VIII Jornada Nacional de Seguridad Informática
ACIS

Métricas en Seguridad Informática:
Una revisión académica

Jeimy J. Cano, Ph.D, CFE
GECTI
Facultad de Derecho
Universidad de los Andes

jcano@uniandes.edu.co

Agenda

- Introducción
- Parte 1. La industria de la seguridad de la información, las vulnerabilidades y el factor humano
- Parte 2. La evolución de las organizaciones, la cultura organizacional y la seguridad de la información
- Parte 3. Iniciativas internacionales en el tema de Métricas en Seguridad de la Información
- Parte 4. Fundamentación conceptual de las métricas en seguridad de la Información
- Parte 5. Modelo Estratégico de Métricas en Seguridad de la Información - MEMSI
- Consideraciones del Modelo
- Reflexiones finales
- Referencias

Introducción

- Declaraciones sobre las métricas de seguridad de la información
  - Las métricas debe ser objetivas y tangibles – (F o V)
  - Las métricas deben tener valores discretos – (F o V)
  - Se requieren medidas absolutas y concretas – (F o V)
  - Las métricas son costosas – (F o V)
  - Ud no puede administrar lo que no puede medir; por tanto no puede mejorar lo que no puede administrar – (F o V)
  - Es esencial medir los resultados – (F o V)
  - Necesitamos los números para expresarnos – (F o V)

Parte 1. La industria de la seguridad de la información, las vulnerabilidades y el factor humano

La industria de la seguridad informática

¿Cómo nos vende?

- ***Uso del miedo e incertidumbre*** para crear la sensación de que estamos en el filo del abismo.
- **Productos de seguridad de la información** que son expuestos a los intrusos para que intenten quebrarlo y cuando no lo hacen, se proclaman "***imposibles de hackear***".
- ***Productos y servicios que son utilizados por una compañía específica*** o una entidad del gobierno, lo cual le ofrece al proveedor una visibilidad en el mercado.
- Los servicios y productos son sometidos a ***evaluación en revistas populares*** de la industria, las cuales emiten conceptos sobre los mismos.
- Se establecen y recomiendan por parte de los proveedores y organizaciones internacionales ***listas de chequeo, certificaciones de negocio y modelos de control*** que procuran salvaguardar a las organizaciones de los más importantes peligros en temas de seguridad de la información.
- Los productos y servicios se encuentran ***alineados con las "buenas prácticas"***, las cuales representan lo que la industria y la práctica sugieren que es lo más adecuado

Tomado de: Shostack, A. y Stewart, A. 2008. Cap. 2

Las vulnerabilidades

¿Porqué aumentan los ataques?

- Incremento en la velocidad del desarrollo tecnológico: ***Mayor curva de aprendizaje*.**
- El tiempo requerido para obtener el salario de un mes, ahora requiere un poco de paciencia, una porción de información y algunas horas de trabajo: ***Más motivación para los atacantes****.*
- El software sin errores no existe. Somos humanos y como tal debemos aceptarlo: ***Aprender y desaprender***.
- Las configuraciones actuales de la infraestructura de seguridad se hacen cada vez más complejas, por lo tanto se incrementa la probabilidad de configuraciones inadecuadas y se debilita el seguimiento al control de cambios: ***Se compromete la visión holística****.*
- La falta de coordinación transnacional de los agentes gubernamentales para tratar el tema del delito informático: ***Limitación para adelantar investigaciones****.*

El factor humano

La psicología de la seguridad en el individuo

- La seguridad ***es una sensación***, una manera de percibir un cierto nivel de riesgo.
- Existen ***personas con perfiles*** de mayor o menor apetito al riesgo.
- Las personas ***confrontan la inseguridad*** para sacar el mejor provecho de ella, bien sea para obtener mayores dividendos en un negocio o salvar incluso su vida.
- A medida que las personas se ***sienten más seguras*** con las medidas de protección, ***más propensas a los riesgos*** se vuelven.
- La psicología de la seguridad informática debe estar animada por la constante ***evolución de la percepción del individuo*** sobre la protección de los activos.

Parte 2. La evolución de las organizaciones, la cultura organizacional y la seguridad de la información

Cambios en los diseños organizacionales

- **Viejo Modelo**
  - Con límites definidos
  - Jerárquico
  - Fijo (Reglas y procedimientos)
  - Homogéneo
  - Esquema local
- **Nuevo Modelo**
  - En red
  - Aplanada
  - Flexible
  - Diverso
  - Esquema Global

Tomado y traducido de: Van Maanen, J. (2008) The changing organization: New models of the corporation. MIT Sloan School of Management. Executive Program. June

