Prácticas con los clientes, productos y negocios

Abusos de confianza	Abuso de información confidencial sobre el cliente	Negociación fraudulenta en las cuentas del banco	Blanqueo de capitales	Venta de productos no autorizados

Prácticas con los clientes, productos y negocios

- Revelar información a lo externo de la organización por empleados
- Administración de proveedores

→ PO6 Comunicar las aspiraciones y la dirección de la gerencia

→ DS2 Administrar servicios de terceros

Daños a los activos físicos

Daños a los activos físicos

- Daño accidental o deliberado a la infraestructura física de TI

→ DS4 Garantizar la continuidad del servicio

→ DS12 Administrar el ambiente físico

Alteraciones en las actividades y fallos en los sistemas

Fallas en el hardware	Fallas en el software	Problemas en las telecomunicaciones	Interrupción en la prestación de servicios públicos

Interrupción de las actividades y fallos en los sistemas

- Mal funcionamiento del hardware o software
- Fallas en las comunicaciones
- Sabotaje de empleados
- Pérdida de personal clave de TI
- Destrucción del software o datos
- Robo de software o datos sensitivos
- Virus
- Fallas del respaldo
- Ataques de negación de servicio
- Errores en las configuraciones

→ DS3 Administrar desempeño y capacidad

→ DS4 Garantizar la continuidad del servicio

→ DS5 Garantizar la seguridad de los sistemas

→ DS9 Administrar la configuración

→ DS10 Administrar los problemas

Ejecución, entrega y procesamiento

Errores en la introducción de datos	Fallos en la administración del colateral	Documentación jurídica incompleta	Concesión de acceso no autorizado a las cuentas de los clientes	Prácticas inadecuadas de contrapartes distintas de clientes	Litigios con distribuidores

Administración de los procesos, entrega y ejecución

- Manejo electrónico de errores
- Estaciones de trabajo desatendidas
- Entrada de datos incompleta
- Errores en los datos de entrada y salida
- Errores en los pruebas de programación
- Errores operacionales

→ AI5 Adquirir recursos de TI

→ AI6 Administrar cambios

→ DS5 Garantizar la seguridad de los sistemas

→ DS10 Administrar los problemas

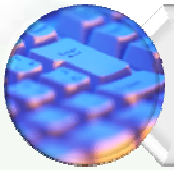
Procesos de COBIT según eventos de riesgos (13)

- PO6 Comunicar las aspiraciones y la dirección de la gerencia
- PO9 Evaluar y administrar los riesgos
- DS2 Administrar servicios de terceros
- DS3 Administrar desempeño y capacidad
- DS4 Garantizar la continuidad del servicio
- DS5 Garantizar la seguridad de los sistemas
- DS9 Administrar la configuración
- DS10 Administrar los problemas
- DS12 Administrar el ambiente físico
- AI5 Adquirir recursos de TI
- AI6 Administrar los cambios
- ME2 Monitorear y evaluar el control interno
- ME4 Proporcionar gobierno de TI

Contenido

Introducción

Basilea II y el Riesgo Operativo



COBIT Y Basilea II

Combinando Basilea II con COBIT

Normativa 14-09

Contenido de la norma

Acuerdo SUGEF 14-09

- Capítulo I
  Disposiciones Generales
- Capítulo II
  Gestión de la Tecnología de Información
- Capítulo III
  Evaluación de la Gestión de TI
- Capítulo IV
  Disposiciones Especiales
- Disposiciones Finales y Transitorios
- Anexo 1 Categorización de procesos
- Anexo 2 Metodología de calificación

