Deloitte.

Information Security Community

Midiendo la efectividad de su programa de seguridad de información

Iván Campos

28 de Mayo de 2014

Contenido

Conversemos

¿Cuál es tu experiencia?

¿Para qué medimos?

¿Qué son las métricas?

¿Quién es el responsable de la medición?

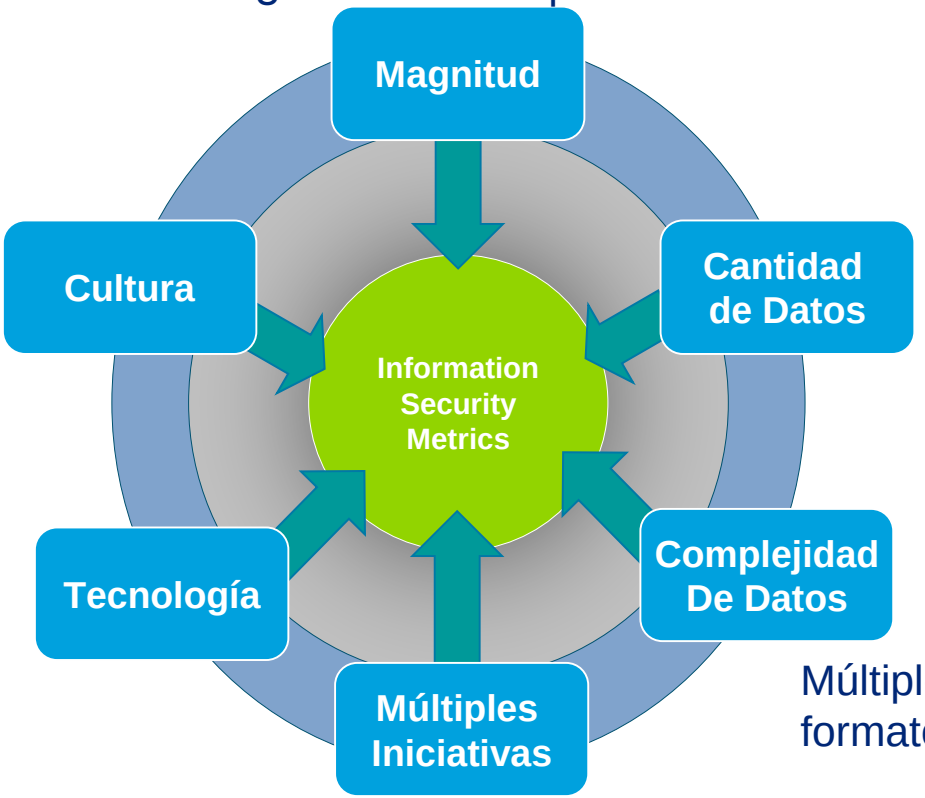
¿Qué medimos?

¿Contamos con datos para medir?

¿Qué datos son relevantes?

Retos identificados

Se percibe como un gran esfuerzo
¿Por dónde empezar?



Falta de una cultura de rendición de cuentas

Demasiada información operativa

Falta de entendimiento, complejidad, compatibilidad

Múltiples fuentes, tipos, formatos

Alineación con otros programas de medición en la organización

Errores Comunes

- Uso de enfoques puntuales, en lugar de enfoques completos y metodológicos
- Métricas aisladas que proporcionan poco valor, en lugar de un programa estructurado
- Falta de un proceso consistente y con objetivos claros
- Falta de visión clara en lo que se persigue medir – Seguridad Técnica vs Efectividad del Programa

Programa de Medición de Seguridad de Información

Definiciones

¿Qué es?

- Un programa con objetivos bien definidos
- Un proceso continuo, no un evento
- Mediciones a la medida para cada área de riesgo específica.
- Un programa alineado a otras iniciativas de medición del desempeño en la organización

¿Qué NO es?

- Una receta de cocina, igual para todos
- Sólo un tablero de medidas
- Lo mismo para cada área de riesgo y área de negocio
- Cientos de diferentes medidas
- Resumen de reportes de herramientas