Perspectivas de análisis sobre la "nueva" organización

Diseño Estratégico

Agrupamiento, Enlaces, Alineación interna y ajuste con el ambiente

Político

Comprensión de intereses, coaliciones, escalamiento de compromisos

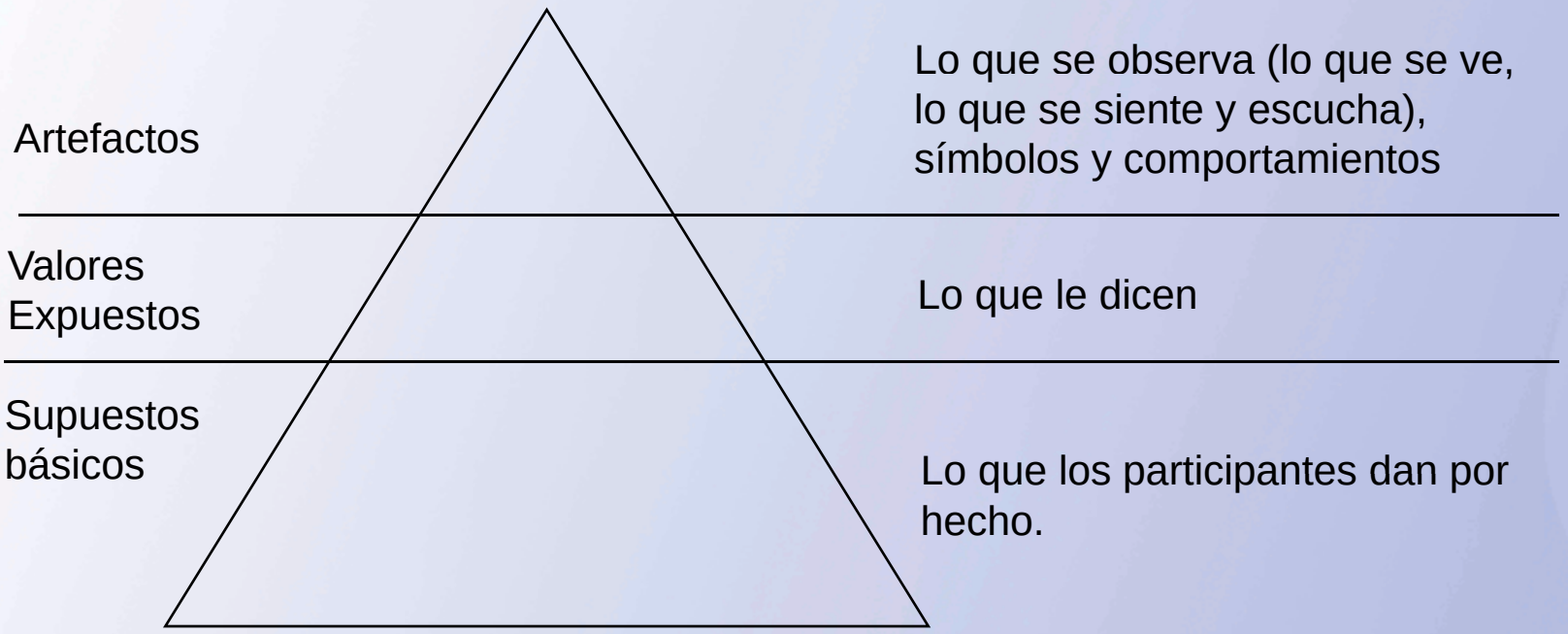
Cultural

Identidad, valores y supuestos básicos

Tomado y traducido de: Westney, E. (2008) Three perspectives on organizational change. Leading Change in Complex Organization. MIT Sloan School of Management. Executive Program. June

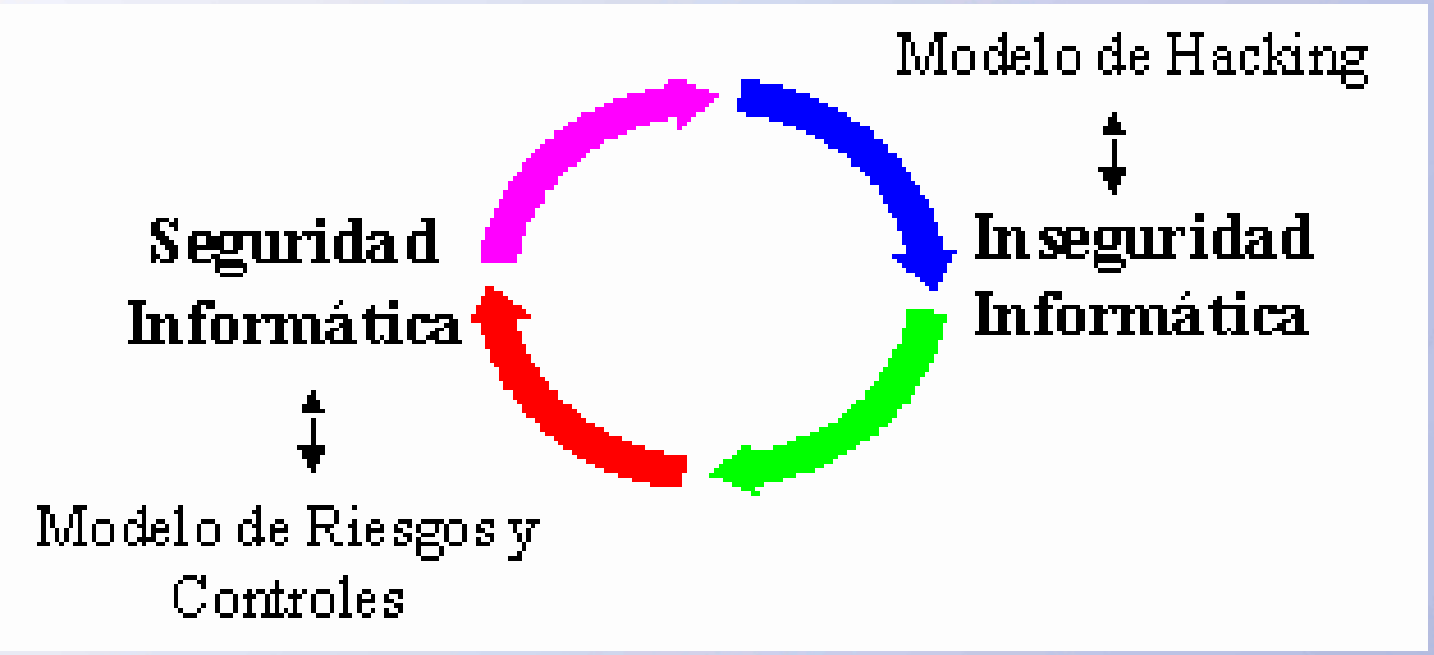
Modelo de Cultura Organizacional

E. Schein



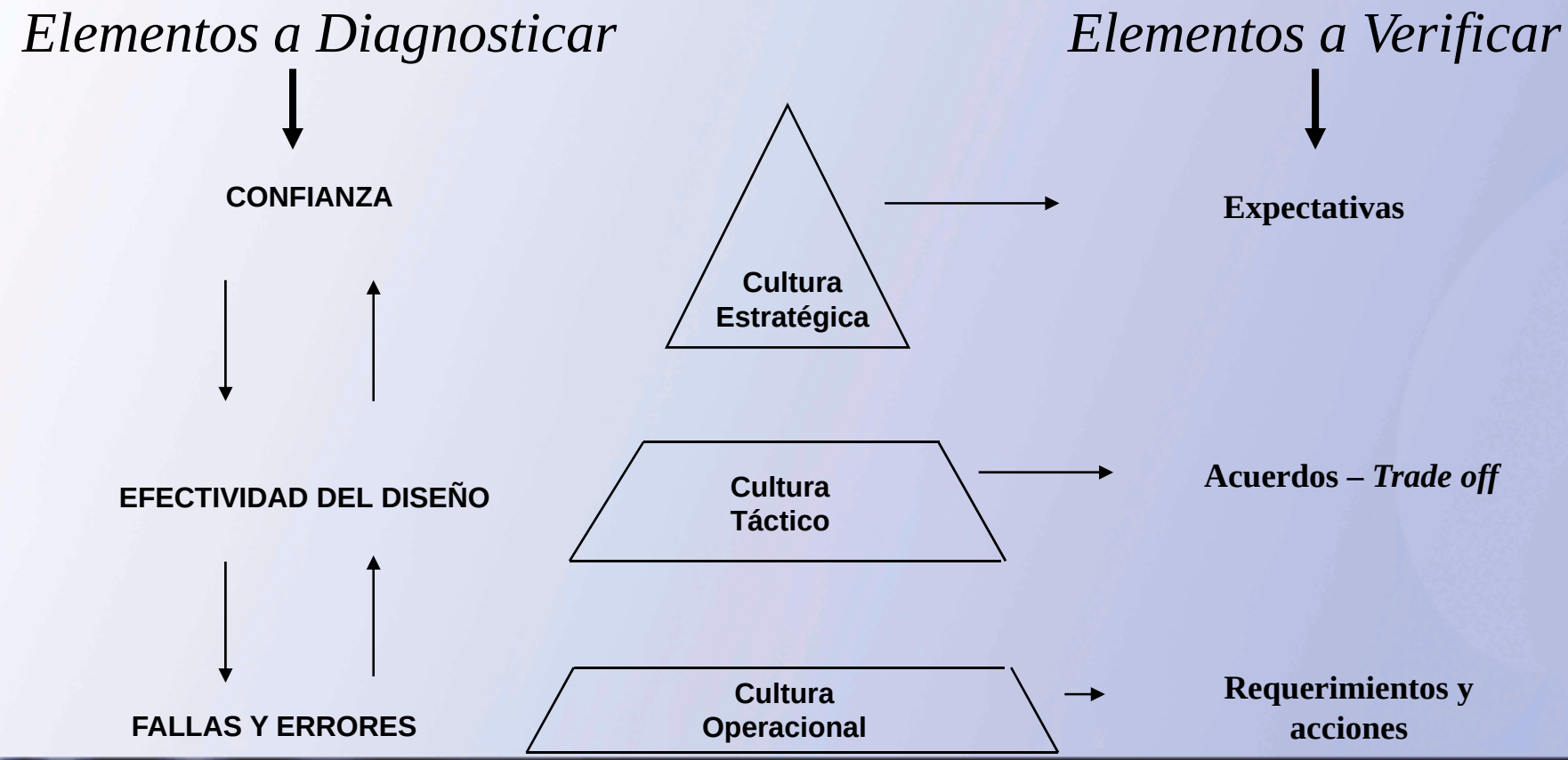
Tomado y traducido de: Westnet, E. (2008) Three perspectives on organizational change. Leading Change in Complex Organization. MIT Sloan School of Management. Executive Program. June

