SIC

www.revistasic.com

Nº 62

Noviembre 2004 - Año XIII

Mark Aslett,
Presidente y Director de Operaciones de Enterasys

Federico de la Mora,
Responsable para España de RSA Security

Clasificación de métricas de seguridad

Inseguridad en plataformas VoIP

El eslabón débil de la firma electrónica

- Adquira
- Arsys Internet
- Ceres-FNMT
- DNI-e belga
- Junta de Andalucía
- Mº de Justicia
- Telefónica Empresas

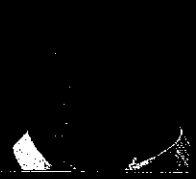
ENTREVISTA

Santiago Moral Rubio,
Director de Seguridad Lógica Corporativa del Grupo BBVA

SIC
Nº 62
Noviembre 2004

>> Sumario

>> Diseño portada: ExtraGráfica



>> en este número

Laboratorio SIC

Edita: Ediciones CODA, S.L. Lombia, 3 - 28009 Madrid (España) Tels.: 91 401 06 26 / 91 309 04 99 Fax: 91 401 09 90 Correo-e: info@revistasic.com / info@codasic.com www.revistasic.com **Editor:** Luis Guillermo Fernández Delgado **Director:** José de la Peña Muñoz **Redacción:** Virgina Moreno Bango **Sección Laboratorio SIC:** Javier Areitio Bertolín **Colaboran en este número:** Rafael Ausejo, Juan Carlos Cañete , Pablo Carretero, Carlos Cela, Juan Carlos Cruellas, Jorge Dávila Muro, José de la Peña Sánchez, Francisco Javier Fernández, Andrés Fernández Baltanás, Eduardo Fernández-Medina, Javier Fernández-Sanguino, Miguel Hormigo, Francisco Jordán, Casimiro Juanes, José Luis Manzano, Francisco Marco, Marc Martínez, Manel Medina, Carlos Molina, Mario Piattini, Francisco Sancho, Miguel Solano, Daniel Solís, Juan Miguel Velasco, Carlos Villarrubia **Coordinación de Marketing/Publicidad:** Rafael Armisén Gil **Administración y suscripciones:** Susana Montero, Maite Montero **Fotografía:** Jesús A. de Lucas **Diseño y Maquetación:** Miguel Salgueiro, Elena Suárez, Fernando Halcón **Diseño y Producción:** EXTRA Comunicación Gráfica Tel: 91 562 36 28 **Imprime:** Gráficas Ruiz Polo, S.A. **ISSN:** 1136-0623 **Depósito Legal:** GU-132/96

Hacia una clasificación de métricas de seguridad

Para la generación de confianza en el uso de las TIC es necesario demostrar la seguridad de estas tecnologías. Las métricas de seguridad son el método más apropiado para generar esa confianza. En este artículo se proponen una serie de características para clasificar las métricas de seguridad y se presentan las principales conclusiones obtenidas con esta clasificación junto con las métricas analizadas. Este trabajo, presentado en la recientemente celebrada VIII RECSI, es parte de la investigación de los proyectos Calipo y Messenger, adscritos respectivamente al antiguo Mº de Ciencia y Tecnología y a la Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha.

Carlos Villarrubia
Eduardo Fernández-Medina
Mario Piattini

INTRODUCCIÓN

La información y sus procesos de soporte, junto con los sistemas y redes son recursos importantes para cualquier organización. Estos recursos están sometidos continuamente a riesgos e inseguridades provenientes de una gran variedad de fuentes, donde se incluyen amenazas basadas en código malicioso, errores de programación, errores de las personas, sabotajes o incendios.

Según [1], las pérdidas producidas solamente por código malicioso sobrepasaron los trece mil millones de dólares en 2001, y el gasto en seguridad calculado para 2004 supera los tres mil millones de dólares.

Esta preocupación ha impulsado a muchas organizaciones e investigadores a proponer distintas métricas para evaluar la seguridad de sus sistemas de información. En general, existe un consenso en afirmar que la elección de estas métricas depende de las necesidades concretas de seguridad de cada organización. La mayoría de las propuestas analizadas proponen metodologías para la elección de estas métricas [2,3,4,5,6,7]. Incluso en algunos casos, se sugiere la necesidad de desarrollo de metodologías específicas para cada organización [8].

