Modelos de Madurez de Seguridad de la Información: cómo debe evolucionar la seguridad en las organizaciones

Roberto Arbeláez CISSP, CISA

Security Program Manager for Latin America

Microsoft Corp.

¿QUÉ ES UN MODELO DE MADUREZ?

Es un conjunto estructurado de elementos que describen el nivel de madurez de un ente en un aspecto determinado

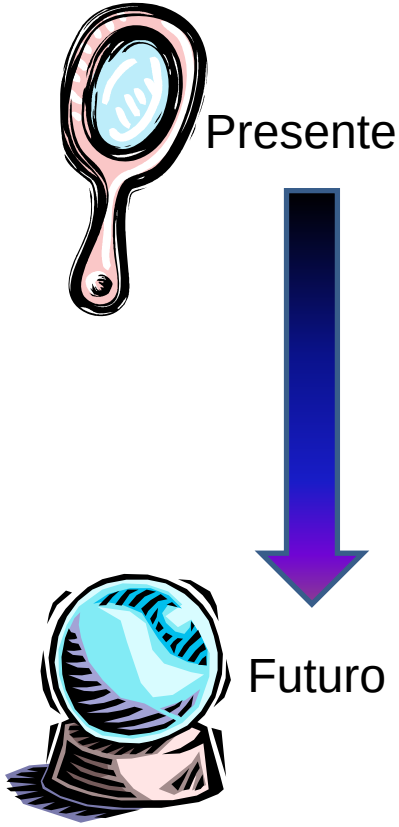
- Establece un orden claro, discreto y absoluto, definiendo niveles o etapas de madurez

- Establece de manera explícita la evolución de la organización en dicho aspecto

¿PARA QUÉ SIRVE UN MODELO DE MADUREZ?

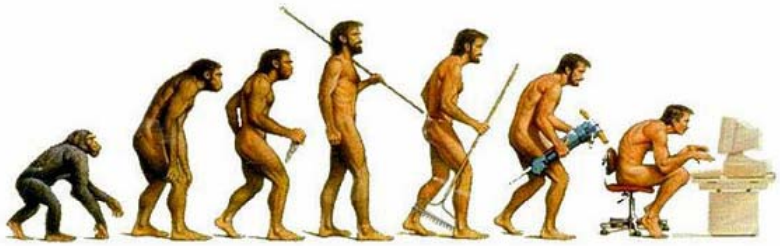
- Me permite medirme: ¿Dónde estoy hoy?
  - Autoanálisis
    - Madurez
    - Capacidad
  - Benchmarking sectorial
  - Benchmarking nacional / regional / global

- Me permite definir dónde debo estar
  - Oportunidades de mejora/optimización
  - Alineación con estrategias organizacionales
  - Alineación con requerimientos presentes y futuros



¿PARA QUÉ SIRVE UN MODELO DE MADUREZ?

- Me permite planear lo que debo lograr para llegar a donde quiero estar
  - Planes, proyectos, tareas
- Me permite gestionar mi crecimiento y evolución
  - Medir si me estoy acercando a donde debo estar
  - Corregir el rumbo si me estoy desviando



¿QUÉ INFORMACION OBTENGO DE UN MODELO DE MADUREZ?

- ¿Qué estoy haciendo?
  - De un conjunto de elementos, cuáles cumplo, cuáles no
- ¿Cómo lo estoy haciendo?
  - De los elementos que cumplo, ¿cómo los cumplo?
    - Mejor, peor...
    - Manual, automatizado…
    - En papel, o en digital…
    - En diferido o en tiempo real…

Algunos Modelos…

- NIST-CSEAT
- CITI-ISEM
- COBIT Maturity Model
- (ISM3)
- SSE-CMM
- CERT-CSO

(ISM3)