La Dualidad de la Seguridad de la Información



Tomado de: CANO, J. (2004) Inseguridad Informática. Un concepto dual en seguridad informática. http://www.virusprot.com/art47.html

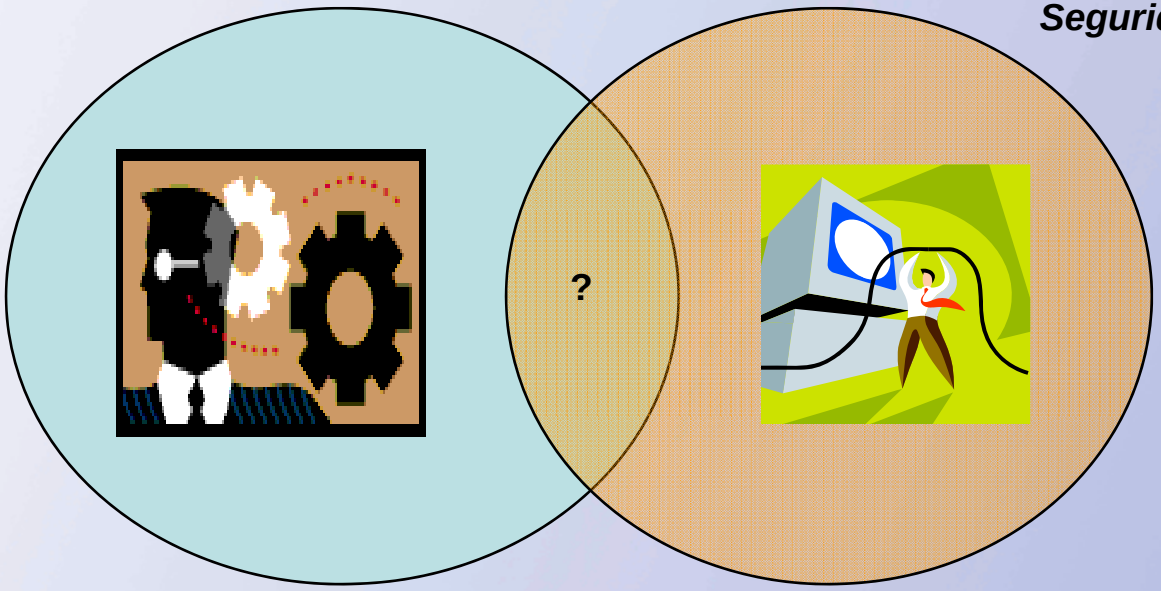
Cultura organizacional y la seguridad informática



Conflicto Natural

Visión de la Gerencia

Visión del área de Seguridad



¿Porqué tenemos más restricciones para el manejo de la información?
Esto no ayuda nuestras estrategias de negocio !

Con estos requisitos cada vez más complejos de los gerentes, tendremos que hacer cosas más elaboradas.

Parte 3. Iniciativas internacionales en el tema de Métricas en Seguridad de la Información

Iniciativas internacionales

Definition	Source
To provide meaningful data, security metrics must be based on IT security performance goals and objectives, and be easily obtainable and feasible to measure. They must also be repeatable, provide relevant performance trends over time, and be useful for tracking performance and directing resources	Security Metrics Guide for Information Technology Systems, National Institute of Standards and Technology Special Publication 800-55
A security metric is the application of quantitative, statistical and/or mathematical analyses to measuring security functional costs, benefits, successes, failures and trends and workload	Security Metrics Management, Kovacich and Halibozek, 2006
A defined form of measurement (measurement method, function of calculation or analytical model) and the scale for carrying out the measurement of one or several attributes	ISO 27004, 2005; Information security metrics and measurements (Draft)

¡ Enfoque numérico !

Tomado de: Information Security Forum (2006) Information security metrics. Pág. 5

Iniciativas internacionales

Características de las métricas

Characteristic	Comments
Title	A meaningful title (or name) to describe the security metric
Purpose	What the security metric is designed to do
Cost	An estimate or actual cost of collecting the security metric
Type	What the security metric is, for example: technical or managerial; leading or lagging; numerical or textual
Location	Where: • the data for the security metric can be collected • previous data used in the security metric is located • previous instances of the security metric can be found
Frequency	How often: • the data needs to be collected • the security metric needs to be presented
Category	The category a security metric should be placed in, such as: • how many times does something happen **(number)** • how often does something happen **(frequency)** • how long does an event last for **(duration)** • how much does an event cost **(cost)**
Start/stop criteria	Criteria for starting and stopping the: • collection of data for the security metric • use and presentation of the security metric
Duration of collection	An estimate of, or actual, time period in which data will be collected
Duration of use	An estimate of, or actual, time period in which the security metric will be used

Tomado de: Information Security Forum (2006) Information security metrics. Pág. 6