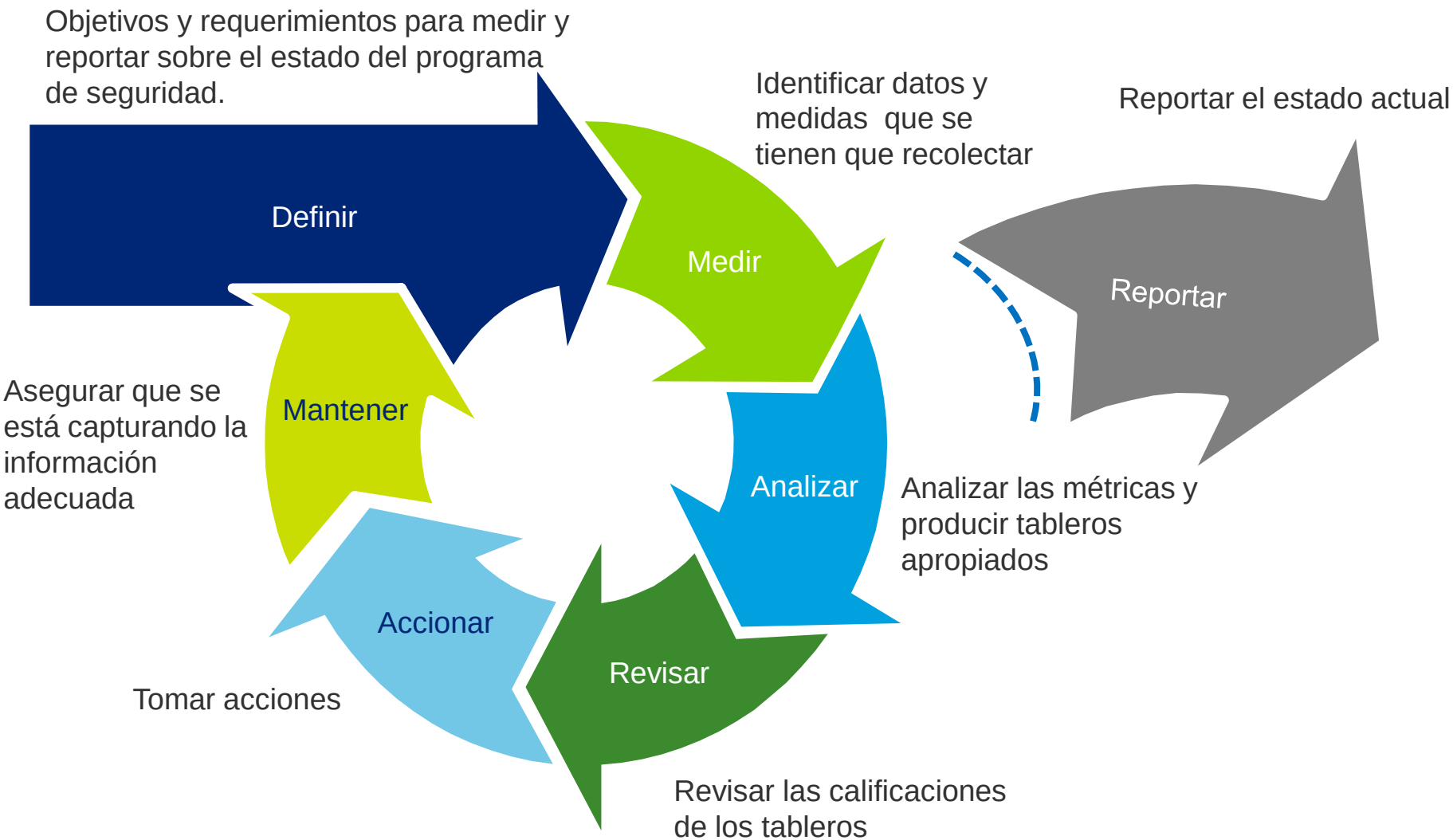
¿Por qué usarlo?

- Obtener visibilidad del desempeño operacional
- Mejorar la toma de decisiones
- Alinear iniciativas en la organización
- Identificar y justificar el ROI en tecnología y seguridad de la información
- Enfocarse más a los resultados que a la práctica
- Soportar decisiones
- Incentivar a la gente - Competencia

Las métricas aisladas proporcionan poco valor, pero si se alinean a un programa con objetivos claros, el valor es evidente.

