CLAIN 2016

Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

"Gobierno Corporativo, Gestión de Riesgos y Auditoría, un enlace que asegura el éxito organizacional"

ASOCIACIÓN DE BANCOS DEL PARAGUAY

De nubes, tormentas y paraguas

José I. Andres

Banco de Santa Fe - Argentina

FELABAN

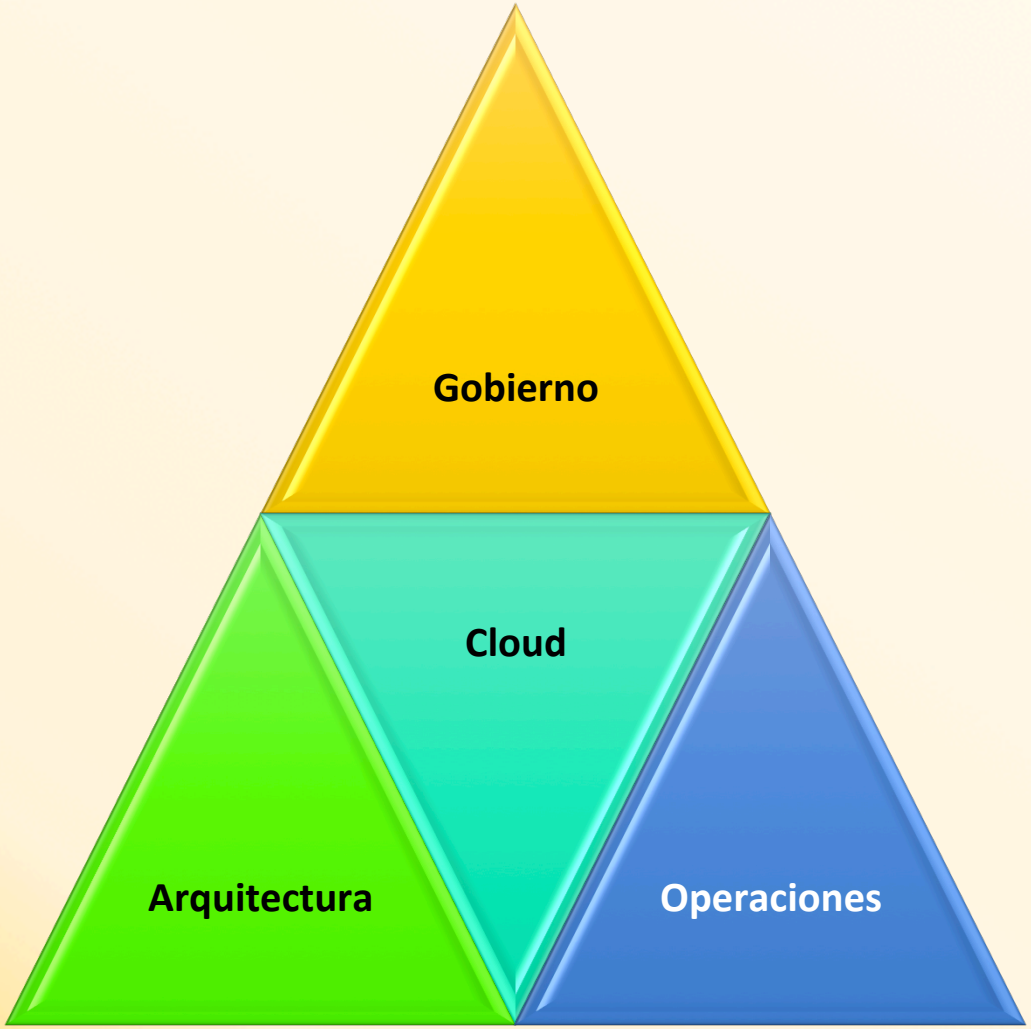
José Ignacio Andres

- Ingeniero en Sistema de Información (Universidad Tecnológica Nacional Argentina).
- Auditor Interno (Sistemas) en Banco de Santa Fe: Desde el año 2009 al 2016.

