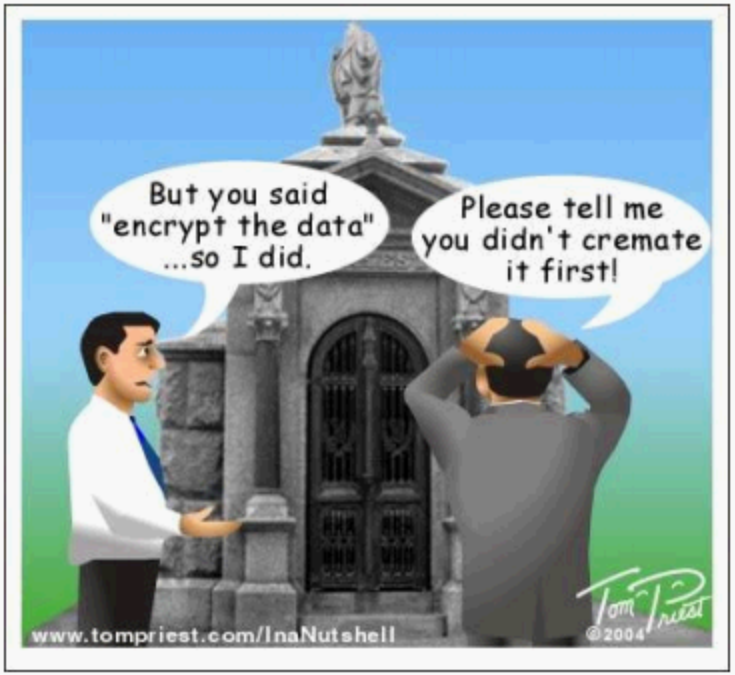
Tratamiento de Datos Personales y su seguridad

Roque C. Juárez,
Consultor de Seguridad de la Información
IBM de México



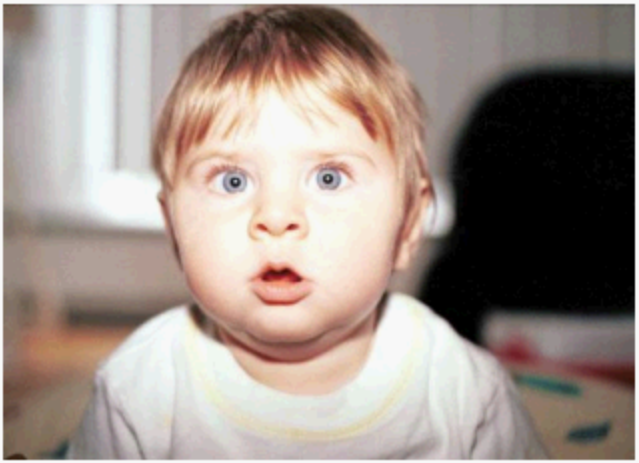
"Encryption isn't the issue here."

- Bruce Schneier.

Contenido

- Otra vez el sentido de la inseguridad
- ¿Cuánta seguridad se necesita?
- Asegurar para operar…
- Premisas para protección y cumplimiento.
- Conclusiones.

Otra vez el sentido de la inseguridad



¿Otra vez el sentido de la inseguridad?

- La operación de TI y Seguridad de la Información se ha fortalecido a través de:

Esfuerzos generales de Seguridad de la Información	S/N
Análisis técnicos del nivel de seguridad	✓
Concientización inicial de riesgos y seguridad de la información	✓
Roles y responsabilidades específicos de seguridad de la información y control interno	✓
Demuestra efectividad en el cumplimiento	✓
Presupuestos específicos de seguridad	✓

¿Otra vez el sentido de la inseguridad?

