AVANCES EN CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN

Benjamín Ramos Álvarez
Arturo Ribagorda Garnacho
(Directores)

RECSI
REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN VIII

DÍAZ DE SANTOS

Benjamín Ramos Álvarez
Arturo Ribagorda Garnacho
(Directores)

AVANCES EN CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN

Co-Directores:
Julio C. Hernández Castro
José M.ª Sierra Cámara

DIAZ DE SANTOS

Benjamín Ramos Álvarez
Arturo Ribagorda Garnacho
(Directores)

AVANCES EN CRIPTOLOGÍA Y SEGURI DE LA INFORMACIÓN

Co-D
Julio C. Hernánc
José M.ª Sier

DIAZ DE SANTOS

Ediciones Díaz de Santos, S. A.
Doña Juana I de Castilla, 22
28027 MADRID
www.diazdesantos.es/ediciones
ediciones@diazdesantos.es

ISBN: 84-7978-650-7
Depósito legal: M. 37.736-2004

Diseño de Cubierta:
Fotocomposición e impresión: Fernández Ciudad, S. L.
Encuadernación: Rústica-Hilo, S. L.

Impreso en España

AGRADECIMIENTOS

Una reunión científica como esta que nos ocupa no podría celebrarse sin la co confianza de diversas personas y entidades. Por ello es de justicia que el Comité agradezca a todos ellos su colaboración y en especial a los organismos y empresas trocinado esta RECSI'04: Ministerio de Educación y Ciencia, Universidad Carlc drid, Computer Associates, Accenture, Revista SIC, Criptored y Secuware. Así mis debemos agradecer la colaboración de Zona Multimedia en el diseño gráfico.

ÍNDICE DE CAPÍTULOS

Parte II
CRIPTOANÁLISIS

Parte III
PROTOCOLOS CRIPTOGRÁFICOS Y VALIDACIÓN

Parte IV
SEGURIDAD EN SISTEMAS DE INFORMACIÓN (BD, aplicaciones, etc.)

Parte V
SEGURIDAD EN REDES E INTERNET

Parte VI
SERVICIOS DE CERTIFICACIÓN Y NOTARIZACI

Parte VII
SEGURIDAD EN DRM

Anexos
UNA VISIÓN EMPRESARIAL

6. AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el Ministerio de Ciencia y Tecnología, a través de sus proyectos TIC-2003-02041 y TIC2001-5108-E.

Referencias

[1] J. Ametller, S. Robles, and J.A. Ortega-Ruiz. Self-protected mobile agents. In *3rd International Conference on Autonomous Agents and Multi Agents Systems*. To appear., 2004.

[2] W. M. Farmer, J. D. Guttman, and V. Swarup. Security for mobile agents: Issues and requirements. In *proceedings of the National Information Systems Security Conference*, pages 591.597, 1996.

[3] J. Mir and J. Borrell. Protecting mobile agent itineraries. In *Mobile Agents for Telecommunication Applications (MATA)*, volume 2881 of *Lecture Notes in Computer Science*, pages 275.285. Springer Verlag, October 2003.

[4] S. Robles, J. Mir, J. Ametller, and J. Borrell. Implementation of secure architectures for mobile agents in marisma. In *Mobile Agents for Telecommunication Applications (MATA)*, volume 2521 of *Lecture Notes in Computer Science*, pages 182.191. Springer Verlag, 2002.

[5] S. Robles, J. Mir, and J. Borrell. Marism-a: An architecture for mobile agents with recursive itinerary and secure migration. In *2nd. IW on Security of Mobile Multiagent Systems*, Bologna, July 2002.

[6] V. Roth. Empowering mobile software agents. In *Proc. 6th IEEE Mobile Agents Conference*, volume 2535 of *Lecture Notes in Computer Science*, pages 47.63. Spinger Verlag, 2002.

[7] M. Straßer, K. Rothermel, and C. Maiöfer. Providing Reliable Agents for Electronic Commerce. In *Proceedings of the International IFIP/GI Working Conference*, volume 1402 of *Lecture Notes in Computer Science*, pages 241.253. Springer-Verlag, 1998.