Agenda

- Nubes – Pronóstico (Cloud Computing)
- La Tormenta – Principales Riesgos
- El Paraguas – Plan de Auditoría
- Lluvia - Controles

Modelo de dominios



Cloud Computing

- Qué es?
- Qué activos podemos migrar?
- Cuán importante es el activo a migrar?
- Qué tipo de nube?
  - Publica, Privada, Hibrida, Comunitaria.
- Qué modelo de servicio?
  - IaaS, PaaS, SaaS.

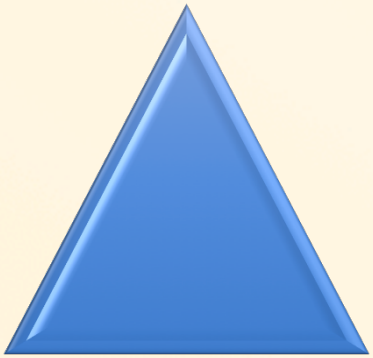
Dominio: Gobierno

¿Como controlar lo que por naturaleza no controlas?

- Cuestiones estratégicas y políticas.

<u>Sub dominios:</u>

- Gobierno y gestión de riesgos en la empresa.
- Aspectos legales y contractuales.
- Cumplimiento legal y auditoria.
- Gestión de la seguridad de la información y de los datos.
- Portabilidad e Interoperabilidad.



Dominio: Operaciones

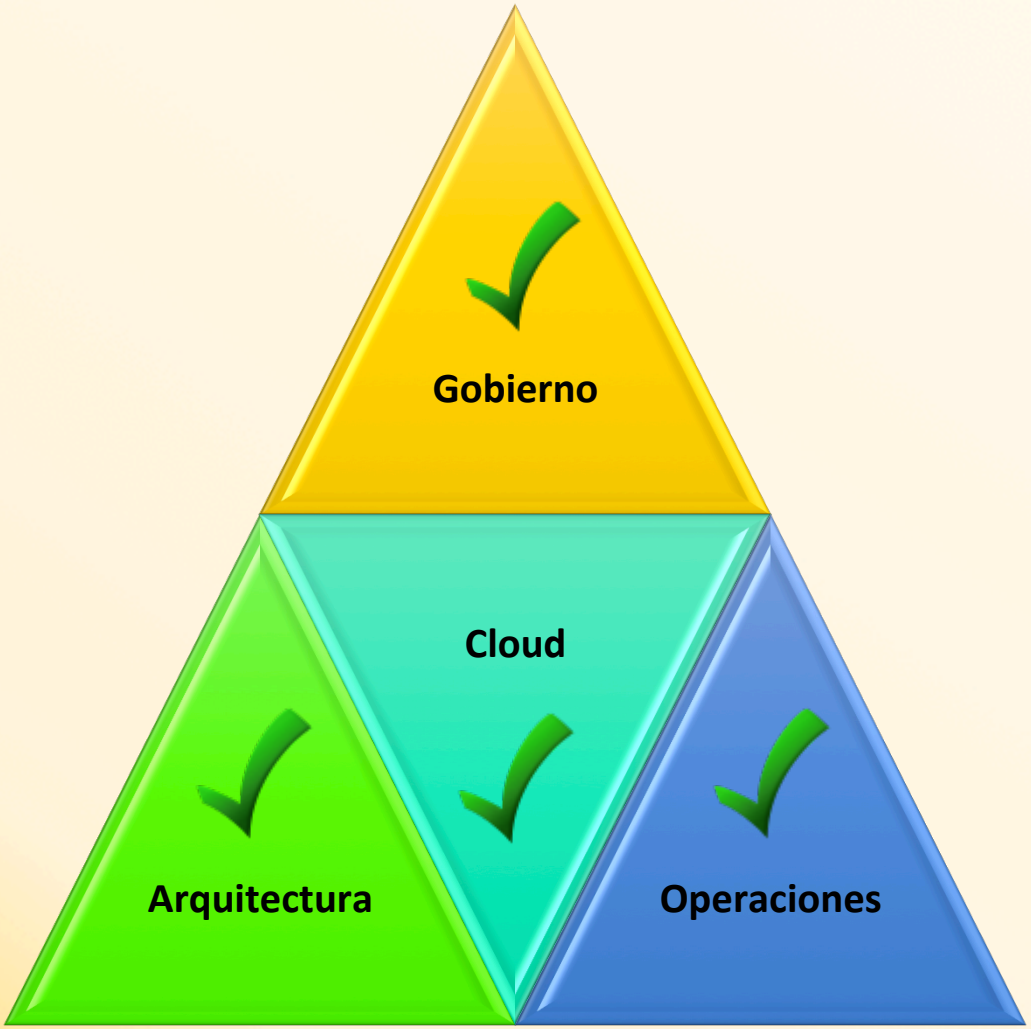
Cuestiones tácticas, de seguridad, y de implementación.

