METODOLOGIA DE ANALISIS DE RIESGO

Autor: Rodrigo Ferrer CISSP
SISTESEG
Bogotá
Colombia

A continuación haremos una descripción detallada de los pasos con que cuenta nuestra metodología de análisis de riesgo, la cual consideramos el punto central de la definición de una estrategia de seguridad, perfectamente alineada con la visión de la organización, dentro de su entorno de operación. Esta metodología es el resultado de la combinación de diferentes propuestas existentes en la industria, y utiliza métodos tanto cualitativos, como cuantitativos, los primeros permiten agilidad en el proceso y facilidad en la asignación de valores de impacto o riesgo, y los segundos nos permiten la precisión y exactitud, necesarias a la hora de tomar decisiones de tipo financiero, por ejemplo, en el caso de la selección de los controles adecuados, para mitigar un posible evento negativo a la operación y continuidad del negocio.

1.1 Entrevistas

Mediante este tipo de aproximación a la organización, se busca entender los diferentes aspectos que la conforman, tanto en el aspecto tecnológico, como en los procesos críticos, los cuales a su vez, son soportados por las aplicaciones y la infraestructura tecnológica.

SISTESEG identificará los siguientes elementos en el marco de la norma de seguridad ISO17799/ISO 27001:

- *Descripción de la Organización y sus Objetivo. Entendimiento de la organización, sus áreas funcionales y su ubicación geográfica.*
- *El levantamiento del detalle topológico de la infraestructura de tecnología existente, en el cual se especificará y detallará la plataforma de hardware, software, comunicaciones y procesos utilizados por XXX.*
- *Listas de verificación de la Infraestructura Tecnológica: El objetivo de las listas de chequeo es identificar las vulnerabilidades de las plataformas tecnológicas.*

1.2 Evaluación de Riesgo.

La evaluación de riesgos identifica las amenazas, vulnerabilidades y riesgos de la información, sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Los dos puntos importantes a considerar son:

- La probabilidad de una amenaza
- La magnitud del impacto sobre el sistema, la cual se mide por el nivel de degradación de uno o combinación de alguno de los siguientes elementos: confidencialidad, disponibilidad, integridad.

1.3 Determinación de la probabilidad.

Con el fin de derivar una probabilidad o una estimación de la ocurrencia de un evento, los siguientes factores deben ser tomados en cuenta:

- Fuente de la amenaza y su capacidad.
- Naturaleza de la vulnerabilidad.

La probabilidad que una vulnerabilidad potencial pueda ser explotada por una fuente de amenaza la podemos clasificar en alta, media-alta, media, media-baja y baja, como se describe a continuación.

Nivel	Definición
Alta = 5	*La amenaza esta altamente motivada y es suficientemente capaz de llevarse a cabo.*
Media-Alta =4	*La amenaza está fundamentada y es posible.*
Media = 3	*La amenaza es posible.*
Media-Baja = 2	*La amenaza no posee la suficiente capacidad.*
Baja = 1	*La amenaza no posee la suficiente motivación y capacidad.*

.

***Tabla 1**. Probabilidad de ocurrencia de un evento determinado.*

1.4 Numero de ocurrencias del evento en un periodo de un año.

Con el fin de poder determinar la probabilidad de ocurrencia de ciertos eventos, como el caso de una pérdida de potencia, falla en las comunicaciones, utilizamos información obtenida de ciertas publicaciones tecnológicas como Information Week e Infosecurity News, www.cert.org, www.sans.org junto con experiencias de casos Colombianos.

De esta manera se define una escala en la cual, a una probabilidad alta, le asignamos el valor P=5, para una probabilidad media le asignamos el valor P=3 y por último para una probabilidad baja le asignamos el valor P=1, esta asignación se define en proporción directa al numero de veces que el evento puede ocurrir en un periodo de un año. Para el caso P=5 se considera que ocurre al menos dos veces al año.

