

¿Cómo puede medirse la Seguridad?

Por David A. Chapin y Steven Akridge

Fecha Publicación: 01/07/2008

Las métricas de seguridad tradicionales son, en el mejor de los casos, fortuitas; en el peor, dan una falsa sensación de seguridad, que lleva a una implantación ineficiente o insegura de medidas de seguridad. Este artículo presenta un enfoque donde se combinan madurez y calidad para proporcionar una imagen más completa y ordenada del estado de seguridad de una organización. Nos referiremos a este enfoque como Modelo de Madurez del Programa de Seguridad.

Las métricas de seguridad -la medida de la eficacia de los esfuerzos en seguridad de una organización a lo largo del tiempo- han sido siempre difíciles de evaluar. ¿Cómo puede determinar una organización si se encuentra segura? La medida de la calidad del programa de seguridad sólo puede probarse realmente cuando la organización se ve agobiada por una crisis. Pero para evitar esa situación es precisamente para lo que se realiza el esfuerzo en seguridad.

La gerencia necesita alguna medida de cómo de segura está la organización. Las organizaciones necesitan preguntarse:

- ¿Cuántos *recursos* son necesarios para estar "seguro"?
- ¿Cómo puede *justificarse* el coste de nuevas medidas de seguridad?
- ¿Recibe la organización algo a *cambio* de su inversión?
- ¿Cuándo sabe la organización que está "segura"?
- ¿Cómo puede *comparar* la organización su estado con otras del sector y con los estándares de buenas prácticas?

La respuesta tradicional a estas preguntas se relaciona con la evaluación del riesgo y el riesgo residual que la organización está dispuesta a asumir en función de sus necesidades de negocio y limitaciones de presupuesto. La gestión del riesgo puede darse por sentada, no conduciendo necesariamente a un estado de mayor seguridad.

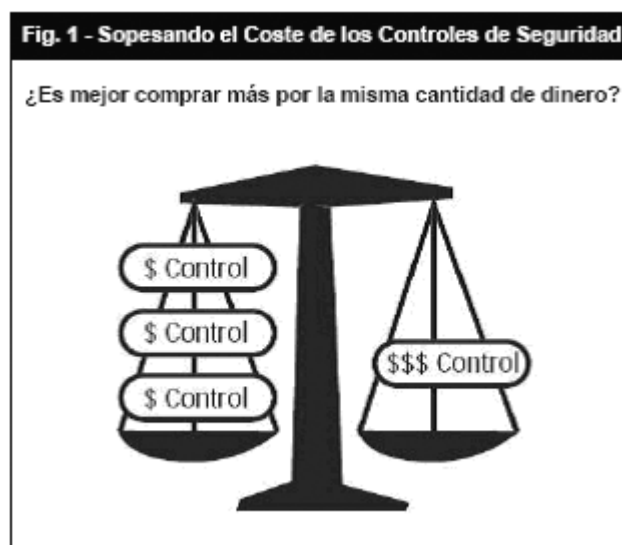
Imagine, por ejemplo, un análisis de riesgos que contiene una matriz de amenazas y el coste de mitigar los riesgos. Algunos de los elementos de la lista tendrían un coste insignificante. Otros elementos serían muy caros (**figura 1**). Con frecuencia, la gerencia puede decidir mitigar el mayor número de elementos por la menor cantidad de dinero, posiblemente dejando de lado los elementos más caros. La suposición es que añadir controles de reducción del riesgo es la mejor opción. Por ello, hay una tendencia a comprar grandes cantidades de herramientas de seguridad y evitar los controles más caros y menos glamorosos. Los controles más complicados tienden a ser de naturaleza organizativa, requiriendo cambios culturales (tales como un plan de recuperación de desastres), más que soluciones llave en mano (tales como cortafuegos y sistemas de detección de intrusos -IDSs-). La dirección piensa que está comprando más seguridad por menos dinero.

Sin embargo, ¿quién dice que se compre más seguridad? ¿Cómo puede medir la organización la protección relativa obtenida con cada adquisición? ¿Está comprando la organización las salvaguardas de seguridad en el orden correcto? ¿Está exponiéndose la organización a más riesgo debido al enfoque no sistemático de la implantación?

