Definición Métricas de seguridad

Definition of security metrics

Ignacio Briones Martínez

Resumen

Este proyecto surge por la necesidad de conocer cómo de segura es una entidad refiriéndome a entidad a una empresa, pyme, conjunto de elementos que forman el departamento de TI.
Con este proyecto se intenta medir la seguridad, teniendo en cuenta todos los factores que influyen en la seguridad de una entidad. Desde aspectos meramente de software, pasando por durabilidad de los equipos físicos, establecimiento de políticas, cumplimiento de normativas, uso de controles, seguridad física, pérdidas económicas... y todo influenciado por el factor humano.
De esta manera obtenemos una medida de la seguridad, de todos los componentes de una empresa, de su funcionamiento y de sus interrelaciones en conjunto.

Palabras clave: métrica, seguridad, metodología, magerit, medida.

Summary

This project arises from the need to define the security level of an entity, referring to company, SME, group of elements that comprise the IT department, etc.
The aim of this project is to measure security, taking into account all the factors that influence the security of an entity, from mere software-related aspects, to the durability of physical equipment, establishment of policies, fulfilment of regulations, use of controls, physical security, financial losses, etc., all of this influenced by human factors.
This makes it possible to measure the security level of all the components of a company and of its operations and interrelationships as a whole.

Keywords: metrics, security, methodology, magerit, measurement.

Este proyecto surge por la necesidad de conocer cómo de segura es una entidad

1. El fallo como medida

Todos los elementos que van a ser objetos de medida, son diferentes pero han de tener un nexo común para relacionarlos y así conseguir una solidez en combinarlos. Ese nexo de unión es el fallo.

El fallo es común a todos los elementos del sistema, se puede medir la posibilidad de fallo de un elemento, se pueden realizar predicciones de fallo del sistema[1] , se puede ver si afecta a más componentes.

Con el fallo como elemento común a todos se definen las relaciones entre los elementos de forma jerárquica, representando las relaciones de composición y las relaciones vecinales.

Cada elemento puede tener asociado la existencia de controles los cuales mitigan su fallo. Estos controles influyen mucho en la medida del elemento porque para medir el elemento no sólo usamos su fallo, es el elemento primordial pero tiene atenuantes y agravantes. Para realizar la medición que va a determinar su nivel de seguridad uso la siguiente fórmula:

Fallo = Fiabilidad - posibilidad de fallo + (Fiabilidad x Mantenimiento) + (Fiabilidad x Exposición) + ((1-Fiabilidad) x Reparación)

Esta fórmula la mitigo con un corrector, evaluado según la eficacia de los controles existentes para el elemento medido:

Cada elemento puede tener asociado la existencia de controles los cuales mitigan su fallo

1 "*Técnicas de Predicción con aplicaciones en Ingeniería*" Manuel R. Arahal, Manuel Berenguer, Francisco Rodríguez. Editorial: Universidad de Sevilla

Control= (1+ Revisiones - (#controles usados/ (#controles iso+ #controles cobit + #controles adicionales)))
Uniendo los dos apartados nos da una aproximación del fallo:

Fallo Total = Control x Fallo

Siendo este valor su medida tomada de forma individual y aislada, garantizando así su independencia y posibilita la comparación con otros elementos.

2. Conceptos básicos

Mediremos el fallo que puede tener un condensador hasta niveles abstractos

La granularidad de los elementos se puede establecer en niveles muy finos. Mediremos el fallo que puede tener un condensador hasta niveles abstractos como la pérdida de imagen o las políticas establecidas.

Los diferentes elementos que van a entrar en la medida se van agrupar en estos ocho grupos:
- Datos eléctricos
- Datos Hardware
- Datos Servidores y PCS
- Datos Aplicaciones Comerciales
- Datos Aplicaciones Propias
- Datos Instalaciones
- Datos Políticas
- Datos Perfil Empleados

Para cada grupo se definen diferentes puntos para establecer su posibilidad de fallo. De esta forma, en cada grupo podemos evaluar su fallo de forma individual, generando una base de datos con los diferentes elementos y sus medidas, individuales y aisladas.

La importancia de obtener medidas individuales y aisladas de los elementos es poder compartir los elementos entre diferentes empresas y situaciones

La importancia de obtener medidas individuales y aisladas de los elementos es poder compartir los elementos entre diferentes empresas y situaciones. Al ser individuales podemos obtener medidas objetivas de cada elemento siendo un valor extrapolable a distintas empresas con distintas configuraciones.

Como los elementos pueden ser comunes, y sobretodo medidos de forma individual, llegamos a comparaciones de configuraciones. Las configuraciones representan a cada empresa o entidad evaluada y obtenemos comparativas entre diferentes entidades o empresas obteniendo la medida.