1.5 Identificación de Vulnerabilidades.

Para la identificación de vulnerabilidades sobre la plataforma de tecnología, se utilizan herramientas como listas de verificación y herramientas de software que determinan vulnerabilidades a nivel del sistema operativo y firewall:

- *Seguridad Física.*
  - *Monitoreo ambiental*
  - *Control de acceso*
  - *Desastres naturales*
  - *Control de incendios*
  - *Inundaciones*
- *Seguridad en las conexiones a Internet.*
  - *Políticas en el Firewall*
  - *VPN*
  - *Detección de intrusos*
- *Seguridad en la infraestructura de comunicaciones.*
  - *Routers*
  - *Switches*
  - *Firewall*
  - *Hubs*
  - *RAS*
- *Seguridad en Sistema Operacionales(Unix, Windows)*
- *Correo Electrónico*
- *Seguridad en las aplicaciones Críiticas*
  - *Se define las aplicaciones que son críticas para la organización y por cada una de ellas se obtendrá una matriz de riesgo. Es importante considerar que las aplicaciones están soportadas por: Sistemas operativos, hardware servidor, redes LAN y WAN, y el Centro de cómputo.*

También con el fin de realizar una correspondencia con los datos obtenidos por medio de las listas de verificación, contamos con el uso de una herramienta especializada fabrica por GFI Languard, la cual identifica vulnerabilidades en los sistemas operativos, ayudándonos de esta forma en el proceso de identificación de vulnerabilidades. A continuación mostramos algunas de las características de esta herramienta:

- Búsqueda de vulnerabilidades en su red (Windows y Linux)

- Directorios compartidos, puertos abiertos, cuentas no usadas.
- Revisión de actualizaciones aplicadas en los sistemas operativos.
- Detección de dispositivos USB

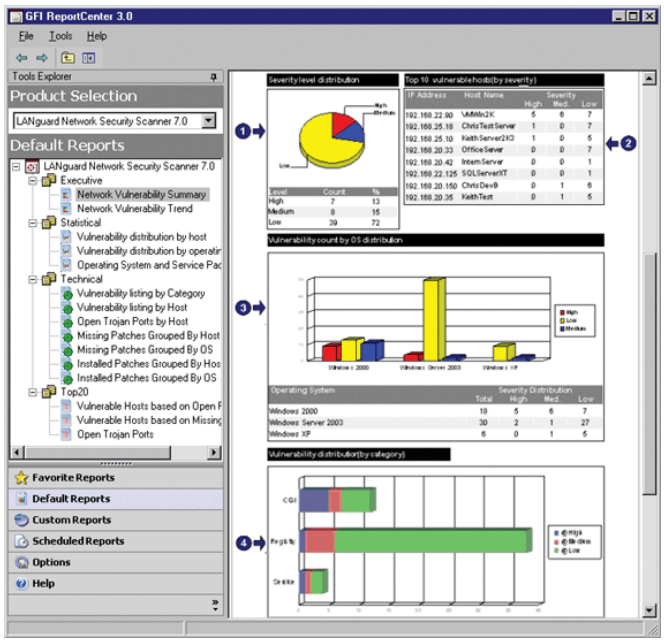

Figura 1. Resultados herramienta de análisis de vulnerabilidades.

1.6 Análisis del impacto y el factor de riesgo

El próximo paso en la metodología que estamos describiendo, es poder determinar el impacto adverso para la organización, como resultado de la explotación por parte de una amenaza de una determinada vulnerabilidad, para ello se deben considerar los siguientes aspectos:

- Consecuencias de tipo financiero, es decir pérdidas causadas sobre un activo físico o lógico determinado y las consecuencias que este activo no funcione, y afecte la operación de la compañía.
- La importancia critica de los datos y el sistema (importancia a la organización).
- Sensibilidad de los datos y el sistema.

1.7 Identificación de Controles.

En esta fase se evaluarán las conclusiones de la valoración respecto a ISO17799 y la matriz de riesgo con el fin de identificar los controles que mitiguen los riesgos encontrados.

1.8 Plan de Implementación Tecnológica.

El plan de Implementación tecnológica, se presenta como una herramienta para el control por parte de XXX de las actividades que se deben llevar a cabo para mitigar los riesgos identificados, en la evaluación de riesgo del proyecto en curso y de acuerdo al alcance definido.

De esta forma la seguridad hoy en día se ha convertido en la carta de navegación para el tema de la inversión en tecnología, debemos en toda inversión tecnológica considerar aspectos relacionados con la gestión de la seguridad, con el fin de que esta inversión este alineada plenamente con la estrategia del negocio y garantice de manera efectiva y eficiente su continuidad.