Crear programas de seguridad desde cero permite abordar estos problemas tradicionales de métricas de seguridad de otra forma. Una mirada renovada a dichos problemas facilita el desarrollo de una solución exhaustiva para cualquier sector.

Este enfoque nuevo, más sistemático, de las métricas de seguridad permitirá:

- Generar mediciones reproducibles y justificables.
- Medir algo que tenga valor para la organización.
- Determinar el progreso real en el estado de la seguridad.
- Ser aplicable a un amplio espectro de organizaciones, al tiempo que produce resultados similares.
- Determinar el orden en que deberían aplicarse los controles de seguridad.
- Determinar los recursos que necesitan ser destinados al programa de seguridad.



Métricas de seguridad tradicionales. ¿Qué medir?

Una medida, por sí misma, no es una métrica. Debe incluirse también el factor *tiempo*; tampoco la métrica sola es la respuesta a todos los problemas de la organización. Hay que considerar y analizar el significado temporal de las métricas. El truco está en desarrollar métricas que sean simples y proporcionen información útil a la gerencia, a la vez que se corresponden con objetivos relacionados con la seguridad. Las métricas tienen que iluminar a la organización mostrando algún tipo de progreso.

Obviamente, la tarea de las métricas de seguridad es contar o medir *algo*. Pero, ¿qué debería contarse? ¿Cómo puede medirse la seguridad? La **figura 2** muestra ejemplos

de métricas de seguridad utilizadas tradicionalmente. Muchas organizaciones cuentan los incidentes tratados, p. ej., virus detectados o eventos registrados. ¿Cómo proporciona esto una medida de la calidad del programa de seguridad? ¿Cómo muestra esto el progreso?

Figura 2 - Métricas de Seguridad Tradicionales		
Métrica	Supuesta Medición	Peligros
Número de virus o códigos malignos detectados	Eficacia de los controles antivirus automáticos	¿Por qué pasan tantos virus en primer lugar? ¿Cuántos pasaron y nunca se detectaron?
Número de incidentes e investigaciones de seguridad	Nivel de actividad de la monitorización de eventos de seguridad	¿Qué umbral desencadena un incidente o una investigación? ¿Se desencadenan incidentes por defectos en los procedimientos organizativos?
Coste de las brechas de seguridad	Pérdidas económicas reales debidas a fallos de seguridad	¿Qué riesgos residuales eligió asumir la empresa? ¿Es una medida de la respuesta ante crisis o desastres, pero no necesariamente función de las salvaguardas sensatas implantadas?
Recursos asignados a las funciones de seguridad	Coste económico real de utilizar un programa de seguridad	¿Son ineficientes las herramientas, tareas asignadas o procedimientos, llevando al personal a perder tiempo?
Cumplimiento de las reglas de seguridad	Nivel de cumplimiento de los objetivos del programa de seguridad	¿Cómo se relaciona el cumplimiento con la eficacia? ¿Cuál es el orden de cumplimiento? Una vez logrado el cumplimiento, ¿se "acaba" el programa de seguridad?

Los totales de incidentes son medidas poco fiables, por la siguiente razón: imagine una pequeña población con un solo agente de policía. No realiza otra tarea policial más que patrullar la carretera con un radar, deteniendo a cientos de conductores por exceso de velocidad. Ahora, imagine una gran ciudad con muchos policías. No usan radares y han parado a pocos conductores por exceso de velocidad, pero tienen un gran programa de conducción defensiva y otro de prevención de alcohol al volante. ¿Es más segura la pequeña población que la gran ciudad? La cuenta de conductores por exceso de velocidad es sólo tan buena como el mecanismo de detección, pero ese número no ofrece ninguna profundización. ¿Qué hay de los conductores borrachos que no exceden la velocidad en la pequeña población? ¿no son potencialmente más peligrosos?

Ahora, compare esto a una herramienta antivirus en un entorno de sistemas de información. El hecho de que esté reportando un gran número de virus puede dar la sensación al equipo de seguridad que su herramienta está funcionando pero, ¿qué dice realmente acerca de la seguridad? En primer lugar, ¿por qué están entrando tantos virus? ¿Cuántos entran y no son detectados? ¿Cómo mide esto la calidad del

programa de seguridad? ¿Debería considerarse como un gran éxito el que el antivirus no detecte nunca un virus debido a que ninguno llega a entrar en el sistema!

