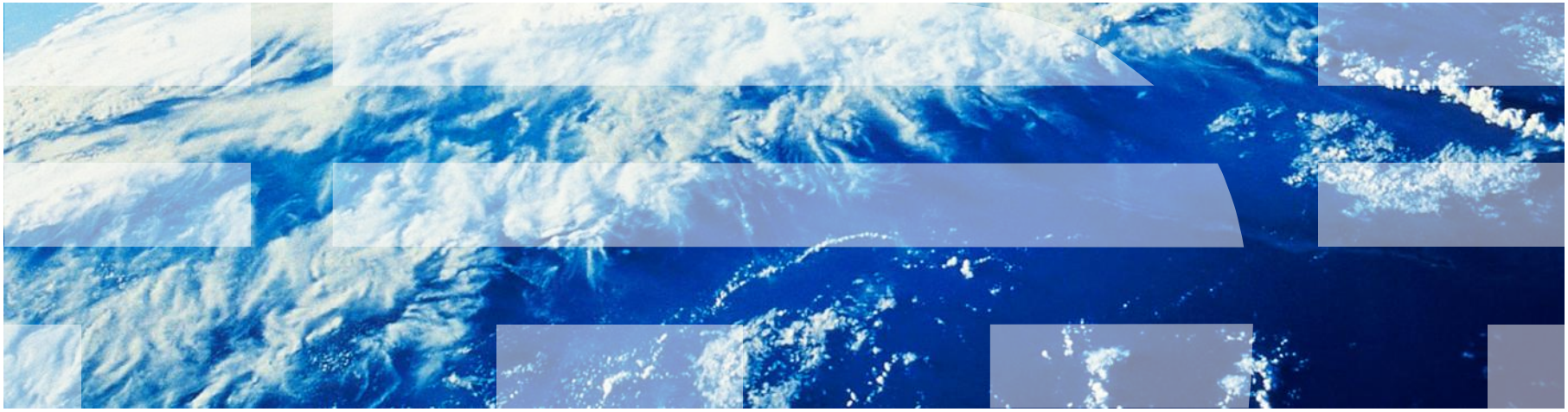
IBM – Seguridad de la Información

Mejores prácticas para la privacidad de datos

Roque C. Juárez
Consultor de Seguridad de la Información



"Secrets are only as secure as the least trusted person who knows them."

Bruce Schneier

Contenido

- Contexto de la privacidad y protección de datos.
- Implicaciones de las regulaciones de privacidad.
- Premisas para el esfuerzo.
- Enfoque práctico recomendable.
- Conclusiones

Contexto de la privacidad y protección de datos

Contexto de la privacidad y protección de datos

- La privacidad se apoya en seguridad de la información.
  - –No es posible la privacidad sin seguridad.
  - –Pero es posible tener buena seguridad sin privacidad.

Contexto de la privacidad y protección de datos

- La privacidad es personal.
  - Definida por el individuo.
  - Varía en cada cultura corporativa y social.
  - Un «esquema» no se aplica en forma generalizada.

Contexto de la privacidad y protección de datos

- En el mundo existen políticas y principios para promover privacidad.
  - –Principios de protección de datos (OECD, APEC)
  - –Leyes y regulaciones por sector (HIPAA)
  - –Enfoques de auto regulación.
    - Mejores prácticas de publicidad online.
    - Empresas con prácticas globlales.

Contexto de la privacidad y protección de datos – En el caso de México.

- Desde los años 2000/2001 se venían haciendo esfuerzos relativos a la legislación sobre la protección de datos personales.
- El 25 de Marzo de 2010, el Senado aprueba la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- La LFPDPPP se publica en el Diario Oficial de la Federación hasta el ***5 de Julio de 2010***.

Contexto de la privacidad y protección de datos – En el caso de México.

Objeto

- Art. 1. «…la **protección** de los datos personales en posesión de los particulares, con la finalidad de regular su **tratamiento legítimo, controlado e informado**, a efecto de garantizar **la privacidad y el derecho** a la autodeterminación informativa de las personas.»

