RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Mónica Beatriz Rela
Responsable de la Unidad Auditoría de Sistemas
Banco de la Nación Argentina
mrela@bna.com.ar

Representante por parte de CLAIN ante ISACA

Cosme Juan Carlos Belmonte
Director Ejecutivo de Auditoría
Banco de la Nación Argentina
cbelmonte@bna.com.ar

Representante Titular por Argentina y Past President CLAIN

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

El auditor debe considerar:

- *las necesidades de la Organización*
- *las Leyes y Regulaciones aplicables*
- *el nivel de madurez del gobierno de la contratación de servicios en la Organización*
- *las características del Proveedor de Servicios y el Servicio Contratado*
- *las diversas formas que puede asumir la contratación de Servicios*
- *los Riesgos Asociados*

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Gobierno de la contratación de servicios externos

- *Es el conjunto de responsabilidades, roles, objetivos, interfaces y controles requeridos para anticipar el cambio y manejar la introducción, el mantenimiento, el desempeño, los costos y el control de los servicios provistos por terceros.*

- *Es un proceso activo que el cliente y el proveedor de servicio debe adoptar para proveer un enfoque común, congruente y efectivo que identifique la información necesaria, las relaciones, los controles y los intercambios entre muchas de las partes interesadas en ambas partes.*

Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Gobierno de la contratación de servicios externos

(continuación)

- *Uno de los principales objetivos del proceso es **asegurar la continuidad del servicio en los niveles apropiados, la rentabilidad y el valor agregado para sostener la viabilidad comercial de ambas partes.***

- *Mientras que no es ni posible ni rentable definir contractualmente cada detalle y cada acción, **el proceso de gobierno provee el mecanismo para equilibrar el riesgo, la demanda de servicio, la provisión de servicio y el costo**.*

Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

¿Qué preguntas podemos hacernos?

- *Sobre la Organización Contratante*
- *Sobre el Proveedor de Servicios*
- *Sobre la Gestión de Riesgos*
- *Sobre los Servicios Contratados y el Contrato*
- *Sobre el Control y monitoreo de los Servicios Contratados*
- *Sobre aspectos particulares de Servicios de TI*

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Organización Contratante - Proveedor de Servicios

- *Qué normas/leyes regulan el servicio contratado? Y la delegación en terceros?*
- *Existen particularidades transfronterizas y/o transculturales que contemplar?*
- *Existen mejores prácticas y/o estándares relacionados?*
- *Existen políticas organizacionales que regulen la delegación de servicios dentro de la organización?*
- *Establecen estas políticas las responsabilidades de la Dirección y Gerencias de la Organización?*
- *El proveedor del servicio brinda otro servicio a la organización? De ser así, pueden existir incompatibilidades al respecto?*

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Gestión de Riesgos

- *Las políticas organizacionales reconocen los riesgos a los cuales se expone la Organización al delegar actividades en Terceros?*
- *Se realiza la evaluación de riesgos correspondiente a la delegación de servicios?*
- *Se eleva el análisis de riesgos a la Dirección de la Organización para su aprobación?*
- *Se contemplan contramedidas para mitigar los riesgos y/o seguros para transferirlos?*
- *Se establecen mecanismos de monitoreo de riesgos?*

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Servicios contratados y Contrato

El contrato define claramente:

- *el alcance de los servicios delegados?*
- *roles y responsabilidades de las partes?*
- *cumplimiento de requerimientos legales, regulatorios, de políticas organizacionales, por parte del proveedor?*
- *cumplimiento de estándares?*
- *acuerdos de confidencialidad?*
- *niveles mínimos de prestación de servicios y su tipo (SLA's)?*
- *participación de subcontratistas, responsabilidades para con éstos, aprobación de la organización para cambiarlos?*

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Servicios contratados y Contrato *(continuación)*

- *derechos a realizar auditorías al proveedor por parte de la entidad contratante y/o autoridad de contralor?*
- *cláusulas de renovación, finalización anticipada, transición por cambio de proveedor?*
- *notificación de cambio de niveles gerenciales, de dirección, de control accionario?*
- *posibilidad de incorporar solicitudes de mejora y/o nuevas necesidades de la organización?*
- *derechos de propiedad intelectual, de corresponder?*
- *mecanismos de resolución de disputas?*
- *penalidades por incumplimiento del nivel de servicio acordado?*

