Cuadros de Mando de Seguridad de los Sistemas de Información

José A. Mañas <jmanas@dit.upm.es>

Dept. de Ingeniería Telemática
Universidad Politécnica de Madrid

Agencia Nacional de Seguridad
Centro Criptológico Nacional

Palabras clave

Seguridad, cuadros de mando, medidas, métricas, gestión, indicadores clave de rendimiento, indicadores de eficacia, gobierno de los sistemas de información.

Resumen

La seguridad es una preocupación constante, cuando no creciente, tanto para los técnicos a cargo de los sistemas, como para los gestores de la organización y los usuarios de los sistemas. La seguridad técnica de los sistemas es un requisito indispensable; pero más allá de la confianza técnica, los gestores necesitan tener confianza en que el sistema de información permitirá alcanzar los objetivos propuestos y establecer relaciones fructíferas con otras organizaciones: la llamada administración electrónica. En este contexto, un cuadro de mando aparece como herramienta necesaria para conocer la evolución y el estado actual de la seguridad y poder reaccionar con conocimiento; decir, para gestionar actuaciones, gastos e inversiones.

A continuación se describen los componentes necesarios para armar un cuadro de mando y las actuaciones que estamos llevando a cabo actualmente en el CCN para alcanzar un sistema base que sirva de plataforma para organismos de la Administración.

Introducción

La gestión de una organización es un asunto complejo. Gestionar su seguridad también es complejo e interdisciplinar, pues no es una asunto meramente técnico, sino que requiere personal técnico y de otros perfiles[1].

Algunas decisiones son de carácter técnico:

- respuesta ante incidencias: incidentes de seguridad o problemas de disponibilidad de redes y sistemas
- configuración y re-configuración [dinámica] de sistemas
- planificación de recursos

Otras decisiones escapan a los meramente técnicos:

- dónde, cuánto y cuánto dinero dedicar a seguridad informática

[1] La distinción entre técnicos y no técnicos es a menudo borrosa. Los operadores, técnicos por excelencia, necesitan gestionar los sistemas día a día. Los responsables de informática necesitan gestionar adquisiciones, desarrollos e implantaciones. Y los gestores necesitan gestionar la asignación de recursos económicos y de otra índole. Cada papel requiere sus elementos de trabajo, sus indicadores específicos, para saber si se acercan o se alejan de sus objetivos.

- qué riesgos se aceptan y cual es el margen de riesgo total que puede tolerarse
- el equilibrio entre las diferentes áreas afectadas por los sistemas de información.

Se aprecia frecuentemente que mientras los perfiles más técnicos buscan un mundo perfectamente seguro, los responsables empresariales incorporan otros factores como el coste de la seguridad y la seguridad percibida por los interesados. De esta forma son capaces de alinear necesidades y actuaciones.

Aún cuando la decisión última es gerencial, la seguridad hunde sus raíces en los sistemas de información que son elementos esenciales para producir eficientemente en casi cualquier administración moderna. Cuando los sistemas de información funcionan perfectamente, se alcanzan grandes cotas de productividad y eficacia; pero cuando fallan, sus defectos repercuten en la prestación última de los servicios y en la custodia de la información gestionada por la organización. Son pues los sistemas de información al tiempo imprescindibles y peligrosísimos. Las amenazas se materializan sobre los medios técnicos; las consecuencias afectan al negocio.

Es difícil analizar sobre el papel la seguridad efectiva de un sistema aislado; pero lo es aún más predecir la seguridad de dos sistemas si se interconectan. Los defectos de seguridad pueden afectar más o menos a un sistema aislado; pero presentan una desagradable tendencia a magnificarse cuando unos sistemas se interconectan con otros y pequeños desencuentros tienen consecuencias críticas.

En consecuencia, en un mundo que es peligroso e inseguro y donde el análisis exhaustivo no basta, necesitamos establecer cauces de cooperación entre técnicos y gerentes, entre los que están a pie de obra y los que toman decisiones, de forma que las actuaciones sean técnicamente correctas y estén alineadas a la misión de la organización.

