



# Métricas de Seguridad, Indicadores y Cuadro de Mando

LAS MÉTRICAS PERMITEN A LOS RESPONSABLES DE SEGURIDAD DEMOSTRAR LA EFICIENCIA DEL PROGRAMA DE SEGURIDAD Y EL VALOR QUE APORTA A LA COMPAÑÍA



**Alejandro Corletti**

DIRECTOR DIVISIÓN  
SEGURIDAD INFORMÁTICA  
NCS



**Carmen de Alba Muñoz**

RESPONSABLE ISO-27000  
NCS

**E**n el mundo de la seguridad se dice mucho que "la seguridad es un estado de ánimo", es decir, en función de cómo perciba la Dirección lo segura que está la compañía, se invertirá más o menos dinero para implantar controles de seguridad. Es evidente que concebir la seguridad así es peligroso, ya que uno puede pecar por exceso o por defecto. Responder a preguntas tales como: "¿cómo puedo determinar si mi compañía se encuentra segura?", "¿son realmente eficaces los controles que tengo implantados?", "¿cuántos recursos necesito para estar seguro?" suele ser una tarea difícil y subjetiva de responder en la mayoría de los casos.

A día de hoy, las métricas de seguridad siguen siendo un tema novedoso e incluso desconocido para algunos en el mundo de la seguridad. Las empresas en donde la seguridad es una actividad más de la compañía (control de accesos, gestión de usuarios...), sí que incluyen tareas de

planificación y eficacia de los controles implantados.

Antes de continuar, introduciremos un par de definiciones sobre las que basamos el texto (cuyo origen data del borrador ISO-27004, del cual ya escribimos en su momento):

**A día de hoy, las métricas de seguridad siguen siendo un tema novedoso e incluso desconocido para algunos en el mundo de la seguridad**

■ Un **Indicador de Seguridad** es un valor que se obtiene comparando datos (o atributos según ISO-27004) lógicamente relacionados, referentes

al comportamiento de una actividad, proceso o control, dentro de un tiempo específico.

■ Una **Métrica de Seguridad** podría definirse como el conjunto de preceptos y reglas, necesarios para poder medir de forma real el nivel de seguridad de una organización.

■ Un **Cuadro de Mando** es una herramienta de gestión que facilita la toma de decisiones que recoge un conjunto coherente de indicadores que proporcionan a la Dirección y a los responsables, una visión comprensible del estado de seguridad de la compañía y de su área de responsabilidad, que indica si se han marcado los objetivos propuestos.

La ISO/IEC 27001:2005 introduce un concepto nuevo de **indicador de la eficacia de los controles**, que permite al Sistema de Gestión de Seguridad de la Información (SGSI) evaluar la eficacia y la calidad del mismo. A lo largo de la norma aparece este nuevo concepto, como en el punto 4.2.2 c) Implementación y Operación del SGSI "Definir el modo de medir la eficacia de los controles o de los grupos de controles seleccionados y especificar cómo tienen que usarse estas mediciones para evaluar la eficacia de los controles de cara a producir unos resultados comparables y reproducibles", en el punto 4.2.3 Supervisión y Revisión del SGSI c) "Medir la eficacia de los controles para verificar si se han



cumplido los requisitos de seguridad”, o en el punto 7.2 Datos Iniciales de la Revisión f) “Los resultados de las mediciones de la eficacia”.

Es posible que la obligatoriedad de utilizar métricas de seguridad en el SGSI permita a la norma perdurar en el tiempo como un estándar eficaz y potente para gestionar la seguridad de forma óptima, ya que las métricas de seguridad no se contemplan como un “accesorio” más a añadir al SGSI según le convenga a la compañía (como ocurría con la norma anterior BS7799-2), sino que lo absorbe y pasa a formar parte de él a lo largo de su ciclo de vida. Esto garantiza que tanto el SGSI como su sistema de medición son revisados y mejorados de forma continua.

A día de hoy, existen dos estándares del NIST para la implementación de métricas de seguridad, el NIST 800-55 *Security Metrics Guide for Information Technology Systems* y el NIST 800-80 *Guide for Developing Performance Metrics for Information Security*. En la actualidad el subcomité SC 27, como ya comentamos varias veces, está desarrollando la futura norma ISO 27004 *Information Security Management Measurements* que permitirá evaluar el grado de efectividad, eficiencia, nivel de implantación y madurez del SGSI.

## PLAN: Definir las Métricas

Para que una métrica de seguridad sea efectiva, debe cumplir con los siguientes requisitos:

- Debe ser relevante para la organización.
- De ser reproducible y justificable.
- Debe ser objetiva e imparcial.
- Debe ser capaz de medir la evolución de la seguridad en la compañía a lo largo del tiempo.