En cualquiera de las propuestas, la necesidad es cuantificar los distintos aspectos de la seguridad para poder comprender, controlar y mejorar la confianza en el sistema de información. Si una organización no usa métricas de seguridad para su toma de decisiones, las elecciones estarán motivadas por aspectos subjectivos, presiones externas e inclusive motivaciones puramente comerciales.

MÉTRICAS DE SEGURIDAD

Clasificación de métricas

Para el análisis de las diferentes métricas propuestas es necesario utilizar distintos enfoques para su clasificación y así poder obtener conclusiones. La selección de estos criterios de clasificación está basada en las diferentes propuestas anteriores [9,3,4,7], teniendo en cuenta que cubren distintas necesidades de la seguridad de una organización, eliminando las repeticiones en diferentes propuestas y seleccionando aquellos enfoques con mayor nivel de generalidad.

Las criterios seleccionados para clasificar las métricas de seguridad corresponden a los distintos objetivos de seguridad perseguidos, las áreas de control usadas para conseguir esos objetivos, el momento cuando esos controles son usados y el tipo de persona a la cual está dirigida la métrica.

1. Objetivo de Seguridad (OS). La seguridad de un sistema de información está caracterizada por la persecución de los siguientes objetivos:

– Confidencialidad, asegurando que sólo acceden a la información los usuarios legítimos.

– Integridad, ofreciendo garantías contra las modificaciones no autorizadas de la información.

– Disponibilidad, asegurando que los usuarios autorizados pueden acceder a la información y sus recursos asociados cuando sea necesario.

– Autenticación, comprobando que la identidad de las personas y los sistemas es cierta.

En este estudio, se ha incluido un objetivo general para caracterizar aquellas métricas que persiguen dos o más objetivos de seguridad.

2. *Área de Control (AC).* Los objetivos anteriores son alcanzados usando distintos controles en el sistema de información. Según [9], los distintos tipos de controles empleados para alcanzar los objetivos de seguridad se pueden clasificar en:

– Gestión. Estos controles de seguridad pueden ser caracterizados de tipo gerencial. En general, están orientados a la administración de la política de seguridad y a la gestión de riesgos en la organización.

– Operacionales. Son controles de seguridad implementados y ejecutados por personas (a diferencia de los sistemas).

– Técnicos. Controles de seguridad que un sistema informático ejecuta.

3. *Dimensión Temporal (DT).* Desde el punto de vista de gestión de riesgos, los controles usados pueden ser aplicados en diferentes instantes:

– Preventivos. Diseñados para reducir el nivel de impacto de una amenaza.

– Detección. Usados para detectar una amenaza.

– Correctivos. Implementados para ayudar a disminuir el impacto de una amenaza.

– Recuperación. Permiten la recuperación de un sistema a un estado previo al ataque.

4. *Público Objetivo (PO).* Las métricas de seguridad tienen la misión principal de informar de los distintos aspectos de seguridad. [7] clasifica una métrica dependiendo del siguiente público objetivo:

– Técnico. Personal técnico de la organización.

– Ejecutivos. Las distintas personas responsables de una empresa.

– Autoridades Externas. Cualquier entidad externa a la cual la organización deba informar sobre la situación de la seguridad de la institución.

Características de las métricas

La información del apartado anterior puede ser más útil si está acompañada por información adicional sobre las propiedades de las métricas que puede ayudar a discriminar entre métricas con la misma funcionalidad y propósito. Basado en la propuesta de [10], se distinguen seis características para cualquier métrica. El primer grupo identifica tres propiedades básicas (intrínsecas) de una métrica. Las otras tres características determinan si la métrica ha sido validado o no, la clase de validación utilizada (teórica o empírica), y si la métrica tiene una herramienta que automatiza su proceso de medida.

