



XX CLAIN 2016

Asunción, Paraguay 19 y 20 de mayo. Hotel Excelsior
"Gobierno Corporativo, Gestión de Riesgos y Auditoría, un enlace que asegura el éxito organizacional"

La Gobernabilidad de las TIC en el Ecosistema del Gobierno Corporativo

Carlos G. Masi
Gerente de Informática Corporativo
Grupo Riquelme - Paraguay

ASOCIACION

DE BANCOS DEL PARAGUAY



Carlos G. Masi

Gerente de Informática Corporativo
Grupo Riquelme
Asunción, Paraguay

- ✓ Paraguay (46)
- ✓ Lic. Analista de Sistemas 
- ✓ Especializado en Auditoría y Control de TI (*desde 1996*)
- ✓ Posgrado en Alta Gerencia
- ✓ Auditor Informático Interno – 10 años (*Bancard S.A.*)
- ✓ Auditor Informático Externo – 9 años (*PwC. KPMG, Amaral & Asociados*)



Agenda

- La visión de los Sistemas Informáticos
 - Directorio
 - Gerencia
 - TI
 - Usuario administrativo
- La gobernabilidad de los Sistemas
 - Información
 - Automatización
 - Control
- Conclusiones y recomendaciones

La visión del negocio y los sistemas TIC

- Directorio
 - Rentabilidad
 - Comercial - Negocios
- Gerencia
 - Comercial - Negocios
 - Procesos - Operativa
- TI
 - Procesos - Operativa
 - Infraestructura
- Soporte Técnico
 - Infraestructura



Gobernabilidad de TI

Lo que los clientes internos esperan de la implementación de sus sistemas e infraestructura TIC

1. Información

- Directorio
- Gerencia

2. Automatización

- Gerencia
- Usuarios

3. Control

- Directorio
- Seguridad
- Auditoría

Generación de Información

- Factores de riesgo

- a) La revolución cognitiva informática aún sigue en curso.

- El eslabón más débil de la cadena de valor TIC es la información producida por los sistemas. Reportes no satisfacen expectativa de usuarios.

- b) El grado de automatización de la generación de información sigue siendo limitado.

- Numerosos reportes gerenciales y de información de alta sensibilidad para el negocio continúan siendo producidos de manera manual (Excel)

- c) Los controles de seguridad sobre la información que llega hasta la gerencia son limitados o básicos.

- Reportes se modifican o alteran hasta el último momento de ser presentados y por cualquier método.

Proceso de automatización

- Factores de riesgo

- a) La revolución agrícola informática está en sus inicios.

- La cosecha de datos para su explotación operativa y comercial es una tarea no iniciada por la mayoría de las organizaciones. Aunque la necesidad real existe.

- b) El grado de automatización de los procesos es variable.

- Las soluciones integrales son muy costosas para muchas organizaciones por lo que optan por un enfoque modular.
 - Las soluciones informáticas se centran sobre procesos específicos lo que genera asimetrías en la automatización de la operativa del negocio.

- c) La implementación de los sistemas sigue dejando de lado la seguridad de la información.

- Implementadores usan perfiles de alto nivel para asegurar el funcionamiento operativa básica.

Ambiente de control

- Factores de riesgo

- a) Los controles siguen siendo en su mayoría del tipo post-mortem.

- Controles de tipo preventivo son los más efectivos para reducir índices de fraude, accesos no autorizados y errores en el procesamiento.

- b) El correo electrónico se ha convertido en el nuevo servidor de archivos.

- Usuarios adoptan la costumbre de intercambiar toda la información del negocio por medio del email ocasionando serios riesgos de confidencialidad.

- c) Los sistemas de aplicación no poseen una seguridad adecuada.

- Módulos de auditoría/seguridad consisten sólo en reportes básicos del log de transacciones. Aportan poco para el trabajo de los auditores.

Conclusiones

- a) Los reportes gerenciales deben ser generados por el sistema sin intervención del usuario.
- b) Incluir controles preventivos en los sistemas de aplicación. Revisar existencia de perfiles de alto nivel en usuarios comunes luego de la implementación.
- c) Acordar con el proveedor/desarrollador del sistema el diseño de reportes de auditoría/seguridad que agreguen valor al trabajo de auditoría/seguridad.

Información de Contacto

Carlos G. Masi

- carlos.masi@gmail.com



Muchas Gracias
Por su Atención!