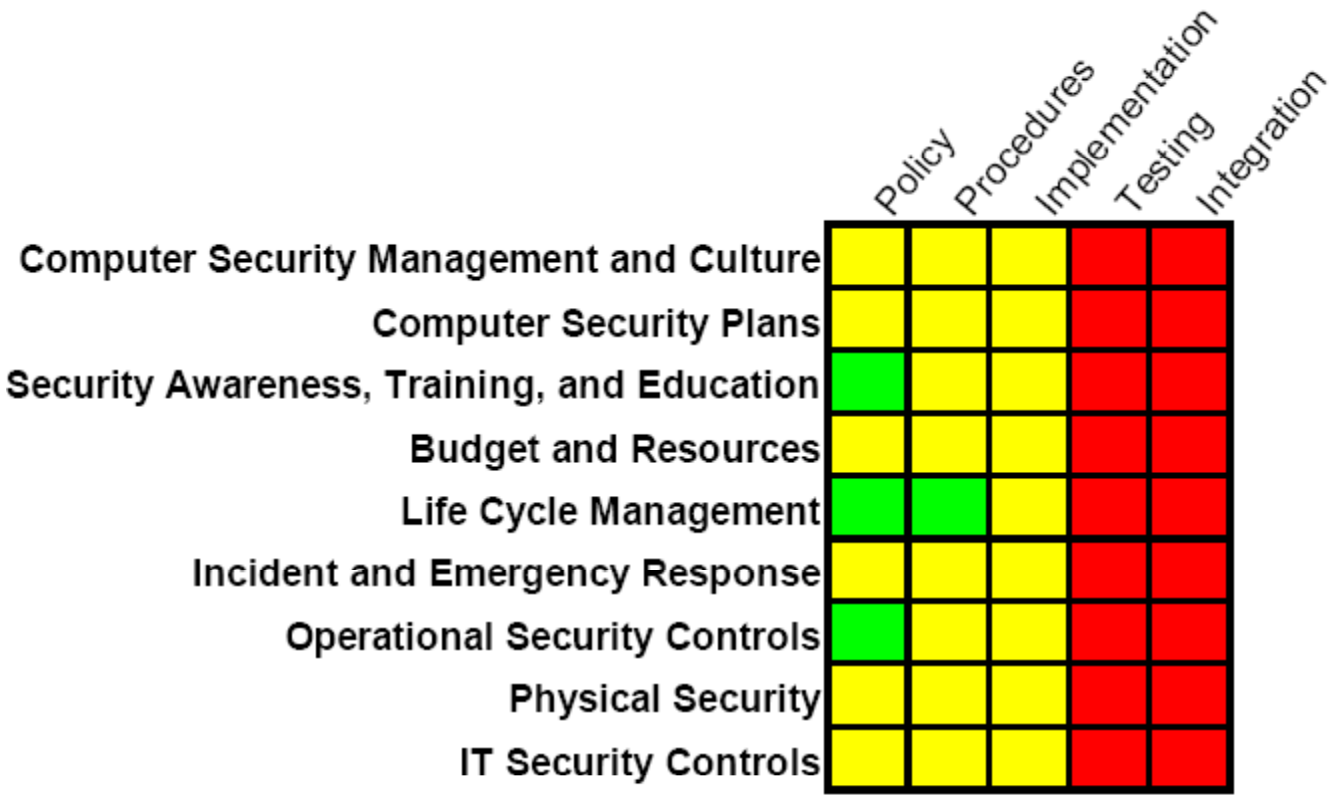
- Information Security Management Maturity Model

- Este modelo es tratado en profundidad en otra presentación de la *VIII Jornada Nacional de Seguridad Informática*!