1. *Objetiva/Subjetiva (O/S).* Una métrica es objetiva si sus valores son calculados por un algoritmo o fórmula matemática. Por el contrario, una métrica es subjetiva si sus medidas son (total o parcialmente) suministradas por una persona. En el caso de las métricas subjetivas, es importante registrar la persona o experto que realizó la evaluación y suministra los valores.

2. *Directa/Indirecta (D/I).* Se-

gún ISO 9126, una medida directa es una medida de un atributo que no depende de la medida de ningún otro atributo. En cambio, una medida indirecta es una medida que se deriva de la medida de dos o más atributos.

3. *Estática/Dinámica (E/D).* Esta característica clasifica una métrica dependiendo del momento en que puede ser medida. En las métricas dinámicas sólo se pueden medir durante la operación del sistema, actuando en algún componente del sistema evaluado. Las medidas estáticas pueden ser obtenidas basándose exclusivamente en las propiedades de los componentes del sistema. Ejemplos de métricas dinámicas son el porcentaje de medios desechados comprobados antes de su eliminación o el número de intentos de intrusión detectados. Las métricas estáticas incluyen el porcentaje de sistemas con un plan de contingencia o el porcentaje de equipos portátiles con mecanismos de cifrado para archivos sensibles.

4. *Validación Teórica (VT).* El principal objetivo de la validación teórica es comprobar que la métrica realmente mide aquello que se persigue [11]. La validación teórica puede ayudar a conocer cuando y cómo se aplica la métrica. En esta clasificación, esta característica indica si la métrica ha sido validada teóricamente y el método utilizado. Aunque se han propuesto varios métodos y principios para la validación teórica de métricas (principalmente en el contexto de ingeniería del software), no existe todavía una propuesta ampliamente aceptada. Actualmente, las dos principales propuestas son:

– Enfoques basados en la teoría de la medida como los propuestos por [12], [13], y [14].

– Enfoques basados en propiedades (también llamados enfoques axiomáticos), como los propuestos por [15] y [16,17].

5. *Validación Empírica (VE).* La validación empírica intenta demostrar con evidencias reales que la métrica satisface su objetivo y que son útiles en la práctica. Existen tres tipos de estrategias en la investigación empírica:

– Experimentos. Los experimentos son investigaciones controladas, rigurosas y formales. Son utilizados cuando se desea controlar una situación y manipular directamente su comportamiento de forma precisa y sistemática. Por lo tanto, el objetivo es manipular una o más variables y fijar el resto de variables a unos valores predeterminados. Un experimento puede ser realizado en una situación no real, por ejemplo, en un laboratorio con condiciones controladas, donde los eventos son organizados para simular un entorno parecido al mundo real. Alternativamente, los experimentos pueden ser realizados en un entorno real donde la investigación se realiza en condiciones normales [18,19].

– Casos de estudio. Un caso de estudio es un análisis por observación, por ejemplo, realizado por la observación de un proyecto o actividad. El caso de estudio normalmente tiene como objetivo el registro de un atributo específico o establecer relaciones entre diferentes atributos. En cualquier caso, el nivel de control en un caso de estudio es menor que en un experimento [20].

– Encuestas. Una encuesta es típicamente una investigación realizada de forma retrospectiva cuando, por ejemplo, una herramienta o técnica ha sido usada durante un período de tiempo. El método principal de recogida de los datos cuantitativos o cualitativos son cuestionarios o entrevistas. Estos son recogidos tomando muestras representativas de la población estudiada. Los resultados de la encuesta son analizados para obtener conclusiones explicativas o descriptivas. En general, las encuestas no permiten controlar el entorno de obtención de la medida, aunque es posible comparar aquellas que sean similares [21].

6. *Automatización (A).* Esta característica indica cuándo la métrica tiene una herramienta específica para su tratamiento. No sólo un soporte metodológico sino también tecnológico es necesario para el uso efectivo de las métricas en un entorno productivo [22].

