



Métricas en los SGSI

ESTE ARTÍCULO PRETENDE SER UNA REFLEXIÓN QUE MANTENGA VIVOS CONCEPTOS BÁSICOS EN LA ELABORACIÓN DE MÉTRICAS Y QUE CONJUGUE LOS INTERESES DE TODAS LAS PARTES IMPLICADAS



**Rafael
González Moro**

CONSULTOR DEL ÁREA DE
SEGURIDAD INFORMÁTICA
Grupo Gesfor

Cualquier SGSI está basado, de una u otra manera, en un modelo de evaluación y de mejora continua sin el cual no tendría sentido. La gestión de la seguridad no es algo que se implanta y se "deja", es algo que se implanta y se "cuida". Sólo de esta forma podremos aprender de los propios errores y alcanzar el modelo de madurez deseado.

Un sistema de métricas correcto debe nacer en el mismo instante que nace la implantación del SGSI. Por desgracia, esta práctica no siempre se sigue y es común ver cómo alguna persona, en una fase avanzada de diseño del SGSI, se da cuenta que hay que hacer un "parón y vuelta atrás" para retomar el sistema de métricas.

Este documento no pretende ser una lista exhaustiva de indicadores a medir o una "toma de muestras", para ello existe suficiente documentación en la red. La red tiene abundante información al respecto (ver referencias al pie del documento). Únicamente pretende ser una

reflexión que mantenga vivos conceptos básicos en la elaboración de métricas y que conjugue los intereses de todas las partes implicadas.

¿Qué medir?

No tiene sentido definir un programa de métricas que inunde los despachos de cifras, índices, valores y

La gestión de la seguridad no es algo que se implanta y se "deja", es algo que se implanta y se "cuida"

gráficos que nadie va a tener tiempo de mirar detalladamente. La falta de información es mala, pero el exceso incontrolado también. **Es necesario medir aquello que realmente es representativo, significativo** y que se ajusta a las necesidades de seguridad de la organización. Hay que pensar que los indicadores o métricas útiles para los técnicos no tienen por qué serlo para otro grupo involucrado en la gestión de la seguridad. Cada uno debe recibir lo que realmente le interesa y cada uno debe aportar al sistema aquello de lo que realmente sabe. Por eso es necesario que en el

desarrollo y definición de métricas, mucho antes de decidirse a implantarlas, se involucre al personal que va a hacer un tratamiento de las mismas. De esta forma se podrán determinar claramente qué métricas son útiles para cada colectivo.

Hay que distinguir entre medida y métrica. La primera es simplemente un valor, la segunda es una colección de valores a lo largo del tiempo. Sólo el factor "tiempo" nos da una visión adecuada de la evolución de la medida y por lo tanto se convierte en un verdadero indicativo del parámetro que queremos analizar. Sin embargo, esto hace necesario asegurar que las medidas que se definan ahora tengan un recorrido a largo plazo. De nada sirve definir métricas asociadas a medidas que pasados unos meses van a tener que redefinirse porque la tecnología ha variado o porque no existen ya medios técnicos para recogerlas.

El sistema de métricas debe ser **claro, conciso, efectivo** y estar ajustado al fin para el cual se diseña, es decir, ofrecer una "fotografía" del estado del SGSI así como permitir detectar acciones de futuro (entre otras cosas).

¿Cómo medir?

De la misma forma que se ha hablado del "tiempo" como elemento esencial a la hora de establecer



sistemas de medición, es necesario poder comparar nuestros indicadores con respecto a un parámetro lo más estándar o "sensato" posible. Los "totales" son malos consejeros si no se comparan o se estudian inmersos en las circunstancias que los producen. Los valores "medios" también pueden inducir a error. Muchas veces la estadística mal utilizada puede llevar a confusión y a una incorrecta toma de decisiones.

Las métricas deben ser comparadas con objetivos realistas previamente definidos (cuando proceda). Los objetivos deben poder ser alcanzables y depender en buena medida de nuestro propio esfuerzo, no de factores externos que no podemos controlar. No es razonable, por tanto, definir objetivos bajos, fácilmente superables, que permitan concluir siempre que los resultados son excelentes y la seguridad funciona perfectamente.

El sistema de métricas debe ser **objetivo e imparcial**, y sobre todo **reproducible**, es decir, siempre que se apliquen los criterios sobre una colección de indicadores, se deben obtener los mismos resultados. Es importante obtener mediadas de sitios "asépticos", esto es, registros de sistemas, registros de sucesos del sistema operativo o cualquier otro medio que nos garantice que si repetimos el cálculo tres meses después, el resultado será el mismo. Sólo así garantizamos la imparcialidad y posibilidad de reproducir los resultados obtenidos.

Igualmente, se deben utilizar medidas que, en la medida de lo posible se puedan extrapolar de forma automática de sistemas existentes. Hacer depender la recogida de información de procesos manuales lleva, inevitablemente, a que en algunas circunstancias (exceso de trabajo, bajas, incidencias) no se tomen medidas en los periodos definidos. Como consecuencia, se perderá el valor del histórico de la



Es necesario medir aquello que realmente es representativo, significativo y que se ajusta a las necesidades de seguridad de la organización

información y la capacidad de analizar una serie y su tendencia.