Modelo NIST-CSEAT

- NIST CSEAT: National Institute of Standards and Technology - Computer Security Expert Assist Team
- 5 niveles de madurez progresiva
  - Política,Procedimiento,Implantación,Prueba, Integración

Modelo NIST-CSEAT



Tópicos del Modelo NIST-CSEAT

- Management and Culture
  - Roles y responsabilidades de TI
  - Revisión de controles de seguridad
  - Reglas de comportamiento y documentación
  - Análisis de desempeño y retroalimentación
  - Protección de Infraestructura física
  - Controles de personal
  - Controles específicos de programa

Tópicos del Modelo NIST-CSEAT

- Plans
  - Plan de seguridad del sistema
  - Administración de riesgos
  - Procesamiento autorizado
  - Documentación

Tópicos del Modelo NIST-CSEAT

- Training and Education
  - Sensibilización y Entrenamiento en seguridad del usuario final
  - Sensibilización y Entrenamiento en seguridad del profesional de TI
  - Sensibilización y Entrenamiento en seguridadde la Gerencia y equipo de liderazgo
  - Entrenamiento de seguridad específico de programas

Tópicos del Modelo NIST-CSEAT

- Budget and Resources
  - Seguridad de la información como parte del proceso de planeación general
  - Se aplican recursos adecuados a la seguridad de la información
  - Presupuesto y recursos de seguridad de TI basados en un modelo de riesgos
  - Soluciones de Seguridad de TI costo-efectivas
  - Controles de adquisición (procurement)

Tópicos del Modelo NIST-CSEAT

- Lifecycle management
  - Ciclo de vida de desarrollo del sistema de información (SDLC- Security Development Life Cycle)
  - Cambios controlados y probados a través del SDLC

Tópicos del Modelo NIST-CSEAT

- Incident and Emergency Response
  - Identificación de activos críticos y sensibles
  - Respuesta ante desastres / contingencias
  - Identificación, reporte y respuesta ante incidentes
  - Continuidad de las operaciones

Tópicos del Modelo NIST-CSEAT

- Operational Security Controls
  - Mantenimiento de hardware y de software
  - Integridad de datos
  - E/S de producción
  - Confidencialidad de datos
  - Disponibilidad de datos
  - Documentación de operaciones del sistema