Iniciativas internacionales

Modelo de entendimiento de métricas

Components of the model for understanding security metrics	Examples of Member usage of security metrics (from Part 3)	Main issues identified
Why security metrics are used Why?	• managing information security in an organisation • providing information for management reporting • indicating compliance to legislation, regulation and standards • supporting risk management activities	• no clear purpose • difficult to relate security metrics to the business • incompatibility of security metrics with business metrics
What is currently used and collected What?	• incidents • virus protection • risk management • patch management • compliance to internal policies • audit findings • cost	• difficult to select security metrics • few high-level, business-oriented security metrics • lack of a clear, enterprise-wide view of information security
How security metrics are used and presented How?	• presented to a range of audiences • presented using a variety of different formats	• difficult to identify the correct audience • difficult to select and match the presentation format to the audience • inaccurate portrayal of information security

→ Estratégico

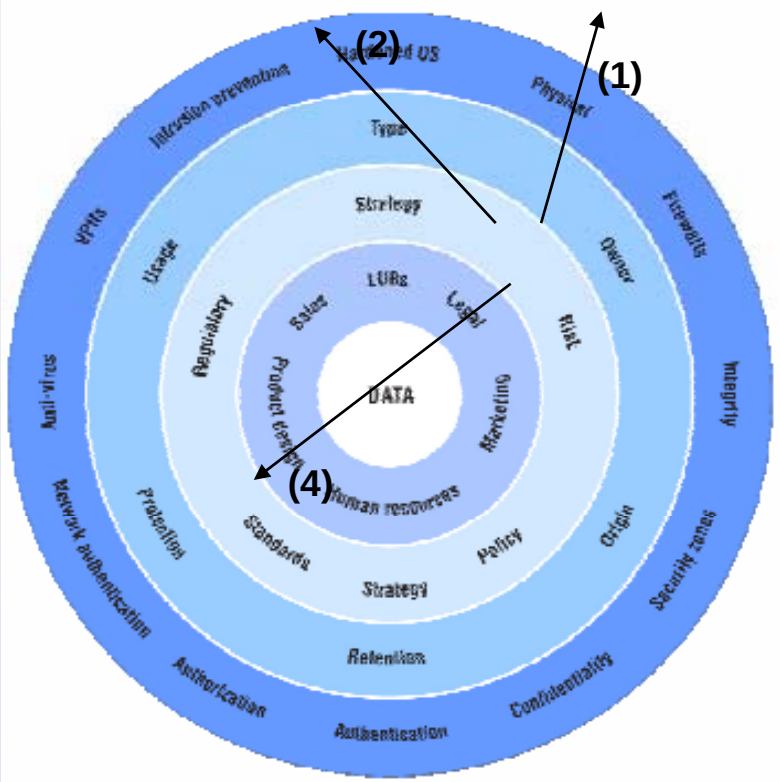
→ Estratégico y Táctico

→ Cultural y organizacional

Adaptado de: Information Security Forum (2006) Information security metrics. Pág. 15

Iniciativas internacionales

Data-centric approach



(1) Estratégico
(2) Operacional
(3) Táctico

Adaptado de: Grandison, T., Bilger, M., O'Connor, L., Graf, M., Swimmer, M. y Schunter, M. 2007

Iniciativas internacionales

Data-centric approach

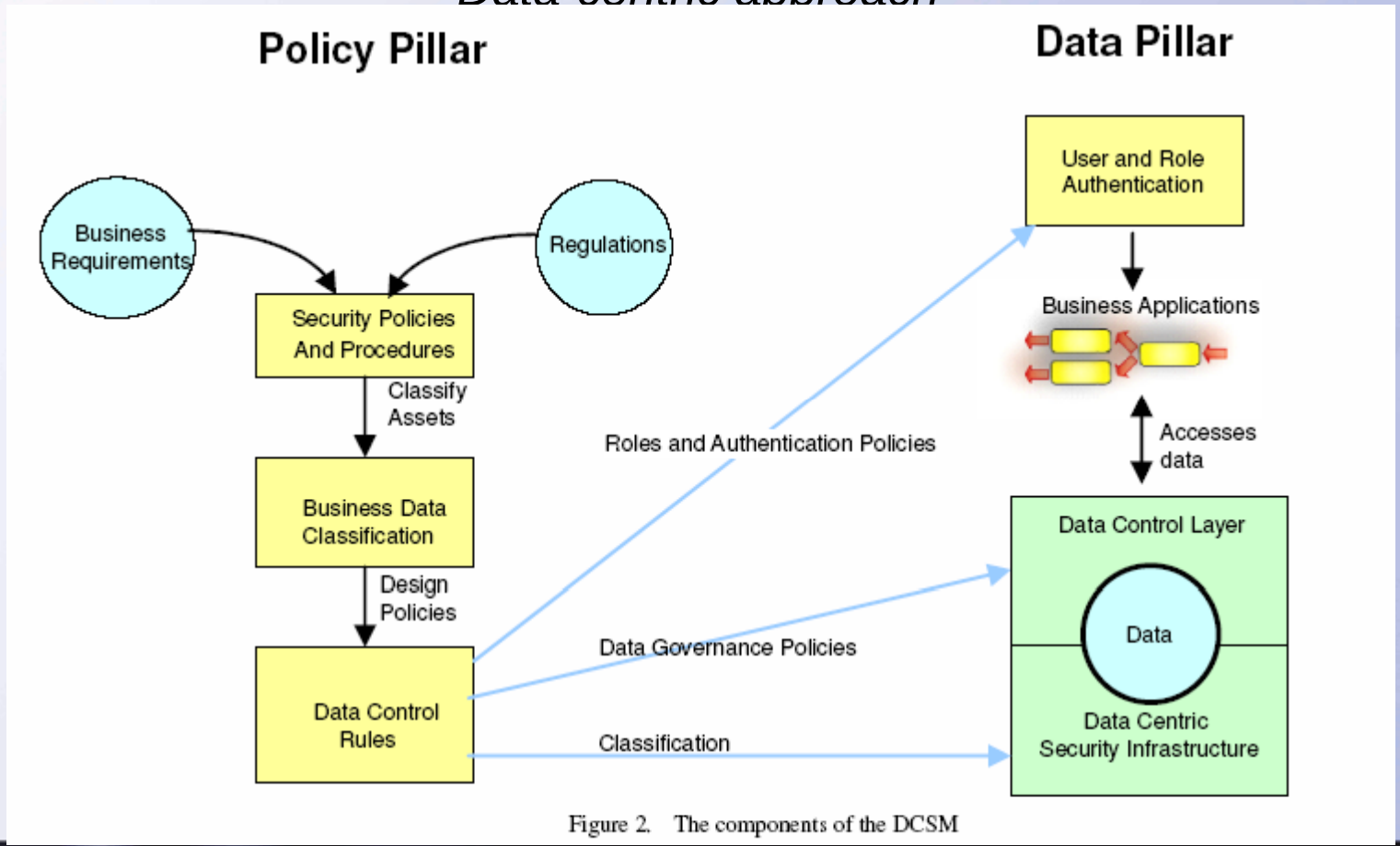


Figure 2. The components of the DCSM

Adaptado de: Grandison, T., Bilger, M., O'Connor, L., Graf, M., Swimmer, M. y Schunter, M. 2007