<u>Sub dominios:</u>

- Seguridad física, continuidad del negocio y recuperación de desastres.
- El centro del procesamiento de datos.
- Tratamiento de incidentes.
- Seguridad de las aplicaciones.
- Cifrado y gestión de claves.
- Gestión de identidades y de acceso.
- Seguridad de la virtualización.

Dominio: Arquitectura

Modelo de dominios



Tormenta - Riesgos

- Pérdida de control de gobierno y gestión de riesgos deficiente.
- Pérdidas por vacíos contractuales y legales, incumplimientos y carencia de especificaciones por ausencia de participación de los responsables en la confección de los mismos.
- Imposibilidad de migración a un nuevo PSC o vuelta a un entorno de tecnologías de la información interno.
- Imposibilidad de incorporar nuevos servicios del mismo PSC u otros.
- Imposibilidad de restaurar funciones críticas y de sobreponerse a desastres, así como posibilidad de robos, espionaje, infiltraciones entre otros daños.
- Pérdidas por un inadecuado Centro de Procesamiento de Datos (CPD) contratado, e inexistencia de responsables claramente definidos.

Tormenta - Riesgos

- Pérdidas económicas y de reputación, por no cumplir el PSC con mecanismos de detección, respuesta, notificación, y remediación de incidentes.
- Posibilidad de fraude por incorrecta parametrización de seguridad e inadecuados métodos de desarrollo de aplicaciones, así como imposibilidad de autogestión por parte de la EF.
- Fallas en la protección de los datos.
- Pérdidas económicas y de reputación por acciones maliciosas de miembros internos.
- Fallo de aislamiento y supresión de datos insegura o incompleta.

Lluvia - Controles

El Gobierno

12	Gobierno y Gestión de Riesgo en la Empresa (GGRE)
11	Aspectos Legales y Contractuales (ALC)
6	Cumplimiento Legal y Auditoria (CLA)
7	Gestión de la Información y Seguridad de los Datos (GISD)
4	Portabilidad e Interoperabilidad (PI)

