



Riesgo Tecnológico

Programa de Capacitación sobre Gestión de Riesgos con enfoque en seguros

Julio de 2017



Superintendencia de Bancos
Guatemala, C. A.



Presentación elaborada con fines informativos, en el marco del Programa de Educación Financiera. La Superintendencia de Bancos no es responsable por los usos que se dé o las decisiones que se tomen, basadas en la información contenida, ya que ésta no podrá considerarse como asesoría u opinión técnica vinculante. El uso, reproducción, edición, copia, publicación o distribución parcial o total, por cualquier medio, por parte de terceros, deberá contar con autorización de la Superintendencia de Bancos.

Agenda

✓ La Tecnología de la Información

✓ Riesgo Tecnológico

✓ Riesgo Tecnológico Inherente

✓ Gestión del Riesgo Tecnológico

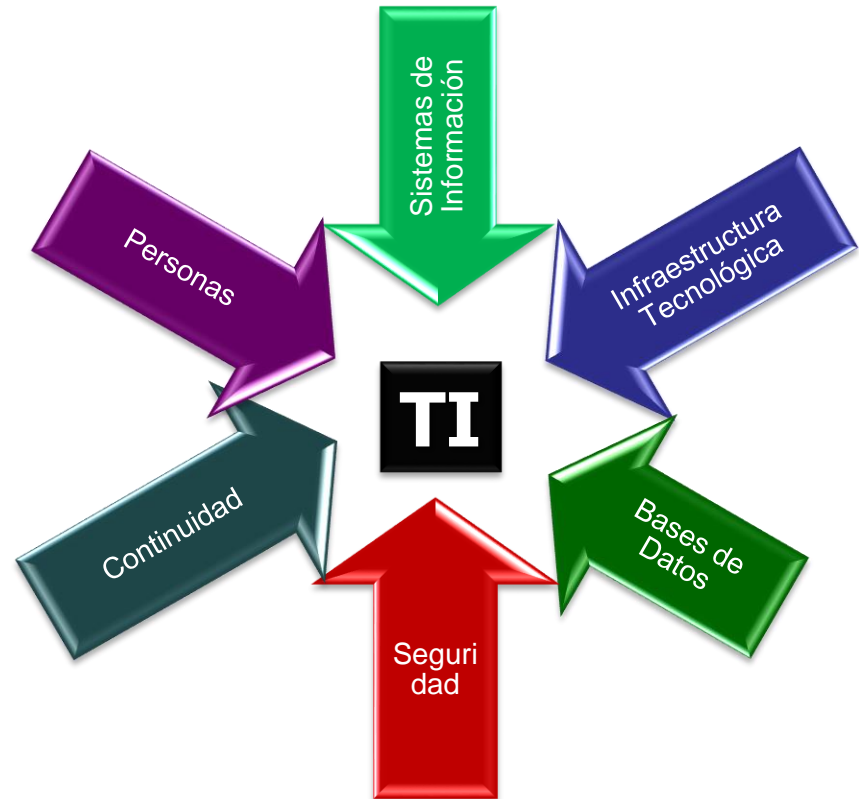
✓ Caso de estudio



La Tecnología de la Información

Tecnología de la Información:

Es el uso de la tecnología para obtener, procesar, almacenar, transmitir, comunicar y disponer de la información, para dar viabilidad a los procesos de negocio.





Superintendencia de Bancos
Guatemala, C. A.