Otra métrica de seguridad tradicional es el tiempo dedicado a una tarea -cuánto tiempo dedica el personal a funciones relacionadas con la seguridad-. En algunos casos, desde un punto de vista de dirección de proyecto, esta métrica puede ser valiosa, porque los dos únicos recursos que la gente aporta a una organización son su capacidad intelectual y el tiempo que emplean utilizándola. Pero, desde el punto de vista de la seguridad, el tiempo de las personas puede no ser una métrica valiosa. Por ejemplo, al medir el tiempo dedicado a investigaciones de seguridad, ¿más tiempo dedicado indica necesariamente un mejor estado de la seguridad? Pudiera ser que el tiempo se esté usando ineficientemente investigando incidentes de seguridad debido a que los procedimientos de la organización son débiles -desencadenando más incidentes para ser tratados por el equipo de seguridad, cuando podrían ser prevenidos de otra forma, como, p. ej., con mejor formación.

Finalmente, otra métrica clásica es el coste del daño provocado al negocio por un incidente de seguridad. En primer lugar, esto parte de que algo malo ha sucedido. Mientras que puede que mida la eficacia de la respuesta ante el desastre, no es necesariamente una buena medida de la calidad del programa de seguridad. Algunos incidentes son función del riesgo residual que la empresa está dispuesta a asumir, combinados con circunstancias desafortunadas. O bien, otros incidentes pueden ser el resultado de prácticas de seguridad pobres que abren la puerta al desastre. ¿Cómo pueden distinguirse estos? O, puede que sucediera una de estas dos cosas y la gestión de la crisis fue tan buena que produjo mínimo impacto en el negocio. Las salvaguardas proporcionan sólo un cierto grado de seguridad; siempre habrá riesgos.

La clave de las métricas de seguridad está en obtener medidas que tengan las siguientes características ideales:

- Deberían medir cosas *significativas* para la organización.
- Deberían ser *reproducibles*.
- Deberían ser *objetivas e imparciales*.
- Deberían ser capaces de medir algún tipo de *progresión* a lo largo del tiempo.

En la práctica, casi todas las métricas de seguridad publicadas carecen una o varias de estas características. Las métricas de seguridad tradicionales eran un asunto de "toma todo lo que puedas", es decir, cualquier métrica que estuviese disponible se agarraba y reportaba. Esta forma de pensar debería cambiar.

Se necesita un enfoque más sistemático para el desarrollo de métricas que encajen directamente en las características mencionadas anteriormente.

Madurez del Programa de Seguridad

Una pieza del puzzle de métricas de seguridad es la medida del progreso del programa de seguridad frente a un modelo de madurez. Este enfoque apunta directamente al menos a dos de las cuatro características mencionadas con

anterioridad: mide cosas significativas para la organización y la progresión hacia un objetivo.

Los pocos modelos de madurez de seguridad publicados están resumidos en la **figura 3**. Por alguna razón, cada uno tiene sólo cinco niveles de madurez. Cada modelo parece sufrir de sus propios prejuicios acerca de la definición de madurez.

Aquí se propone que se use un nuevo estándar de madurez. La madurez debería ser una medida sólo del progreso del programa a lo largo del tiempo, no necesariamente de la calidad de los elementos del mismo. Esta definición de madurez tiene varias características importantes:

- Proporciona el plan para un programa de seguridad completo.
- Muestra a la gerencia el orden en el que implantar los elementos de seguridad.
- Conduce hacia la utilización de estándares de buenas prácticas (p. ej., ISO 17799).¹
- Siempre y cuando se use un estándar, proporciona una forma de comparar el programa de seguridad de una organización con el de otra.

Siguiendo este estándar de madurez, los modelos previos sufren estas tres deficiencias clave:

1. Confunden calidad con existencia. Uno tiene que aprender a andar antes de correr. La calidad de lo bien que uno anda no es necesariamente una indicación de la habilidad de correr.
2. Los modelos existentes necesitan ser adaptados específicamente a la organización. Por ello, es difícil comparar directamente los resultados de una organización con los de otra.
3. Los modelos actuales tienden a provenir de perspectivas de ingeniería o de gestión de proyectos. Por ello, se centran en que los elementos cumplan con ciertas especificaciones de estilo *ingenieril*. No dirigen necesariamente el programa hacia un objetivo organizacional concreto y, por ello, funcionan mal para un programa de seguridad. La incorporación filosofías de gestión de la calidad total (TQM) y Seis Sigma son un ejemplo de esto.