Aparentemente, el trabajo que viene ahora es “sencillo”: empezar a

<b>PLAN</b>	Establecer SGSI.	Definir las métricas.
<b>DO</b>	Implementar y Operar el SGSI.	Implantar las métricas.
<b>CHECK</b>	Supervisar y Revisar el SGSI.	Revisar los datos de las métricas.
<b>ACT</b>	Mantener y Mejorar el SGSI.	Revisar/Mejorar las métricas.

traducir la estrategia de seguridad que ha planeado la Dirección de la compañía en un conjunto de **objetivos estratégicos**. Cada objetivo estratégico tiene unos **indicadores** asociados que miden el grado de cumplimiento del objetivo. Cada indicador, tiene una **meta** asociada que es el valor que deben alcanzar los indicadores.

**El proyecto de implantación de un Cuadro de Mando de Seguridad es un proyecto complejo desde el punto de vista técnico y organizativo**

Pero, **¿qué métricas e indicadores interesa poner en marcha?** Es evidente que existen un sin fin de métricas e indicadores posibles a desarrollar y que la mayoría de ellos sean interesantes para la compañía. Sin embargo, los recursos de cualquier compañía son limitados (y muchas veces escasos) por lo tanto, sólo se deben desarrollar aquellos que son rentables para la compañía, es decir, aquellos para los cuales la importancia de la información que

aporten justifique el esfuerzo que hay que realizar para su obtención. (Esto, sinceramente no es tarea fácil, es más... tal vez sea la más difícil de todas)

Como herramienta de gestión, un Cuadro de Mando debe poner el foco en aquellos indicadores de la compañía que no se ajustan a los límites establecidos por ésta, y avisar sobre aquellos otros indicadores que puedan llegar a sobrepasar los límites establecidos. Debe también ser útil para asignar responsabilidades y facilitar la comunicación entre los diferentes niveles de responsables, permitiendo mejorar los resultados.

Las claves para implantar un buen Cuadro de Mando son:

- Obtener el apoyo de la Dirección y alcanzar el mayor consenso posible entre los participantes del diseño.
- Ligar los indicadores a los objetivos, es decir conocer qué es lo que se está midiendo.
- Plasmar la información que sea imprescindible, de una manera sencilla, resumida y eficaz para la toma de decisiones.
- Destacar lo relevante para la compañía, poniendo de relieve aquellos indicadores que no evolucionan según lo planificado.
- Simplificar su representación utilizando un juego de colores que sirva para marcar los cambios de estado (ojo con los daltónicos).



■ Uniformidad en su construcción para facilitar el trabajo de comparar resultados entre áreas diferentes.

No debemos olvidar que en función a quien vaya dirigido el Cuadro de Mando, los indicadores se irán agrupando de manera diferente. Por ejemplo, si el Cuadro de Mando va dirigido a los técnicos, se podría elaborar un "Cuadro de Mando de Impacto de Fallos Técnicos", mientras que si éste va dirigido a la Dirección habrá que elaborar un "Cuadro de Mando de Valoración Económica de los Impactos Técnicos".

### DO: Implantar las Métricas

Es posible que en esta fase surja la necesidad de adaptar ciertos controles y procedimientos para que la obtención de los datos sea posible.

**Un Cuadro de Mando es una de las herramientas más potentes y valiosas que puede utilizar la Dirección para evaluar su estado de seguridad**

Toda métrica debe tener asignado un responsable que se encargue de recoger, procesar y comunicar los resultados obtenidos al Cuadro de Mando. Esto implica que hay que formar y concienciar al personal involucrado en los procesos a evaluar, ya que el hecho de implantar métricas de seguridad implica un trabajo

adicional para los afectados y la inversión de recursos adicionales. Es evidente que no sirve de nada tener un sistema de medición fabuloso, si luego resulta que las prácticas asociadas al proceso de recogida de los datos son ajenas al proceso establecido.

La comunicación periódica a las personas del resultado de su trabajo, sirve para mejorar los resultados. En muchos casos, la visualización de los resultados a través de un Cuadro de Mando, puede generar un cambio en la manera de afrontar el trabajo de los empleados de la compañía.

### CHECK: Revisar los Datos de las Métricas

El grado de desarrollo del cuadro de mando, y por ende, de las métricas y de los indicadores, irá reflejando el nivel de madurez de la compañía. De hecho, la calidad de las decisiones que tome la Dirección está estrechamente ligada a la información utilizada.

La revisión de los datos obtenidos, se realiza una vez que se han implantado los indicadores. Lo que se pretende comprobar es que los indicadores sean útiles y rentables. Al revisar los datos obtenidos, es muy recomendable considerar la opinión de los usuarios de los indicadores.

### ACT: Revisar/Mejorar las Métricas

Se planearán revisiones de los objetivos y de la calidad de las métricas para asegurarse que siguen siendo útiles y que siguen cumpliendo con los objetivos definidos.

Durante estas revisiones es necesario comprobar que:

■ Las métricas son leídas y revisadas por las personas destinatarias, ya que, en caso contrario, terminarán por dejar de utilizarse.