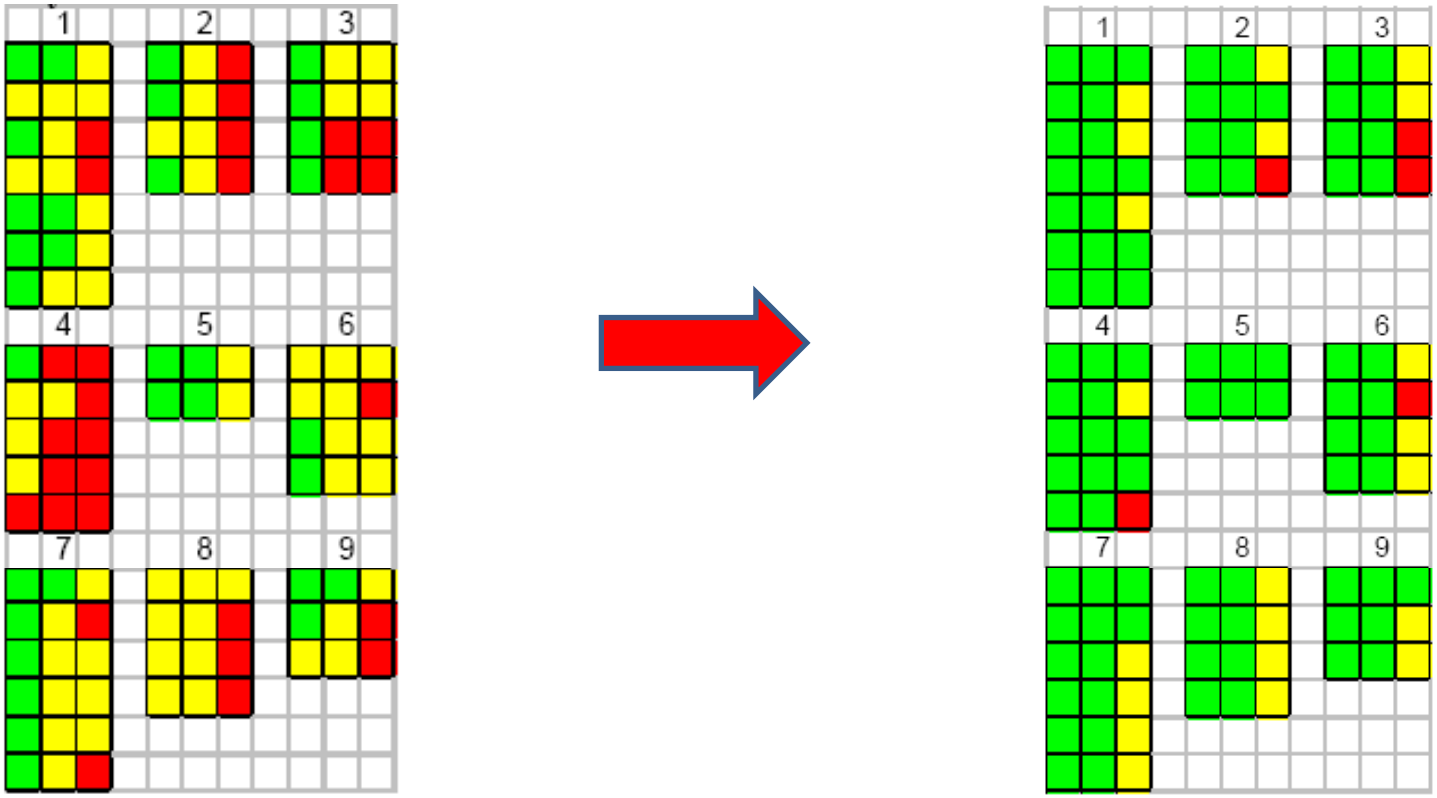
Tópicos del Modelo NIST-CSEAT

- Seguridad Física
  - Implementación de Controles de Seguridad Físicos
  - Protección de dispositivos electrónicos personales
  - Control de emanaciones (radiaciones) – *ver TEMPEST*
  - Controles en instalaciones temporales

Tópicos del Modelo NIST-CSEAT

- Controles de Seguridad de TI
  - Identificación y autenticación
  - Controles de acceso lógico
  - Auditoría

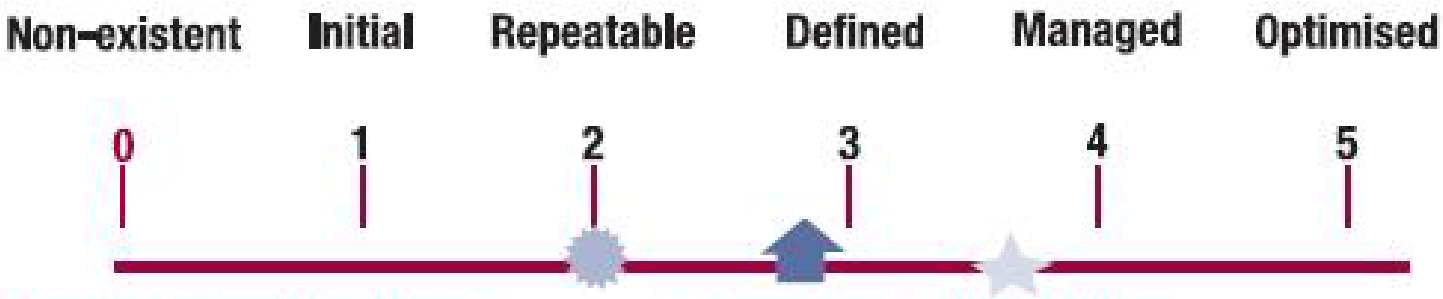
Resultados del Modelo NIST-CSEAT



Cobit Maturity Model

- Modelo de madurez, hace parte de COBIT (Control Objectives for Information and Related Technologies)
- Es muy conocido, y muy popular
- Existen herramientas gratuitas para medir la madurez bajo este modelo

Cobit Maturity Model



LEGEND FOR SYMBOLS USED

- Enterprise current status
- Industry average
- Enterprise target

LEGEND FOR RANKINGS USED

0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

Niveles de Cobit Maturity Model

- **Inexistente:** Se carece totalmente de un proceso. La empresa no ha reconocido la necesidad.