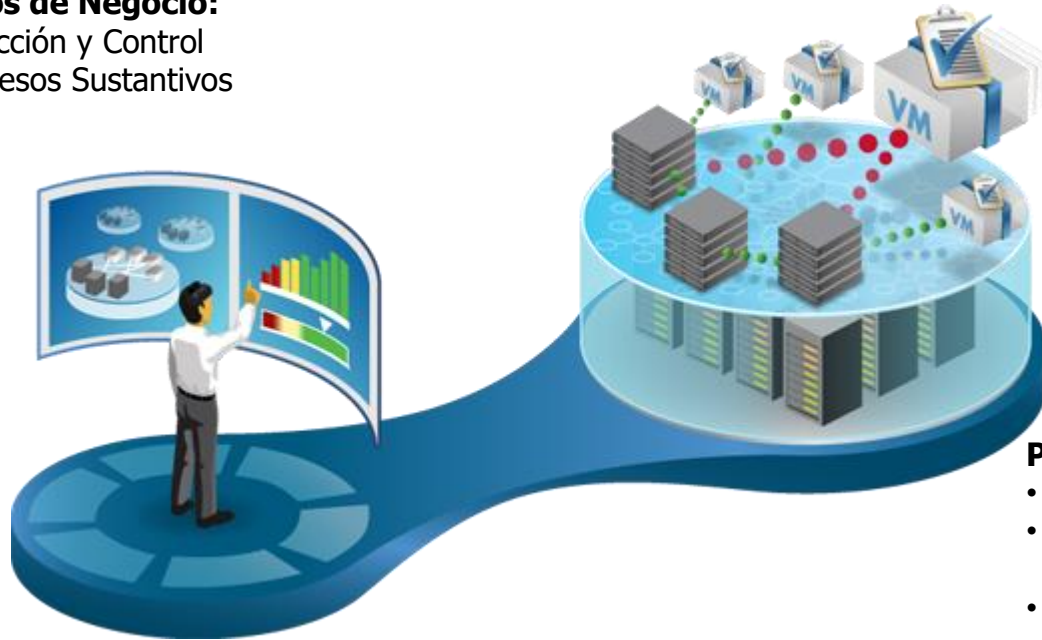
La Tecnología de la Información

Procesos de Negocio:

- Dirección y Control
- Procesos Sustantivos

Aplicaciones

- Gestión de Pólizas
- Gestión de Reaseguro
- Gestión de Clientes
- Gestión de Cobros y Pagos



Procesos de TI

- Gestión de sistemas
- Gestión de Continuidad
- Gestión de la Infraestructura

Agenda

✓ ~~La Tecnología de la Información~~

✓ Riesgo Tecnológico

✓ Riesgo Tecnológico Inherente

✓ Gestión del Riesgo Tecnológico

✓ Caso de estudio





Superintendencia de Bancos
Guatemala, C. A.

Riesgo Tecnológico



Definición:

La contingencia de que la interrupción, alteración, o falla de la infraestructura de TI, sistemas de información, bases de datos y procesos de TI, provoque pérdidas financieras a la institución.

Es uno de los componentes de riesgo operacional.

Riesgo Tecnológico: Incidentes de seguridad

PREOCUPACIONES EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS DE LATINOAMÉRICA



INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS DE LATINOAMÉRICA

Por tamaño de empresa

Pequeña
Mediana
Grande





Superintendencia de Bancos
Guatemala, C. A.

Agenda

✓ ~~La Tecnología de la Información~~

✓ ~~Riesgo Tecnológico~~

✓ Riesgo Tecnológico Inherente

✓ Gestión del Riesgo Tecnológico

✓ Caso de estudio





Superintendencia de Bancos
Guatemala, C. A.

Riesgo Tecnológico Inherente

- Las decisiones organizacionales conllevan un riesgo inherente o asociado.
- El riesgo de dichas decisiones debe identificarse (conocerse), valorarlo y aprender a controlarlo.
- El riesgo no es únicamente una potencial amenaza...es una oportunidad de negocio.



Riesgo Tecnológico Inherente

Gobierno de TI:

- Nivel de alineación estratégica
- Brechas de conocimiento del personal de TI
- Nivel del ambiente de gestión y control
- Estrategias de seguimiento a metas
- Nivel de rotación de personal
- Etc.



Sistemas de Información

- Metodología de ciclo de vida
- Integración de los sistemas
- Nivel transaccional
- Dependencia/Interfaces con terceros
- Etc.

Seguridad de TI

- Alineamiento con el negocio
- Nivel de ataques cibernéticos
- Diversidad de ataques internos/externos
- Vulnerabilidad de marco de seguridad
- Etc.

Infraestructura de TI:

- Nivel antigüedad de la infraestructura
- Nivel de integración del hardware
- Trafico de información
- Dependencia con terceros
- Uso de tecnologías (IoT, Cloud, etc.)
- Etc.



Continuidad de Operaciones de TI

- Alineamiento con el negocio
- Capacidad de la estrategia de continuidad
- Dependencia con terceros
- Etc.





Riesgo Tecnológico Inherente

Superintendencia de Bancos
Guatemala, C. A.

		Consecuencias				
Probabilidad		Insignificante 1	Menor 2	Moderada 3	Mayor 4	Catastrófica 5
Raro	1	Bajo	Bajo	Moderado	Alto	Alto
Improbable	2	Bajo	Bajo	Moderado	Alto	Extremo
Posible	3	Bajo	Moderado	Alto	Extremo	Extremo
Probable	4	Moderado	Alto	Alto	Extremo	Extremo
Casi seguro	5	Alto	Alto	Extremo	Extremo	Extremo

- Extremo:** Los riesgos extremos deben ponerse en conocimiento de los Directores y ser objeto de seguimiento permanente.
- Alto:** Los riesgos altos requieren la atención del Presidente / Director General / Director Ejecutivo.
- Moderado:** Los riesgos moderados deben ser objeto de seguimiento adecuado por parte de los niveles medios de Dirección.
- Bajo:** Los riesgos bajos deben ser objeto de seguimiento por parte de los supervisores.