Figura 3 - Modelos de Madurez de Seguridad Publicados		
Modelo	Descripción	Comentarios
Modelo de Madurez de Seguridad TI de NIST CSEAT ²	Cinco niveles de madurez progresiva: 1. Política 2. Procedimiento 3. Implantación 4. Prueba 5. Integración	Centrado en niveles de documentación
Modelo de Evaluación de la Seguridad de la Información de Citigroup (CITHSEM) ³	Cinco niveles de madurez progresiva: 1. Autocomplacencia 2. Reconocimiento 3. Integración 4. Prácticas comunes 5. Mejora continua	Centrado en concienciación y adopción por parte de la organización
Modelo de madurez de COBIT® ⁴	Cinco niveles de madurez progresiva: 1. Inicial / <i>ad hoc</i> 2. Repetible pero intuitivo 3. Proceso definido 4. Gestionado y medible 5. Optimizado	Centrado en procedimientos específicos de auditoría
Modelo SSE-CMM ⁵	Cinco niveles de madurez progresiva: 1. Realizado informalmente 2. Planificado y perseguido 3. Bien definido 4. Controlado cuantitativamente 5. Continuamente mejorado	Centrado en ingeniería de seguridad y diseño de software
Evaluación de la Capacidad de Seguridad de CERT/CSO ⁶	Cinco niveles de madurez progresiva: 1. Existente 2. Repetible 3. Persona designada 4. Documentado 5. Revisado y actualizado Mide usando cuatro niveles: 1. Inicial 2. En desarrollo 3. Establecido 4. Gestionado	Centrado en la medición de la calidad relativa a niveles de documentación

Con la seguridad, el resultado debería ser más parecido a una póliza de seguros. No es como fabricar un producto. En vez de ello, la organización está socializando infraestructura y cultura.

Este nuevo acercamiento hacia un modelo detallado de madurez de seguridad (llamado Modelo de Madurez del Programa de Seguridad) toma un enfoque de sistema de gestión. Por ello, sigue el estándar ISO 17799 para desarrollar un programa de seguridad completo. Implica la existencia o no existencia de un gran número de elementos (**figura 4**).

Figura 4 - Resumen General del Modelo de Madurez de Seguridad		
Categorías ISO 17799	Nº de Elementos Medidos	Cuestiones cubiertas por los elementos
1. Gestión general de la seguridad	11	Necesidad, estrategia, compromiso, roles y responsabilidades, políticas y procedimientos
2. Clasificación y control de activos	5	Valoración, evaluación de riesgos, propiedad, etiquetado y manejo, inventario
3. Seguridad relativa al personal	8	Contratación y finalización de contrato, roles y responsabilidades, investigación de antecedentes, formación, reporte, revisión
4. Seguridad física y del entorno	12	Perímetros, riesgos ambientales, evaluación de riesgos, controles de acceso, seguridad, eliminación y destrucción de activos, monitorización, gestión de incidentes, concienciación, cooperación
5. Control de accesos	11	Perímetros, evaluación de riesgos, controles de acceso, autenticación, necesidad de acceso, responsabilidad del usuario, actualización de accesos, monitorización, informática móvil, gestión de incidencias
6. Desarrollo y mantenimiento de sistemas	9	Estándares, modelo de ciclo de vida, revisión, análisis de diferencias, planificación de requerimientos, integridad y certificación de tests, repositorio de código, gestión de versiones, retirada
7. Gestión de comunicaciones y operaciones	16	Estándares, todos los métodos de comunicaciones electrónicas, procedimientos operativos, monitorización, backups, gestión de excepciones, actualizaciones y parches, helpdesk, gestión de cambios, sistemas criptográficos, gestión de soportes, código maligno, aceptación de sistemas, librería de documentación, planificación de capacidades
8. Seguridad organizacional	11	Función de seguridad, monitorización, asesoría, auditoría, comité de seguridad, concienciación, segregación de tareas, tests de penetración y vulnerabilidad, gestión de incidencias, cooperación
9. Gestión de continuidad de negocio	7	Evaluación de riesgos, gestión de prioridades, backups, planificación de continuidad de negocio y recuperación de desastres, pruebas, actualizaciones
10. Conformidad	10	Reglamentaciones, contratos, propiedad intelectual, etiquetado y manejo, retención de registros, auditoría, sanciones