Capitulo I disposiciones generales

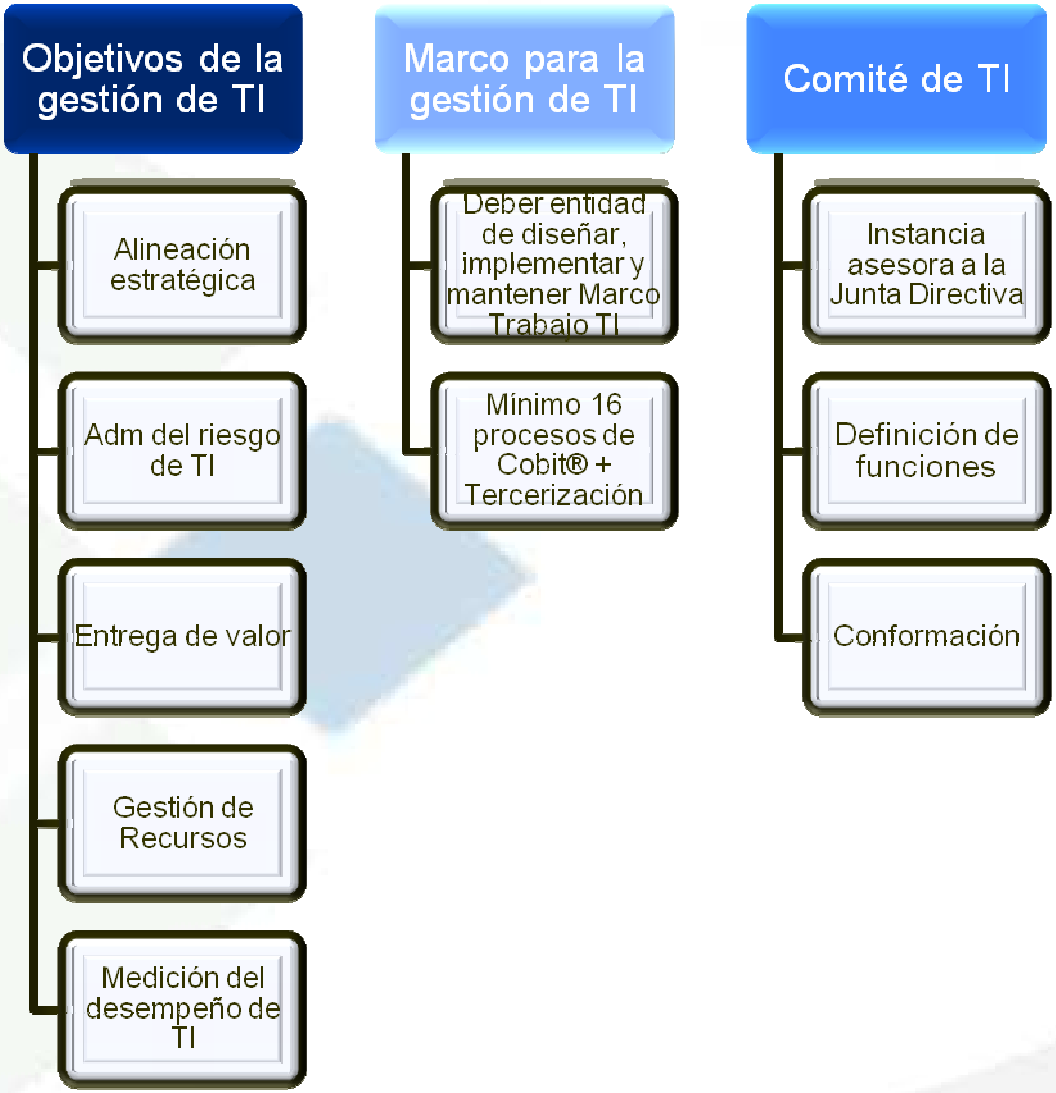
OBJETO

1. Establecer los lineamientos sobre la gestión de TI,
2. Definir los criterios y la metodología para la calificación y supervisión de la gestión de TI.

ALCANCE

1. Entidades financieras supervisadas.
2. Sistema Nacional de Pagos Electrónicos (SINPE).

Capitulo II
Gestión de la tecnología de Información



Capitulo III
EVALUACION DE LA GESTION DE TI

Perfil Tecnológico

- Descripción de la estructura organizacional, procesos y la infraestructura de TI
- Deber de la entidad de remisión en junio de cada año
- Deber de la entidad de actualización permanente
- SUGEF define la forma y medio para la remisión – Anexo 2-

Revisión externa independiente

- Periodicidad: cada 2 años
- SUGEF define el alcance y fecha de remisión de resultados con anticipación 9 meses
- Alcance mínimo de 16 procesos , extensivo a un número mayor
- Cubre los procesos delegados en proveedores locales o extranjeros de TI

Directrices sobre la revisión

- Norma Técnica: "Norma Internacional de trabajos para atestiguar (NITA 3000)"
- Productos de la revisión: Informe con conclusiones, Presentación salida y matriz de calificación
- Deber de comunicar la designación del especialista
- SUGEF facultada para verificar cumplimiento de requisitos del especialista