Niveles de Cobit Maturity Model

- **Inicial:** Existe evidencia que la empresa ha reconocido la necesidad del proceso. No existe un proceso formal – estandarizado - si no que existe enfoques ad-hoc que se aplican de manera individual o caso a caso. La gestión del mismo es desorganizada.

Niveles de Cobit Maturity Model

- **Repetible:** El proceso se encuentra suficientemente desarrollado y distintas personas ejecutan más o menos los mismos procedimientos. No existe una comunicación ni entrenamiento formal de los procedimientos, y la responsabilidad es individual. Existe una gran dependencia del conocimiento que tiene los individuos y, por tanto existe una probabilidad de error importante.

Niveles de Cobit Maturity Model

- **Definido:** El proceso está estandarizado, documentado y difundido mediante entrenamiento. Sin embargo, se deja a voluntad de los individuos la aplicación de los procedimientos del proceso y es poco probable que se detecten las desviaciones en su uso. Los procedimientos en sí no son sofisticados y corresponden a la formalización de las prácticas existentes.

Niveles de Cobit Maturity Model

- **Gestionado:** Es posible monitorear y medir la conformidad en la aplicación de los procedimientos del proceso y es posible tomar acciones cuando el proceso no está operando adecuadamente. Los procesos están mejorándose continuamente. Se dispone de automatizaciones y de herramientas que son usadas de una manera limitada o fragmentada.

Niveles de Cobit Maturity Model

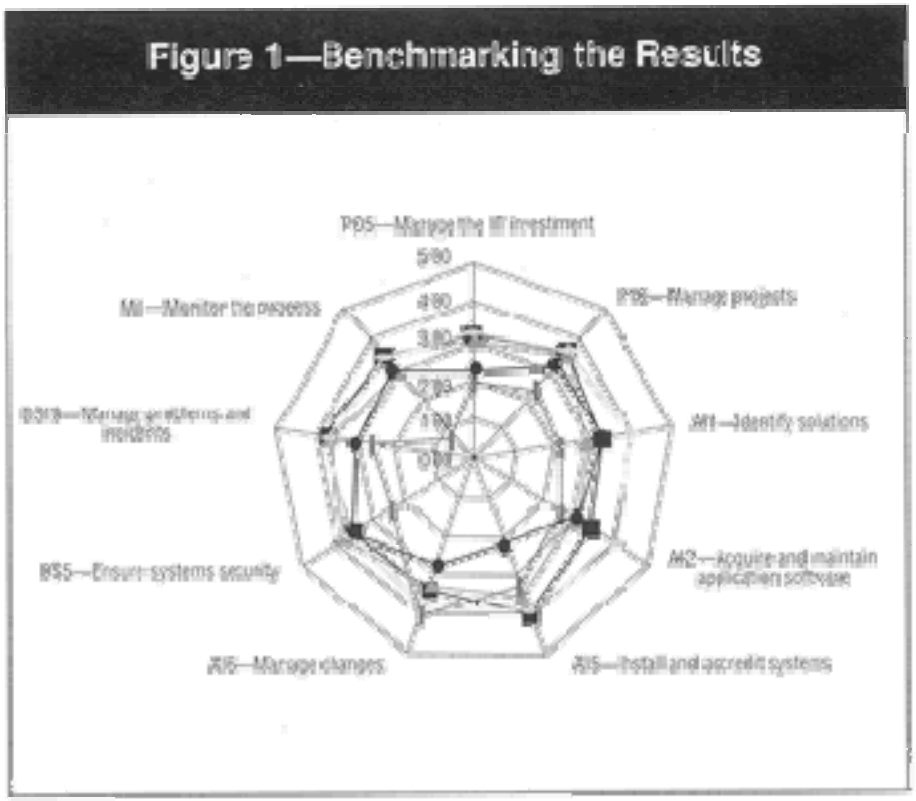
- **Optimizado:** El proceso ha sido refinado al nivel de las mejores prácticas, basado en los resultados del mejoramiento continuo y de los modelos ya maduros de otras compañías. Las TI son usadas integralmente para automatizar workflow, entregando herramientas que mejoran la calidad y efectividad, aumentando la capacidad de adaptación de le empresa.

