Tema 3. Análisis de riesgo

3.1 Introducción

Como se ha mencionado, en un entorno informático existen una serie de recursos que están constantemente expuestos a diferentes tipos de riesgos: aquellos comunes a cualquier entorno, y los excepcionales, originados por situaciones concretas que pueden afectar a parte de una organización o a toda ella.

Para tratar de minimizar los efectos de un problema de seguridad se realiza un análisis de riesgos, que es un proceso necesario para responder a tres preguntas básicas sobre nuestra seguridad:

- ¿Qué queremos proteger?
- ¿Contra qué lo queremos proteger?
- ¿Cómo lo queremos proteger?

En la práctica existen dos aproximaciones para responder a estas cuestiones, una cuantitativa y otra cualitativa. La primera es la menos usada, ya que en muchos casos implica cálculos complejos o datos difíciles de estimar. Se basa en dos parámetros: la probabilidad de que un suceso ocurra y una estimación de las pérdidas en caso de que así sea. Aunque es posible conocer el riesgo de cualquier evento y tomar decisiones en función de estos datos, en la práctica la inexactitud en la estimación o en el cálculo de parámetros hace difícil esta aproximación.

El segundo método es el cualitativo, de uso muy común en la actualidad. Es mucho más sencillo que el anterior, ya que ahora no entran en juego probabilidades exactas sino sólo una estimación de pérdidas potenciales. Para ello se interrelacionan cuatro elementos: las amenazas, las vulnerabilidades, el impacto asociado a una amenaza y las contramedidas para minimizar las vulnerabilidades o el impacto. Con estos cuatro elementos podemos obtener un indicador cualitativo del nivel de riesgo en el que un activo determinado se encuentra, considerándolo como la probabilidad de que una amenaza se materialice sobre un activo y produzca un determinado impacto.

En este capítulo explicamos las fases necesarias para realizar con éxito un análisis de riesgos, desde su preparación y puesta en práctica hasta el correcto análisis de los resultados obtenidos.

3.2 Preparación del proyecto

En esta fase se recoge toda la información necesaria para la identificación de activos informáticos, así como sus vulnerabilidades y amenazas potenciales a los cuáles están sujetos. Se obtiene la probabilidad de ocurrencia de la explotación de una vulnerabilidad y el impacto que tendrá en el funcionamiento de la empresa o negocio si esto llegara a suceder.

Esta fase es fundamental para la construcción de una estrategia de seguridad perfectamente coherente con la operación y las necesidades de la organización.

Según la IEC 27001:2005 la evaluación del riesgo incluye las siguientes acciones:

- Identificación y valoración de los activos
- Identificación de las amenazas y vulnerabilidades importantes para los activos identificados.
- Evaluación del riesgo, de las amenazas y vulnerabilidades con cierta incidencia a ocurrir.
- Cálculo del riesgo.
- Evaluación de los riesgos frente a una escala de riesgo preestablecida. [104]

3.3 Identificación de activos

Un activo es un bien importante para el funcionamiento o manejo de la empresa y que la seguridad informática tiene como objetivo proteger. Los activos están conformados por los siguientes elementos:

- Información. Ya sea que esté guardada en un medio físico o electrónico, la información es el bien de mayor valor para una organización.
- Hardware. El equipo físico que conforma la estructura del sistema de comunicación.
- Software. Las aplicaciones y programas que son usadas en la empresa u organización.
- Usuarios. Los individuos que están en contacto con la información y que hacen uso del hardware y software. [105]

Para realizar la identificación de los activos es necesario contar con la presencia de personal calificado que tenga conocimiento del proceso informático de la organización.

3.4 Evaluación de activos

Una vez que los activos han sido identificados, se procede a evaluar su valor desde el punto de vista de la seguridad de la información y no sólo con base en

[104] "Análisis de riesgos. Seguridad Informática" en http://74.125.93.132/search?q=cache:izpLYC9qhlUJ:www.felaban.com/memorias_mayo_09/viernes_15_mayo/santiago_lioza_clain_v4.ppt+p%C3%A9rdida+esperada+seguridad+inform%C3%A1tica&cd=7&hl=es&ct=clnk&gl=mx, 22/10/2009.
[105] *Ídem.*

su valor intrínseco. El valor del activo se debe calcular según su misión crítica, costo, sensibilidad o una combinación de ambos valores. [106]

El valor de los activos es un factor importante en la decisión para modificar la operación o incrementar la protección a dichos elementos.