Iniciativas internacionales

Forrester

Figure 4 Measure People, Process, And Technology

People metrics	Process metrics	Technology metrics
Identity and access management	Information risk management	Network
Information security organization	Policy and compliance framework	Endpoints
Training awareness and personnel	Information asset management	Database
	Business continuity and disaster recovery	Application infrastructure
	Physical and environmental risk	Messaging and content
	Incident and threat management	Data
	System development and IT operations management	

42354 Source: Forrester Research, Inc.

Medida: Sugiere tamaño o magnitud.
Métrica: Colección de medidas que deben ser analizadas para establecer tendencias, dirección futura y prioridades

Tomado de: Kark, K. y Stamp, P. 2007

Parte 4. Fundamentación conceptual de las métricas en seguridad de la Información

¿Qué significa medir?

- Definición – RAE
  - Comparar una cantidad con su respectiva unidad, con el fin de averiguar cuántas veces la segunda está contenida en la primera.
  - Tener determinada dimensión, ser de determinada altura, longitud, superficie, volumen, etc.

↓

“Es una acción que requiere un objeto, un sujeto y un contexto”

↓

“En este escenario, medir no es un problema numérico, sino cultural.

Es decir, responde a un interés particular”

¿Qué son buenas métricas de seguridad?

- Aquellas que proveen *mediciones* o valores concretos, como respuesta a *preguntas* concretas.

- Las características más sobresalientes:
  - Sin criterios subjetivos
  - Fáciles de recolectar
  - Expresadas en números cardinales o porcentajes
  - Detalladas con unidades de medida (defectos, horas, pesos)
  - ***Relevante para la toma de decisiones***

Beneficios de las métricas de seguridad

- Si las organizaciones establecen las preguntas requeridas, las respuestas a éstas preguntas le ayudarán a:
  - Comprender mejor sus riesgos
  - Identificar problemas emergentes
  - Comprender las debilidades de la infraestructura
  - Medir el desempeño de los controles
  - Actualizar las tecnologías y mejorar los procesos actuales
  - Evidenciar la evolución de la cultura de seguridad de la información

Tomado de: Jaquith, A. 2007

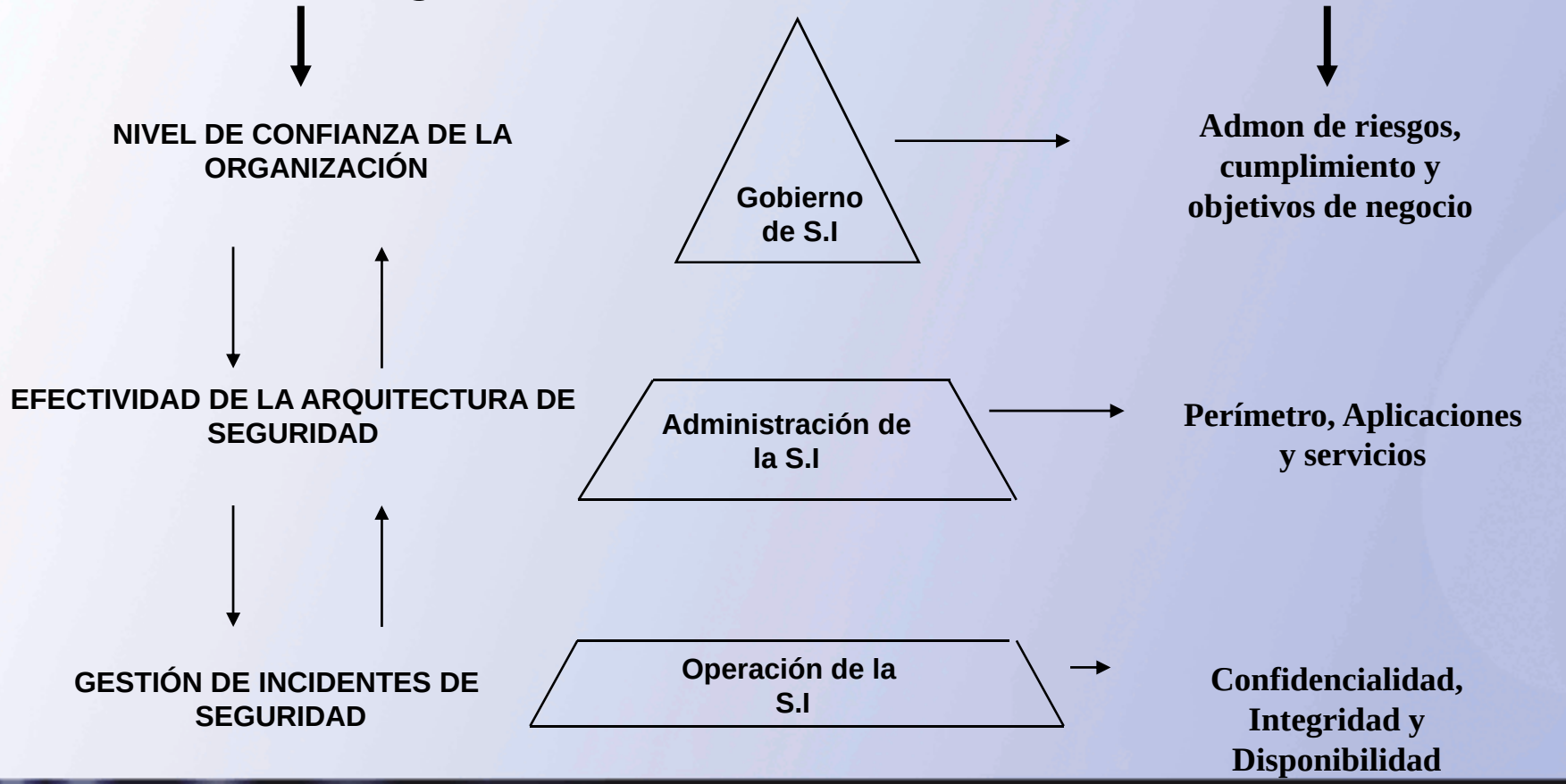
Errores frecuentes en la definición de métricas

- Querer ajustarse a los dominios o variables definidas en los estándares de la industria.
- Ignorar la ***dinámica*** propia de la seguridad en la organización.
- No comprender los riesgos de la organización y la ***percepción*** de los mismos.
- Querer abarcar toda la gestión de seguridad en el primer ejercicio.
- Ignorar las ***expectativas*** de alta gerencia sobre el tema.
- Desconocer las características de la cultura organizacional
- Ignorar que es un ejercicio de evaluación y diagnóstico

