Métricas de Seguridad de la Información

y su Aplicación en Nuevos Escenarios

Ing. Carlos Ormella Meyer

Marzo 2015

Agenda

- Tema 1: **Seguridad de la Información y Seguridad Informática**.
- Tema 2: **Evaluación de la concientización**
- Tema 3: **Oportunidades y Riesgos Positivos**
- Tema 4: **Efectividad de los Controles y Balanced Scorecard (BSC)**
- Tema 5: **Computación en la Nube**
- Tema 6: **Móviles BYOD**
- **Tema 7: Big data y Analítica**

Seguridad Información vs. Informática

Vulnerab. Organiz., Operac. y Físicos

- Ausencia de Normas y Políticas
- Control insuficiente de cambios
- Actitud y comportamiento personal
- Errores, actos deliberados personal
- información verbal o en papel, etc.

Vulnerab. y Amen. TIC

- Virus
- Spam - Phising
- Contraseñas
- Ataques DoS
- Internet, e-mail, etc.

Efectividad de la Concientización

		CRITERIOS			TOTALES
		Conocimiento	Actitud	Comportamiento	
TEMAS	Peso Relat.	30%	20%	50%	
Políticas	20%	46%	53%	35%	42%
BIA	25%	81%	76%	72%	76%
RA	25%	70%	67%	41%	55%
Respuesta	15%	70%	65%	53%	61%
Cultura	15%	47%	36%	29%	36%
TOTALES		64%	61%	48%	55%

- Los resultados se han semaforizado en 3 niveles (rojo/amarillo/verde) con límites al 50% y 75% y pueden presentarse gráficamente de distintas maneras.

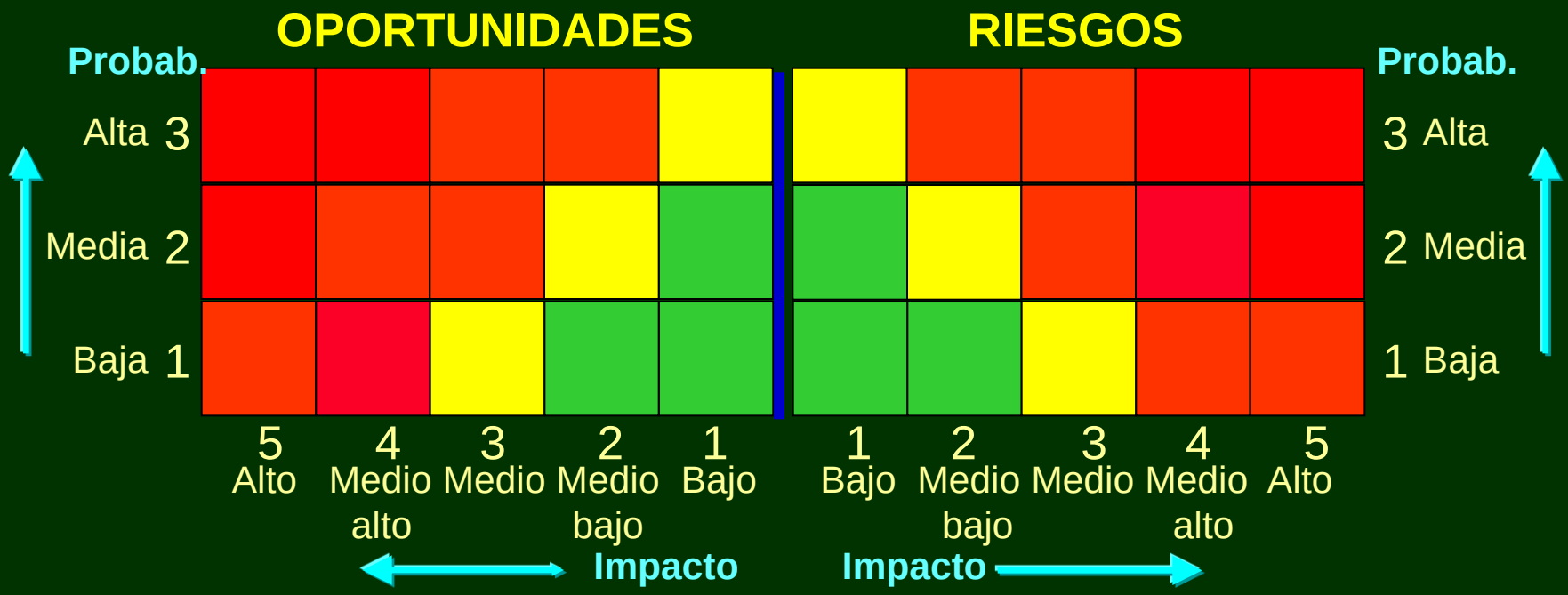
Oportunidades: Riesgos positivos

- La norma **ISO 31000**, a la que se ajusta la nueva versión de la **ISO 27001**, ha redefinido los riesgos como ***inseguridad en el logro de objetivos***.
- Esto implica que, además de los riesgos tradicionales de efectos negativos, puede haber riesgos de efectos positivos que constituyen **Oportunidades** que se pueden ***aprovechar*****.**
- Pueden encontrarse oportunidades existentes que podrían mejorarse y lograr mayor aprovechamiento.
- Pero también se pueden ***generar*** oportunidades.
- Por ejemplo, un plan de Concientización que permita luego verificar los niveles de conocimiento, actitud y comportamiento que se hayan inducido.