3.5 Impacto

El impacto puede definirse como las pérdidas que resultan de la explotación de una vulnerabilidad. Las pérdidas, por lo general, son expresadas en una o más áreas de impacto como destrucción, denegación de servicio, revelación o modificación. Aquí también toma parte el concepto de pérdida esperada, la cual es el impacto anticipado a los activos, resultado de la manifestación de una amenaza. [107]

Para poder considerar esto, es necesario tomar en cuenta los siguientes aspectos:

- Consecuencias de tipo financiero, es decir, pérdidas causadas sobre un activo físico o lógico determinado y las consecuencias de que éste no funcione y afecte la operación de la compañía.

- La importancia crítica a la organización de los datos y el sistema.

- Sensibilidad de los datos y sistema. [108]

3.6 Pasos del análisis de riesgo

El análisis y manejo del riesgo se resume mediante la interacción de los siguientes pasos:

- Determinación del alcance. Etapa en la que se define el motivo por el cual se está realizando el análisis, además, se definen los procesos que serán objeto de evaluación.

- Definición del equipo de trabajo. Como su nombre lo indica, se establecerá el personal involucrado en la elaboración del análisis.

- Fase de entrevistas. Etapa primordial del análisis de riesgo, puesto que permitirá conocer el bien visto desde el punto de vista del usuario de la información y de los dueños.

- Identificación de activos. En esta etapa se enumeran los activos con los que cuenta la empresa, se les asigna un valor considerando lo aprendido en la fase de entrevista con los dueños y usuarios. Este valor asignado es significativo puesto que será un indicador de la protección que necesitará

[106] Ídem.
[107] Ídem.
[108] Ídem.

dicho activo, y del impacto de su pérdida en caso de que un ataque ocurra.

- Identificación de amenazas. Consecuente con cada organización, lugar geográfico en que la empresa se encuentra, y la información anteriormente recabada, se deben definir las amenazas, ya sean externas o internas que pesan sobre los activos, se elabora además una estimación sobre la ocurrencia con que estas pueden presentarse.

- Priorización de amenazas. A partir de la estimación de ocurrencia anteriormente elaborada y siguiendo fórmulas sencillas descritas por organismos internacionales y aceptadas como normas, se deberá prestar especial atención a aquellas cuya ocurrencia sea inminente y sus consecuencias serias.

- Identificación de controles.

  i. Controles requeridos. Como su nombre lo indica, son todas aquellas normas que pueden fundamentarse en las reglas escritas, se espera que su cumplimiento reduzca la posibilidad de un ataque.

  ii. Controles discrecionales. Estos se aplican cuando el nivel de riesgo no se minimiza a un nivel aceptable siguiendo los controles requeridos, son aplicados por los administradores del sistema.

- Riesgo residual. Si tenemos que cuenta que todo sistema está sujeto a sobrellevar algún riesgo, el llamado riesgo residual invariablemente existirá, no importando qué tan estrictos sean nuestros controles o que tan capaces nuestros administradores. En esta fase se concluirá si el riesgo residual es aceptable se precisa de la implementación de controles adicionales.

- Informe del análisis. Cuando se completa el análisis, debe prepararse un reporte escrito que incluya, como mínimo, los siguientes aspectos:

  i. El nivel de vulnerabilidad en que se encuentra un activo.

  ii. Amenazas, estableciendo prioridad de acción y fijando su riesgo de ocurrencia.

  iii. Ambiente bajo el cual se realizó el análisis.

  iv. Estado de la conexión del sistema.

  v. Sensibilidad de los datos; se hará una lista de ellos clasificándolos según su importancia en la organización.

  vi. El invariable riesgo residual al que está expuesta la empresa.

vii. Cálculos de la expectativa de pérdida. [109]

3.7 Análisis costo-beneficio

En esta etapa dentro del análisis de riesgo se deberá elaborar además, un análisis costo-beneficio; esto se trata de una técnica que evalúa, en nuestro caso, el peso total del gasto que se desembolsará para llevar a cabo la salvaguarda de los activos, el valor de la totalidad que a los mismos que se les da, y el costo en tiempo y recursos para que un atacante logre pasar las medidas de defensa.

Dentro del análisis de riesgo deben considerarse tres costos principales:

- Costo del sistema (Ca). Valor de los activos a proteger.
- Costo de los medios (Cm). El costo que un atacante requiere para destruir las medidas de seguridad implementadas.
- Costo de las medidas de seguridad (Cs). El costo para proteger el sistema o activo.

Para que la implementación de las medidas de seguridad sea viable, debe cumplirse la siguiente relación:

$$Ca > Cm > Cs$$

Esto significa que el costo que significa atacar al sistema debe ser mayor que el valor o información al que se tendrá acceso si se tiene éxito. Además, la información no debe ser más costosa que la información protegida, de lo contrario, no convendría protegerla y sería mejor obtener la información de nuevo en caso de pérdida.[110]

[109] María Jaquelina López Barrientos, Cintia Quezada Reyes, *Fundamentos de seguridad informática*, México, Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2006, pp. 163-168.
[110] *Idem*.