XIV Teleconferencia del CLAIN
Riesgos de TI
04/03/2009

Participantes:
- Argentina
- Brasil
- Colombia
- Honduras
- Panamá
- Uruguay

A continuación se resumen las preguntas y respuestas desarrolladas en la undécima Teleconferencia del CLAIN:

1) **¿Existen reglamentaciones en su país que involucre la gestión o el tratamiento de los Riesgos de TI?**

Argentina: Existen reglamentaciones dictadas por el Banco Central (BCRA) Resolución A4609 (Anteriormente Resolución A3198), basada en COBIT ISO17799/27001 Buenas prácticas de Basilea y SOX para TI.

La misma es de cumplimiento obligatorio y dicta los "Requisitos Mínimos de Gestión, Implementación y Control de los Riesgos Relacionados con Tecnología Informática, Sistemas de Información y Recursos Asociados para las Entidades Financieras.

Brasil: Sí, ejemplos:

PCI DSS para tarjetas de crédito.

SPB – Sistema de Pagamentos Brasileiros tiene reglas que tratan de riesgos de TI y seguridad para la implementación de soluciones que utilicen a RSFN – Rede do Sistema Financeiro Nacional dispuesta por el Banco Central;

Adicionalmente hay otras legislaciones que abordan de manera general los riesgos de TI:

ITI – Instituto Nacional de Tecnología de la Información, por medio del órgano legislador **ICP-Brasil** (Infraestructura de Chaves Públicas) reglamenta las normas para el uso de certificación digital e instalación

de AC – Autoridades Certificadoras y AR – Autoridades Registradoras en el país, inclusive aquellas que irán a operar vía SPB.

CVM89 – trata de controles sobre el ambiente general de TI para instituciones autorizadas a prestar servicios de custodia de títulos mobiliarios y escrituración de valores.

Panamá: El ente regulador, la Superintendencia de Bancos de Panamá, ha emitido su regulación relacionada con los procedimientos y controles que debe cumplir cada entidad bancaria, relacionados con la tecnología.

Uruguay: Existen principalmente dos reglamentaciones que atienden esta temática. La primera, apunta al sector financiero y fue establecida por el Banco Central denominada Estándares mínimos de gestión para las Instituciones de Intermediación Financiera – Estándares de Tecnología TI, en la cual se dan un conjunto de pautas que los bancos deben cumplir para gestionar los riesgos de TI, - y la segunda -, es la ley 18.331 – Ley de Protección de Datos Personales y acción de "Habeas Data", en donde las organizaciones deben cumplir con una serie de requisitos y controles para asegurar la integridad y confidencialidad de la información respecto a los datos personales.

2) Con respecto a TI, ¿cuál es el riesgo principal a las que actualmente se enfrentan sus organizaciones?

Argentina: Los riesgos que se presentan en la organización se enfocan básicamente en los siguientes aspectos:

- Confidencialidad: Accesos no autorizados, Hurto de Información. Nuevos Canales de ingreso de transacciones como la Banca Online que requiere reforzar los esquemas de seguridad.
- Disponibilidad: Contar con los recursos TI, y el nivel de servicio a efectos de poder brindar una continuidad de los servicios.
- Integridad de datos: Perdidas contar con políticas que permitan el recupero de la información.

No contar con contramedidas para estos riesgos, lleva a un impacto económico y de reputación para la organización.

Brasil: Además de los procesos de fusión e incorporación de otros Bancos, existen los siguientes riesgos que son identificados en la organización:

Continuidad de los Negocios, Pérdida de Informaciones, Quiebra del Secreto Bancario, Integridad de la Información, Imagen Implementación de una estructura efectiva y activa de Gobierno de TI, Gestión de Proyectos, Inovación e implementación de nuevas soluciones tecnológicas que estén integradas al Legado, Gestión eficiente de los costos de TI, gestión de "backlogs" de demandas sistémicas para atender las necesidades del negocio y demostrar de modo consistente el ROI referente a los proyectos liderados y conducidos por TI.

Panamá: El riesgo de la gobernabilidad de los sistemas.

Que la inversión y la dirección en los sistemas de tecnología no estén alineados con la estrategia del negocio.

Uruguay: El Banco hace frente a dos riesgos muy importantes con respecto a TI: por un lado, se necesita cumplir con los requisitos financieros para poder asegurar una protección adecuada de los activos de información; y por otro, se apuesta a la obtención de determinados niveles de rendimiento y calidad de servicio que aseguren la disponibilidad de los sistemas y por lo tanto la disponibilidad de la operativa del banco.

3) ¿Se realizan valoraciones cualitativa o cuantitativa de los Riesgos de TI?