2 **DEFINICION DE POLITICAS**

Se entiende por política, las reglas generales de comportamiento definidas para la interacción entre los usuarios y los activos informáticos. Las políticas son independientes de los ambientes propios de la entidad y representan la base de un modelo de seguridad.

Las Políticas de seguridad dependen de la cultura de la organización. Por esta razón las políticas y procedimientos deben estar hechos a la medida, según los requerimientos específicos de cada organización. Para la definición de las políticas y procedimientos se realiza un proceso de validación en conjunto con la organización con el fin de generar políticas y procedimientos que se ajusten a esta. Como punto de partida para la definición de las políticas se tendrá como referencia el análisis de riesgo realizado, los controles del ISO 1 7799/ISO 27001.

Las políticas cubrirán los siguientes temas:

Seguridad en la Organización:

- *Roles y Responsabilidades de Seguridad de la Información*
- *Políticas para la conexión con terceros.*

Clasificación de la Información:

- *Importancia de la información según la organización.*

Seguridad en el recurso Humano:

- *Responsabilidades de seguridad de la información para los diferentes cargos.*

- *Entrenamiento a empleados en seguridad de la información como parte de su proceso de inducción y mejoramiento continuo.*

Seguridad Física:

- *Seguridad ambiental*
- *Control de Acceso físico.*

Administración de las operaciones de cómputo y comunicaciones.

- *Políticas sobre el uso del correo electrónico*
- *Políticas sobre el uso de Internet.*
- *Políticas sobre el uso de recursos.*

Control de Acceso.
Desarrollo y mantenimiento de Sistemas.
Continuidad de Negocio.
Conformidad con leyes civiles, legales y contractuales.

Las políticas constan de:

- *Audiencia*
- *Introducción*
- *Definiciones*
- *Objetivo*
- *Enunciado de la Política*
- *Políticas y Procedimientos relacionados*
- *Roles y responsabilidades*
- *Violaciones a la política*

3 DEFINICION DE PROCEDIMIENTOS

Los procedimientos son la descripción detallada de la manera como se implanta una política. El procedimiento incluye todas las actividades requeridas, los roles y responsabilidades de las personas encargadas de llevarlos a cabo.

Los procedimientos a definir son los siguientes:

- Administración de cuentas de usuario.
- Manejo de Incidentes
- Manejo de Virus
- Administración de cuentas privilegiadas.
- Procedimiento de Control de Cambios.
- Procedimiento de Acceso al edificio.
- Procedimiento de acceso al centro de Cómputo.
- Procedimiento de respaldo

Los procedimientos constan:

- Introducción
- Objetivo
- Alcance
- Responsable de su administración
- Responsables de la implementación y ejecución.
- Responsable del control

4 DEFINICION DE ESTANDARES

Es la definición cuantitativa o cualitativa de un valor o parámetro determinado que puede estar incluido en una política o procedimiento.

Algunos de los principales estándares a definir son:

- Longitudes de contraseñas
- Histórico de contraseñas
- Eventos a registrar en logs
- Switches
- Routers
- Firewall
- VPNs
- Sistema Operativo Windows

AUTOR: EL ing Rodrigo Ferrer (rodrigo.ferrer@sisteseg.com) es egresado de la universidad de los Andes como ingeniero Eléctrico, en donde también ha realizado estudios de postgrado y especialización en telecomunicaciones y Gestión de sistemas de información. Se ha desempeñado laboralmente en empresas de redes y seguridad tales como: 3com, Extreme Networks, Sonicwall, Sisteseg, desempeñándose como Network Consultant para la región andina y como académico en varias universidades del país. Recibió en el 2006 la certificación CISSP (Certified Information System Security Profesional) del International Information Systems Security Certification Consortium (www.isc2.org), la certificación internacional más reconocida a nivel mundial en el área de seguridad de la información, seguridad física y seguridad en redes. Tambien esta en proceso de obtener la certificación CISA de ISACA y es LEAD AUDITOR 27001.

Como complemento a su formación tecnológica, ha realizado también realizado estudios de educación continuada en la Universidad de Cambridge en el Reino Unido y actualmente está finalizando la Maestría en Filosofía, en la Universidad Javeriana orientado al tema "filosofía de la ciencia y la tecnología".