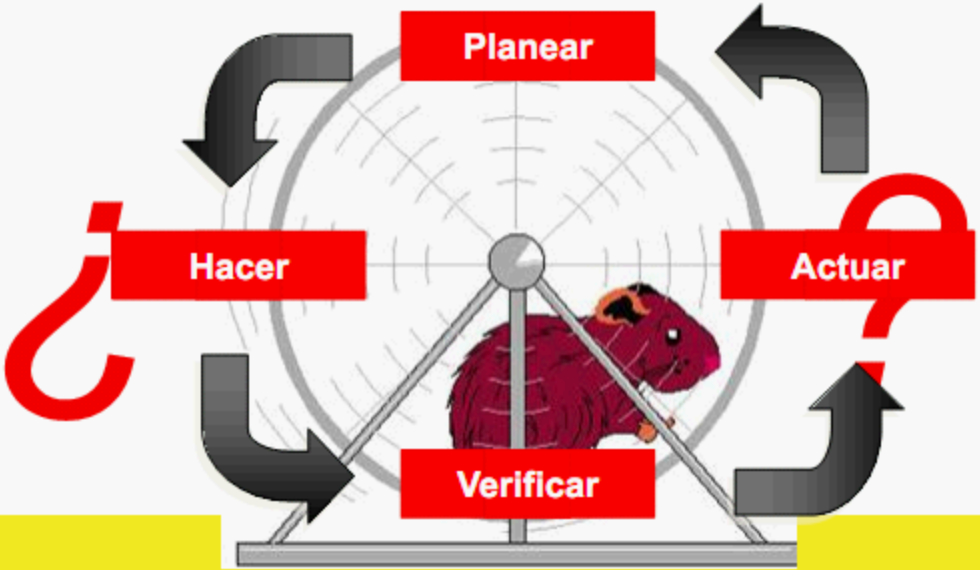
- Algunas organizaciones están más preocupadas y, ocupadas que antes:

Hay más problemas, más brechas, más riesgos…

- Siempre han existido, solamente que ahora las identificamos y, sabemos cosas que antes no sabíamos…

¿Otra vez el sentido de la inseguridad?

- Se obtienen certificaciones de estándares, mejores prácticas y cumplimiento con leyes aplicables.



Rueda del Hámster en Seguridad

¿Otra vez el sentido de la inseguridad?

- La seguridad de la información ha sido tratada con una visión tecnológica.

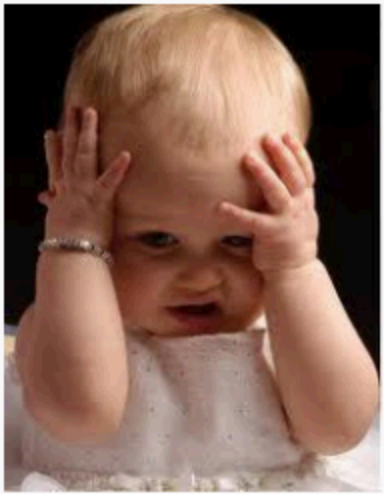
¿Prioridades de protección?

¿Métricas de gestión de seguridad?

¿Inversión o gasto de seguridad?

¿Niveles de criticidad?

¿Cuánta seguridad se necesita?



¿Cuánta seguridad se necesita?

- *¿Mucha seguridad?¿Poca seguridad?¿Toda la posible?¿La que recomienden los proveedores?...*

- Es el momento de:
  - Implantar las ***necesidades*** reales de ***protección*** y ***operación*** de sus entidades, áreas y procesos relacionadas con datos personales.
  - Demostrar ***efectividad*** de los controles como parte de su naturaleza.
  - Encontrar nuevas ***formas de operación*** de los controles de seguridad.

¿Cuánta seguridad se necesita?

- Desarrollen análisis y evaluación de riesgos de seguridad de la información.