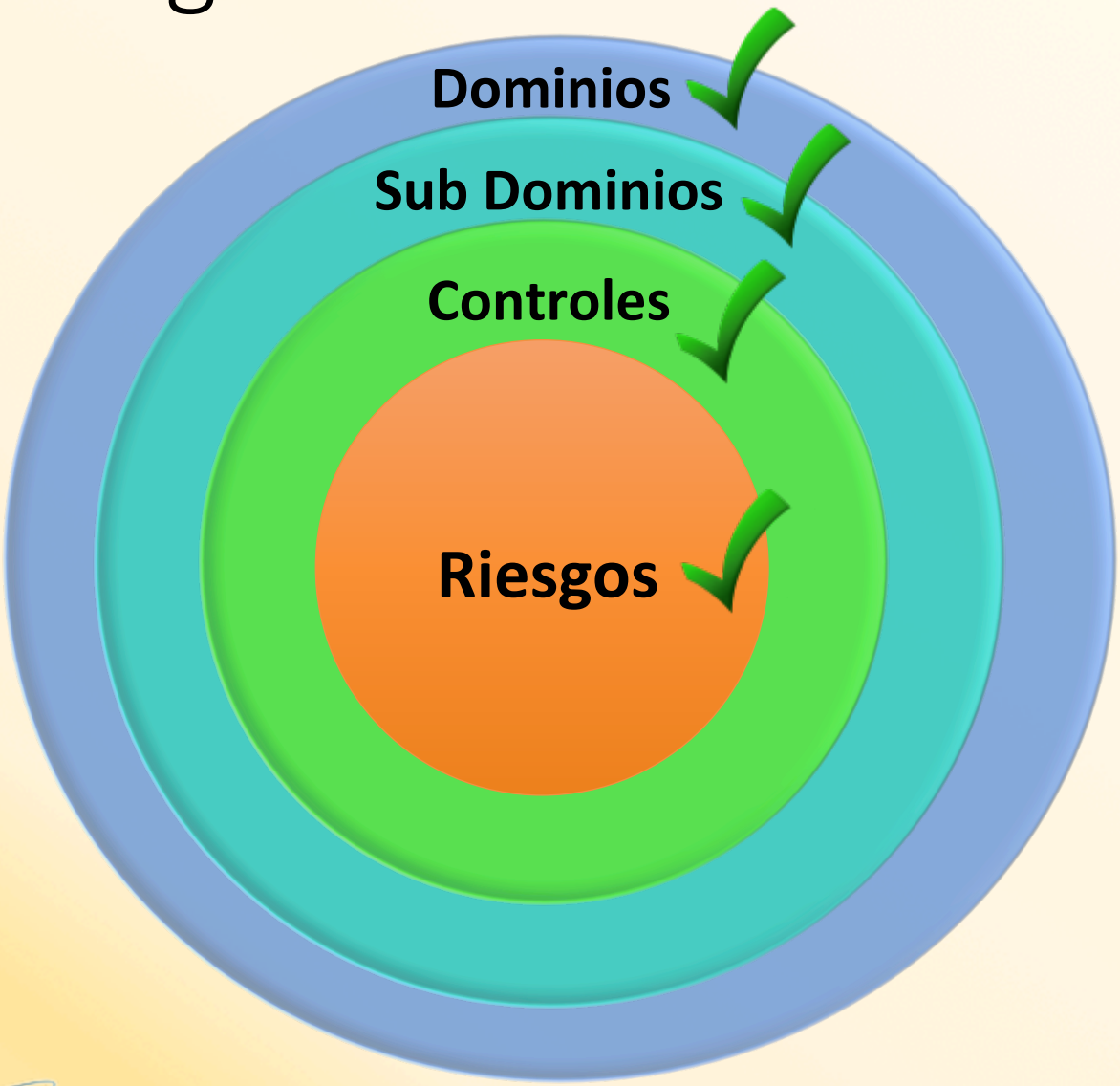
40

Las Operaciones

9	Seguridad Física, Continuidad de Negocio y Recuperación de Desastres (SFCNRD)
4	El Centro de Procesamiento de Datos (CPD)
11	Tratamiento de Incidentes (TI)
8	Seguridad de las Aplicaciones (SA)
8	Cifrado y Gestión de Claves (CGC)
3	Gestión de Identidades y de Acceso (GIA)
8	Infraestructura y Virtualización (VI)

51

Paraguas – Plan de auditoria



Caso Práctico

Una EF, con interés del sector de Tecnología Informática por la posibilidad de disponer de manera casi inmediata de la información en las cintas de backup, sustentado por el análisis de costos realizados por la gerencia de compras, ***planea utilizar los servicios de la nube para gestionar el almacenamiento secundario****.*