Tópicos cubiertos por Cobit Maturity Model

- Todos los dominios de Cobit!
  - Plan and Organize
  - Acquire and Implement
  - Deliver and Support
  - Monitor and Evaluate
- Y todos sus objetivos!

Resultados de Cobit Maturity Model

Figure 1—Benchmarking the Results



SSE-CMM

- Modelo de Capacidad y Madurez en la Ingeniería de Seguridad de Sistemas
- Es un modelo derivado del CMM
- Describe las características esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad de sistemas

SSE-CMM

- Cinco niveles de madurez progresiva:
  - Existente
  - Repetible
  - Persona designada
  - Documentado
  - Revisado y actualizado

SSE-CMM

- Mide usando cuatro niveles:
  - Inicial
  - En desarrollo
  - Establecido
  - Gestionado

Tópicos de SSE-CMM

- Administer System Security Controls
- Assess Operational Security Risk
- Attack Security
- Build Assurance Argument
- Coordinate Security
- Determine Security Vulnerabilities
- Monitor System Security Posture
- Provide Security Input
- Specify Security Needs
- Verify and Validate Security

Administer System Security Controls

- Objetivos:
  - Determinar si los controles de seguridad son configurados y usados de manera apropiada
- Prácticas Base:
  - Establecer responsabilidades de seguridad
  - Administrar las configuraciones de seguridad
  - Administrar los programas de sensibilización, entrenamientoy educación en seguridad
  - Administrar servicios de seguridad y mecanismos de control

Assess Operational Security Risk

- Objetivos:
  - Obtener un entendimiento de los riesgos de seguridad asociados con la operación de sistemas dentro de un entorno específico
- Prácticas Base:
  - Seleccionar el método de análisis de riesgos
  - Priorizar los activos y las capacidades operacionales
  - Identificar amenazas
  - Analizar el impacto operacional

Attack Security

- Objetivos:
  - Identificar las vulnerabilidades del sistema y determinar su potencial de ser explotadas.
- Prácticas Base:
  - Ataques focalizados
  - Desarrollar escenarios de ataques
  - Realizar ataques
  - Sintetizar resultados de ataques

Build Assurance Argument

- Objetivos:
  - Determinar si los productos y procesos de trabajo proveen evidencia de que los requerimientos de seguridad del cliente han sido cubiertos
- Prácticas Base:
  - Identificar los objetivos de aseguramiento
  - Definir la estrategia de aseguramiento
  - Controlar la evidencia de aseguramiento
  - Analizar la evidencia
  - Proveer argumentos de aseguramiento

Coordinate Security

- Objetivos:
  - Todos los miembros del equipo conocen y están involucrados con actividades de ingeniería de seguridad de manera suficiente para realizar su trabajo de manera adecuada.
  - Las decisiones y recomendaciones relacionadas con seguridad se comunican y se asumen de manera coordinada.
- Prácticas Base:
  - Definir los objetivos de coordinación
  - Identificar los mecanismos de coordinación
  - Facilitar la coordinación
  - Coordinar decisiones y recomendaciones de seguridad

Determine Security Vulnerabilities

- Objetivos:
  - Obtener un entendimiento de las vulnerabilidades del sistema
- Prácticas Base:
  - Seleccionar método de análisis de vulnerabilidades
  - Analizar los activos del sistema
  - Identificar amenazas
  - Identificar vulnerabilidades
  - Sintetizar vulnerabilidades del sistema