Mitigar

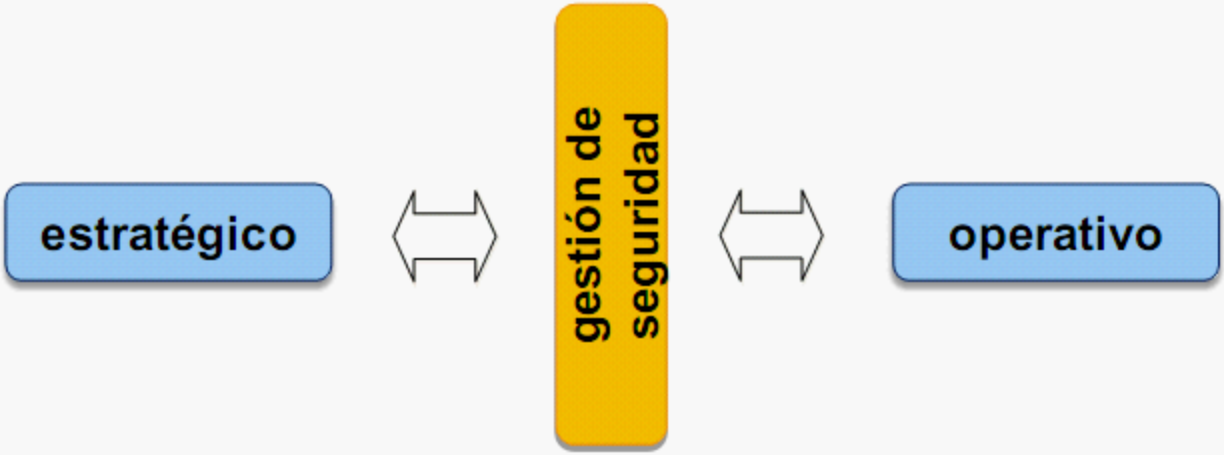
Transferir

Aceptar

Asegurar para operar

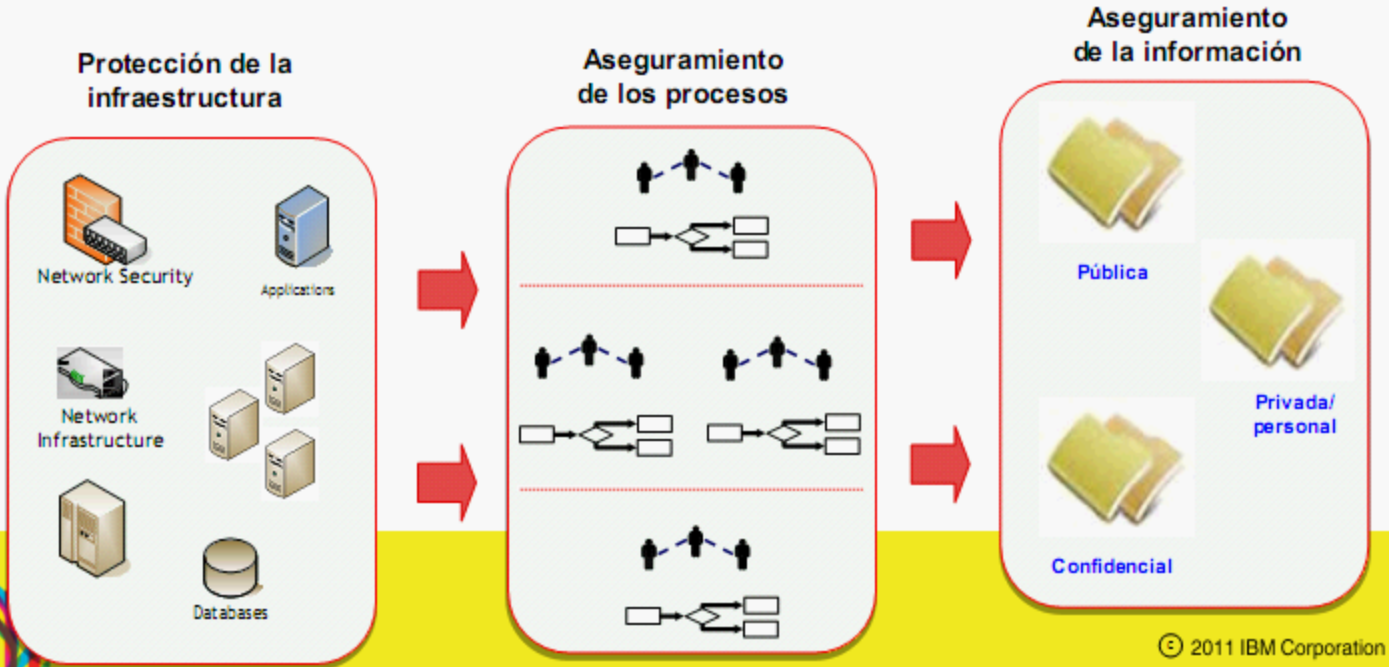
Asegurar para operar...