Para evaluar los integrantes de cada grupo, nos guiaremos por los controles expuestos en la ISO como los correspondientes de COBIT para obtener resultados estándar y reconocidos por entidades de certificación.

3. El Factor humano

El factor humano va a influenciar todo el sistema. Se puede ver en los siguientes casos:
- Las personas configuran y usan los elementos de toda la empresa
- Las personas son las encargadas de desarrollar el software y negocio de la empresa
- Las personas gestionan la empresa y su seguridad
- Las personas toman las decisiones sobre los sistemas
- Las personas son las encargadas de atacar, hacer vulnerables a los sistemas

Por ello las personas son un punto muy importante en todo el sistema y lo afectan en sus engranajes. Cada persona es distinta pero se pueden usar patrones y formas para evaluar tanto su destreza en el uso de alguno de los elementos pertenecientes al sistema.

Para medir a las personas se usan los juicios expertos. Esta evaluación usa tanto tests para conocer el grado de actuación como la valoración de un conjunto de personas encargadas de dicha valoración.

4. De la configuración de la empresa a la aplicación

Con todos los elementos de una empresa medidos de forma individual, conociendo su nivel de implantación, sus funciones y relaciones, se inicia el proceso de pasar la configuración de la empresa a la aplicación, para obtener su medida global.

Para medir a las personas se usan los juicios expertos

4.1. Vecinos

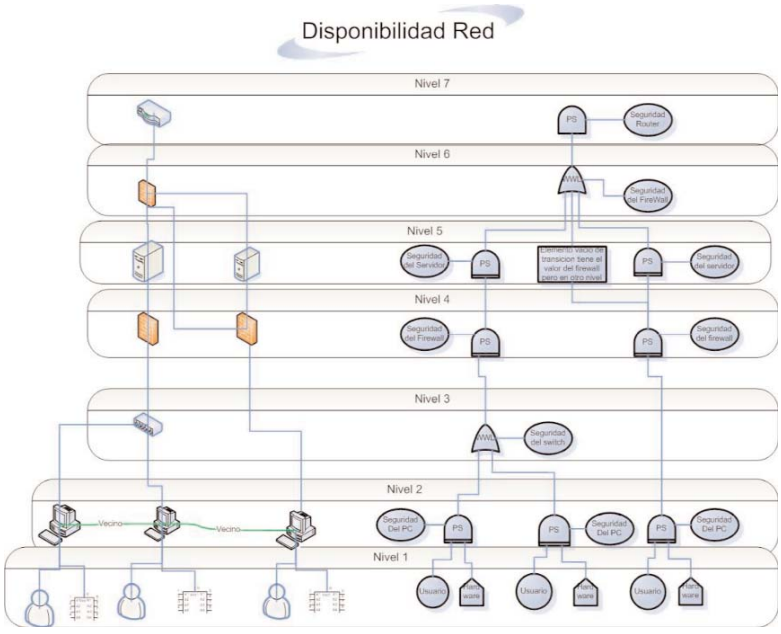
Para establecer la configuración global se van a establecer relaciones vecinales entre los elementos.
Una relación vecinal es: Una conexión entre diversos elementos que pueden afectar unos a otros. La existencia de esta relación es la necesidad de evaluar las repercusiones que tiene el fallo de un elemento entre sus elementos vecinos, tanto vecinos físicos como lógicos. Un ordenador que no está bien configurado y tiene un virus se lo puede comunicar a sus vecinos, estos vecinos pueden estar bien fortificados, pero al ser vecinos del infectado pueden ser infectados.
Esta repercusión se ve reflejada en el algoritmo que se explica más adelante.

4.2. Estructura

La forma de colocar los diferentes elementos de la empresa va a ser la generación de un árbol. Este árbol representará de forma jerárquica los elementos de la empresa y como están relacionados. Un ejemplo es la figura 1:

Para establecer la configuración global se va a establecer relaciones vecinales entre los elementos

FIGURA 1



Al pasar la empresa a una configuración de árbol nos posibilita la evaluación de todos los nodos propagando su seguridad a los padres y así poder evaluar todos los nodos y obtener una única medida en su nodo raíz. La medida de seguridad del nodo raíz es la medida final influenciada por todos los elementos del árbol y nos deja tener una gran profundidad.
Como toda empresa, cada nivel del árbol va ser un nivel de la empresa, y cada nivel dispone de un número de puntos para distribuir entre los elementos de dicho nivel.
Estos puntos son los denominados pesos de cada elemento, que reflejan la importancia de cada elemento en comparación con los de su mismo nivel.
Estos pesos se distribuyen según la configuración e importancia del elemento en dicho nivel y según su alineación con el negocio.