Caso Práctico – Check List de Controles

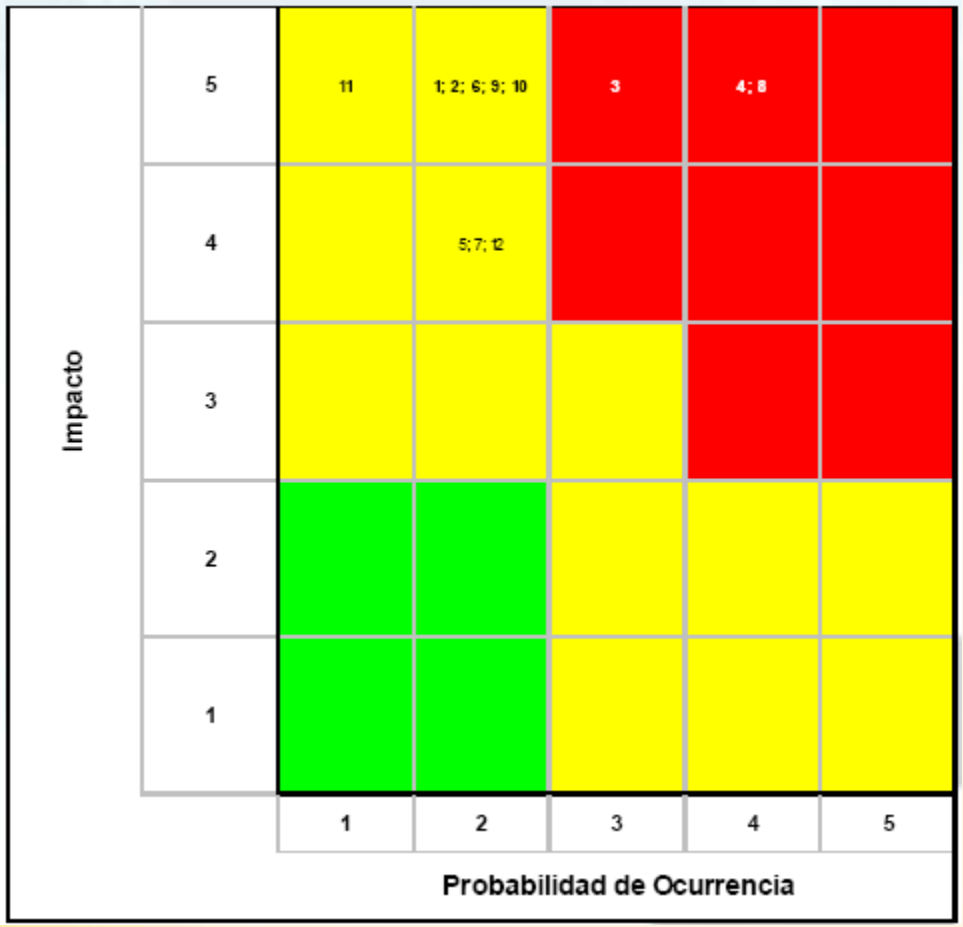
Check List de Controles Cloud Versión 1.0				
Riesgo Inherente	Dominio	Controles	Cumple	Pruebas de control-Comentario
Pérdida por vacíos contractuales y legales	El gobiemo	ALC11	👍	El PSC es el responsable de la eliminación de la información que involucran los servicios contratados, en caso de así requerirlo la EF.
Incumplimiento legal y contractual		CLA1	👍	Se verificó en el sitio web del PSC información actualizada de balances, referentes, misión y visión, entre otros aspectos. Además la EF recibió la documentación que respalda y avala la transparencia del PSC (trayectoria del PSC, referencias de clientes, referencias internas, inexistencias de sanciones legales, análisis de deudor sobre los referentes y el titular responsable del servicio, premios de calidad, entre otros).
		CLA2	👎	Si bien se cumplen los controles GGRE6 y GGRE7, el plan no contempla un procedimiento que permita medir los niveles de servicios requeridos. La adecuación se contempla en la Matriz de Riesgo Cloud Versión 1.0 con su respectivo Plan de Acción.