Elementos

A fin de establecer un cuadro de mando que sintetice el estado de seguridad del sistema al nivel de detalle que requiera su utilizador (lo cual depende de su misión y responsabilidades dentro de la organización), necesitamos una serie de indicadores. Los indicadores sintetizan cantidades ingentes de información de forma que descubran su sentido global, ignorando los detalles. La información básica está en el sistema y basta medirla. Entre las medidas y los indicadores lo que necesitamos es un mecanismo de cocina y presentación. En conjunto hay que definir una serie de métricas que permitan interpretar los indicadores y una forma de medir o, más precisamente, de sintetizar indicadores concisos a partir de un gran conjunto de medidas.

Datos en bruto

Esta es la parte fácil, demasiado fácil. Los sistemas de información son capaces de suministrar millones de detalles siempre y cuando se les requiera con anterioridad. Hay que saber lo que se necesita para registrarlo cuando se sabe (después ya es tarde) y hay que saber lo que no se necesita para poder desecharlo. O, algo intermedio, saber qué necesitamos durante cuánto tiempo de forma que los registros de actividad (*logs*) no nos desborden y el sistema dedique su actividad a su propia medición antes que su misión última. En la práctica

- hay que decidir de antemano que vamos a registrar
- hay que establecer un plan de destrucción progresiva de *logs*

- en cada destrucción hay que guardar parte de la información, bien en bruto, bien consolidada
- hay que automatizar todo el proceso de captura y gestión de *logs* para prevenir errores humanos, olvidos y ataques intencionados

La recolección de datos es mecánica; pero la decisión de qué se mide y qué se conserva durante cuánto tiempo debe hacerse con un objetivo. Los objetivos los marcan, en última instancia, las necesidades del negocio; un poco más cercano, las necesidades de los gestores del negocio y, en concreto, las medidas que se requieran para gestionar el negocio en sus diferentes niveles de responsabilidad.

Agregación de datos

Los datos, en bruto, son poco relevantes. Desde cualquier punto de vista, la información atomizada es irrelevante. La información pasa a ser interesante cuando se agrega. A modo de ejemplo, la trayectoria arbitraria de un automóvil es de escaso interés para las autoridades; pero una concentración de coches en un cierto lugar significa un atasco de tráfico.

Para agregar datos debemos satisfacer algunos criterios básicos de calidad:

- debe estar claro cómo se calcula el valor agregado a partir de los datos en bruto; si dos aplicaciones diferentes derivan el mismo resultado de los mismos datos, la salida debería ser equivalente
- debe estar claro cuándo (y cada cuánto tiempo) se evalúa la medición agregada, de forma que desviaciones u oscilaciones rutinarias no oculten desviaciones o comportamientos que denoten un problema
- desde un punto de vista de buena organización, debe estar claro quién es el responsable de la especificación de la agregación, de su mantenimiento, de su elaboración regular, de la custodia de sus datos históricos, de la gestión de cambios y de la resolución de incidencias

Cuando se agregan datos es importante racionalizar su significado:

- ¿qué significa un cierto valor?
- estableciendo umbrales: ¿cuánto es "insuficiente"? ¿cuánto es "demasiado"? ¿qué valores son las frontera para dedicarle atención? ¿qué valores denotan situaciones de peligro? (se establecen líneas amarillas y líneas rojas)
- mostrando su evolución en el tiempo: se necesitan reglas para interpretar el significado de los cambios, ¿cuánto es excesivo? ¿cuánto es demasiado poco? ¿es buena la estabilidad? ¿qué significan los picos? ¿y las variaciones abruptas? Y así un largo etcétera que permita entender el sistema observando la evolución de sus mediciones.

Se dice que definimos una métrica. Realmente hay una métrica de datos en bruto (suele ser sencilla) y métricas para los diferentes grados de agregación (esta exige más cuidado para no llamar a engaño y acabar perdiéndose en la masa de números).

Las métricas permiten a los responsables interpretar lo que ocurre. A los más técnicos les permite controlar el comportamiento de los sistemas; a los menos técnicos les permite escudriñar el alineamiento de gastos y beneficios.

Indicadores

Las medidas, en bruto o agrgadas, cuando están acompañadas de una métrica que las recionaliza, permiten ser utilizadas como indicadores que resumen el "estado de salud" o denotan la "enfermedad" del sistema bajo observación.