Como conclusión, una entrevista a un miembro de la organización no es el mejor método de obtener información objetiva a la hora de medir nada ni debería utilizarse nunca como base de una métrica.

¿Cómo presentar?

Evidentemente no todo el mundo tiene los mismos intereses en lo que a gestión de seguridad se refiere, entre otras cosas porque no todas las

personas dentro de la organización tienen las mismas responsabilidades ni los mismos objetivos. Es necesario elaborar la información obtenida del sistema de métricas conforme a las necesidades de los distintos destinatarios.

Un Director de Informática recibirá un tipo de medidas distintas de las que recibe el Director Financiero. Es común caer en la idea de que todo el mundo sabe de todo, y nada más lejos de la realidad.

Por ejemplo, a un Director de Informática le interesará saber que el antivirus del servidor de correo ha detectado y eliminado 2.000 virus en un mes. Al Director Financiero le interesará más saber cuánto cuesta el sistema antivirus y cuánto costaría si un virus se extiende por la red de área local (por esa terrible enfermedad que se llama síndrome del ROI). En este sentido cabe destacar que el personal técnico muchas veces ve el sistema de métricas una excelente herramienta para justificar su trabajo y la necesidad de ciertas inversiones.



Conclusiones

Teniendo todo esto en consideración, para que unas métricas de seguridad asociadas a un SGSI sean útiles y aprovechables habrá de:

- Concienciar al personal de la importancia del sistema de métricas desde el documento de Política de Seguridad.
- Establecer las que realmente son necesarias y se alinean con los objetivos de seguridad de la organización.
- Automatizar los procesos de obtención de medidas y tratamiento de las mismas.
- Hacer un seguimiento periódico conforme a los plazos establecidos en el Plan de Seguridad.
- Utilizar las métricas como datos de entrada de procesos de revisión y auditorías internas.
- Realizar y documentar las acciones de mejora que nacen del estudio de las métricas.

A efectos de presentación hay que tener en cuenta que, dependiendo del destinatario, los valores numéricos no tienen la misma fuerza que los colores o las gráficas. Esto, que no deja de ser una verdad obvia, es tristemente cierto. Un gráfico donde un valor va oscureciendo su tono rojizo, puede ser más efectivo que una tabla donde aumenta un valor numérico.

Los conflictos

En todo sistema de control surgen controversias entre quien recoge los datos, quien los aporta y quien los analiza, de ahí la importancia de poder reproducir resultados. Si los indicadores son obtenidos de registros

de sistemas, no suele haber problemas, pero si los indicadores requieren algún tipo de manipulación o elaboración pueden surgir conflictos.

Por lo general quien aporta los datos suele sentirse "controlado" y eso no siempre crea buen estado de ánimo. Por este motivo, es esencial que el modelo de métricas nazca en el mismo instante que nace el SGSI. El "presunto controlado" debe ser

Por este motivo, es esencial que el modelo de métricas nazca en el mismo instante que nace el SGSI

consciente que forma parte de un sistema de GESTION y no de un sistema de CONTROL. No se analizan métricas para "castigar", se analizan para detectar, prevenir y mejorar.

Si el sistema de métricas nace al mismo tiempo que el SGSI, todo el mundo que participa en él será consciente que lleva el máximo apoyo de la gerencia y por lo tanto deberá ser siempre tomar una actitud participativa y positiva. Así, es recomendable incluir en el documento de Políticas de Seguridad, una referencia expresa al diseño e implantación del sistema de métricas.

Otras recomendaciones

- Los indicadores deben obtenerse de la forma más automatizada posible.
- Los resultados deben ser siempre revisados por quien tiene conocimiento para ello y capacidad de actuación.
- El coste de implantar una métrica debe ser proporcional al beneficio que se obtiene.

■ Las métricas deben ser coherentes con los objetivos de seguridad marcados.

No falta más que hacer hincapié en el concepto de "conocimiento" o "capacidad" a la hora de establecer, analizar o evaluar la métrica. En una situación se definió una métrica como el "porcentaje de visitantes que eran acompañadas al lugar al que iban" y trimestralmente el valor de esa medida lo establecía el Director de Personal (no estaba muy claro el motivo). Curiosamente, si uno preguntaba a los vigilantes sobre el valor real, los valores que ellos proporcionaban eran sustancialmente inferiores.

El caso de ISO 27001

En el caso particular de un SGSI basado en ISO 27001, hay que recordar los puntos donde la norma hace referencia expresa a la necesidad de establecer métricas y sistemas de evaluación de controles.

Estos puntos son:

- 4.2.2.d: Definir cómo medir la efectividad de los controles seleccionados y especificar cómo esas mediciones van a ser usadas para evaluar la efectividad de los controles para producir resultados comparables y reproducibles.
- 4.2.3.c: Medir la efectividad de los controles para verificar que los requerimientos de seguridad se han cumplido.
- 7.2.f a la hora de establecer los datos de partida de las revisiones: Resultados de efectividad de las métricas.

Dentro de los muchos puntos críticos de un SGSI, se pueden destacar dos que son muy indicativos de cómo se ha diseñado e implantado: uno es el sistema de métricas y el otro el plan de continuidad de negocio. ♦