[8] James E. White. Telescript technology: Mobile agents. In Jeffrey Bradshaw, editor, *Software Agents*. AAAI Press/MIT Press, 1996.

39

HACIA UNA CLASIFICACIÓN DE MÉTRICAS DE SEGUF

Carlos Villarrubia, Eduardo Fernández-Medina y Mario Piattini
Universidad de Castilla - La Mancha, Grupo de Investigación Alarcos
Paseo de la Universidad, 4, 13071, Ciudad Real(España),
{Carlos.Villarrubia, Eduardo.FdezMedina, Mario.Piattini}@uclm.es [1]

Resumen. Para la generación de confianza en el uso de las tecnologías de la infor comunicaciones es necesario demostrar la seguridad de estas tecnologías. Las métricas de el método más apropiado para generar esa confianza. En este artículo se proponen características para clasificar las métricas de seguridad. Finalmente, se presentan l conclusiones obtenidas con esta clasificación junto con las métricas analizadas.

1. INTRODUCCIÓN

La información y sus procesos de soporte, junto con los sistemas y redes sc importantes para cualquier organización. Estos recursos están sometidos contir riesgos e inseguridades provenientes de un gran variedad de fuentes, donde s amenazas basadas en código malicioso, errores de programación, errores de la sabotajes o incendios.

Según [1], las perdidas producidas solamente por código malicioso sobrej trece mil millones de dólares en 2001, y el gasto en seguridad calculado para 200 tres mil millones de dólares.

Esta preocupación ha impulsado a muchas organizaciones e investigadores distintas métricas para evaluar la seguridad de sus sistemas de información. En ger un consenso en afirmar que la elección de estas métricas depende de las necesidade de seguridad de cada organización. La mayoría de las propuestas analizadas metodologías para la elección de estas métricas [2,3,4,5,6,7]. Incluso en alguno sugiere la necesidad de desarrollo de metodologías específicas para cada organizaci

En cualquiera de las propuestas, la necesidad es cuantificar los distintos asp seguridad para poder comprender, controlar y mejorar la confianza en el información.

Si una organización no usa métricas de seguridad para su toma de deci elecciones estarán motivadas por aspectos subjectivos, presiones externas motivaciones puramente comerciales.

2. MÉTRICAS DE SEGURIDAD

2.1. Clasificación de Métricas

Para el análisis de las diferentes métricas propuestas es necesario utilizar distinto para su clasificación y así poder obtener conclusiones. La selección de estos

[1] Esta investigación es parte del proyecto CALIPO, financiado por la Dirección General de Investigaci *Ministerio de Ciencia y Tecnología (TIC2003-07804-C05-03), y el proyecto MESSENGER, financiad* Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha (PCC-03-003-

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 accede 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 utilizando distintos controles en el sistema de información. Según [9], los distintos tipos de controles utilizados 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 or informar sobre la situación de la seguridad de la institución.

2.2. Características de las Métricas

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

1. Objetiva/Subjetiva (O/S). Una métrica es objetiva si sus valores son ca algoritmo o fórmula matemática. Por el contrario, una métrica es subjetiva son (total o parcialmente) suministrados por una persona. En el caso e subjetivas, es importante registrar la persona o experto que realizó la evaluaci los valores.

2. Directa/Indirecta (D/I). Según ISO 9126, una medida directa es una medid que no depende de la medida de ningún otro atributo. En cambio, una med una medida que se deriva la medida de dos o más atributos.

3. Estática/Dinámica (E/D). Esta característica clasifica una métrica de momento en que puede ser medida. En las métricas dinámicas sólo se pueden la operación del sistema, actuando en algún componente del sistema evaluad estáticas pueden ser obtenidas basándose exclusivamente en las propi componentes del sistema. Ejemplos de métricas dinámicas son el porcent desechados comprobados antes de su eliminación o el número de intento detectados. Las métricas estáticas incluyen el porcentaje de sistemas co contingencia o el porcentaje de equipos portátiles con mecanismos de cifrados sensibles.