- La seguridad de la información se establece en forma práctica con tres componentes fundamentales:



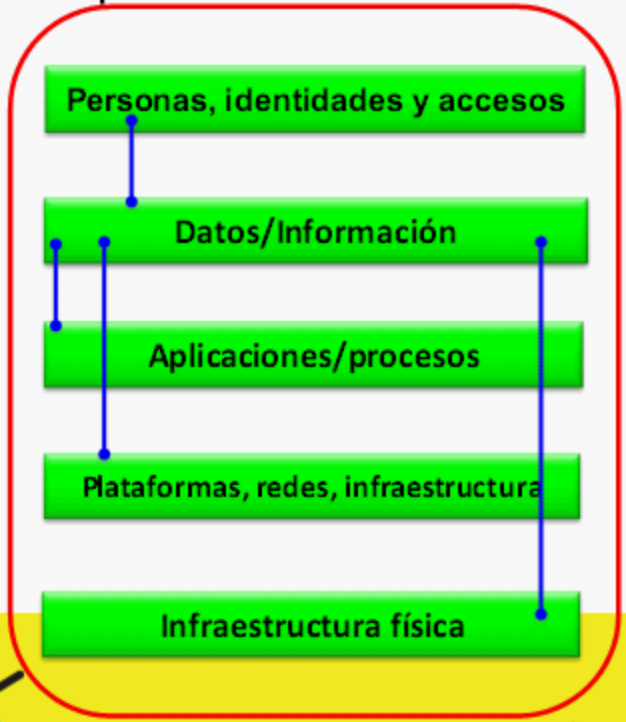
Asegurar para operar...

- Complementar el enfoque tradicional de **protección y aseguramiento** de la tecnología y la infraestructura.



Asegurar para operar…

- Implantación de controles de seguridad.



- Desarrollar proyectos específicos de controles de seguridad en más de una capa de activos.
- Fortalecer el marco normativo y la concientización.
- Considerar la creación, preservación y control de evidencias.

Asegurar para operar…

- Implantación de controles de seguridad.

Requerimiento de la Ley

- Bloqueo de datos.
- Disociación de datos.
- Obtención de datos.
- Cancelación de datos.
- Resguardo de datos.
- Transmisión de datos.
- Almacenamiento de datos.
- Control de las vulnerabilidades.
- Control actividades para derechos ARCO.

Premisas para protección y cumplimiento

Premisas para protección y cumplimiento

- Evitar el ***falso sentido*** de la seguridad y ***el nada va a pasar***.

Premisas para protección y cumplimiento

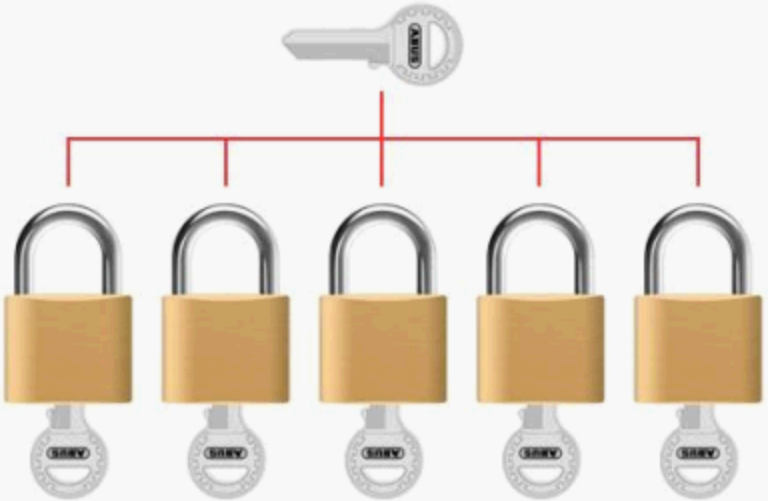
- Consolidemos el alcance organizacional de la seguridad de la información.
  - –“Una política firmada no garantiza su aplicación.”
  - –“Un indicador bajo de incidentes, no significa que estemos seguros.”