Contexto de la privacidad y protección de datos – En el caso de México.

Alcance

- Art. 2. «…los particulares sean **personas físicas o morales** de carácter privado que lleven a cabo el tratamiento de datos personales, **con excepción de**:
  - Las sociedades de información crediticia…
  - Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal…»

Contexto de la privacidad y protección de datos – En el caso de México.

Sanciones

- "**…Multa de 100 a 160,000 días de salario mínimo** vigente en el Distrito Federal, en los casos previstos en las fracciones II a VII del artículo anterior;

- **Multa de 200 a 320,000 días de salario mínimo** vigente en el Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo anterior," Art. 64

- "…***tres meses a tres años de prisión***… provoque una vulneración de seguridad…" Art. 67
- "…***prisión de seis meses a cinco años***… trate datos personales mediante engaño…" Art. 68

Contexto de la privacidad y protección de datos – En el caso de México.

- Las fechas para recordar.

- Publicación de la Ley

- Entrada en vigor.
- Aprobación del reglamento.
- **Función de Datos Personales y Aviso de privacidad.**

- Ejercicio de derechos **ARCO.**
- Procedimiento de protección de derechos

Contexto de la privacidad y protección de datos

Controles de divulgación

Controles de acceso

Controles de divulgación (Privacidad)

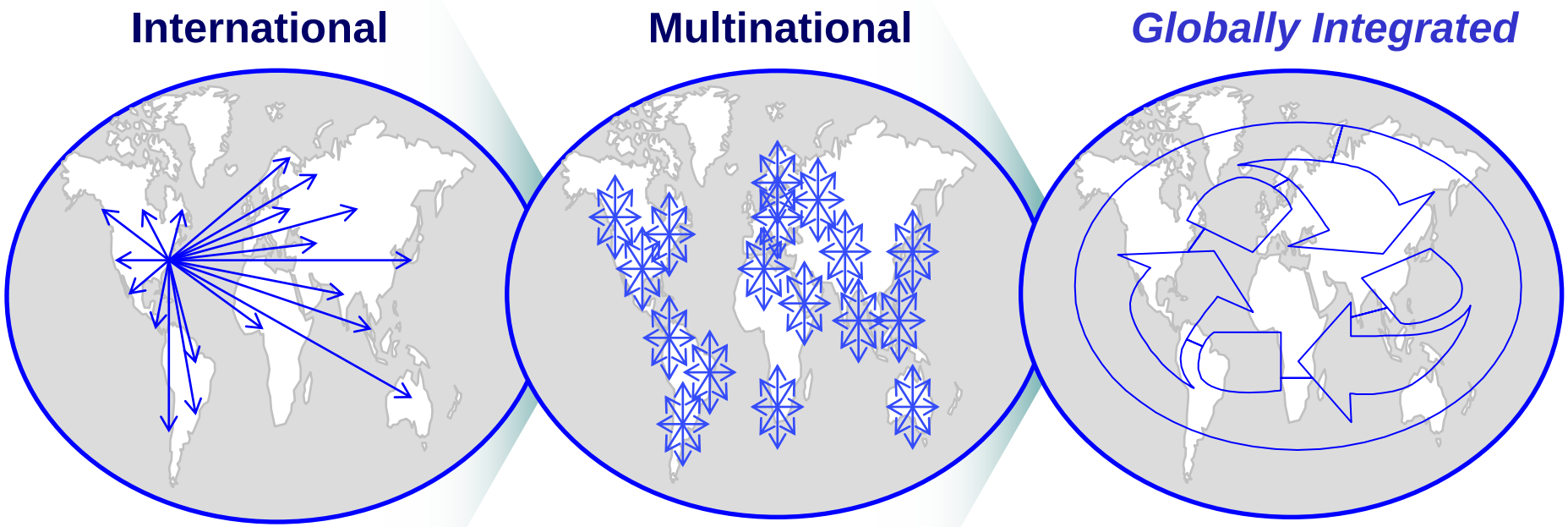
¿Qué datos viste/usaste?
¿Cuál fue el propósito del negocio?
Auditoria: Qué datos fueron revelados, a quién, por qué y, si se cumplió con la política de la empresa.