4. Validación Teórica (VT). El principal objetivo de la validación teórica es c la métrica realmente mide aquello que se persigue [11]. La validación teórica p conocer cuando y cómo se aplica la métrica. En esta clasificación, esta caract si la métrica ha sido validada teóricamente y el método utilizado. Aunque se varios métodos y principios para la validación teórica de métricas (princip contexto de ingeniería del software), no existe todavía una propuesta ampliam Actualmente, las dos principales propuestas son:

- Enfoques basados en la teoría de la medida como los propuestos por [14].
- Enfoques basados en propiedades (también llamados enfoques axiom 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 uno o más variables y fijar el resto de variables a una valores predeterminados. Un experimento puede ser realizada 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 estudios. 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 cuando 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].

3. ANÁLISIS DE LAS MÉTRICAS DE SEGURIDAD PROPUESTAS

Como se ha mencionado en la introducción, actualmente están apareciendo distintas métricas de seguridad. Para el presente estudio, se ha analizado la literatura existente en estos tópicos, 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 utilizadas 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, 57 métricas han sido seleccionados 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% sor disponibilidad y autenticación respectivamente, el 7% son confidencialidad y sólo una métrica es específica a la integridad.
- Área de Control: 44% son métricas operacionales, el 30% son rela técnica y el resto son métricas de gestión.
- Dimensión Temporal: 84% son métricas preventivas, el 10% son de d 3% son métricas correctivas y de recuperación respectivamente.
- Público Objetivo: 44% son métricas para ejecutivos, el 39% son p técnico y el resto para autoridades externas.

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

- Objetiva/Subjectiva: 96% de las métricas son objetivas y el resto subjet
- Directa/Indirecta: 61% de las métricas son indirectas y el resto directas.
- Estáticas/Dinámicas: 63% de las métricas son estáticas y el resto dinámi
- Validación Teórica: Ninguna de las métricas analizadas ha sic teóricamente.
- Validación Empírica: Sólo una de las métricas ha sido validada empír inclusive, ninguna del resto de métricas propuestas tiene como traba utilización de algún método de validación empírica.
- Automatización: Sólo una de las métricas analizadas tiene una herr 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 ge clase de métricas sólo miden acciones genéricas relativas a la segurida forma indirecta los objetivos específicos como confidencialidad, in disponibilidad.
- La mayor parte de las métricas tienen un carácter preventivo mc importancia concedida a la evitación de los problemas de seguridad.
- Con respecto al área de control y el público objetivo, existe un equilibric indicando que las métricas propuestas cubren estos aspectos de forma cor
- La mayoría de las métricas son objetivas. Esto es positivo pues est métricas son más fiables y fáciles de automatizar.
- Un número importante de métricas son directas. Aunque estas mé importantes, son un primer paso hacia el objetivo final de satisfacer las n de información del usuario. En este aspecto, las métricas indirectas of información que las métricas directas y los indicadores están normalmen en estas métricas indirectas.
- La escasez de validación y automatización de métricas es común a disciplinas donde la aplicación de métricas es todavía inmadura, y el ofrece un área de investigación que necesita un esfuerzo para obtener her y métodos de ingeniería productivos.

4. 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 dimensiones 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.