4.3. Tipos de Nodos

Todos los elementos se distribuyen en forma jerárquica formando un árbol

Todos los elementos se distribuyen en forma jerárquica formando un árbol. En este árbol se tiene dos tipos de nodos principales denominados *Weakest Link* (wl) y *Prioritized Siblings* (ps).
Los nodos WL tienen una interdependencia e influencia total entre sus nodos hijos mientras que en los nodos PS cada hijo es individual y no tiene la dependencia de los demás. Estos nodos "padre" van a relacionar de forma distinta la seguridad de sus hijos.

$$PS \Rightarrow \Sigma\,(\text{Seguridad} \times \text{Pesos})$$

$$WL \Rightarrow \sqrt{(\Sigma\,(\text{Seguridad} \times \text{Pesos})) \times \text{Seguridad del Más débil}}$$

4.4. Normativa ISO

La Normativa ISO evaluará la capacidad de la pyme para garantizar la confidencialidad de los datos que se poseen

Cómo reflejar todas las partes de una empresa es muy general. Iniciamos este proceso agrupando los diferentes procesos según los 4 pilares que marca las nueva ISO :

- Disponibilidad
- Confidencialidad
- Integridad
- Económicos

Partiendo de estos 4 grandes marcos configuramos los diferentes elementos de nuestra empresa en forma de árbol.
Podemos repetir el mismo árbol o crear diferentes según la implicación de los elementos en cada uno de los 4 pilares.

4.4.1. La Normativa ISO

Evaluará la capacidad de la pyme para garantizar la confidencialidad de los datos que se poseen, y con los datos que trata.
En este nodo se incluyen todos los elementos de la pyme que contengan datos o den acceso a los mismos. El reparto de pesos irá en función del grado de confidencialidad que se le exige a un elemento dentro del árbol.
Este nodo lo podemos dividir en elementos criptográficos, redes... O simplemente variando la asignación de pesos teniendo en cuenta el apartado que se está midiendo.
De esta forma el árbol ya lo tenemos creado y solo modificamos los pesos para adecuarlos a la importancia que le queramos dar a cada elemento en el ámbito de la confidencialidad.

4.4.2. Subnodo integridad

Evaluará la capacidad de la pyme para garantizar la integridad de los datos que se poseen, y con los datos que trata. En este nodo se incluyen todos los elementos de la pyme que contengan datos o den acceso a los mismos.

El reparto de pesos irá en función del grado de integridad que se le exige a un elemento dentro del árbol. Está íntimamente relacionado con los datos que alberga, llegando a medir la eficacia y posibilidad de fallo de escritura en el disco duro de un ordenador o cuál es la vida útil de los discos duros instalados o de los medios en los que se almacenan los datos.
En esta parte del árbol puede ser no necesario incluir todo el árbol. Como en los elementos anteriores, se pueden realizar las podas necesarias para sólo adaptarlas a los dispositivos que incurran en esta medida.

4.4.3. Subnodo disponibilidad

Evaluará la capacidad de la pyme para garantizar la disponibilidad de los datos que se poseen, y con los datos que trata. En este nodo se incluyen todos los elementos de la pyme que contengan datos o den acceso a los mismos.
El reparto de pesos irá en función del grado de disponibilidad que se le exige a un elemento dentro del árbol.
Sobre cada elemento se valora su posibilidad de ser repuesto de forma automática, o como las revisiones periódicas ralentizan su deterioro y así amplían el rango de un fallo, también se valora su exposición a recibir ataques de denegación de servicio procedentes del exterior.
Conforme a lo escrito anteriormente se distribuyen los pesos del árbol para adecuarlos a realizar la medida de la disponibilidad de la empresa.

Sobre cada elemento se valora su posibilidad de ser repuesto de forma automática

4.4.4. Subnodo financiero

En este nodo se evalúa la viabilidad de los recursos puestos en marcha, como los empleados, o cuánto costarían las recuperaciones de un fallo del sistema.
Para realizar este apartado, el reparto de los pesos sería en función del coste de la pérdida de los elementos sumado a los costes derivados de esta pérdida.
Por ejemplo la pérdida de un servidor por un fallo eléctrico nos supondrá un coste del recambio del servidor, pero también se ha de calcular la pérdida que origina en el negocio. Mientras el servidor este in operativo no podremos ofrecer un servicio a un determinado precio originando pérdidas.
Por ello la adecuación de los pesos se ha de hacer conforme a los dos valores