Se suelen identificar tres tipos de indicadores: de implantación, de eficacia y eficiencia, y de impacto.

Indicadores de implantación

Denotan en qué medida una cierta política de seguridad es un mero deseo o ha sido llevada a la práctica; son indicadores que suelen nacer con niveles muy bajos en sistemas nuevos, y se van acercando a los niveles deseados con el tiempo. Miden el efecto del esfuerzo y la inversión para determinar si nos llevan al punto deseado.

Cuando el sistema madura, los indicadores de implantación se estabilizan y simplemente sirven para corroborar que el sistema no se degrada o para detectar si se produce algún retroceso en el sistema. Son importantes pues durante procesos de cambio hasta que el sistema se estabiliza, y deben monitorizarse posteriormente para detectar descuidos.

Indicadores de eficacia y eficiencia

Son indicadores más propios de un sistema maduro.

Los indicadores de eficacia se centran en demostrar si el sistema desplegado alcanza los resultados propuestos. Por ejemplo, si un sistema anti-virus es capaz de reaccionar en menos de 5 minutos a nuevos ataques.

Los indicadores de eficiencia se centran en mostrar la proporcionalidad entre el gasto y el beneficio. Por ejemplo, si los costes de personal en seguridad física son proporcionados a la reducción en el número de incidentes que hay que escalar a servicios externos de protección.

Tanto la efectividad como la eficiencia permiten conocer si alcanzamos razonablemente los objetivos propuestos.

Indicadores de impacto

Se llaman así los que distanciándose de los detalles de qué se hace o cómo de eficazmente se hace, analizan el efecto sobre la misión u objeto final de la organización.

Son típicos los indicadores de opinión de los usuarios, satisfacción de reglamentaciones o sellos de calidad, mejoras en la prestación de los servicios, etc.

Estos suelen ser los indicadores manejados en los altos niveles de Dirección para establecer políticas y marcar objetivos de negocio.

Al haber sido construidos agregando datos más sencillos y pasando por indicadores de eficacia y eficiencia, así como por indicadores de implantación, será posible correlacionar todos estos de forma que podamos seguir la evolución de los indicadores de implantación o de eficacia para saber si los indicadores de impacto avanzarán en la dirección adecuada. Es decir, si alineamos indicadores y entendemos su correlación seremos capaces de alinear comportamientos y reacciones tempranas.

A menudo se habla de "indicadores claves de rendimiento" cuando se logra establecer una relación fuerte, clara y directa entre indicadores de implantación, eficacia o eficiencia e indicadores de impacto; tan fuerte que es posible predecir la evolución de los últimos observando la progresión de los primeros.

Cuadro(s) de mando

A cada nivel de gestión del sistema le incumben una serie de indicadores: los que necesitan para tomar las decisiones que competen a su nivel de responsabilidad corporativa.

El personal más técnico necesita indicadores para tomar decisiones técnicas, típicamente de reacción o de configuración de sistemas, llegando hasta la planificación de recursos técnicos necesarios con visión de necesidades futuras.

- salud de los sistemas, razonabilidad de la configuración, priorización de procesos, reparto de carga, etc.

Cuadros gerenciales intermedios necesitan indicadores para gestionar los recursos disponibles o planificar su futuro.

- recursos humanos: ubicación y planificación
- salud financiera: razonabilidad del gasto, capacidad para acometer proyectos

Los niveles superiores de la organización requieren indicadores muy sintetizados para ser integrados con otros indicadores de otras áreas, no necesariamente de los sistemas de información, de forma que tengan datos para tomar decisiones estratégicas.

- percepción de los clientes y proveedores
- capacidad para una reacción rápida y efectiva a cambios del entorno
- capital humano: estabilidad, compromiso y capacidad para afrontar el futuro a corto y medio plazo

Debe quedar caro que mientras que una variedad de indicadores impide que los problemas pasen desapercibidos[2], la profusión de indicadores es inmanejable. Es una necesidad práctica determinar unos pocos indicadores que reflejen sucintamente lo que se necesita para dirigir la organización. Una mala elección de indicadores llevará a la dirección a tomar decisiones equivocadas por trabajar con información escasa, desafortunada o, simplemente, que induce a error.