Capitulo III
EVALUACION DE LA GESTION DE TI

Comunicado SUGEF y plan de acción

- SUGEF remite un comunicado con principales hallazgos y calificación de la entidad en TI
- SUGEF puede requerir plan de acción. Plazo entidad 20 días hábiles.
- Calificación se considera para juzgar situación económica-financiera
- Calificación se obtiene mediante un sistema de ponderación de factores –

Recursos y Seguimiento SUGEF

- Posibilidad de una única revisión de la calificación, verificaciones con cargo a la entidad.
- Facultad para solicitar informes parciales y efectuar verificaciones in situ (ordinarias o extraordinarias)

Requisitos del especialista

- Requisitos técnicos: formación base, experiencia y certificación
- Requisitos de independencia: relación laboral, participación capital y relación comercial

Capitulo IV
disposiciones especiales

Seguridad

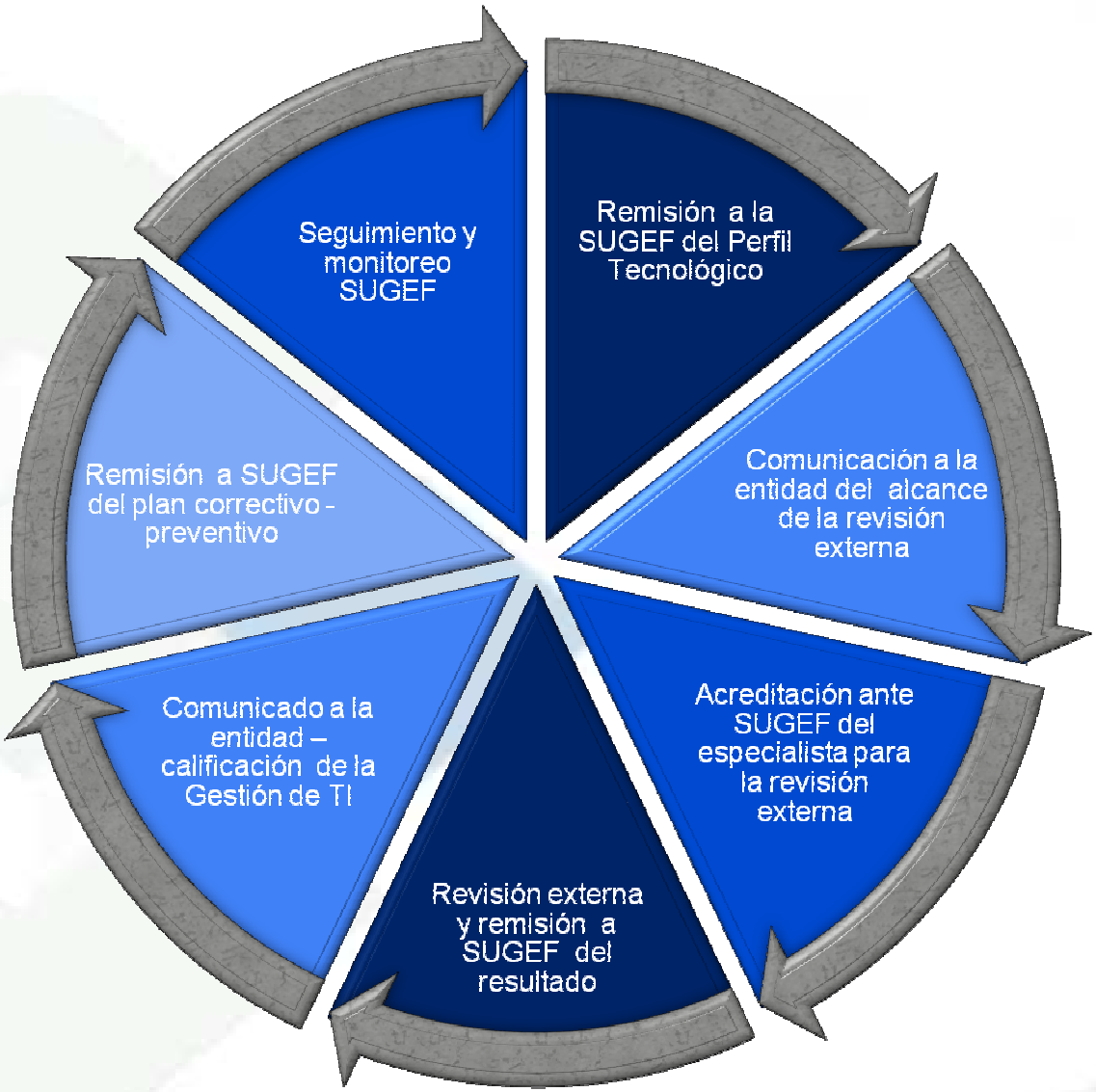
- Deber de la entidad de implementar las mejores prácticas relacionadas con banca electrónica y otros servicios a través de internet