Coste del elemento en sí + Impacto de pérdidas en el Negocio

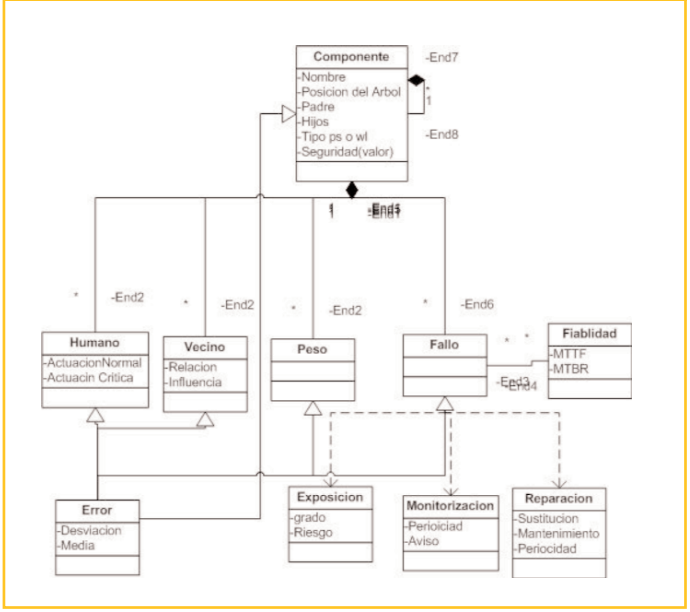
El componente representa cada elemento de la empresa

4.5. El Componente

Como todos los elementos son diferentes y los hemos de abstraer a una forma de trato común, se genera la figura del componente.
El componente representa cada elemento de la empresa y esta representado en la figura 2.

Cada elemento de la empresa se modeliza en este componente que va ser cada nodo del árbol.

FIGURA 2



4.5.1. Seguridad

El componente tiene un campo denominado seguridad. Este campo va a almacenar la seguridad propia del componente cuando se le asocia un elemento de la empresa y el valor tras aplicarle los cálculos de seguridad según si tiene hijos o no.
Para darle un valor numérico a este campo se pondera de la siguiente manera:

Seguridad = Peso x ((1-Fallo) + (1-Fallo) Humano% - Σ(Fallo x FalloVecino) - Tasa Tiempo) ± Error

Seguridad Total = (SeguridadHijos + Seguridad)/2

La seguridad total evalúa la seguridad propia del elemento condicionada a la de sus hijos. Esta seguridad total se va propagar a los niveles superiores, para dictaminar el nivel de seguridad final de la empresa y procesado por el árbol.

La seguridad total evalúa la seguridad propia del elemento condicionada a la de sus hijos

5. Funcionamiento

Como funciona el árbol para evaluar y procesar todos los datos:

1) Inventario de los elementos de la empresa
2) Obtención de la base de datos de los elementos que tiene la empresa
3) Dibujar cada árbol de los 4 pilares de la ISO
4) Definir pesos de cada elemento
5) Cálculo de la seguridad del componente influenciado por sus vecinos.
6) Se inicia un proceso que va ascendiendo por los diferentes niveles del árbol.
7) Se calcula la seguridad según el tipo de nodo padre que corresponda WL o PS
8) Obtención de la seguridad del nodo raíz. Del nodo raíz parten los 4 pilares de la ISO y es la representación abstracta y global de la empresa.

El camino crítico muestra la relación de nodos más débiles desde el nodo raíz hasta alguno de sus niveles inferiores

6. Finalización y camino crítico

Al finalizar el proceso de análisis del árbol, nos retorna dos resultados:

- La seguridad total de la empresa
- Camino Crítico

Nos da la medida de seguridad de nuestra empresa valorada sobre 100, según los valores dados a las 4 ramas iniciales del árbol.

El camino crítico muestra la relación de nodos más débiles desde el nodo raíz hasta alguno de sus niveles inferiores. Este camino muestra cuál es el camino más débil de la empresa y sobre el cuál sería necesaria una revisión o tener un mayor cuidado en la revisión y establecimiento de controles en sus componentes.

7. Agradecimientos

A Dolores de la Guía, Responsable de Seguridad del CTI CSIC, por impulsar el poder escribir este artículo.
A mi director de tesis, Eloy Anguiano, por dirigir esta tesis.
A mi codirector de tesis, Manuel Carpio, por ser el primer motor de esta idea.

Referencias

[1] "*Towards a Framework for security measurements*" Chenxi Wang, William Wulf
http://csrc.nist.gov/nissc/1997/proceedings/522.pdf

[2] Thesis Caesar "*A proposed method for evaluating security*" Mikael Peterson
www.diva-portal.org/diva/getDocument?urn_nbn_se_liu_diva-2470-1__fulltext.pdf

[3] Métodos cuantitativos para el análisis de riesgos
http://www.proteccioncivil.org/centrodoc/guiatec/Metodos_cuantitativos/cuant_22.htm

[4] Juicio Experto
http://www.mtas.es/Insht/ntp/ntp_401.htm

Ignacio Briones Martínez
Ingeniero Superior en Informática

Eloy Anguiano
Profesor Titular de la Escuela Politécnica de Madrid
Director de tesis

Manuel Carpio
Director Seguridad de la Información y Prevención del Fraude de Telefónica