Controles de Acceso (Seguridad)

¿Quién eres tú?
¿A qué grupo/categoría perteneces?
¿Tienes acceso/privilegio para accesar las herramientas?
Auditoría: ¿Quién ingreso al sistema y cuándo?

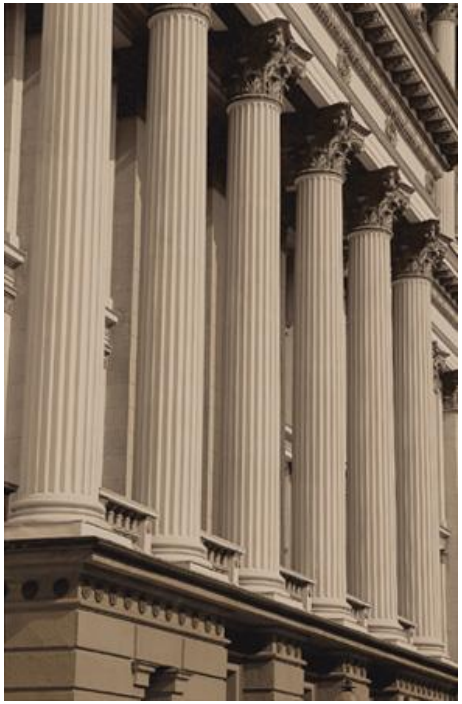
La privacidad cambia el contexto de negocio

- Cambios en los modelos de negocio.
  - Las empresas están aprovechando ventajas de la globalización.



La privacidad cambia el contexto de negocio

- Presiones externas.
  - –Ambiente regulatorio dinámico.
  - –Expectativas de la sociedad, clientes y asociados de negocio.