Oportunidades: Riesgos positivos

- Las Oportunidades pueden tratarse en forma similar a los Riesgos, en cuanto a establecer en forma cualitativa el nivel a partir del **impacto** que puede causar su aprovechamiento y la **probabilidad** de que se produzca tal situación
- A la inversa de los riesgos, en que los de mayores probabilidades e impactos son los primeros que hay que ***mitigar***, tales valores mayores con las oportunidades señalan las oportunidades más convenientes para ***aprovechar***.
- Las métricas a aplicar para las oportunidades pueden basarse apelando a **ROSI** (*Retorno Sobre la inversión en Seguridad de la Información*).

Mapa de Oportunidades y Riesgos



Color	Oportunidades	Riesgos
Rojo	Las más aprovechables	Los más críticos a mitigar
Amarillo	Las que podrían aprovecharse, sobre todo si se mejoran	Los que conviene mitigar
Verde	Las menos aprovechables pero que podrían mejorarse	Los menos riesgosos

Efectividad de los controles

- La efectividad de los controles implementados se puede establecer por medio de métricas.
- La norma **ISO 27004** establece el marco de trabajo y las características que deben dichas métricas, pero no estipula detalles de cuáles son.
- Para eso pueden usar dos publicaciones **NIST**.
- La **NIST 800-55v1** ofrece una guía sobre métricas respecto a los controles de seguridad **NIST**.
- Por su parte, **NIST 800-53** define dichos controles y los mapea a controles de la norma **ISO 27002**.
- Se puede elaborar una tabla de mapeo inverso, de controles **ISO 27002** a controles **NIST**, y usar así las métricas respectivas de **NIST 800-55**.

Efectividad de los controles

- Más amplio y completo resulta al aplicar la metodología **GQM** ***(Métricas de Metas por Cuestionario)***.
- **GQM** parte de establecer **Metas p**ara luego plantear **Preguntas** cuyas **Respuestas** serán las **Métricas**.
- ***Meta:*** Seguridad de los recursos humanos.
- ***Preguntas:*** ¿Cuáles fueron los resultados de un plan de concientización?
- ***Métricas:***

  a) % del total del personal que asistieron al programa.

  b) % del total del personal con roles y responsabilidades significativas.

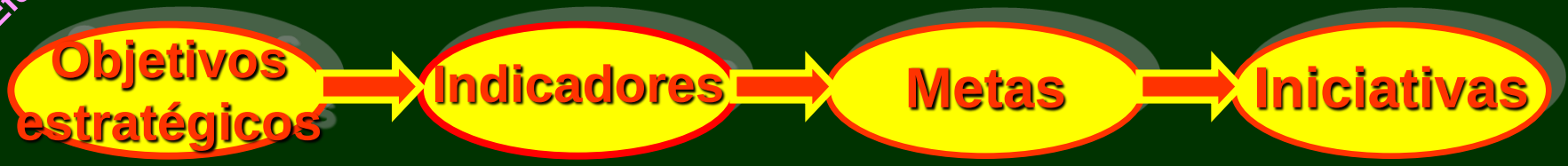
  c) % del porcentajes obtenidos en cuanto a criterios de *conocimiento, actitud y comportamiento* en una encuesta posterior?

Efectividad de los Controles

- Más completo es el **Balanced Scorecard (BSC)** para implementar la estrategia, además de la efectividad y gestión de las medidas y controles, y que además balancea *indicadores financieros y no financieros.*
- El **BSC** usa cuatro Perspectivas**:**
  1) Finanzas
  2) Clientes
  3) Procesos internos
  4) Aprendizaje y Crecimiento
- El **BSC** se compone de dos partes o secciones:
  1) **Mapa Estratégico:** consta de ***objetivos estratégicos*** enlazados por relaciones de *causa y efecto.*
  2) **Tablero de Control o de Comando:** es la parte más conocida del **Balanced Scorecard**.

Efectividad

Tablero de Control del BSC



En c/Perspectiva:

Objetivos	Lo que se quiere conseguir.
Indicadores	Parámetros basados en ***métricas*** para monitorear el progreso hacia el alcance de cada objetivo.
Metas/hitos (targets)	Lo que quiere lograrse a lo largo del tiempo; se mide con indicadores.
Iniciativas	Planes para lograr los objetivos y las metas correspondientes.

- Los objetivos ***estratégicos*** derivan en ***operacionales*** con sus indicadores, metas e iniciativas propias.

Efectividad

Métricas de seguridad y BSC

- Los **objetivos operacionales** de seguridad se mapean en ***objetivos de control*** y las **iniciativas** en **controles** de la ISO 27002 (versión 2005 en la Figura) para cumplir los objetivos y metas deseados.