Referencias

[1] Mercuri, R.T.: Analyzing security costs. Communications of the ACM 46 (2003) 15–18
[2] Swanson, M., Bartol, N., Sabato, J., Hash, J., Graffo, L.: Security metrics guide for information technology systems. Technical Report NIST 800-55, National Institute of Standards and Technology (2003)
[3] Vaughn, Jr., R.B., Henning, R., Siraj, A.: Information assurance measures and metrics - state of practice and proposed taxonomy. In: Proceedings of the 36th Hawaii International Conference on Systems Sciences. (2003)
[4] Bouvier, P., Longeon, R.: Le tableau de bord de la sécurité du système d'information. Sécurité Informatique (2003)
[5] Nielsen, F.: Approaches of security metrics. Technical report, NISTCSSPAB (2000)
[6] Payne, S.C.: A guide to security metrics. Technical report, SANS Institute (2001)
[7] ACSA, ed.: Proceedings of the Workshop on Information Security System Scoring and Ranking, Williamsburg, Virginia (2001)
[8] Colado, C., Franco, A.: Métricas de seguridad: una visión actualizada. SIC. Seguridad en Informática y Comunicaciones 57 (2003) 64–66
[9] Swanson, M.: Security self-assessment guide for information technology systems. Technical Report NIST 800-26, National Institute of Standards and Technology (2001)
[10] Calero, C., Martín-Albo, J., Piattini, M., Vallecillo, M.B..A., Cechich, A.: A survey on software component metrics. Submitted to ACM Computing Surveys (2003)
[11] Fenton, N., Pfleeger, S.: Software Metrics: A Rigorous Approach. 2nd edn. Chapman Hall, London (1997)
[12] Whitmire, S.: Object Oriented Design Measurement. Wiley, New York (1997)
[13] Zuse, H.: A Framework of Software Measurement. Walter de Gruyter, Berlin (1998)
[14] Poels, G., Dedene, G.: Distance-based software measurement: Necessary and sufficient properties for software measures. Information and Software Technology 42 (2000) 35–46
[15] Weyuker, E.J.: Evaluating software complexity measures. IEEE Transactions on Software Engineering 14 (1988) 1357–1365
[16] Briand, L.C., Morasca, S., Basili, V.R.: Property-based software engineering measurement. IEEE Transactions on Software Engineering 22 (1996) 68–86

[17] Briand, L.C., Morasca, S., Basili, V.R.: Property-based software engineering measurei additivity properties. IEEE Transactions on Software Engineering 23 (1997) 196–197
[18] Juristo, N., Moreno, A.: Basics of Software Engineering Experimentation. Kluwer Ac (2001)
[19] Wohlin, C., Runeson, P., Ohlsson, M., Regnell, B., Wesslen, .A.: Experimentation in Soft An Introduction. Kluwer Academic Publishers (2000)
[20] Yin, R.: Case Study Research: Design and Methods. 2nd edn. Applied Social Research Me Sage Publications Inc, Thousand Oaks, CA (1994)
[21] Pfleeger, S., Kitchenham, B.: Principles of survey research. Software Engineering Notes 26
[22] Lavazza, L.: Providing automated support for the gqm measurement process. IEEE Softwarc
[23] Departament of the Air Force: AFI33-205. Information Protection Metrics and Measu (1997)
[24] Calero, C., Piattini, M., Genero, M.: Empirical validation of referential integrity metrics. Software Technology 43 (2001) 949–957
[25] ISO: ISO 7498-2. Open Systems Interconnection - Basic Reference Model - Part 2: Secu (1989)
[26] ISO/IEC: ISO/IEC TR 13335-1. Guidelines for the Management of IT Security. Part 1: Con of IT Security. (1996)
[27] ISO/IEC: ISO/IEC 15408. Evaluation Criteria for IT Security. (1999)
[28] ISO/IEC: ISO/IEC 17799. Code of Practice for Information Security Management. (2000)
[29] King, G.: Best security practices: An overview. In: Proceedings of the 23rd National Info Security Conference, Baltimore, Maryland, NIST (2000)
[30] Marcelo, J.M.: Identificación y Evaluación de Entidades en un Método AGR. In: S Tecnologías de la Información. AENOR (2003) 69–103
[31] McKnight, W.L.: What is information assurance? CrossTalk. The Journal of Defense Softw (2002) 4–6
[32] Schuedel, G., Wood, B.: Adversary work factor as a metric for information assurance. In: P New Security Paradigm Workshop, Ballycotton, Ireland (2000) 23–30
[33] Carnegie Mellon University Pittsburgh, Pennsylvania: SSE-CMM Model Description Doc (2003)
[34] Vaughn, Jr., R.B., Siraj, A., Dampier, D.A.: Information security system rating and ranking. Journal of Defense Software Engineering (2002) 30–32

Apéndice

Este apéndice presenta, en forma tabular, las métricas analizadas y las din características asignadas a cada una de ellas.