Premisas para protección y cumplimiento

- Incrementen el nivel de implementación y monitoreo de las definiciones formales, políticas y estándares que han creado.

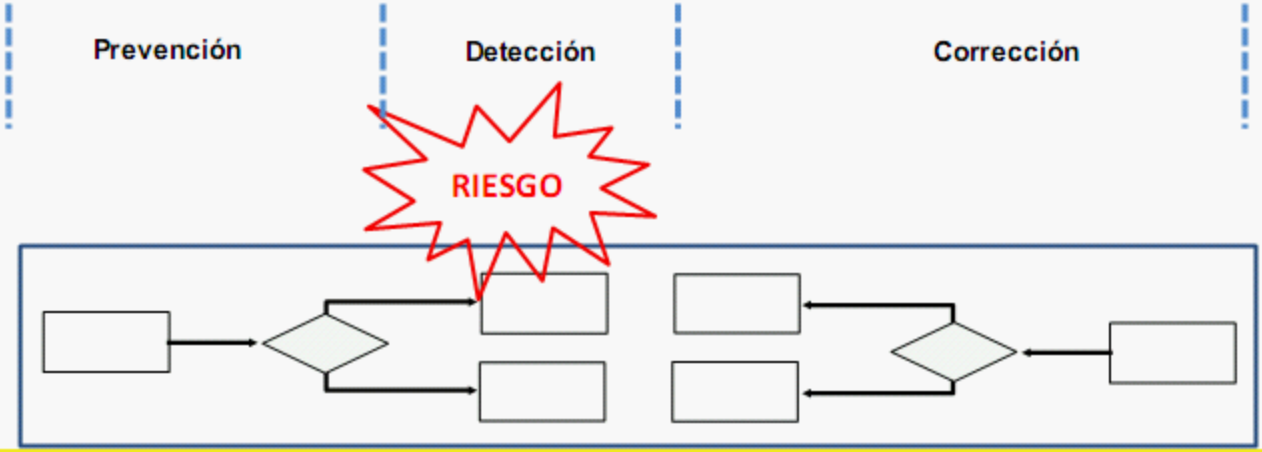
Premisas para protección y cumplimiento

- Terminar la búsqueda de la *«llave mágica»* de la protección de datos personales.



Premisas para protección y cumplimiento

- Implementación de la seguridad en diferentes fases de la operación con objetivos complementarios: ***Prevención, Detección y Corrección.***



Consideraciones finales

Consideraciones finales

- La seguridad es un proceso… seguiremos teniendo costos altos, impactos ignorados y cierto nivel de “inseguridad”.

Consideraciones finales

- No sirve de nada llenarse de miedo ante los diferentes requerimientos de la Ley.

¡¡pero hay que informarnos!!

Consideraciones finales

- La gestión asertiva de la seguridad ***no requiere*** renovar toda la tecnología, sino definir como obtener el mayor beneficio.

- Las ***soluciones específicas*** para un problema actual, requerirá esfuerzos ***posteriores*** para su integración al esquema operativo.

Consideraciones finales

- Se aumentan las capacidades de prevención, detección, corrección y seguimiento de brechas de seguridad.

Consideraciones finales

- Lograr el cumplimiento de la Ley sin identificar el nivel de seguridad aceptado por la organización no agrega valor.

¿?

El cumplimiento de la Ley debe ser una muestra natural del éxito de la gestión de seguridad de la información en la organización.

¿¿Preguntas??

Gracias.

Roque C. Juárez
rjuarez@mx1.ibm.com
Consultor de Seguridad de la Información