Tercerización

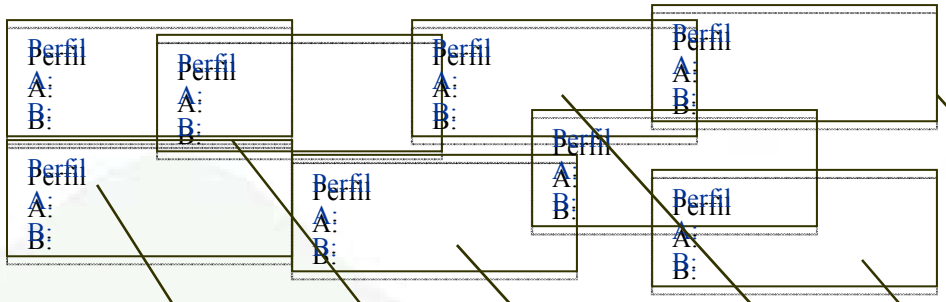
- Deber de comunicación a SUGEF de los servicios delegados a proveedores –contenido mínimo-
- Deber de la entidad por la actualización anual de la información
- Deber de mantener a disposición de SUGEF de las bases de datos

	Procesos COBIT®	Primera Auditoría Externa: 1 año contado a partir de la entrada en vigencia del reglamento	Segunda Auditoría Externa	Auditorías subsecuentes
1	PO9 Evaluar y administrar los riesgos de TI	Nivel madurez mínimo requerido: **tres**	Nivel madurez mínimo requerido: **tres**	Nivel madurez mínimo requerido: **tres**
2	PO10 Administrar proyectos			
3	AI6 Administrar cambios			
4	DS2 Administrar los servicios de terceros *			
5	DS4 Garantizar la continuidad del servicio			
6	DS5 Garantizar la seguridad de los sistemas			
7	DS11 Administrar los datos			
8	ME2 Monitorear y evaluar el control interno			
9	PO1 Definir un plan estratégico de TI	Nivel madurez mínimo requerido: **dos**	Nivel madurez mínimo requerido: **tres**	Nivel madurez mínimo requerido: **tres**
10	PO3 Determinar la dirección tecnológica			
11	PO5 Administrar la inversión en TI			
12	AI3 Adquirir y mantener infraestructura tecnológica			
13	AI5 Adquirir recursos de TI			
14	DS3 Administrar el desempeño y la capacidad			
15	DS 9 Administrar la configuración			
16	DS10 Administrar los problemas			
17	DS12 Administrar el ambiente físico			
Resto de los procesos que integran el marco para la gestión de TI		Nivel madurez mínimo requerido: **uno**	Nivel madurez mínimo requerido: **dos**	Nivel madurez mínimo requerido: **tres**

Ciclo Operativo

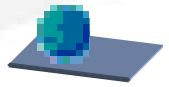


PERFIL TECNOLOGICO



Ejemplo del perfil tecnológico

TABLA 3 "Mapeo de procesos del negocio"													
Identificador del Proceso$_1$	Nombre		Descripción		Responsable$_5$		Proceso crítico$_6$	Dependencia tecnológica$_7$	Soporte$_8$				
	Proceso$_2$	Subproceso$_2$	Objetivo$_3$	Atención$_4$	Nombre	Puesto	S/N		A	B	C	D	E



