Universidad de los Andes, 1999.

[SANT-99] Santos Luz Marina, "*Metodologia para la implantación de seguridad en aplicaciones distribuidas".* Tesis de Postgrado en Ingeniería de Sistemas y Computación, Universidad de los Andes.

7. AUTORA

Luz Marina Santos Jaimes
Ingeniera de Sistemas
Magíster en Ingeniería y Sistemas y Computación, Univ. de los Andes
Ocupación actual: Docente de tiempo completo Universidad de Pamplona
Area de interés: seguridad computacional, internet, sistemas distribuidos y trabajo cooperativo.
Correo:
lsantos@unipamplona.edu.co
teléfono: 5685303 Ext. 141
5681672

8. GLOSARIO

Una ***amenaza*** es cualquier evento que puede causar daño sobre los recursos del sistema.

Las ***vulnerabilidades*** son puntos débiles de seguridad que presenta el sistema que podrían permitir la ocurrencia de una amenaza.

El ***Factor de exposición*** representa una medida de la magnitud de pérdidas o impacto sobre el valor de un recurso, es expresado como un porcentaje que va desde 0% a 100%.

Los **recursos** de un sistema pueden ser de naturaleza tangible o intangible, su **valor** depende de su naturaleza. Los recursos tangibles incluyen hardware, documentación, y presupuesto que soportan el almacenamiento, procesamiento y entrega de la información, su valor típicamente se da en el costo de reemplazarlos. El valor de los recursos intangibles como por ejemplo la información, puede darse en el costo y tiempo de recuperación de la misma, o en el valor de la confidencialidad, integridad y disponibilidad de la información (ISSA-published GIV reference).

Impacto (i) es el daño potencial sobre un sistema cuando una amenaza se presenta. Este daño puede ser expresado en términos cuantitativos o cualitativos.

La ***frecuencia de ocurrencia (f)*** determina las veces que una amenaza puede ocurrir en un periodo de tiempo. La frecuencia se da en número de ocurrencias por año.

Posibilidad de ocurrencia: es una medida cualitativa que indica la opción que tiene la amenaza de materializarse o no.