Monitor System Security Posture

- Objetivos:
  - Detectar y rastrear eventos de seguridad internos y externos.
  - Responder a los incidentes de acuerdo con las políticas
  - Identificar y administrar los cambios a las posturas operativas de seguridad de acuerdo con los objetivos de seguridad
- Prácticas Base:
  - Analizar los registros de eventos
  - Monitorear cambios
  - Identificar incidentes de seguridad
  - Monitorear Salvaguardas de Seguridad

Provide Security Input

- Objetivos:
  - Todos los incidentes en el sistema se revisan para detectar implicaciones de seguridad y se resuelven de acuerdo con los objetivos de seguridad
  - Todos los miembros del equipo tienen un entendimiento adecuado de la seguridad para llevar a cabo sus labores.
  - La solución refleja los insumos de seguridad provistos
- Prácticas Base:
  - Entender las necesidades de insumos de seguridad
  - Determinar constreñimientos y consideraciones
  - Identificar alternativas de seguridad
  - Analizar la seguridad de las alternativas de ingeniería
  - Proveer guías de seguridad para ingeniería
  - Proveer guías de seguridad para operaciones

Specify Security Needs

- Objetivos:
  - Llegar a un entendimiento común de las necesidades de seguridad entre todas las partes, incluyendo clientes.
- Prácticas Base:
  - Entender las necesidades de seguridad de los clientes
  - Identificar leyes, políticas, estándares y constreñimientos aplicables
  - Idenficar el contexto de seguridad del sistema
  - Capturar la perspectiva de seguridad de las operaciones del sistema
  - Capturar los objetivos de seguridad de alto nivel
  - Definir los requerimientos de seguridad del sistema
  - Obtener acuerdos sobre la seguridad

Verify and Validate Security

- Objetivos:
  - Garantizar que las soluciones cumplan con los requerimientos de seguridad
  - Garantizar que las soluciones cumplan con los requerimientos operacionales de seguridad de los clientes
- Prácticas Base:
  - Identificar objetivos de verificación y validación
  - Definir la aproximación a la verificación y validación
  - Ejecutar la verificación
  - Ejecutar la validación
  - Proveer resultados

¿PARA QUE NECESITO UN MODELO DE MADUREZ?

- Nadie tiene un sistema óptimo de la noche a la mañana
- No se puede optimizar la seguridad de un sistema en una implantación "Big Bang"
  - La optimización debe ser gradual
  - No debe interrumpir la operación normal del sistema
  - Debe darse tiempo a la organización para que absorba los cambios

¿PARA QUE NECESITO UN MODELO DE MADUREZ?

- Un modelo de madurez me permite ir creciendo de manera estructurada, planeada y balanceada
- Mi crecimiento siempre debe estar alineado con los requerimientos de seguridad de mi organización (no hay que crecer por crecer…)

¿Y SI QUIERO APLICAR UNO, QUE DEBO HACER?

- Estudiar la oferta de modelos disponibles
- Escoger el más adecuado a mi organización
  - Por su enfoque (sistemas, procesos, documentación, etc.)
- Medirme contra el modelo
- Determinar adónde quiero estar

¡¡¡NO SIEMPRE ES NECESARIO TENER **TODO** EN EL NIVEL MAS ALTO DE MADUREZ!!!

¿Y SI QUIERO APLICAR UNO, QUE DEBO HACER (2)?

- Realizar un estudio costo/beneficio y una justificación de por qué debo llegar al novel de madurez deseado
- Desarrollar un plan para llegar a dicho nivel de madurez
  - Desarrollar portafolio de inciativas, programas y proyectos
- Empezar a ejecutar mi plan de optimización
- Medirme continuamente para verificar que estoy avanzando hacia mis metas

Conclusiones

- Algunos modelos están orientados a madurez, otros a capacidades
- Algunos modelos están orientados a sistemas, otros a procesos
- Unos se ajustan más a las necesidades de una organización que otros

Conclusiones (2)

- Son una herramienta estratégica muy importante
- Me permiten crecer de manera organizada y equilibrada
- Me permiten compararme con otras organizaciones

¿Preguntas?

roberto.arbelaez@microsoft.com