Caso Práctico - Riesgos

Matriz de Riesgos Cloud Versión 1.0

	Riesgo			Evaluación		Tratamiento del Riesgo				
	Riesgo Inherente	Mitigantes	Descripción del Riesgo Residual	P	I	Tipo de Respuesta al Riesgo Residual	Plan de Acción	Responsable	Fecha Compromiso	Estado
1	Perdida de gobierno y gestión de riesgos deficiente	GGRE1, GGRE2, GGRE3, GGRE4, GGRE5, GGRE6, GGRE7, GGRE8, GGRE9, GGRE10, GGRE11, GGRE12.	No se identifica riesgo residual.	2	5	Aceptar	Sin acciones pendientes			
2	Pérdidas por vacios contractuales y legales	ALC1, ALC2, ALC3, ALC4, ALC5, ALC6, ALC7, ALC8, ALC9, ALC10, ALC11.	No se identifica riesgo residual.	2	5	Aceptar	Sin acciones pendientes			
3	Incumplimiento legal y contractual	CLA1, CLA2, CLA3, CLA4, CLA5, CLA6.	Falta de control sobre los acuerdos establecidos e incumplimientos contractuales. Falta de la razonabilidad para evaluar los sistemas y procedimientos de uso en una empresa, con el propósito de determinar si su diseño y aplicación son correctos; y comprobar el sistema de procesamiento de información como parte de la evaluación de control interno; así como para identificar aspectos	3	5	Tratar	Si bien la EF no cuenta con un procedimiento que describa como realizar la medición de los niveles de servicios del PSC contra los establecidos en el contrato, se está analizando con los referentes de Tecnología Informática el armado del mismo.	Gerencia de Tecnología Informática y Gerencia de Auditoria Interna	1/6/2016	Pendiente

Caso Práctico – Mapeo de Riesgos



Caso Práctico - Conclusión

- En el desarrollo del práctico pudimos entender la mecánica de los controles, sus relaciones, interacciones, e intersecciones (por ejemplo VI8, VI3, CLA4).
- En cuanto al relevamiento de las áreas involucradas el sector de Tecnología Informática consideró aspectos contractuales, tecnológicos, de seguridad, y aristas de encuadre legal propuestos, que no habían sido contemplados hasta la intervención de AI.
- El sector de Tecnología Informática consideró incluir en su matriz de riesgos, los riesgos detectados por AI en los servicios Cloud.
- Del relevamiento por cada riesgo detectado, los mitigantes asociados se consideraron razonables.
- Para los casos con riesgo residual, el plan de acción descripto se consideró razonable.

Por tanto se concluyó que el proceso de migración a la nube del almacenamiento de respaldo, con el proveedor propuesto, los riesgos detectados y controles aplicados, se considera razonable.

Conclusión

*El proceso es solo una tormenta más a la cual haciendo frente con **profesionalismo** redundará en el **éxito** del tratamiento de la problemática.*

Bibliografía Recomendada

- COSO, Control Interno y Marco Integrado.
- Guía de seguridad de áreas críticas en Cloud Computing V 3.0.
- Matriz de controles CSA_CCM_v.3.0.1.
- Manual de normas ISO/IEC 27001, e ISO/IEC 27018.
- http://www.auditool.org
- http://www.isaca.org

Muchas Gracias

Por su Atención!

Información de Contacto

E-Mail: *andresj@bancobsf.com.ar*

Teléfono: 54-341-4294243

- Otros e-mails de Auditoría en Banco de Santa Fe:
  - cormonsj@bancobsf.com.ar
  - casadidic@bancobsf.com.ar
  - nunezj@bancobsf.com.ar