ifai

CNBV
COMISION NACIONAL BANCARIA Y DE VALORES

COBIT

ITIL®

ISO

PCI Security Standards Council

Personas

Datos/Información

Aplicaciones/procesos

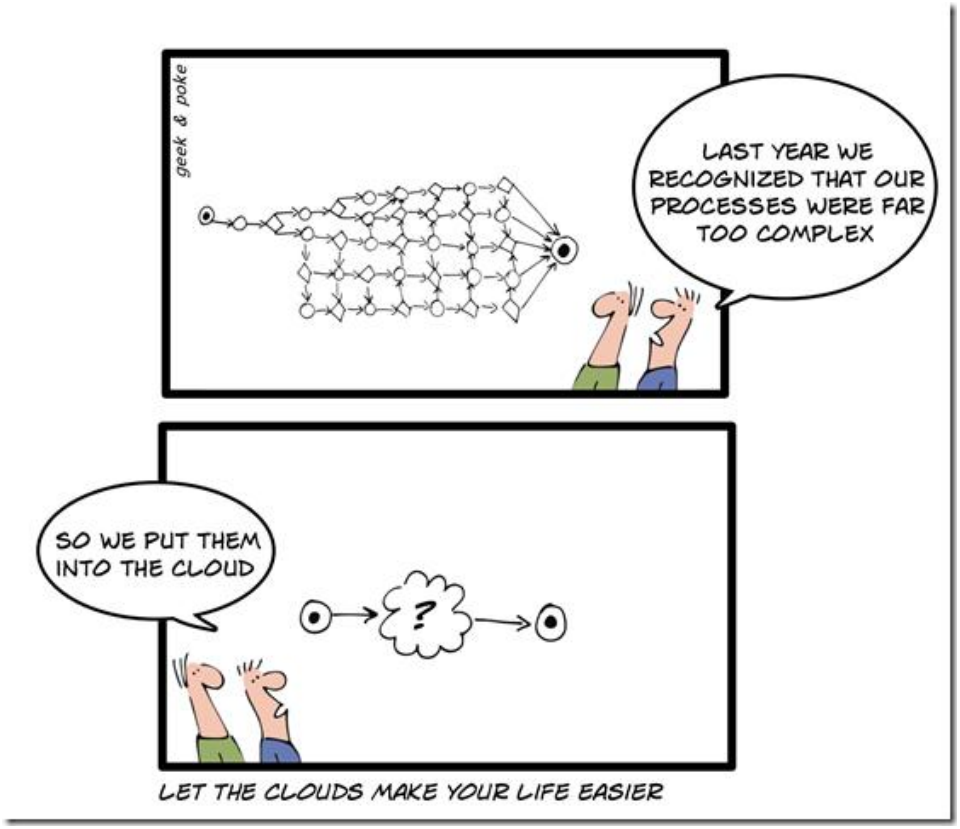
Plataformas, redes, infraestructura

Infraestructura física

Ambiente de operación y procesamiento de TI

La privacidad cambia el contexto de negocio

- Evolución de los modelos tecnológicos que apoyan al negocio (ej. Cloud Computing)



«La seguridad y la privacidad, no sólo son un problema ***tecnológico***, son un problema ***organizacional*** y de ***gente,*** con ***implicaciones de negocio***»

Implicaciones de las regulaciones de privacidad

Implicaciones de las regulaciones de privacidad

- Generación de una cultura del miedo a las brechas de seguridad.

Implicaciones de las regulaciones de privacidad

- Adopción reactiva y limitada de medidas de seguridad tecnológica.

Implicaciones de las regulaciones de privacidad

- Búsqueda de resquicios y excepciones de las regulaciones de privacidad.

Implicaciones de las regulaciones de privacidad

- Reconocimiento gradual de un tópico organizacional.

Implicaciones de las regulaciones de privacidad

- Incremento de los recursos y presupuestos para el esfuerzo de privacidad y seguridad.

Ahora la seguridad de la información además de compleja, es obligatoria.