Puesto que implica muy poca valoración subjetiva, los resultados son reproducibles y objetivos. No se mide la calidad o eficacia de la implantación del elemento, aunque ciertos elementos (como los programas de auditoría), si son ejecutados, pueden

llevar hacia otros controles de calidad. Esto es parecido a las inspecciones de Sanidad de los restaurantes. Las puntuaciones de inspección pueden decir qué restaurantes evitar, pero no dicen nada acerca de si uno comerá bien en aquéllos que superaron la inspección.

El nivel de madurez es una medida importante cuando se compara una organización con otra. Si el coeficiente de madurez de una organización es de un 75%, ¿querrá conectar su red con la de otra que sólo llega al 25%?

El nivel de madurez lleva a una organización a comprender mejor su programa de seguridad en comparación a otras semejantes. Proporciona un criterio con el cual evaluar el grado de confianza que puede ponerse en sistemas informáticos interconectados entre diferentes organizaciones.

Este modelo de madurez de seguridad es también una guía para el orden en que se deberían implantar los elementos del programa. La **figura 5** muestra un ejemplo del acercamiento paso a paso hacia la implantación de elementos. En un programa maduro, los elementos son ejecutados basándose en el resultado de las etapas de implantación previas. Consecuentemente, le indica directamente a la gerencia cuándo "comprar" seguridad. Responde a las preguntas expuestas en la **figura 1**.

Figura 5 - Ejemplos de Elementos de un Modelo de Madurez de Seguridad	
Orden de ejecución	Elementos del programa de madurez 2. Clasificación y control de activos
1	2.1 Se realiza una valoración para identificar y comprender los activos de información a proteger.
2	2.2 Se realiza una evaluación de riesgos para identificar y cuantificar las amenazas a los activos de información.
3	2.3 Los activos de información tienen definidos encargados de sistemas y propietarios.
4	2.4 Se desarrollan procedimientos de etiquetado clasificatorio y de manejo de activos de información.
5	2.5 Se instala un programa de inventario de gestión de activos para manejar éstos de forma continua.

Esto también evita el peligro de implantar medidas de seguridad en el orden incorrecto, introduciendo riesgos de seguridad precisamente por no implantar las salvaguardas sistemáticamente. Por ejemplo, en la **figura 5**, la organización podría, de hecho, sufrir un daño si se implanta un sistema activo de gestión de inventario (elemento 2.5) antes de valorar los activos y realizar una evaluación de riesgos (elementos 2.1 y 2.2). Si se completa en el orden incorrecto, podría suponer años de rediseño del sistema de inventario para categorizar correctamente y, en última instancia, proteger los activos.

Puesto que este modelo es esencialmente una herramienta detallada de conformidad, la gerencia puede malinterpretar quizás la madurez del programa. Un alto nivel de madurez puede dar la falsa impresión de conclusión de proyecto. Puede indicar a la

gerencia que ahora la organización está "segura" y que no hay ya necesidad de apoyar el esfuerzo en seguridad, cuando, en cambio, sólo si los elementos han sido ejecutados con un alto nivel de calidad, puede ser indicativo de un estado seguro. Pero, por otra parte, sólo porque una organización haya completado un elemento de seguridad en particular, no quiere decir necesariamente que esté haciendo un buen uso de él. Esto es por lo que debe utilizarse una herramienta de medida separada para medir la calidad o eficacia de la implantación actual.