Programa de Medición - Enfoque iterativo

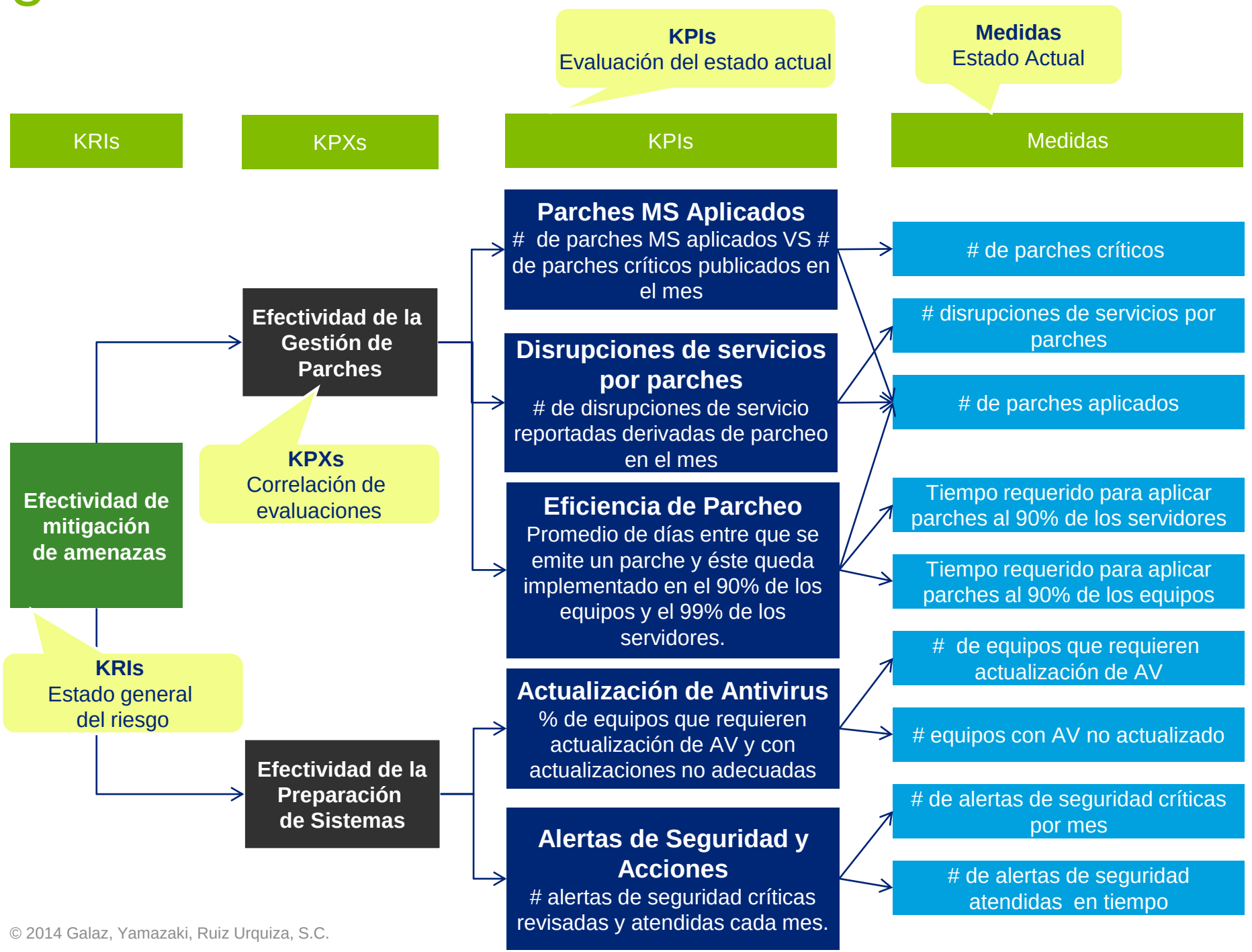
El programa de métricas de seguridad provee un único punto de referencia para información concisa a nivel ejecutivo, para dueños de negocio y tecnología.



Todo programa necesita habilitadores

Medidas	Información basada en datos relevantes de un elemento del programa de seguridad.
Key Performance Indicator (KPI)	Medida de una **actividad** de seguridad de información, o un indicador importante del estado de la seguridad de un componente de seguridad de información. Ej. Certificaciones alcanzadas, # parches aplicados, # de incidentes en el mes, # de personal capacitado.
Key Performance Index (KPX)	Un resumen o correlación de uno o más KPI's que proveen visión del desempeño global de **un área** del programa de seguridad de información. Ej. Gestión de parches, gestión de vulnerabilidades, concientización.
Key Risk Indicator (KRI)	Un resumen o correlación de uno o más KPX's que provee una visión del estado de **los riesgos y objetivos clave de todo el programa** de seguridad de información. Ej. Reducción de amenazas, disminución de fugas de información, etc.
Information Security Dashboard	Un mecanismo de reporteo que provee una visión de la efectividad del programa de seguridad de información, mostrando KPIs, KPXs and KRIs

¿Cómo interactúan los habilitadores?



Ejemplos de métricas

Seguridad en aplicaciones

- # de aplicaciones
- % de aplicaciones críticas
- Cobertura de la gestión de riesgos
- Cobertura de pruebas de seguridad

Gestión de Incidentes

- Tiempo de descubrimiento de incidentes
- Tasa de incidentes por mes
- % de incidentes detectados por los controles internos
- Tiempo transcurrido entre incidentes de seguridad
- Tiempo transcurrido para la recuperación

Financieras

- Presupuesto de seguridad como % del presupuesto de TI
- Distribución del presupuesto de seguridad de información

Gestión de parches

- Cumplimiento de la política de parches
- Cobertura de la gestión de parches
- Tiempo transcurrido para aplicar parches

Gestión de la configuración de cambios

- Tiempo transcurrido para completar cambios
- % de cambios con revisiones de seguridad
- % de cambios con excepciones de seguridad

Gestión de Vulnerabilidades

- Cobertura de los escaneos de vulnerabilidades
- % de sistemas sin vulnerabilidades conocidas
- Tiempo transcurrido para mitigar vulnerabilidades
- # de vulnerabilidades conocidas en equipos

Conclusiones
Factores críticos de éxito

- Compromiso de la alta gerencia y soporte con los recursos adecuados.
- Implementación de proceso y procedimientos formales
- Desarrollo de proceso repetible y capaz de capturar y reportar información relevante
- Medidas cuantificables basadas en objetivos del programa de seguridad
- Facilidad en la obtención de la información, herramientas y automatización
- Orientación a las acciones y mejora del programa de seguridad
- Orientación de los reportes al negocio
- Evaluar periódicamente la eficiencia y relevancia de las medidas para implementar mejoras y actualizaciones

Deloitte.