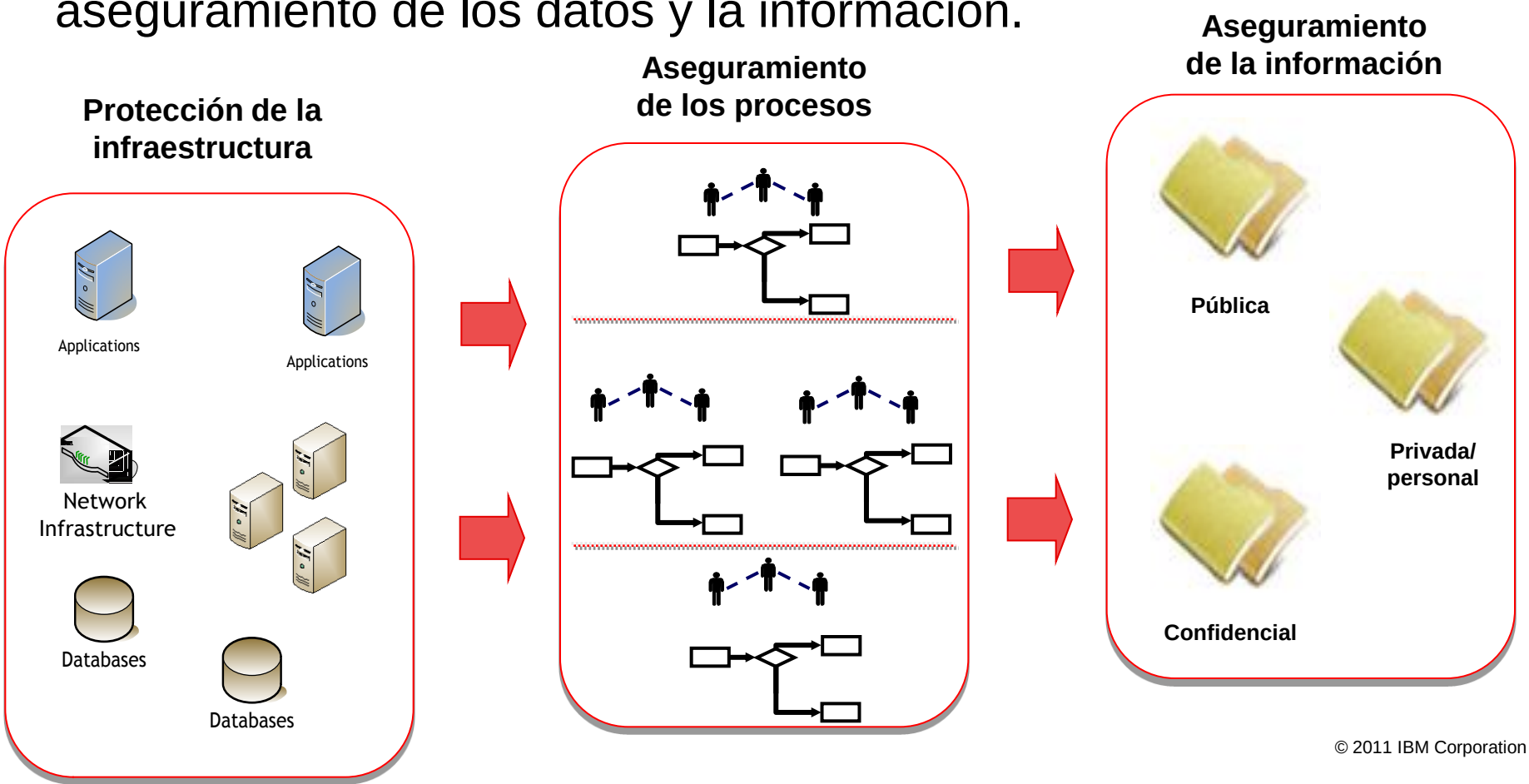
Premisas para el esfuerzo

Premisas para el esfuerzo

- Evitar el falso sentido de la seguridad o confianza excesiva.

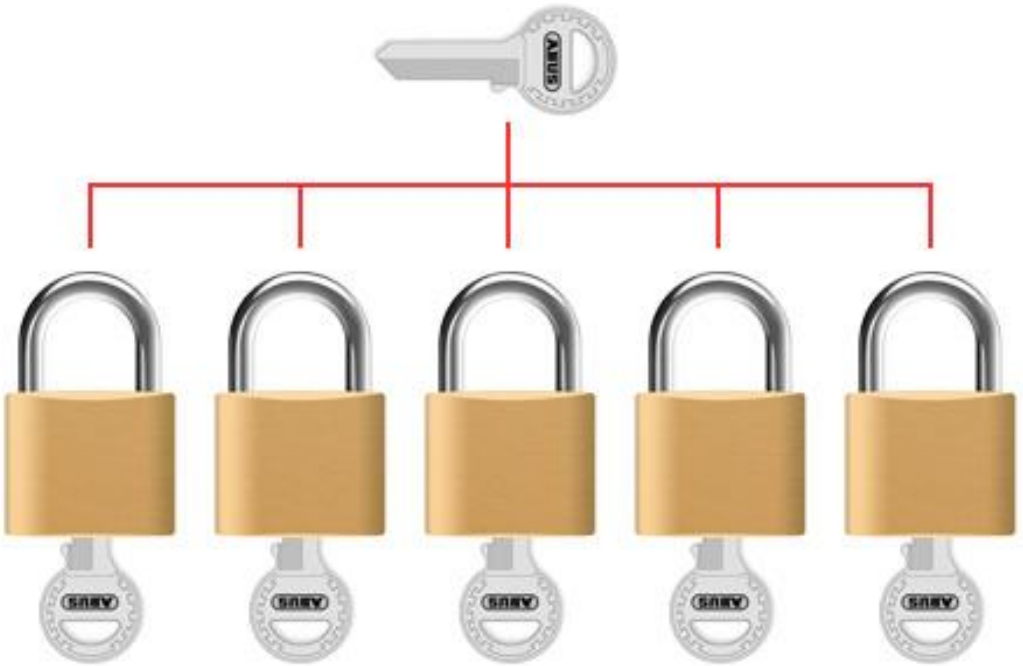
Premisas para el esfuerzo

- Cambiar el paradigma de aseguramiento de infraestructura, por el aseguramiento de los datos y la información.