Cultura organizacional y las métricas de seguridad

Elementos a Diagnosticar

Elementos a Evaluar



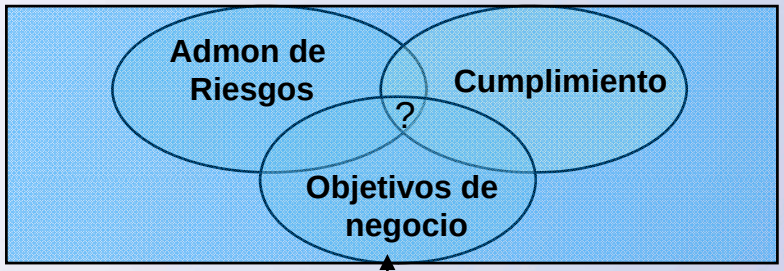
Parte 5. Modelo Estratégico de Métricas en Seguridad de la Información - MEMSI

Fundamentos del Modelo

- Reconoce las diferentes culturas de la organización en diferentes niveles.
- Exige análisis (top-down) y un diagnóstico (bottom-up)
- Establece las preguntas que integran las expectativas, los acuerdos y acciones de los diferentes actores de la organización
- Reconoce que la seguridad es un fenómeno dual (circular) y no dualista (causa-efecto).
- Sugiere una manera de integrar los principios de seguridad informática, las tecnologías de seguridad y los incidentes.
- Vincula los objetivos del negocio como parte fundamental para el desarrollo de las métricas.

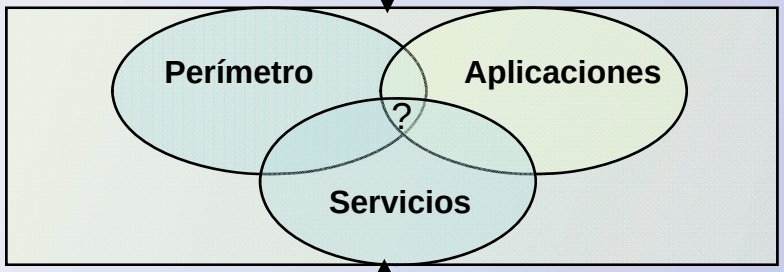
Modelo Estratégico de Métricas en Seguridad de la Información

ESTRATÉGICO



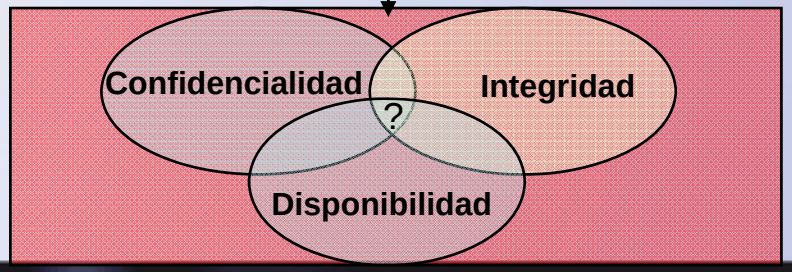
¿Cuál es el nivel de confianza de la organización en temas de seguridad informática?

´TÁCTICO



¿Qué tan efectivas son las tecnologías de seguridad informática disponibles en la organización?

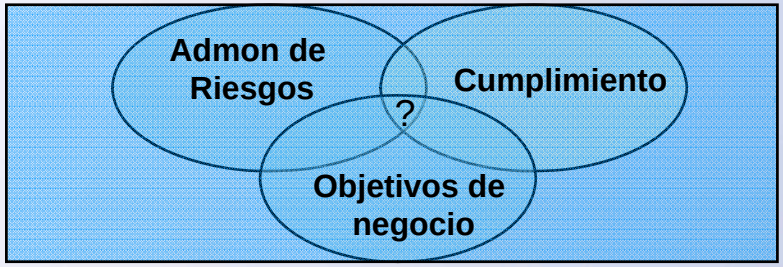
OPERATIVO



¿Qué tipo de incidentes se presentan en la organización?

Modelo Estratégico de Métricas en Seguridad de la Información

ESTRATÉGICO



¿Cuál es el nivel de confianza de la organización en temas de seguridad informática?

Admon de Riesgos

-Identificación de activos a proteger
- Ejercicios de análisis de riesgos y controles
- Planes de actualización y seguimiento
- Pruebas de vulnerabilidades
- Mapas de riesgos y controles

Objetivos de negocio

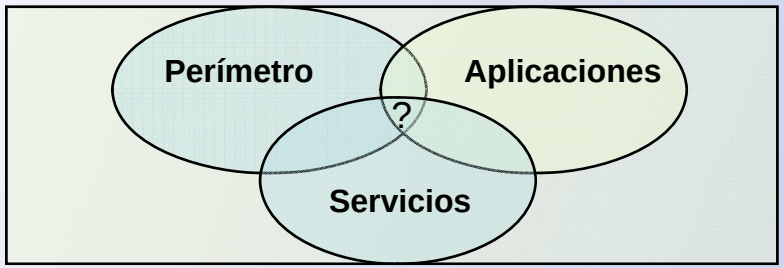
- Relaciones con los clientes
- Expectativas de la gerencia sobre la confianza de los sistemas
- Significado de la seguridad en los procesos de negocio
- Generación de valor agregado a los clientes
- Responsabilidad y agilidad ante incidentes

Cumplimiento

- Ajuste con buenas prácticas internacionales en el tema
- Revisión y análisis de regulaciones nacionales e internacionales
- Estándares de debido cuidado en seguridad informática
- Auditorías y pruebas de cumplimiento

Modelo Estratégico de Métricas en Seguridad de la Información

´TÁCTICO



¿Qué tan efectivas son las Tecnologías de seguridad informática Disponibles en la organización?

Perímetro

- Efectividad del antivirus
- Efectividad del AntiSpam
- Efectividad del Firewall
- Efectividad del IDS/IPS
- Efectividad del Monitoreo 7x24

Aplicaciones

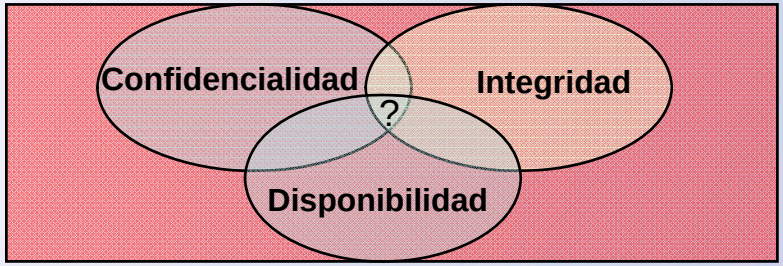
- Defectos identificados en el software
- Vulnerabilidades identificadas
- Revisión de código fuente
- Utilización de funciones no documentadas
- Pruebas de vulnerabilidades al software

Servicios

- Administración de parches
- Aseguramiento de equipos
- Copias de respaldo
- Recuperación ante fallas
- Control de cambios

Modelo Estratégico de Métricas en Seguridad de la Información

OPERATIVO



¿Qué tipo de incidentes se presentan en la organización?