Uso de los indicadores

Los indicadores se usan principalmente para gestionar cambios. Una organización está en continuo cambio, buscando alcanzar sus objetivos inmediatos que, esperemos, están alineados con sus objetivos a medio y largo plazo. Pero el problema en cada momento es alcanzar los objetivos inmediatos y los indicadores deben permitir si estamos progresando según lo previsto hacia el objetivo deseado. O si vamos adelantados, o atrasados, o va a ser enteramente imposible llegar a donde se pretende en plazo y formas. Cuando los proyectos se expanden en plazos prolongados (años) los indicadores deben dar señales inmediatas de las desviaciones, mientras sea posible reaccionar con el mínimo esfuerzo extra.

Pero, sirviendo los indicadores para gestionar proyectos a corto plazo, ¿qué hacer cuando los objetivos se alcanzan? Por una parte, conviene mantenerlos monitorizados para detectar posibles desviaciones de lo que se cree conseguido. Por otra parte nos encontraremos con nuevos objetos, nuevos proyectos y, probablemente, necesitados de otros indicadores, los idóneos para la nueva situación.

---

[2] Uno u otro indicador reflejará que hay un problema.

Tenemos requisitos contradictorios: las métricas deben ser evaluadas durante largos periodos de tiempo para saber interpretar su evolución y los indicadores tienen que adaptarse dinámicamente a las necesidades del periodo. Necesitamos unos pocos indicadores que resuman la salud de la organización; pero al tiempo que se adapten a la situación presente. Además, cuando aparece un nuevo indicador en escena, los usuarios no esperan pacientemente a ver cómo evoluciona para aprender a interpretarlo: desde el primer día necesitamos ver cómo hubiera lucido el nuevo indicador en el pasado inmediato. Esto se consigue conservando las series históricas, lo que permite evaluar los nuevos indicadores sobre los datos del pasado inmediato.

¿Indicadores útiles?

Permítaseme definir seguridad como evitar desastres. O, por ser un poco menos dramático, impedir que los incidentes se conviertan en desastres. Porque los incidentes son difícilmente inevitables en tu totalidad; pero los desastres son eso, desastrosos. Las indicadores fallan cuando son incapaces de prevenir un desastre, cuando no perciben los incidentes o las tendencias y, por tanto, no indican al responsable que debe actuar[3]. La capacidad de detectar incidentes es una obligación de todo indicador; pero pudiera no ser suficiente.

A veces los incidentes son más que evidentes. Otras veces van creciendo en silencio. A los indicadores se les pide que detecten lo que ocurre y que descubran su preparación para así poder actuar con tiempo. A veces cuando el incidente se detecta ya es tarde para evitar el desastre: ese indicador es poco útil[4]. ¿Estamos cerca de un incidente relevante? ¿Cómo de cerca? ¿Nos alejamos o nos acercamos a la zona de riesgo? Es decir, un indicador debe medir la distancia que nos separa del desastre.

Hay dos métricas básicas para determinar la distancia que nos separa del desastre: tiempo para que ocurra y margen de seguridad. El tiempo es obvio. El margen mide cuántas cosas tienen que fallar para que el incidente se convierta en desastre. A veces oiremos hablar de “comprar tiempo para reaccionar” o de “defensa en profundidad” que son formas de referirse al margen de seguridad.

Ojo: los números son fáciles de calcular; incluso los modelos formales son fáciles de desarrollar. Pero la última palabra la tiene la cruda realidad. Es decir, el tiempo nos dará la experiencia para saber si un conjunto de indicadores es más o menos adecuado como indicador de dónde estamos y qué va a pasarnos.

Si los indicadores están disponibles tarde y pobremente, son inútiles[5]. Pero si se arrojan a los gestores antes de que los necesiten o en cantidades ingentes, también devienen inútiles pues la dirección no estará preparada para cuando hagan realmente falta, sino que puede estar incluso anestesiada por falsas alarmas.

Por último, cabe recordar que la gente maneja el concepto de confianza, más allá del de seguridad. La confianza es una percepción subjetiva; pero en base a ella tomamos multitud de decisiones. La confianza crece con el tiempo: cada vez que el sistema se comporta como dicen (y predicen) los indicadores. La confianza decae cada vez que los indicadores yerran en su predicción o diagnóstico. En la medida en que los indicadores prevén los fallos, el sistema está

---

[3] El indicador de gasolina de un coche indica al conductor cuánto le queda antes de tener que reposar. La luz roja avisa de que es inminente la necesidad de una recarga.