Premisas para el esfuerzo

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

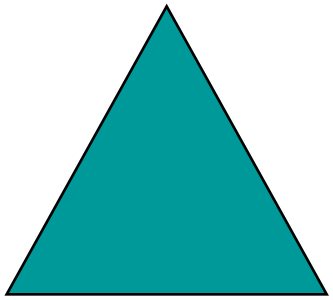


Enfoque práctico recomendable

Enfoque práctico recomendable

- Desarrollar un modelo de privacidad simple.
  - Definir criterios de clasificación de información.
  - Desarrollar un marco normativo aplicable a la organización y sus filiales.

Nota: Privacidad descansa en un modelo de seguridad sólido.

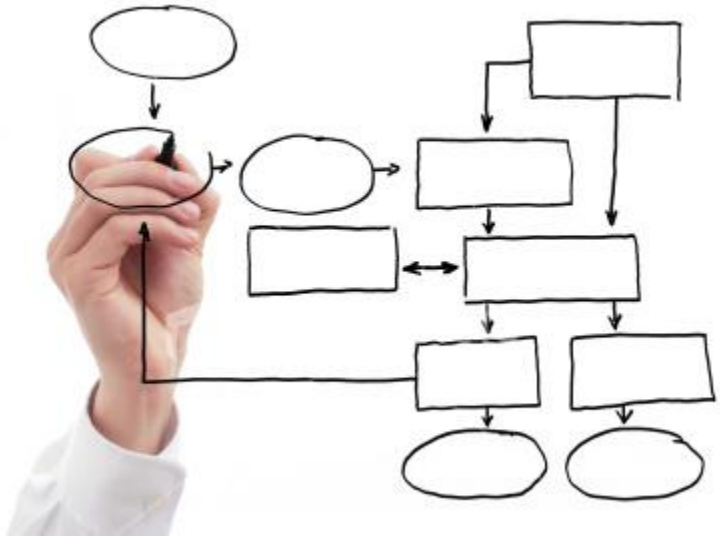


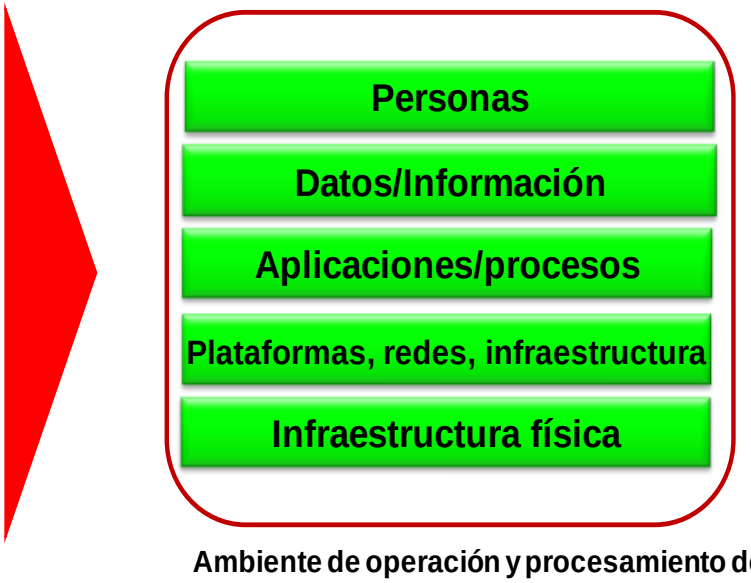
Enfoque práctico recomendable

- Asignar roles y responsabilidades específicos de seguridad de la información y privacidad.
  - Dueño de los procesos/información/datos.
  - Custodios.
  - Usuarios.
  - Oficial de Privacidad.
  - Contacto para derechos ARCO.