Confidencialidad

- Accesos no autorizados
- Configuración por defecto
- Suplantación de IP o datos
- Monitoreo no autorizado
- Contraseñas débiles

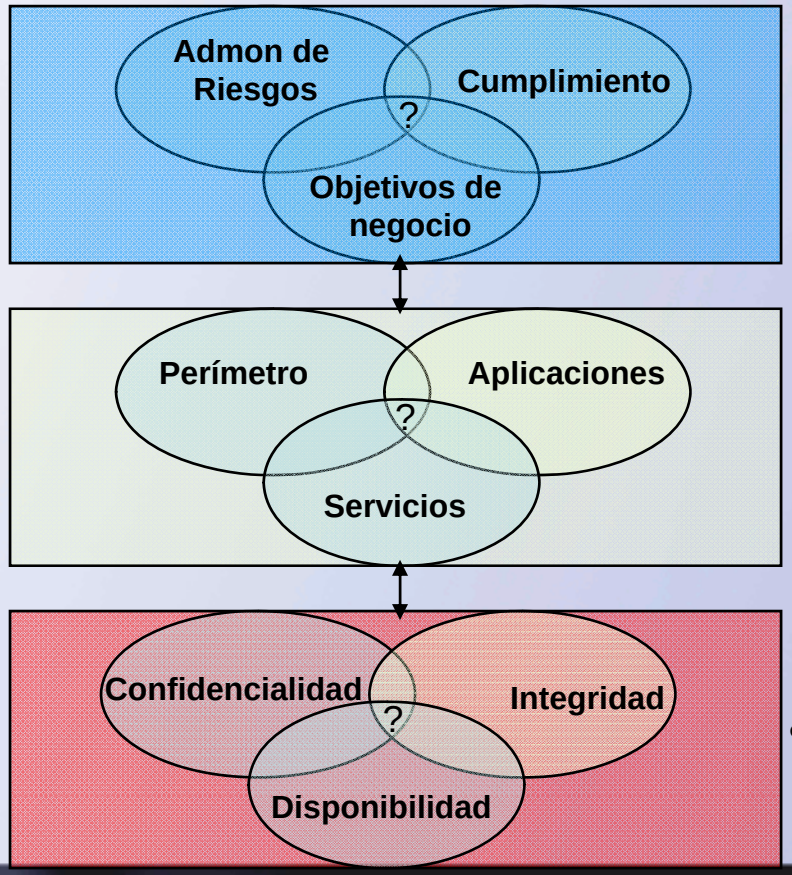
Integridad

- Eliminar, borrar u manipular datos
- Virus informáticos

Disponibilidad

- Negación del servicio
- Inundación de paquetes
- Eliminar, borrar u manipular datos
- Suplantación de IP o datos

Modelo Estratégico de Métricas en Seguridad de la Información



Efectividad de la Arquitectura de Seguridad

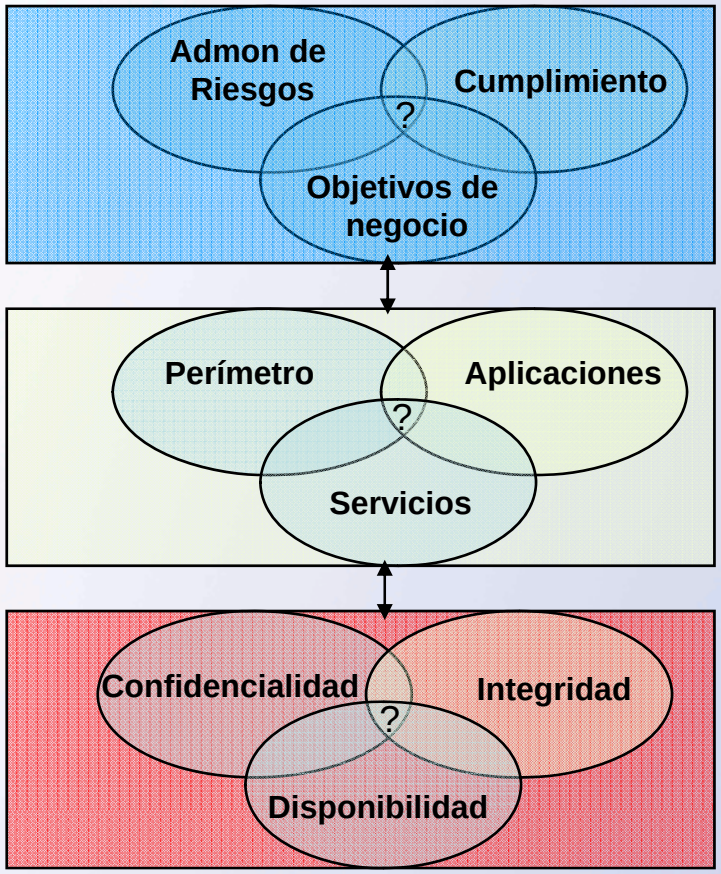
Efectividad de la Administración de Incidentes

¿Cuál es el nivel de confianza de la organización en temas de seguridad informática?

¿Qué tan efectivas son las Tecnologías de seguridad informática Disponibles en la organización?

¿Qué tipo de incidentes se presentan en la organización?

Modelo Estratégico de Métricas en Seguridad de la Información



¿Cuál es el nivel de confianza de la organización en temas de seguridad informática?

¿Qué tan efectivas son las Tecnologías de seguridad informática Disponibles en la organización?

¿Qué tipo de incidentes se presentan en la organización?