Matriz	Impacto	Insignificante	Menor	Moderado	Mayor	Catastrofe
Probabilidad						
Certeza						
Probable						
Moderado						
Poco probable						
Muy Raro						



Superintendencia de Bancos
Guatemala, C. A.

Agenda

✓ ~~La Tecnología de la Información~~

✓ ~~Riesgo Tecnológico~~

✓ ~~Riesgo Tecnológico Inherente~~

✓ Gestión del Riesgo Tecnológico

✓ Caso de estudio



Gestión del Riesgo Tecnológico

¿Por qué gestionar el Riesgo Tecnológico?

- La tecnología de la información juega un rol importante en el desarrollo de las actividades de las organizaciones.
- ¿Pueden hacerse negocios sin el apoyo de la tecnología de la información?
- Aseguramiento del valor que las tecnologías de la información aportan al negocio.
- Marco normativo y de control.
- Parte del proceso de gestión de uno de los activos mas importantes de las organizaciones.

- Artículo 55 de la Ley de Bancos y Grupos Financieros
- Artículo 29 de la Ley de la Actividad Aseguradora
- Normativa prudencial
- Normas ISO



Gestión del Riesgo Tecnológico



ACEPTARLO • Monitorear

TRANSFERIRLO • Ceder la gestión

MITIGARLO • Control {

- Políticas y procedimientos
- Regulación
- Estándares internacionales
- Buenas prácticas

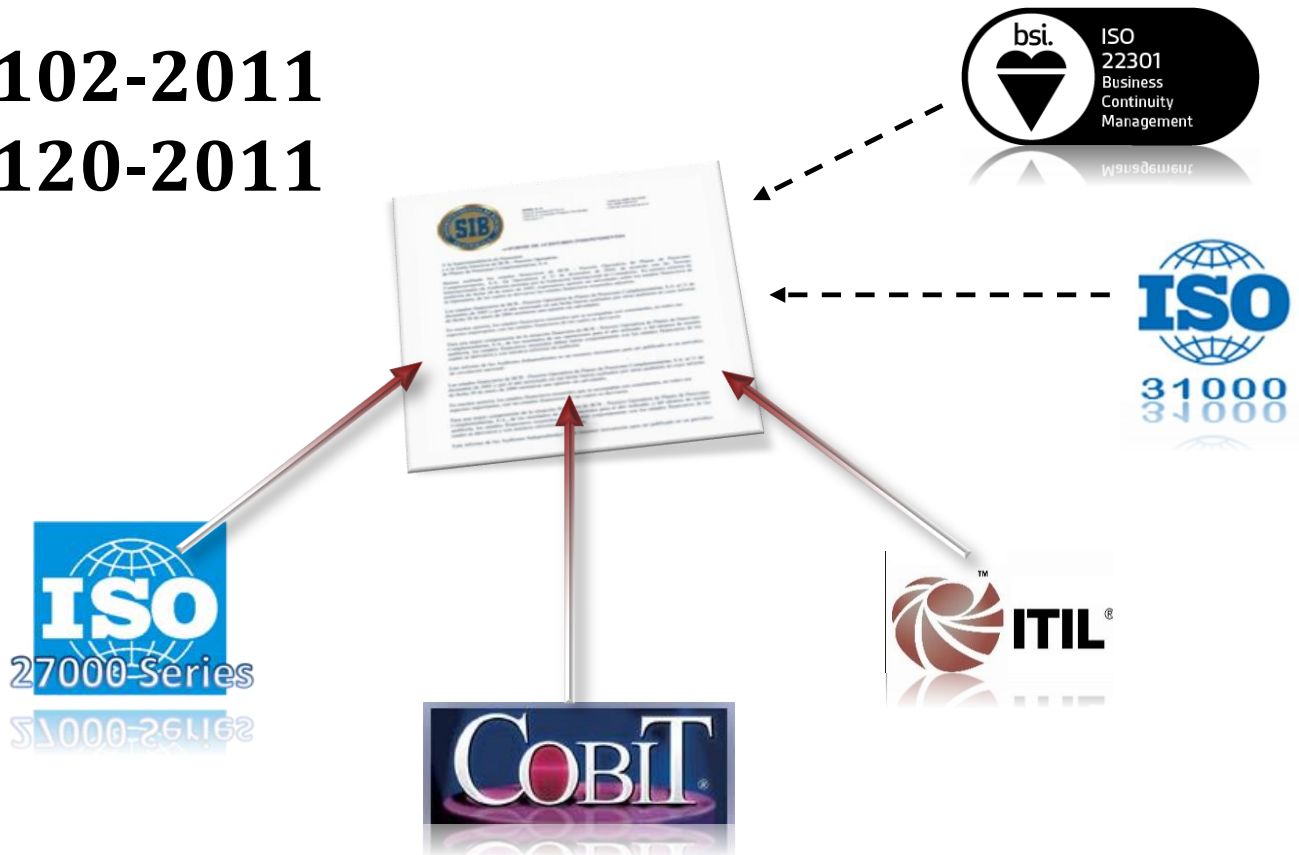


Superintendencia de Bancos
Guatemala, C. A.