Matriz de evaluación - Controles

Áreas de Revisión		Evaluación			Referencias	Observación
PO7 Administrar los Recursos Humanos de TI		Si	No	NA		
PO7.1	Reclutamiento y Retención del Personal					
1	¿El proceso de reclutamiento de personal de TI está alineado con las políticas y procedimientos generales de la organización (ejemplo: contratación, ambiente positivo de trabajo y orientación)?					
1	¿La gerencia de T.I. ha implementado procesos para asegurar que la fuerza de trabajo de TI cuenta con las habilidades necesarias para alcanzar las metas organizacionales?					
0%		**0**	**0**			
PO7.2	Competencias del Personal					
1	¿Se verifica periódicamente que el personal tenga las competencias para realizar sus roles tomando como base su educación, capacitación y experiencia?					
1	¿Existe una base definida para los requerimientos de competencias de TI?					
1	¿Dicha base es mantenida utilizando programas de calificación y certificación donde sea apropiado?					
0%		0	0			

Matriz de evaluación - Madurez

Áreas de Revisión		Evaluación			Referencias	Observación
PO7 Administrar los Recursos Humanos de TI		Si	No	NA		
	NIVEL DE MADUREZ					
Nivel 1	Inicial					
1	¿La gerencia de T.I. ha expresado formalmente la necesidad de gestionar los recursos humanos de TI?					
1	¿El proceso de gestión de recursos humanos de TI es repetible y proactivo?					
1	¿Se contemplan los cambios tecnológicos en el momento de establecer los niveles de competencia y habilidades?					
0%		**0**	**0**	**0**		
Nivel 2	Repetible pero intuitivo					
1	¿La gestión y contratación del personal de TI sigue una aproximación estratégica?					
1	¿Existe un plan de capacitación para el personal nuevo?					
0%		**0**	**0**	**0**		
Nivel 3	Proceso definido					
1	¿Existe un proceso definido y documentado para la gestión de los recursos humanos de TI?					
1	¿Existe un plan de administración de recursos humanos de TI?					
1	¿Existe un plan de capacitación formal diseñado para suplir las necesidades de recursos humanos de TI?					