[4] Si el coche sólo tiene luz roja que se enciende cuando queda carburante para 100 kilómetros, si las estaciones de servicio distan unas de otras 300 kilómetros, el indicador es probablemente inútil.

[5] En realidad, también hay que ser capaces de análisis post-mortem; para lo que sí pudieran ser útiles métricas a posteriori.

bajo control; cada vez que un indicador yerra en la predicción o mera detección, el sistema está fuera de control y el indicador bajo sospecha: hay que retirarlo, revisarlo o, simplemente, acompañarlo de otros indicadores que, como colectivo, sean capaces de un mejor reporte de situación.

Son útiles aquellos indicadores que merecen confianza.

Por último, recordemos, como se indicaba más arriba, que las métricas requieren una definición limpia, objetiva y estable en el tiempo, de forma que se pueda crear una concienciación en toda la organización que mejore la actitud del personal frente a los temas relacionados con la seguridad de los sistemas de información. La gente se puede acostumbrar a pesetas o a euros, a kilómetros o a millas; en realidad es técnicamente indiferente, pero la percepción de los seres humanos no es sólo técnica sino que hay medidas grabadas en el cerebro que proporcionan reacciones instintivas (vitales en las crisis, fuente de malentendidos a diario). Salvo estricta necesidad, es terriblemente costoso cambiar definiciones.

Actividades en el CCN

En el CCN estamos desarrollando una plataforma denominada Cuadro de Mando que busca la presentación de indicadores a los gestores de los sistemas de información.

Los indicadores se derivan de mediciones del sistema como se explica anteriormente, y se presentan al usuario dependiendo de sus necesidades puntuales a corto, medio y largo plazo, de forma que pueda

- corroborar que el sistema no se desvía del comportamiento previsto
- que el sistema evoluciona hacia la posición deseada
- que el consumo de recursos es adecuado
- ... o que se requiere alguna actuación si alguno de los indicadores anteriores se sale de la pauta prevista

Es importante que diferentes niveles de gestión reciban los indicadores que les interesan para las decisiones que les son propias, pero que todos los indicadores partan de una una base común de información que permita trazar el motivo de su evolución y alinear las actuaciones a todos los niveles.

También parece importante establecer una serie de métricas (semántica de los indicadores) estándar de forma que se pueda establecer una cultura de la Administración y podamos establecer relaciones fluidas entre organismos que necesitan interconectar sus sistemas. Esto es posible en indicadores de implantación y de eficacia y eficiencia, aunque será más complejo de uniformizar en indicadores de impacto, propios de la misión de cada organismo.

Además de indicadores operacionales se estan estableciendo indicadores de satisfacción de normativa legal (protección de datos de carácter personal) o de certificaciones habituales en el sector (cumplimiento de la norma 27002 de buenas prácticas en seguridad de la información).

Conclusión

Los indicadores de seguridad son necesarios para saber si un sistema de información está sano o enfermo, si progresa adecuadamente o si se aprecian problemas en el horizonte. Las métricas definen qué significa salud y qué significa mejorar y empeorar. Los indicadores son la clave para interpretar qué está ocurriendo y lo que se ve venir, y actuar con conocimiento de causa. Los cuadros de mando permiten centrar a cada uno en su role y al tiempo compartir

conocimiento y alinear actuaciones. Y, por último, cuando hay planes de interconexión, los indicadores, acompañados de su métrica, permiten adelantar posibles problemas y alinear actuaciones conjuntas.

Estamos trabajando para definir un conjunto normalizado de indicadores, con una métrica bien definida, que no adolezcan de improvisación ni dudas de interpretación.

Si quiere leer más ...

- NIST Special Publication 800-55: “Security Metrics Guide for Information Technology Systems”, July 2003. (En revision)
- NIST Special Publication 800-80: "Guide for Developing Performance Metrics for Information Security", May 2006.
- R.B. Vaughn, et al: “Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy”. Proc. 36th Hawaii international Conference on System Sciences. January 2003.