Estado de la Seguridad

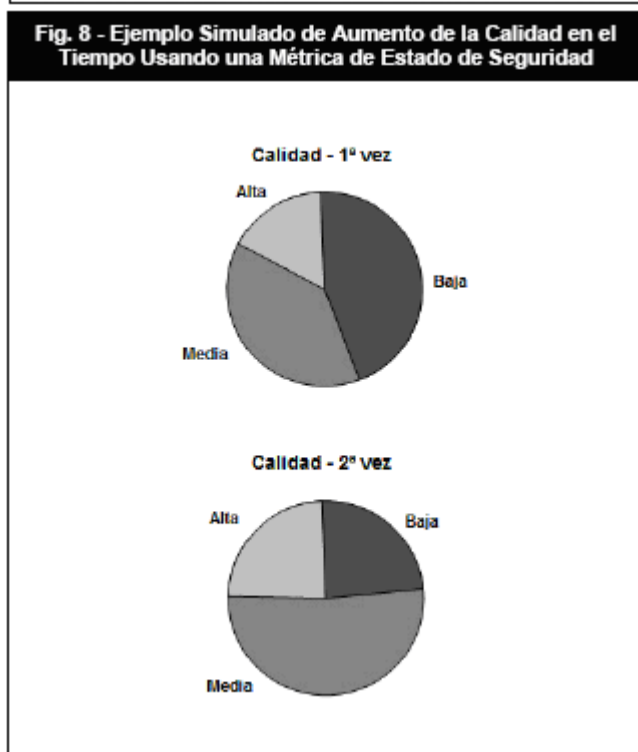
Una mejora del modelo de madurez es el estado de seguridad, que modifica esencialmente el modelo de madurez basándose en la calidad de implantación de cada elemento. Una ventaja de añadir una medida de la calidad es que, a diferencia del índice de madurez, el estado de seguridad no es un nivel estático de realización. Es dinámico y puede cambiar basándose en la calidad de la ejecución continua de los elementos del programa. El mantenimiento de un cierto estado de seguridad requiere una gestión activa del programa de seguridad.

La calidad es una medida subjetiva. Pero, al estar separada de la madurez, los dos valores no pueden confundirse, como en otros modelos. Se aconseja un factor de tres niveles (alto, medio, bajo), tal como se muestra en la **figura 6**. Con descripciones detalladas de los umbrales, es posible ser objetivo y obtener resultados. Este esquema es similar al modelo de criticidad de la Infosec Assessment Methodology (IAM) de la National Security Agency (NSA) de EEUU, donde los elementos también tienen tres niveles de calidad ⁷. Pero, a diferencia del modelo IAM de la NSA, centrado en datos y sistemas, proporciona una imagen más rica de todo el programa de seguridad de la organización.

Figura 6 - Ejemplo de una Medida de la Calidad de un Modelo de Madurez de Seguridad

Elemento del programa de madurez	Si el elemento de madurez está implantado, entonces...		
	Umbral de baja calidad	Umbral de calidad media	Umbral de alta calidad
2.4 Desarrollados procedimientos de etiquetado clasificatorio y de manejo de activos de información	Procedimientos desarrollados pero no implantados	Activos parcialmente clasificados	Clasificación presente en toda la organización

Una métrica ideal de calidad de la seguridad podría utilizarse como un panel de control para la gerencia. Podría dar una visión casi en tiempo real del estado de la seguridad de la organización (**ver figuras 7 y 8**). Debería medirse semanalmente; la propiedad de elementos individuales de madurez del programa debería ser asignada a departamentos específicos. Así, clasificando los elementos por departamentos, la gerencia puede obtener una visión de la seguridad específicamente configurada en función de la estructura de la organización.



La **figura 9** proporciona un ejemplo simulado de una organización ficticia semejante. De un vistazo, se puede comprobar qué nivel alcanza cada departamento en madurez y calidad. Por ejemplo, el departamento 2 está más maduro, pero su calidad es más baja que la de los otros dos departamentos y, mientras los departamentos 1 y 3 están casi al mismo nivel de madurez, la calidad de la implantación del departamento 1 es más alta.

Estas evaluaciones necesitan una gestión activa constante. Mediante el uso de métricas de seguridad de esta manera, la organización incorpora la seguridad profundamente en su estructura. Las métricas de seguridad se convierten entonces en un indicador significativo del rendimiento organizacional, porque fueron diseñadas para satisfacer los objetivos iniciales de las mismas. Una organización puede demostrar fácilmente mejoras en el estado de seguridad a lo largo del tiempo. Además, según los elementos de seguridad se van adoptando de forma más sistemática, la dirección puede empezar a comprender los costes y beneficios de un programa de seguridad organizado, maduro y de alta calidad.

Están ordenados por categorías de ISO 17799, con los números entre paréntesis indicando el número real de elementos del programa utilizados para el índice de madurez.

Todas las medidas de calidad de los elementos existentes del programa se agregan en dos momentos diferentes.