Enfoque práctico recomendable

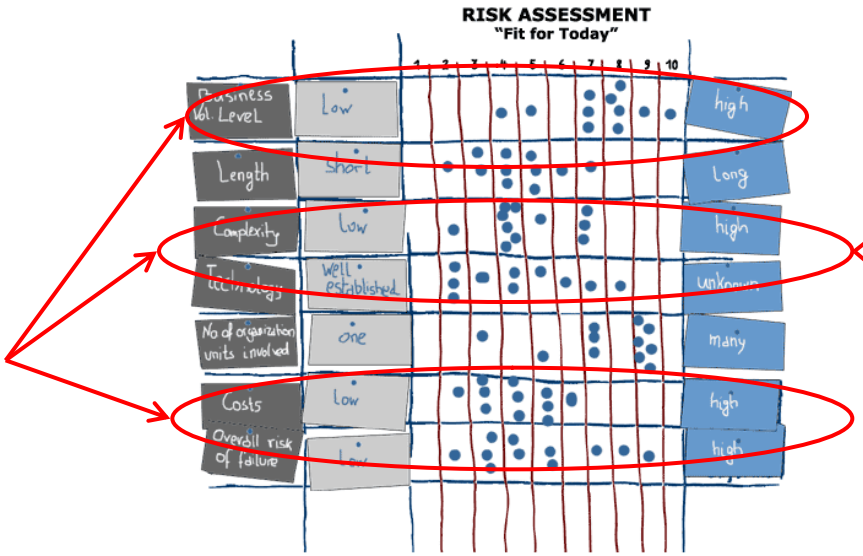
- Determinar procesos organizacionales, sistemas y aplicaciones donde existan datos personales.





Enfoque práctico recomendable

- Desarrollar análisis de riesgos y de impacto para determinar prioridades de protección.



Estrategia de Seguridad

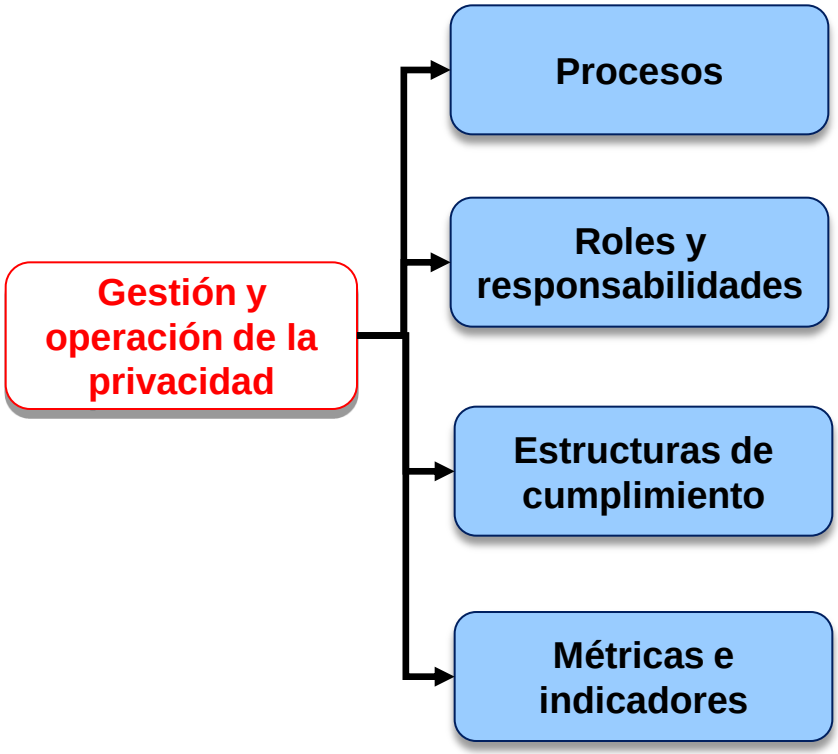
Nivel de riesgo aceptable

Enfoque práctico recomendable

- Capacitar al personal de la organización y terceros, en temas de privacidad de datos.

Enfoque práctico recomendable

- Integrar un marco de gestión de la privacidad.
  - –Procesos administrativos.
    - Solicitud y atención de derechos ARCO.
    - Atención de revisiones externas.
    - Control de comunicaciones.
    - Relación con entidades especializadas.
  - –Procesos de gestión técnica
    - Respaldo de datos personales.
    - Control de vulnerabilidades técnicas.
    - Monitoreo de acceso y uso de datos.
    - Destrucción de información.
    - Transmisión y uso de datos.
    - Gestión de bitácoras y evidencias.
    - Gestión de incidentes y brechas.
  - –Procesos de medición de efectividad.