Argentina: Se clasifican los activos de TI (Aplicaciones / Información / Infraestructura / Gente). Se valora el riesgo inherente – Controles = Determinando el nivel de exposición. (Riego Residual)

Brasil: Aún no hay un procedimiento estructurado para la medición de los riesgos de TI, éstos son seguidos por los Comités Ejecutivos. Adicionalmente, existen los Oficiales de Controles Internos y Riesgos, que son responsables por el seguimiento de los riesgos y efectividad de los controles.

Panamá: En los casos de valorización, son realizados principalmente por las firmas de auditores externos ó consultores de riesgos tecnológicos.

Uruguay: El banco efectúa análisis de riesgos y cuenta con un proceso de administración de Riesgos de TI el cual se aplica a los proyectos tecnológicos. No se aplica en detalle un análisis para todos los activos. En particular, para el caso puntual de Auditoría de TI, el plan anual se efectúa mediante un análisis de riesgo de forma semi-cuantitativa definiendo un conjunto de valores o ponderaciones y estableciendo los factores de riesgo.

4) Que tipo de herramientas, estándares o metodologías se utilizan para la gestión de Riesgos de TI?

Argentina: Las herramientas/estándares que se utilizan actualmente son las siguientes:

- CobiT
- ISO 17799/27001 (SGSI)
- Resolución A 4609 BCRA
-

Brasil: Cobit 4.1, ITIL, ISO 17799, ISO 27022.

Recientemente el área de TI también viene implementando controles para medir la adhesión a las prácticas de mercado como CMM – Capability Maturity Model y OMM – Operational Maturity Model.

Panamá: Existen varias herramientas estándar ó metodología aplicables en la utilización para la gestión de riesgos de tecnología como son: Cobit, Itil, ISO 27001-27002.

Uruguay: Principalmente se ha adoptado COBIT ya que de acuerdo a cómo está diseñado o concebido ayuda a las organizaciones a reducir riesgos en el manejo de TI. Dentro de COBIT y en particular, se ha trabajado con IT Assurance en la cual se definen los riesgos para cada proceso para luego efectuar la valoración correspondiente.

En lo que respecta a la automatización y alineado a lo anterior, se cuenta con el producto Methodware.

5) ¿Cuál es el aspecto en el que Ud. considera que hay que ser más cuidadoso en la gestión del riesgo en TI?

Argentina: Hay que ser especialmente cuidadoso en contar con una adecuada clasificación de los activos de TI para valorar el riesgo inherente de cada uno.

Contar con una base de conocimientos para registrar los eventos que se produzcan y evaluarlos a fin de determinar las acciones correctivas

Contar con una adecuada gestión de la Seguridad informática y realizar capacitación continua de los recursos humanos frente a las nuevas políticas que se apliquen

Brasil: Efectividad de los controles mitigantes de los riesgos

Implementación de los procesos corporativos, con atribución de responsabilidades que viabilicen la aplicación efectiva de los controles y su mantenimiento a lo largo del tiempo.

Panamá: El aspecto de más cuidado en la gestión de riesgo de tecnología es considerado la gestión y seguridad de la información, que son los datos claves del negocio.

Uruguay: En el caso particular del sistema financiero, se considera que la seguridad de la información y los controles relacionados con ella pasan a tener un aspecto primordial. No obstante ello , y alineado con la dependencia tecnológica que tienen hoy en día las organizaciones, se entiende que la gestión de riesgos debe abarcar a todos los procesos estratégicos de planificación a nivel de recursos, productos, servicios, clientes, etc. El análisis de riesgos se debe realizar a través de cada una de las áreas que componen dicho plan y estudiar de qué manera la tecnología de la información (TI), afectaría a cada una de ellas.

6) **¿Existe participación por parte del Directorio o la Alta Gerencia de las organizaciones en el establecimiento y comunicación de políticas para administrar el riesgo de TI y asegurar que la Gerencia de TI las implemente adecuadamente?**

***Argentina*:** Sí, existe participación a nivel de directorio (comités de TI y Auditoría) y un compromiso de la Alta Gerencia en este aspecto.

Brasil: Sí, a través de los Comités Ejecutivos. Ejemplos:

- CSAGRO – Comisión Superior de Auditoría y Gestión de Riesgos Operacionales,
- CEB – Comité Ejecutivo Bancario,
- Comité de Auditoría,
- Comité de Tecnología de la Informacion y Comité de Seguridad de la Información.

Panamá: En las entidades bancarias, las normas del buen gobierno corporativo, exige la participación de las Gerencias y el Directorio en la toma de decisiones. Parte importante es la de salvaguardar la seguridad de la información del negocio como parte integral de la administración. El riesgo de tecnología y el aseguramiento de la integridad de la información deben considerarse de gran importancia para toda la entidad, por el valor que representa la información veraz y rápida, para la toma de decisiones gerenciales.

Uruguay: El banco cuenta con varios ámbitos en donde se discute la temática: Consejo de Informática, Comisión ordenadora de gastos, comisión de Administración, Comité de Auditoría y Comité de Proyectos Tecnológicos.