Perspectivas	Objetivos Control	Indica-dores	Metas			Iniciativas
			2010	Nivel Cumpl	% Cumpl	
Finanzas	10.1 – Ase-gurar opera-ción segura	Reducción pérdidas x vulnerabil.	30 %	8 %	27	Control 10.1.2 – Gestión de cambios
.....	.....	.....	.....	.....	.....	.....
Clientes	6.2 – Mante-ner segurid. con terceros	Accesos controlados clientes	90 %	48 %	53	Controles 6.2.2 – Tratamiento segur. c/clientes
.....	.....	.....	.....	.....	.....	.....
Procesos internos	12.6 – Redu-cir riesgos por vulner.	Vulnerab. verificadas y tratadas	70 %	45%	64	Control 12.6.1 – Control de vulnerabilidades
.....	.....	.....	.....	.....	.....	.....
Aprendizaje y crecimiento	8.2 – Asegu-rar conocim. normas	Nivel de concienti-zación	60 horas	50 horas	83	Control 8.2.2 – Plan de concientización
.....	.....	.....	.....	.....	.....	.....

Computación en la Nube

- Tres Servicios: **SaaS, PaaS e IaaS**. Con **SaaS** se contratan las aplicaciones, **PaaS** ofrece plataforma para desarrollo, e **IaaS** plataforma de hardware.
- Formas de Implementación: **Nube Privada, Comunitaria, Pública e Híbrida.**
- Tres herramientas para complementar la **ISO 27001**:
  a) **CSF de NIST** con mapeado a controles **ISO 27001**.
  b) **CCM de CSA** también se mapea a la **ISO 27001**.
  c) **Controles críticos de SANS**
- Adicionalmente, **SIEM** (*Gestión de eventos de seguridad de la información*) que recoge y analiza datos, y produce alertas.
- **Métricas**, **SLA** (*Acuerdos de Nivel de Servicio*) analizado bajo **GQM**.

Móviles BYOD

- **BYOD** *("Traiga su propio dispositivo")* se refiere a que los empleados de una empresa traigan y usen sus dispositivos móviles, como tablets y celulares inteligentes para acceder a información de la misma.
- Este nuevo foco en la seguridad de la información a nivel corporativo, exige establecer seguridad física, protección lógica de la información residente, protección de acceso y conectividad adecuada.
- Se implementa con *políticas de uso, incluyendo requisitos, procedimientos y guías, así como también responsabilidades, y verificaciones constantes*, aplicando **métricas** adecuadas definidas mediante el mecanismo **GQM**.

Big Data y Analítica

- **Big Data:** gestión y análisis de gran variedad de ***datos***, producidos tanto por dispositivos como por personas.
- **Big Data** se puede definir con cinco indicadores llamados **5v**, aunque los tres primeros son los más mencionados.
- **1) Volumen**, grandes cantidades de datos, desde **Terabytes** (10^{12}), y **Petabytes** (10^{15}), hasta **Exabytes** (10^{18}).
- **2) Variedad**, datos de tres tipos
  a) ***Estructurados***: los de bases de datos relacionales,
  b) ***Semiestructurados***: Registros internos y de servidores, seguimiento de clics en Internet.
  c) **No *estructurados:*** Datos que no pueden almacenarse en una base de datos tradicional, tales como imágenes, video, audio, etc., y texto generado en las redes sociales, foros, e-mails, archivos de Powerpoint y Word, etc.

Big Data y Analítica

- **3) Velocidad**, con que se reciben los datos.
- **4) Veracidad**, como resultado de un análisis así como la validación de su utilidad para mejorar la toma de decisiones.
- **5) Valor**, de los datos para los negocios.
- La Analítica de B**ig Data** es una extensión del **Data Analytics** que permite examinar grandes *volúmenes* de datos que contienen una *variedad* de tipos de datos, que se generan a alta *velocidad* (big data), para poner en claro patrones ocultos, correlaciones desconocidas, tendencias de mercado, y preferencias de clientes, así como otros tipos de información útiles para los negocios.
- Su uso se viene difundiendo especialmente en bancos y compañías de tarjetas de crédito para prevenir el fraude o identificar robos.

Tips

1) Recuerde que las charlas de concientización no deben considerarse como una simple divulgación de conocimiento de seguridad.
2) Recuerde que el **BSC** es una herramienta conocida por los altos niveles en ciertas empresas. Por lo tanto es una forma de hacer conocer la importancia de la seguridad en los negocios.
3) Recuerde que aprovechar una oportunidad puede proveer un beneficio similar a mitigar un riesgo.
4) Con **BYOD** asegúrese de tomar precauciones con los dispositivos y aplicaciones que se accedan.
5) En la Nube tenga presente las características de los diferentes servicios y el tipo de implementación.

Muchas gracias

Ing. Carlos Ormella Meyer

Cursos y Soporte Digital - Asesoramiento
@meyerormella

Hecho el depósito en custodia bajo la Ley Nro. 11.723.