ANÁLISIS DE LAS MÉTRICAS DE SEGURIDAD PROPUESTAS

Como ya se ha expuesto, actualmente están apareciendo distintas métricas de seguridad. Para el presente estudio, se ha analizado la literatura existente en estos temas, buscando métricas que puedan ofrecer información interesante para la descripción, comparación o predicción de cualquier aspecto relacionado con la seguridad de un sistema de información. Con este objetivo, se han descartado algunas métricas porque no ofrecían una descripción suficiente para poder determinar algunos valores de las características utilizadas para clasificar las métricas. Ejemplos de estas métricas son aquellas usadas para describir metodologías para la construcción de las métricas. También se han descartado métricas repetidas que estaban propuestas por autores distintos. En este caso, sólo se ha incluido una métrica. Finalmente, han sido seleccionadas 57 métricas de 85 propuestas diferentes y que están incluidas en el apéndice de este artículo.

Con respecto a los criterios de clasificación específicos a la seguridad, los resultados han sido los siguientes:

– Objetivo de Seguridad: 74% de las métricas son generales, el 9% son métricas de disponibilidad y autenticación respectivamente, el 7% son métricas de confidencialidad y sólo una métrica es específica a la integridad.

– Área de Control: 44% son métricas operacionales, el 30% son relativas al área técnica y el resto son métricas de gestión.

– Dimensión Temporal: 84% son métricas preventivas, el 10% son de detección y el 3% son métricas correctivas y de recuperación respectivamente.

– Público Objetivo: 44% son métricas para ejecutivos, el 39% son para personal técnico y el resto para autoridades externas.

Después de evaluar las características generales de las métricas, el resumen de los resultados obtenidos es el siguiente:

– Objetiva/Subjectiva: 96% de las métricas son objetivas y el resto subjetivas.

– Directa/Indirecta: 61% de las métricas son indirectas y el resto directas.

– Estáticas/Dinámicas: 63% de las métricas son estáticas y el resto dinámicas.

– Validación Teórica: Ninguna de las métricas analizadas ha sido validada teóricamente.

– Validación Empírica: Sólo una de las métricas ha sido validada empíricamente, e inclusive, ninguna del resto de métricas propuestas tiene como trabajo futuro la utilización de algún método de validación empírica.

– Automatización: Sólo una de las métricas analizadas tiene una herramienta de soporte.

Estos resultados ofrecen la siguiente visión del perfil de las métricas analizadas:

– Como se esperaba, la mayoría de las métricas propuestas son de tipo general y esta clase de métricas sólo miden acciones genéricas relativas a la seguridad y en una forma indirecta los objetivos específicos como confidencialidad, integridad y disponibilidad.

– La mayor parte de las métricas tienen un carácter preventivo mostrando la importancia concedida a la evitación de los problemas de seguridad.

– Con respecto al área de control y el público objetivo, existe un equilibrio razonable indicando que las métricas propuestas cubren estos aspectos de forma correcta.

– La mayoría de las métricas son objetivas. Esto es positivo pues esta clase de métricas son más fiables y fáciles de automatizar.

– Un número importante de métricas son directas. Aunque estas métricas son importantes, son un primer paso hacia el objetivo final de satisfacer las necesidades de información del usuario. En este aspecto, las métricas indirectas ofrecen más información que las métricas directas y los indicadores están normalmente basados en estas métricas indirectas.

– La escasez de validación y automatización de métricas es

común a todas las disciplinas donde la aplicación de métricas es todavía inmadura, y claramente, ofrece un área de investigación que necesita un esfuerzo para obtener herramientas y métodos de ingeniería productivos.

CONCLUSIONES Y TRABAJO FUTURO

En este artículo se presentan los resultados del análisis que se ha realizado con las métricas de seguridad existentes más representativas. Los resultados obtenidos muestran la distribución de las métricas y, más importante, las áreas con escasez de métricas que requieren de la definición de nuevas métricas, específicas a estas áreas.

Existen distintas extensiones posibles a este trabajo. En primer lugar, es necesario continuar clasificando las métricas venideras, para poder confirmar y validar las conclusiones extraídas en esta clasificación inicial y poder analizar las tendencias en el tiempo de las nuevas métricas. También es necesario empezar a analizar la importancia relativa de estas métricas para la consecución de los objetivos de seguridad. De esta forma, las propuestas posteriores podrán ser usadas para priorizar el uso de las métricas. También es útil analizar la dificultad en la obtención de las métricas y guiar en su modificación para ser más útiles.