La información de las métricas es mostrada en columnas. La primera col contador (1 a 57). La columna dos muestra el nombre de la métrica y su descri con la referencia al artículo donde la métrica fue originalmente definida. Las colu seis muestra las dimensiones asignadas a la métrica. Finalmente, las columnas muestra los valores asignadas a las características de las métricas.

Los valores asignadas a las celdas de las columnas tres a seis tienen e significado:

- Columna OS (Objetivo de Seguridad): C (Confidencialidad), I (Inte (Disponibilidad), AU (Autenticación) y G (General).
- Columna AC (Área de Control): G (Gestión), O (Operacional) y T (Técn
- Columna DT (Dimensión Temporal): P (Preventivo), D (Detección), C (y R (Recuperación).
- Columna PO (Público Objetivo): T (Expertos Técnicos), E (Ejecuti (Autoridades Externas).

Los valores asignados a las celdas en las dos últimas columnas (Validación E Automatización) necesitan una explicación especial:

- La columna "VE" muestra cuando la métrica cuenta con algún tipo de validación empírica. Las celdas en esta columna puede estar vacía o con los siguientes valores: "IE" (validada por un experimento); o "TF" (mencionado como trabajo futuro por los autores de la métrica).
- La columna "A" indica alguna clase de herramienta automática de soporte para la métrica. Las celdas de esta columna pueden estar vacías o tener el valor "H", indicando que existe una herramienta de soporte a esta métrica. Una descripción de esa herramienta se encuentra en el artículo citado para la métrica.

Nº	Descripción de la Métrica	OS	AC	DT	PO	O/S	D/I	S/D	VT	VE	A
1	Porcentaje de archivos críticos con un sistema de copias de seguridad [2]	D	O	P	T	O	I	S	N		
2	Porcentaje de sistemas con un plan de contingencias [2]	D	O	P	A	O	I	S	N		
3	Porcentaje de sistemas con un plan de contingencias probado el último año [2]	D	O	P	A	O	I	S	N		
4	Número de utilizaciones de las copias de seguridad [4]	D	O	R	E	O	D	D	N		
5	Tiempo de caída anual de un sistema [3]	D	T	D	E	O	D	D	N		
6	Porcentaje de sistemas con una política de claves verificada [2]	AU	O	P	E	O	I	S	N		
7	Porcentaje de usuarios con permisos especiales que ha sido evaluado especialmente [2]	AU	O	P	E	O	I	S	N		
8	Número de intentos fallidos en la verificación de la identidad [3]	AU	O	D	T	O	D	D	N		
9	Porcentaje de sistemas sin claves por defecto [2]	AU	T	P	T	O	I	S	N		
10	Porcentaje de usuarios distintos [2]	AU	T	P	T	O	I	S	N		
11	Porcentajes de sitios Web con una política de confidencialidad pública [2]	C	O	P	E	O	I	S	N		
12	Porcentaje de medios formateados antes de su destrucción [2]	C	O	P	T	O	I	D	N		
13	Número de ciclos de reloj por byte cifrado [3]	C	T	P	T	O	D	D	N		
14	Porcentaje de equipos portátiles con mecanismos de cifrado para archivos sensibles [2]	C	T	P	T	O	I	S	N		
15	Frecuencia de las auditorías [4]	G	G	P	E	O	D	D	N		
16	Número de reglas por política de seguridad [4]	G	G	P	E	O	D	S	N		
17	Nivel de madurez en los procesos de desarrollo [33]	G	G	P	E	O	D	S	N		
18	Porcentaje de presupuesto asignado al programa de seguridad [3]	G	G	P	E	O	D	S	N		
19	Porcentaje de sistemas con niveles de riesgos revisados [2]	G	G	P	E	O	I	S	N		
20	Porcentaje de sistemas recertificados si los controles de seguridad han sido modificados [2]	G	G	P	E	O	I	S	N		
21	Porcentaje de sistemas operativos sin una autorización formal [2]	G	G	P	E	O	I	S	N		
22	Porcentaje de sistemas con planes de seguridad aprobados [2]	G	G	P	E	O	I	S	N		
23	Análisis de riesgos [30]	G	G	P	E	S	D	D	N		H
24	Porcentaje de sistemas con análisis de riesgos realizados y documentados [2]	G	G	P	A	O	I	S	N		
25	Porcentaje de sistemas con controles de seguridad evaluados y comprobados el último año [2]	G	G	P	A	O	I	S	N		
26	Porcentaje de sistemas con los costes de sus controles integrados en su ciclo de vida [2]	G	G	P	A	O	I	S	N		
27	Porcentaje de sistemas totales autorizados con su certificación realizada [2]	G	G	P	A	O	I	S	N		