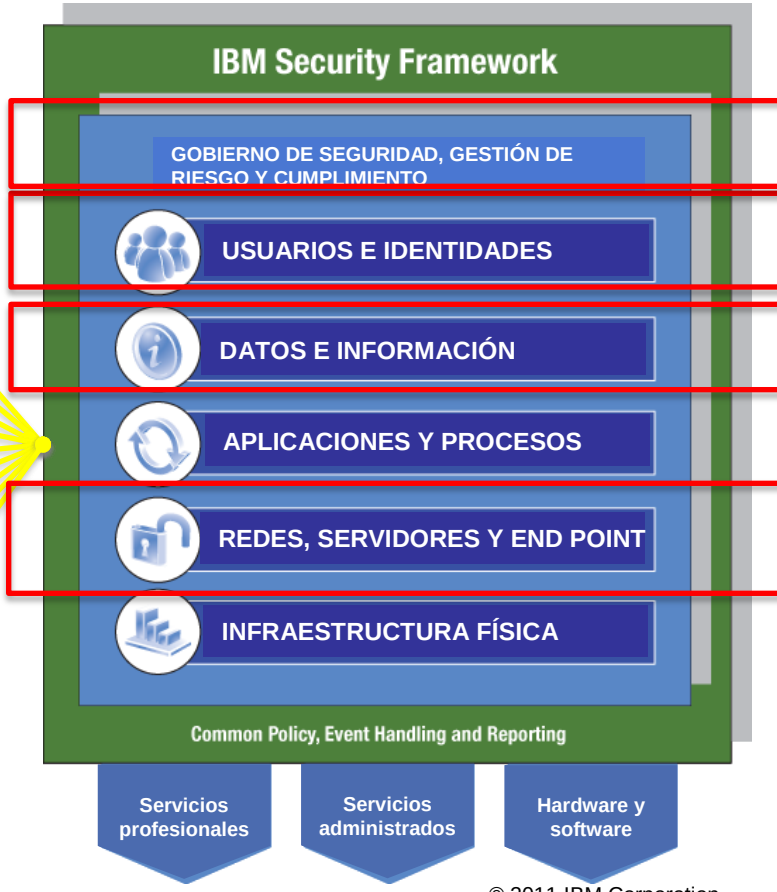


Enfoque práctico recomendable

- Adquisición de nuevos mecanismos integrales de protección de información.

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.**



Enfoque práctico recomendable

- Ejemplo: Modelo integral de IBM para la protección de datos.
  - –Políticas y estándares corporativos.
  - –Amplio esquema de administración de la información.
  - –Mejores prácticas: Desarrollo e incorporación.
  - –Educación/Comunicación.
  - –Controles de negocio.
  - –Modelo de respuesta a incidentes / Aprendizaje.

«La organización debe considerar el desarrollo gradual de una ***cultura de la privacidad***»

Conclusiones

Conclusiones

- Para lograr la protección de datos personales, no es suficiente replicar el esquema tecnológico de seguridad.

Conclusiones

- Cumplir con los ejercicios de auditoría o certificación, no garantiza que estemos logrando el nivel de aseguramiento requerido por la organización.

¿?

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

Conclusiones

- La incorporación de nuevos servicios y métodos de tecnología implica una evaluación de negocio.

Conclusiones

- La seguridad y privacidad son procesos… seguiremos teniendo costos altos, impactos ignorados y cierto nivel de “inseguridad”.

Conclusiones

El cumplimiento de las regulaciones de privacidad aumenta la confianza de los clientes y colaboradores, y desarrolla nuevos diferenciadores de negocio.

¿¿Preguntas??

¡Gracias!

Roque C. Juárez,
IBM de México
Consultor de Seguridad de la Información
rjuarez@mx1.ibm.com
@roque_juarez