La caracterización propuesta para las métricas de seguridad no es completa porque algunas de éstas tienen los mismos valores para todas las di-

APÉNDICE >>> MÉTRICAS ANALIZADAS, DIMENSIONES Y CARACTERÍSTICAS

OG	AC	DT	PO	O/S	D/I	S/D	VT	VE	A
D	O	P	T	O	I	S	N		
D	O	P	A	O	I	S	N		
D	O	P	A	O	I	S	N		
D	O	R	E	O	D	D	N		
D	T	D	E	O	D	D	N		
AU	O	P	E	O	I	S	N		
AU	O	P	E	O	I	S	N		
AU	O	D	T	O	D	D	N		
AU	T	P	T	O	I	S	N		
AU	T	P	T	O	I	S	N		
C	O	P	E	O	I	S	N		
C	O	P	T	O	I	D	N		
C	T	P	T	O	D	D	N		
C	T	P	T	O	I	S	N		
G	G	P	E	O	D	D	N		
G	G	P	E	O	D	S	N		
G	G	P	E	O	D	S	N		
G	G	P	E	O	D	S	N		
G	G	P	E	O	I	S	N		

OG	AC	DT	PO	O/S	D/I	S/D	VT	VE	A
G	G	P	E	O	I	S	N		
G	G	P	E	O	I	S	N		
G	G	P	E	O	I	S	N		
G	G	P	E	S	D	D	N		H
G	G	P	A	O	I	S	N		
G	G	P	A	O	I	S	N		
G	G	P	A	O	I	S	N		
G	G	P	A	O	I	S	N		
G	G	R	A	O	I	S	N		
G	G	R	E	S	D	D	N		
G	O	P	T	O	I	S	N		
G	O	P	T	O	I	S	N		
G	O	P	T	O	I	S	N		
G	O	P	T	O	I	S	N		
G	O	P	T	O	I	S	N		
G	O	P	E	O	D	D	N		

mensiones y características. Un trabajo futuro es refinar esta caracterización para que cada métrica sea diferente en la clasificación.

Finalmente, los indicadores deben ser definidos en función del tamaño de la organización y el sector (por ejemplo, sector público y sector privado) porque no es realista tener un buen conjunto de métricas que sean útiles para todas las organizaciones. ■

CARLOS VILLARRUBIA
Carlos.Villarrubia@uclm.es
EDUARDO FERNÁNDEZ-MEDINA
Eduardo.FdezMedina@uclm.es
MARIO PIATTINI
Mario.Piattini@uclm.es
Grupo de Investigación Alarcos
UNIVERSIDAD DE CASTILLA-LA MANCHA

>>>

DESCRIPCIÓN	OS	AC	DT	PO	O/S	D/I	S/D	VT	VE	A
Porcentaje	G	O	P	E	O	I	D	N		
Porcentaje	G	O	P	E	O	I	S	N		
Porcentaje	G	O	P	E	O	I	S	N		
Porcentaje	G	O	P	E	O	I	S	N		
Número	G	O	P	A	O	D	D	N		
Porcentaje	G	O	P	A	O	I	D	N		
Porcentaje	G	O	P	A	O	I	S	N		
Porcentaje	G	O	C	T	O	D	D	N		
Porcentaje	G	O	C	E	O	I	D	N		
Número	G	O	D	E	O	D	D	N		
Número	G	T	P	T	O	D	D	N		
Porcentaje	G	T	P	T	O	D	S	N		
Número	G	T	P	T	O	D	S	N		
Porcentaje	G	T	P	T	O	D	S	N		
Porcentaje	G	T	P	T	O	I	D	N		
Porcentaje	G	T	P	T	O	I	D	N		
Porcentaje	G	T	P	T	O	I	S	N		
Porcentaje	G	T	P	T	O	I	S	N		
Cantidad	G	T	P	E	O	D	D	N	1E	
Número	G	T	D	E	O	D	D	N		
Número	G	T	D	E	O	D	D	N		
Número	I	T	P	T	O	D	S	N		

REFERENCIAS