Nº	Descripción de la Métrica	OS	AC	DT	PO	O/S	D/I	S/D
28	Porcentaje de planes de seguridad activos [2]	G	G	P	A	O	I	S
29	Valoración de la ejecución de los planes de recuperación [4]	G	G	R	E	S	D	D
30	Porcentaje de sistemas que registra las entradas y salidas de medios [2]	G	O	P	T	O	I	S
31	Porcentaje de dispositivos de transmisión de datos que tiene restringido el acceso a usuarios autorizados [2]	G	O	P	T	O	I	S
32	Porcentaje de cambios de software aprobados y documentados [2]	G	O	P	T	O	I	S
33	Porcentaje de aplicaciones propietarias documentadas [2]	G	O	P	T	O	I	S
34	Porcentaje de usuarios con acceso a software relativo a seguridad que no son administradores [2]	G	O	P	T	O	I	S
35	Número de horas empleadas en formación [4]	G	O	P	E	O	D	D
36	Porcentaje de personal formado [4]	G	O	P	E	O	I	D
37	Porcentaje de sistemas con el requerimiento de separación de funciones [2]	G	O	P	E	O	I	S
38	Porcentaje de sistemas con restricciones al personal de mantenimiento del sistema [2]	G	O	P	E	O	I	S
39	Porcentaje de sistemas con informes de valoraciones de riesgos documentadas [2]	G	O	P	E	O	I	S
40	Número de incidentes informados a FedCIRC, NIPC, y autoridades locales [2]	G	O	P	A	O	D	D
41	Porcentaje de empleados con responsabilidades de seguridad con formación especializada [2]	G	O	P	A	O	I	D
42	Porcentaje de componentes con gestión de incidencias [2]	G	O	P	A	O	I	S
43	Tiempo entre el descubrimiento de una vulnerabilidad y la aplicación de la acción correctiva [2]	G	O	C	T	O	D	D
44	Porcentajes de incidentes de seguridad ligadas al personal resueltos en la primera llamada [2]	G	O	C	E	O	I	D
45	Número de ataques detectados [4]	G	O	D	E	O	D	D
46	Número de paquetes incorrectos rechazados por el cortafuegos [3]	G	T	P	T	O	D	D
47	Número de elementos dedicados a la seguridad de la red [4]	G	T	P	T	O	D	S
48	Número de componentes con mecanismos de auditoría [4]	G	T	P	T	O	D	S
49	Evaluación del Nivel de Confianza según los Criterios Comunes [27]	G	T	P	T	O	D	S
50	Porcentaje de sistemas con los últimos parches de seguridad instalados [2]	G	T	P	T	O	I	D
51	Porcentaje de sistemas con mecanismos actualizados de detección de virus [2]	G	T	P	T	O	I	D
52	Porcentaje de sistemas ejecutando servicios restringidos [2]	G	T	P	T	O	I	S
53	Porcentaje de sistemas con mecanismos de auditoría de acciones de los usuarios [2]	G	T	P	T	O	I	S
54	Cantidad de esfuerzo del atacante [32]	G	T	P	E	O	D	D
55	Número de informes con intentos de intrusión [23]	G	T	D	E	O	D	D
56	Número de informes con intrusiones sufridas [23]	G	T	D	E	O	D	D
57	Número de sistemas con mecanismos de integridad en ficheros [4]	I	T	P	T	O	D	S