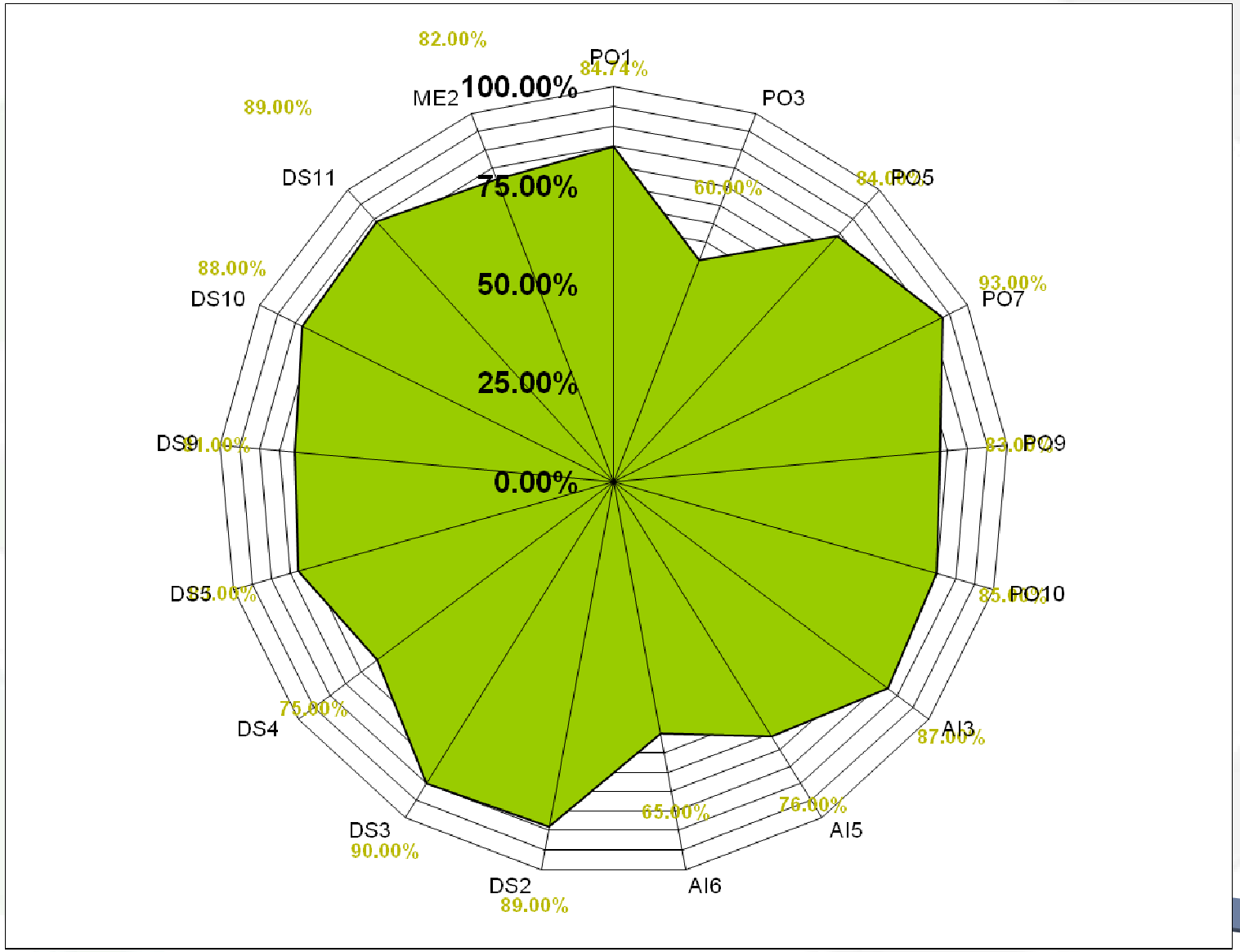
Matriz de evaluación – Por proceso

	PO1 Definir un Plan Estratégico de T.I.	**2.00**	84.74%	**Irregularidad 1**
PO1.1	Administración del valor de T.I.		100.00%	Normal
PO1.2	Alineación de T.I. con el negocio		100.00%	Normal
PO1.3	Evaluación del desempeño actual		100.00%	Normal
PO1.4	Plan Estratégico de T.I.		69.23%	Irregularidad 2
PO1.5	Planes tácticos de T.I.		100.00%	Normal
PO1.6	Administración del portafolio de T.I.		0.00%	Irregularidad 3
NM	Nivel de Madurez		3	Nivel 3

Matriz de evaluación – General

Proceso de Revisión - SUGEF	Peso SUGEF	Calificación	Resultado	
			%	% Ponderado
PO1 Definir un Plan Estratégico de T.I.	3	Irregularidad 1	84.74%	5%
PO3 Determinar la Dirección Tecnológica	3	Normal	95.33%	5%
PO5 Administrar la Inversión de TI	3	Irregularidad 1	84.00%	5%
PO7 Administrar los Recursos Humanos de TI	3	Normal	93.00%	5%
PO9 Evaluar y Administrar los Riesgos de TI	3	Irregularidad 1	83.00%	5%
PO10 Administración de Proyectos	3	Normal	85.00%	5%
AI3 Adquirir y Mantener la Infraestructura Tecnológica	3	Normal	87.00%	5%
AI5 Adquirir Recursos de TI	3	Irregularidad 1	76.00%	4%
AI6 Administración de Cambios	3	Irregularidad 2	65.00%	4%
DS2 Administración de los servicios de terceros	3	Normal	89.00%	5%
DS3 Administrar el Desempeño y la Capacidad	3	Normal	90.00%	5%
DS4 Garantizar la Continuidad de los Servicios	3	Irregularidad 1	75.00%	4%
DS5 Garantizar la Seguridad en los Sistemas	3	Irregularidad 1	83.00%	5%
DS9 Administración de la Configuración	3	Irregularidad 1	81.00%	5%
DS10 Administración de Problemas	3	Normal	88.00%	5%
DS11 Administración de los Datos	3	Normal	89.00%	5%
ME2 Monitorear y Evaluar el Control Interno	3	Irregularidad 1	82.00%	5%
Total	**54**	**Irregularidad 1**	**CG**	**84%**

Matriz de evaluación – General



Resultados esperados

- En un plazo de 2 años tener el estado real del sistema financiero nacional
- Determinar la media del sector financiero, por sector, y por tamaño
- Identificar los riesgos del sistema financiero nacional en materia de TI
- Poder realizar comparaciones entre entidades con características similares
- Mejorar el nivel tecnológico del sector financiero

SUPERINTENDENCIA GENERAL DE ENTIDADES FINANCIERAS

Certificada con ISO-9001/2000

Consultas

Osvaldo Sánchez

osanchez@sugef.fi.cr

Dirección de Informática

SUGEF