Gestión del Riesgo Tecnológico

La regulación vigente y los estándares internacionales

JM-102-2011
JM-120-2011



Gestión del Riesgo Tecnológico: Organización

CONSEJO

Vela por que se implemente e instruye para que se mantenga una adecuada gestión de riesgos.

- Aprobar políticas, procedimientos, PETI, PCO
- Conocer reportes de exposición al RT, cambio, evolución y medidas.
- Conocer nivel de cumplimiento de las políticas y procedimientos aprobados.
- Adoptar medidas correspondientes.



Gestión del Riesgo Tecnológico: Organización

COMITÉ

Evalúa, analiza, propone y dirige la implementación de las directrices del Consejo de Administración.



- Analizar los reportes que le remita la Unidad, sobre el nivel de exposición al riesgo, cumplimiento y actualización de políticas y PETI, PCO TI.
- Definir la estrategia de implementación de políticas.
- Reportar al Consejo, al menos semestralmente sobre la exposición al riesgo tecnológico, cumplimiento de políticas y procedimientos aprobados.



Superintendencia de Bancos
Guatemala, C. A.

Gestión del Riesgo Tecnológico: Organización

UNIDAD

Implementa, propone, monitorea.



- Monitorea la exposición al riesgo tecnológico.
- Analiza el riesgo tecnológico inherente de las innovaciones de TI.
- Reporta al comité al menos trimestralmente sobre el nivel de exposición al riesgo, cumplimiento de políticas y procedimientos.
- Proponer al comité: PETI, PCO TI y el Manual de RT.



Superintendencia de Bancos
Guatemala, C. A.

Gestión del Riesgo Tecnológico: Organización

- **Plan estratégico de TI:**
 - Objetivos alineados a la estrategia del negocio
 - Planes tácticos –proyectos y actividades específicas
 - Presupuesto financiero
- **Organización de TI**
 - Alineada al plan estratégico
 - programas de entrenamiento y capacitación
 - Segregación de funciones
 - Marco de trabajo orientado a procesos
- **Manual de Administración de Riesgo Tecnológico**
 - Políticas y procedimientos para la administración del RT
 - Aprobado por el CA



Gestión del Riesgo Tecnológico

Infraestructura de TI, Sistemas de Información, Bases de Datos y Servicios de TI

- Esquema de la información del negocio.
Inventarios de infraestructura de TI, sistemas de información y Bases de Datos.
- Administración de las Bases de Datos.
- Monitoreo de TI.
- Adquisición, mantenimiento e implementación de TI.
- Gestión de servicios de TI.
- Ciclo de vida de los sistemas de información.



Gestión del Riesgo Tecnológico

Seguridad de la Tecnología de la Información

- Confidencialidad, integridad y disponibilidad de los datos.
- Clasificación de la información
- Roles y responsabilidades
- Monitoreo de la seguridad
- Seguridad física
- Seguridad lógica
- Copias de respaldo



Seguridad de la Tecnología de la Información

- Operaciones y servicios a través de canales electrónicos.
- Seguridad en el intercambio de información.
- Registro y bitácora de transacciones-.
- Control de la infraestructura.
- Protección de datos.



Gestión del Riesgo Tecnológico

Continuidad de operaciones de TI

- Análisis de Impacto al Negocio (BIA).
- Plan de Continuidad del Negocio (BCP).
- Plan de Continuidad de Operaciones de TI (DRP).
- Revisión, pruebas y actualización de los planes.
- Personal clave para la continuidad.
- Centro de cómputo alternativo.



Gestión del Riesgo Tecnológico

Procesamiento de información y tercerización






- **Procesamiento de información**
Dentro o fuera del territorio nacional
Contar con un centro de cómputo alternativo
Personal técnico capacitado
Replicación en tiempo real
Libre acceso a la SIB
- **Tercerización**
Cumplimiento de este reglamento
Acuerdos de niveles de servicio
Confidencialidad





Superintendencia de Bancos
Guatemala, C. A.

Gracias

 SIB Guatemala  @sib_guatemala  SuperBancosGuatemala
 sib_guatemala  Superintendencia de Bancos (SIB)