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Servicios contratados y Contrato *(continuación)*

Otras consideraciones:

- *están previstos mecanismos que aseguren la continuidad de los servicios que se contratan por cualquier situación que pudiera sufrir el proveedor? Dispone el proveedor de un plan de continuidad de servicios debidamente documentado y probado?*
- *posee el proveedor Auditoría Independiente que realice revisiones periódicas relacionadas con los servicios que presta (Ej. SAS 70)? La periodicidad se considera suficiente?.*
- *existe un proceso de revisión continua, mejoramiento y obtención de beneficios para ambas partes?*
- *están los servicios contratados relacionados con servicios de información?*

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Control y Monitoreo de Servicios contratados

Están definidos:

- *los mecanismos de control y monitoreo de niveles de servicios?*
- *los roles y responsabilidades de control y monitoreo de servicios dentro de la organización?*
- *los circuitos de aplicación de penalidades al proveedor del servicio por incumplimiento?*

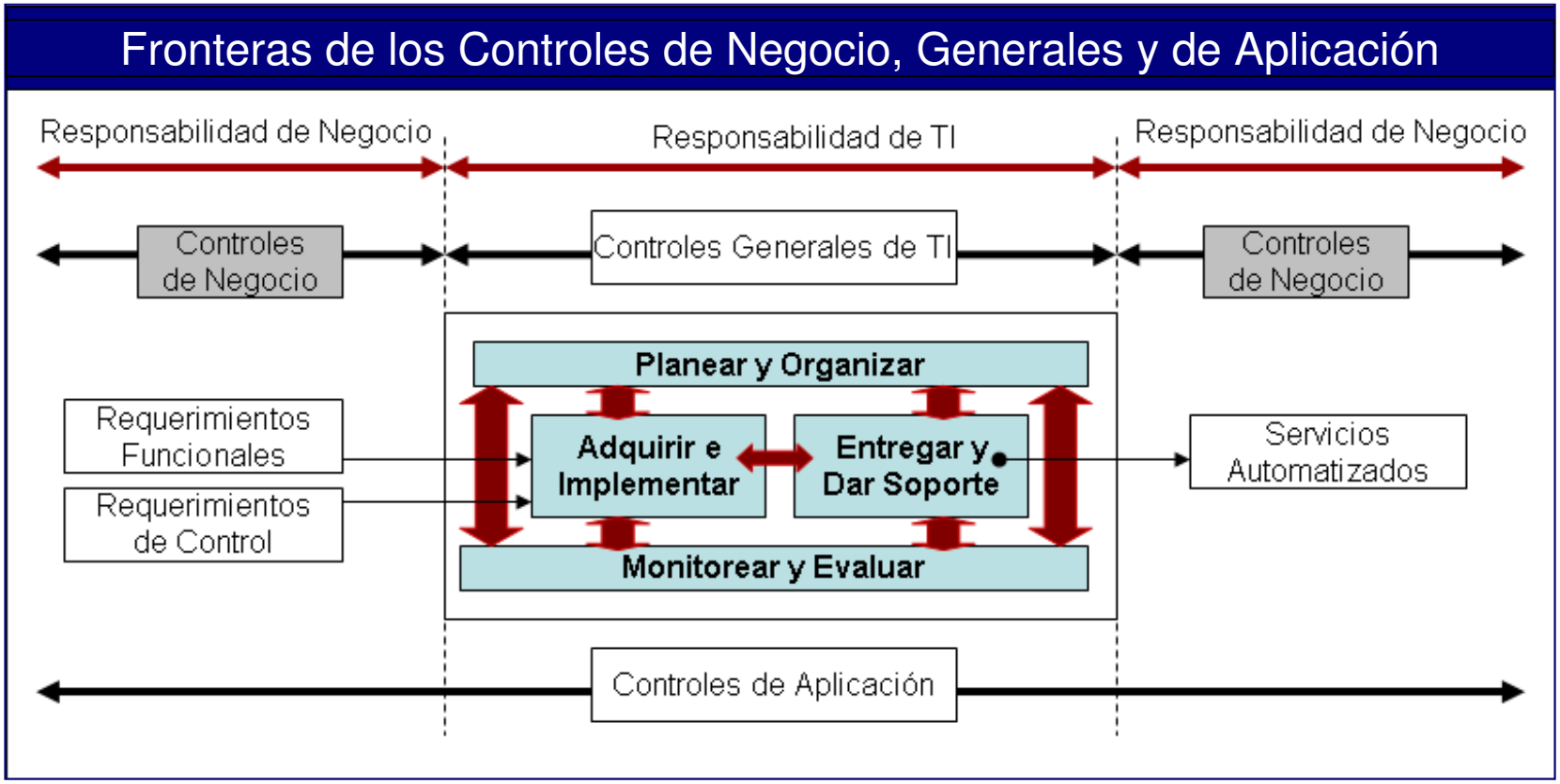
RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Servicios de TI - Algunas particularidades