-% de nuevos empleados que completaron su entrenamiento de seguridad/Total de nuevos ingresos
- % de cuentas inactivas de usuario deshabilitadas / Total de cuentas inactivas
- Valor total de los incidentes de seguridad Informática / Total del presupuesto de Seg. Inf

-No. Mensajes de spam detectados / No. Total de mensajes ignorados
- No. de mensajes salientes con virus o spyware
- No de spyware detectados en servidores o estaciones de trabajo
- No. de Estaciones de trabajo parchadas / Total de las estaciones de trabajo

- No. de incidentes asociados con la confidencialidad / Total de incidentes
- No. de incidentes asociados con la disponibilidad / Total de incidentes
- No. de incidentes asociados con la confidencialidad / Total de incidentes

Modelo Estratégico de Métricas en Seguridad de la Información

	PREGUNTA	EJEMPLO DE MÉTRICA	PROPÓSITO
ESTRATÉGICO	¿Cuál es el nivel de confianza de la organización en temas de seguridad informática?	-% de nuevos empleados que completaron su entrenamiento de seguridad/Total de nuevos ingresos - % de cuentas inactivas de usuario deshabilitadas / Total de cuentas inactivas - Valor total de los incidentes de seguridad Informática / Total del presupuesto de Seg. Inf	**Desempeño de personas y procesos**
´TÁCTICO	¿Qué tan efectivas son las Tecnologías de seguridad informática Disponibles en la organización?	-No. Mensajes de spam detectados / No. Total de mensajes ignorados - No. de mensajes salientes con virus o spyware - No de spyware detectados en servidores o estaciones de trabajo - No. de Estaciones de trabajo parchadas / Total de las estaciones de trabajo	**Desempeño de las tecnologías de seguridad informática**
OPERATIVO	¿Qué tipo de incidentes se presentan en la organización?	- No. de incidentes asociados con la confidencialidad / Total de incidentes - No. de incidentes asociados con la disponibilidad / Total de incidentes - No. de incidentes asociados con la confidencialidad / Total de incidentes	**Desempeño de la administración de incidentes**

Algunas consideraciones del modelo propuesto

- El modelo se puede utilizar bottom-up o Top Down.
  - Esto significa que las preguntas son complementarias entre si: responder una, es soportar la respuesta de la otra.
- Es viable tomar decisiones más concretas sobre aspectos de seguridad informática según el nivel.
- Sugiere una estrategia para justificar los presupuestos de seguridad
- Establece un índice de confianza (nivel de inseguridad permitido)
- No es una propuesta disyunta de las prácticas internacionales. Es una iniciativa complementaria y operacional.
- Se ajusta a la dinámica de negocios y cultural de la organización.
- Integra las buenas prácticas de la industria: Cobit, ISM3, ITIL, entre otras.

Reflexiones finales

- Medir en seguridad informática es *"meditar y plantear en las preguntas adecuadas"*
- Medir en seguridad informática es *"contextualizar las expectativas de la alta gerencia"*
- Medir en seguridad informática *"no es ajustarse a lo expresado por las buenas prácticas", es ajustarse a su propia dinámica de riesgos.*
- Medir en seguridad informática *"es evidenciar el nivel de riesgo permitido"* para desarrollar y potenciar los objetivos de negocio
- Medir en seguridad informática *"no es pensar en los datos"*, sino en lo que dicen y lo que significan los mismos para la gerencia.

¿Han cambiado las respuestas?

- Declaraciones sobre las métricas de seguridad de la información
  - Las métricas debe ser objetivas y tangibles – (F o V)
  - Las métricas deben tener valores discretos – (F o V)
  - Se requieren medidas absolutas y concretas – (F o V)
  - Las métricas son costosas – (F o V)
  - Ud no puede administrar lo que no puede medir; por tanto no puede mejorar lo que no puede administrar – (F o V)
  - Es esencial medir los resultados – (F o V)
  - Necesitamos los números para expresarnos – (F o V)

Para concluir …

- "*Recuerde que un buen sistema de métricas en seguridad informática, no busca dar las mejores respuestas o indicadores, sino la capacidad organizacional para avanzar en la conquista de la "falsa sensación de seguridad"* ".

Referencias

- Information Security Forum (2006) Information security metrics. Disponible: https://www.securityforum.org/index.htm
- Chew, E., Clay, A., Hash, J., Bartol, N. y Brown. (2006) Guide for developing performance metrics for information secuity. NIST. Disponible en: http://csrc.nist.gov/publications/drafts/draft-sp800-80-ipd.pdf
- Grandison, T., Bilger, M., O'Connor, L., Graf, M., Swimmer, M. y Schunter, M. (2007) Elevating the discussion on security management. *Proceedings IEEE Business-Driven IT Management*.
- Vaughn, R., Henning, R. y Siraj, A. (2003) Information assurance measures and metrics. State of practice and proposed taxonomy. *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03)*
- Longstaff, T. y Haimes, Y. (2002) A holistic roadmap for survivable infrastructure systems. *IEEE Transactions on systems, Man and cybernetics- Part A: Systems and Humans*. Vol 32, No.2. March.
- Bellovin, S. (2008) On the brittleness of software and the infeasibility of security metrics. *IEEE Security & Privacy*. Janary/February.
- Savola, R. (2007) Towards a security metrics taxonomy for the information and communicationtechnology industry. *IEEE International Conference on Software Engineering Advances(ICSEA 2007)*
- Gottlieb, R. y Iyer, B. (2004) The four-domain architecture: An approach to support enterprise architecture design. *IBM System Journal*. Vol.43 No.3
- ISACA (2007) Cobit 4.1.
- Rice, D. (2008) *Geekonomics. The real cost of insecure software*. Addison Wesley.
- Cano, J. (2008) Entendiendo la inseguridad de la información. Editorial. *Revista SISTEMAS*. No.105. ACIS.

Referencias

- Hinson, G. (2006) Seven myths about information security metrics. IsecT Ltd. Disponible en: http://www.isect.com
- Koetzle, L., Yates, S., Kark, K. y Bernhardt. (2006) How to measure what matters in security. *Forrester Research*.
- Kark, K. y Stamp, P. (2007) Defining an effective security metrics program. *Forrester Research*.
- Kark, K. y Nagel, B. (2007) The evolving security organization. *Forrester Research.*
- Stamp, P. (2008) Making data-centric security real. *Forrester Research*.
- Kark, K. (2008) Seven habits of effective CISOs. *Forrester Research*.
- Stakhanova, N., Basu, S. y Wong, J. (2007) A taxonomy of intrusion response systems. *International Journal Information and Computer Security*. Vol.1 No.1/2.
- Lee, J. y Lee, Y. (2002) A holistic model of computer abuse within organizations. *Information Management & Computer Security*. Vol.10. No.2/3.
- Foltz, C. B. (2004) Cyberterrorism, computer crime and reality. *Information Management & Computer Security*. Vol.12. No.2/3.
- Kovacich, G. y Halibozek, E. (2006) *Security metrics management. How to manage the cost of an assets protection program*. Butterworth-Heinemann.
- Jaquith, A. (2007) *Security metrics: Replacing fear, uncertainty, and doubt*. Adisson Wesley.
- Herrmann, D. (2007) *Complete guide to security and privacy metrics*. Auerbach.
- Shostack, A. y Stewart, A. (2008) *The New School of Information Security*. Addison Wesley.

VIII Jornada Nacional de Seguridad Informática
ACIS

Métricas en Seguridad Informática:
Una revisión académica

Jeimy J. Cano, Ph.D, CFE
GECTI
Facultad de Derecho
Universidad de los Andes

jcano@uniandes.edu.co