- *Cumplimiento por parte del proveedor de políticas de seguridad de la organización contratante*
- *Para los sistemas críticos, niveles de soporte 24 x 7 x 365 (follow the sun)*
- *Monitoreo preventivo de equipamiento crítico.*
- *Técnicos locales para soporte on-site*
- *Para el caso de reemplazo de equipamiento, cláusulas de actualización tecnológica y/o de homologación en la plataforma existente.*
- *En materia de servicios de procesamiento, DRP y Capacity Planning. No sólo en lo que respecta a infraestructura, sino también a cantidad de personal capacitado.*
- *En materia de software, cláusulas de propiedad intelectual, de entidad depositaria de código fuente; de gestión de requerimientos y cambios.*

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Qué nos ofrece el Marco de Trabajo COBIT?

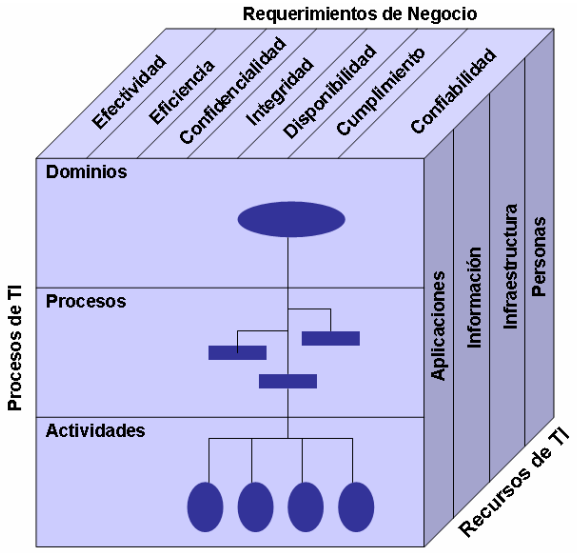


Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Dominios COBIT

- ***Planear y Organizar (PO)*** *– Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).*
- ***Adquirir e Implementar (AI)*** *– Proporciona las soluciones y las pasa para convertirlas en servicios.*
- ***Entregar y Dar Soporte (DS)*** *– Recibe las soluciones y las hace utilizables por los usuarios finales.*
- ***Monitorear y Evaluar (ME)*** *- Monitorear todos los procesos para asegurar que se sigue la dirección provista.*



Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Servicios de TI

Los servicios más comunes en materia de TI son:

- *Data Entry*
- *Implementación de sistemas "llave en mano"*
- *Diseño y desarrollo de nuevos sistemas*
- *Mantenimiento de aplicaciones existentes*
- *Conversión de aplicaciones a nuevas plataformas*
- *Operación del Help Desk o del Call Center*
- *Procesamiento de las operaciones*
- *Instalación de nueva infraestructura de TI (equipamiento, comunicaciones, redes)*
- *Mantenimiento y soporte de infraestructura de TI*
- *Migración de infraestructura de TI*

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Procesos del Dominio Entregar y Dar Soporte (DS)

- *DS1 Definir y administrar los niveles de servicio*
- *DS2 Administrar los servicios de terceros*
- *DS3 Administrar el desempeño y la capacidad*
- *DS4 Garantizar la continuidad del servicio*
- *DS5 Garantizar la seguridad de los sistemas*
- *DS6 Identificar y asignar costos*
- *DS7 Educar y entrenar a los usuarios*
- *DS8 Administrar la mesa de servicio y los incidentes*
- *DS9 Administrar la configuración*
- *DS10 Administrar los problemas*
- *DS11 Administrar los datos*
- *DS12 Administrar el ambiente físico*
- *DS13 Administrar las operaciones*

Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

Procesos del Dominio Entregar y Dar Soporte

NO SOLO APLICABLE A TI

- *DS2 Administrar los servicios de terceros*
  - *DS2.1 Identificación de Todas las Relaciones con Proveedores*
  - *DS2.2 Gestión de Relaciones con Proveedores*
  - *DS2.3 Administración de Riesgos del Proveedor*
  - *DS2.4 Monitoreo del Desempeño del Proveedor*

Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

DS2 Administrar los servicios de terceros

Actividades del Proceso

- *DS2.1 Identificación de Todas las Relaciones con Proveedores*

  Identificar todos los servicios de los proveedores, y categorizar los de acuerdo al tipo de proveedor, significado y criticidad. Mantener documentación formal de relaciones técnicas y organizacionales que cubren los roles y responsabilidades, metas, entregables esperados, y credenciales de los representantes de estos proveedores.

- *DS2.2 Gestión de Relaciones con Proveedores*

  Formalizar el proceso de gestión de relaciones con proveedores para cada proveedor. Los dueños de las relaciones deben enlazar las cuestiones del cliente y proveedor y asegurar la calidad de las relaciones basadas en la confianza y transparencia. (Ej.: a través de SLAs).

Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

DS2 Administrar los servicios de terceros

- *DS2.3 Administración de Riesgos del Proveedor*

  Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de entrega de forma segura y eficiente sobre una base de continuidad. Asegurar que los contratos están de acuerdo con los requerimientos legales y regulatorios de los estándares universales del negocio. La administración del riesgo debe considerar además acuerdos de confidencialidad (NDAs), contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos, etc.

- *DS2.4 Monitoreo del Desempeño del Proveedor*

  Establecer un proceso para monitorear la prestación del servicio para asegurar que el proveedor está cumpliendo con los requerimientos del negocio actuales y que se adhiere continuamente a los acuerdos del contrato y a SLAs, y que el desempeño es competitivo con proveedores alternativos y las condiciones del mercado.

Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

DS2 Administrar los servicios de terceros

- ***Matriz RACI***

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Identificar y categorizar las relaciones de los servicios de terceros				I	C	R	C	R	A/R	C	C
Definir y documentar los procesos de administración del proveedor		C		A	I	R	I	R	R	C	C
Establecer políticas y procedimientos de evaluación y suspensión de proveedores		C		A	C	C		C	R	C	C
Identificar, valorar y mitigar los riesgos del proveedor		I		A		R		R	R	C	C
Monitorear la prestación del servicio del proveedor				R	A	R		R	R	C	C
Evaluar las metas de largo plazo de la relación del servicio para todos los interesados	C	C	C	A/R	C	C	C	C	R	C	C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

DS2 Administrar los servicios de terceros

- ***Entradas desde otros procesos***

Desde	***Entradas***
•P01. Definir un Plan Estratégico de TI.	*•Estrategia de contratación de TI*
•P08. Administrar la Calidad.	*•Estándares de adquisición*
•AI5. Adquirir Recursos de TI	*•Arreglos contractuales, requerimientos de administración de relaciones con terceros*
•DS1. Definir y Administrar los Niveles de Servicio	*•SLAs, reporte de revisión de contrato*
•DS4. Garantizar la Continuidad del Servicio	*•Requerimientos de servicio contra desastre incluyendo roles y responsabilidades*

Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

DS2 Administrar los servicios de terceros

- ***Salidas hacia otros procesos***

Salidas	***Hacia***
• *Reportes de desempeño de los procesos*	•*ME1. Monitorear y evaluar el desempeño de TI*
• *Catálogo del proveedor*	•*P09. Evaluar y Administrar los Riesgos de TI.*

Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

DS2 Administrar los servicios de terceros

- ***Modelos de Madurez***

La administración del proceso de Administrar los servicios de terceros que satisfagan los requerimientos de TI del negocio de brindar servicios de terceros satisfactorios siendo transparentes respecto a los beneficios, costos y riesgos es:

0 No Existente cuando

- *Las responsabilidades y la rendición de cuentas no están definidas.*
- *No hay políticas y procedimientos formales respecto a la contratación con terceros.*
- *Los servicios de terceros no son ni aprobados ni revisados por la gerencia.*
- *No hay actividades de medición y los terceros no reportan.*
- *A falta de una obligación contractual de reportar, la alta gerencia no está al tanto de la calidad del servicio prestado.*

Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

DS2 Administrar los servicios de terceros

- ***Modelos de Madurez***

1 Inicial / Ad Hoc cuando

- *La gerencia está conciente de la importancia de la necesidad de tener políticas y procedimientos documentados para la administración de los servicios de terceros, incluyendo la firma de contratos.*
- *No hay condiciones estandarizadas para los convenios con los prestadores de servicios.*
- *La medición de los servicios prestados es informal y reactiva.*
- *Las prácticas dependen de la experiencia de los individuos y del proveedor (por ejemplo, por demanda).*

2 Repetible pero Intuitivo cuando

- *El proceso de supervisión de los proveedores de servicios de terceros, de los riesgos asociados y de la prestación de servicios es informal.*
- *Se utiliza un contrato pro-forma con términos y condiciones estándares del proveedor (por ejemplo, la descripción de servicios que se prestarán).*
- *Los reportes sobre los servicios existen, pero no apoyan los objetivos del negocio.*

Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

DS2 Administrar los servicios de terceros

- ***Modelos de Madurez***

3 Definido cuando

- *Hay procedimientos bien documentados para controlar los servicios de terceros con procesos claros para tratar y negociar con los proveedores.*
- *Cuando se hace un acuerdo de prestación de servicios, la relación con el tercero es meramente contractual. La naturaleza de los servicios a prestar se detalla en el contrato e incluye requerimientos legales, operativos y de control.*
- *Se asigna la responsabilidad de supervisar los servicios de terceros. Los términos contractuales se basan en formatos estandarizados.*
- *El riesgo del negocio asociado con los servicios del tercero esta valorado y reportado.*

Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

DS2 Administrar los servicios de terceros

- ***Modelos de Madurez***

4 Administrado y Medible cuando

- *Se establecen criterios formales y estandarizados para definir los términos de un acuerdo, incluyendo alcance del trabajo, servicios/entregables a suministrar, suposiciones, cronograma, costos, acuerdos de facturación y responsabilidades.*
- *Se asignan las responsabilidades para la administración del contrato y del proveedor.*
- *Las aptitudes, capacidades y riesgos del proveedor son verificadas de forma continua.*
- *Los requerimientos del servicio están definidos y alineados con los objetivos del negocio.*
- *Existe un proceso para comparar el desempeño contra los términos contractuales, lo cual proporciona información para evaluar los servicios actuales y futuros del tercero.*
- *Se utilizan modelos de fijación de precios de transferencia en el proceso de adquisición.*
- *Todas las partes involucradas tienen conocimiento de las expectativas del servicio, de los costos y de las etapas. Se acordaron los KPIs y KGIs para la supervisión del servicio.*

Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

DS2 Administrar los servicios de terceros

- ***Modelos de Madurez***

5 Optimizado cuando

- *Los contratos firmados con los terceros son revisados de forma periódica en intervalos predefinidos.*
- *La responsabilidad de administrar a los proveedores y la calidad de los servicios prestados está asignada.*
- *Se monitorea el cumplimiento de las condiciones operativas, legales y de control y se implantan acciones correctivas.*
- *El tercero está sujeto a revisiones periódicas independientes y se le retroalimenta sobre su desempeño para mejorar la prestación del servicio.*
- *Las mediciones varían como respuesta a los cambios en las condiciones del negocio.*
- *Las mediciones ayudan a la detección temprana de problemas potenciales con los servicios de terceros.*
- *La notificación completa y bien definida del cumplimiento de los niveles de servicio, está asociada con la compensación del tercero.*
- *La gerencia ajusta el proceso de adquisición y monitoreo de servicios de terceros con base en los resultados de los KPIs y KGIs.*

Fuente: ISACA

RESPONSABILIDAD DE LA AUDITORÍA INTERNA ANTE LOS SERVICIOS TERCERIZADOS

¿Preguntas?

¡Muchas Gracias!

Mónica Beatriz Rela
Responsable de la Unidad Auditoría de Sistemas
Banco de la Nación Argentina
mrela@bna.com.ar

Representante por parte de CLAIN ante ISACA

Cosme Juan Carlos Belmonte
Director Ejecutivo de Auditoría
Banco de la Nación Argentina
cbelmonte@bna.com.ar

Representante Titular por Argentina y Past President CLAIN