Rol del auditor interno para evaluar la gestión del riesgo de Ciber Seguridad

Gabriel Santiago Alderete

Auditor Interno de Sistemas – Banco Macro S.A.

Organizan

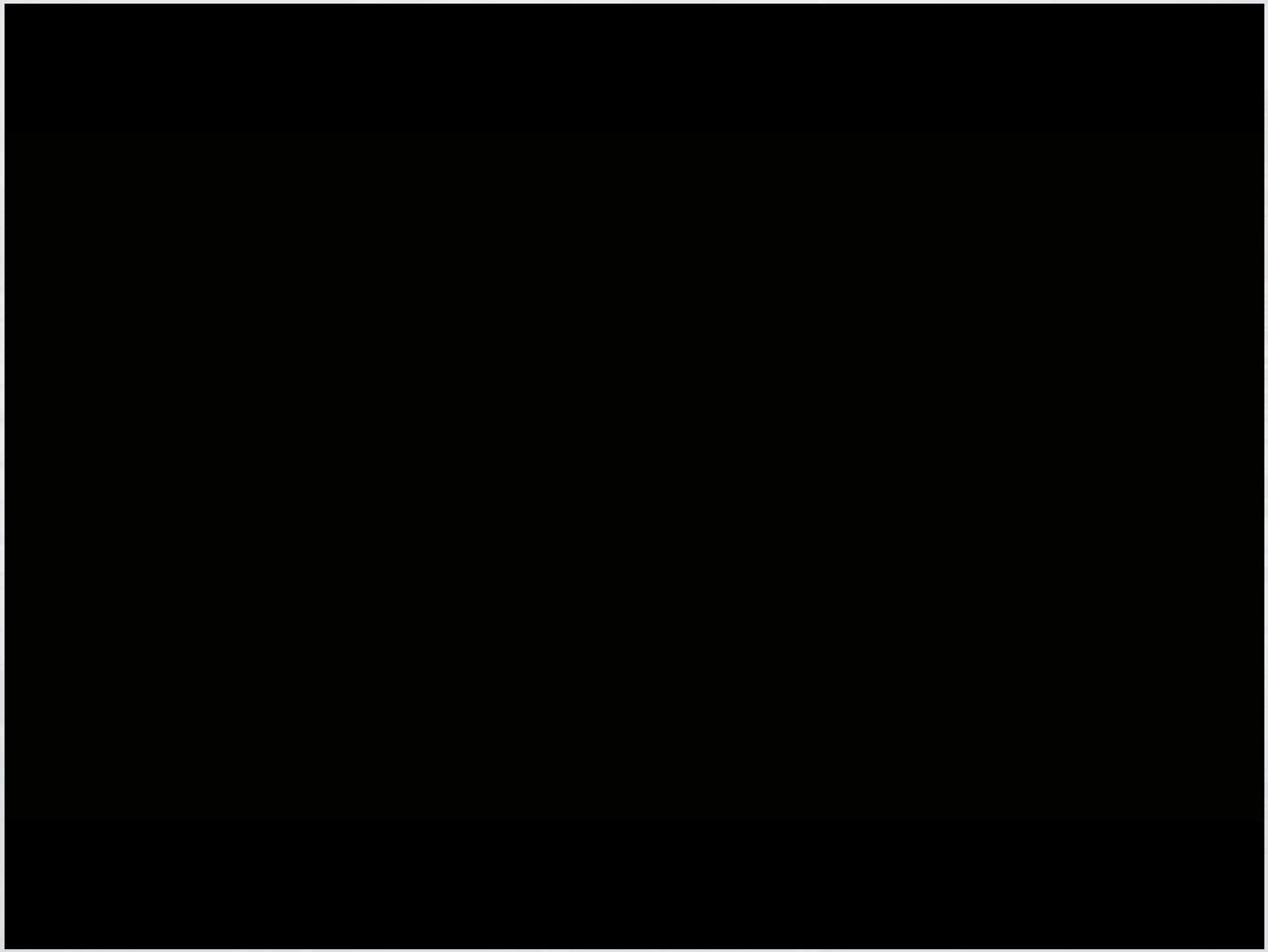
FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Asociación Bancaria Costarricense

Agenda

- Introducción: ¿Qué es Ciber Seguridad? ¿Qué framework usamos? ¿Por qué?
- Desarrollo: ¿Cómo implementamos el framework?
- Conclusión: ¿Cuál es el resultado esperado? ¿Qué rol debe tomar el auditor interno?

¿Qué es Ciber Seguridad?



¿Qué es Ciber Seguridad?

- Ciber Seguridad es toda **protección de activos de información**, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran **interconectados**.

- En este nuevo escenario no es mejor quien no se cae nunca, sino quien **mas rápido se levanta**.

- En este sentido la **convergencia** e interacción entre las tres líneas de defensa, son aspectos claves para brindar a las organizaciones mejores herramientas para **prevenir y minimizar el impacto**.

¿Qué framework usamos? ¿Por qué?

COBIT 5

Information Security Management System ISO 27001 Certified

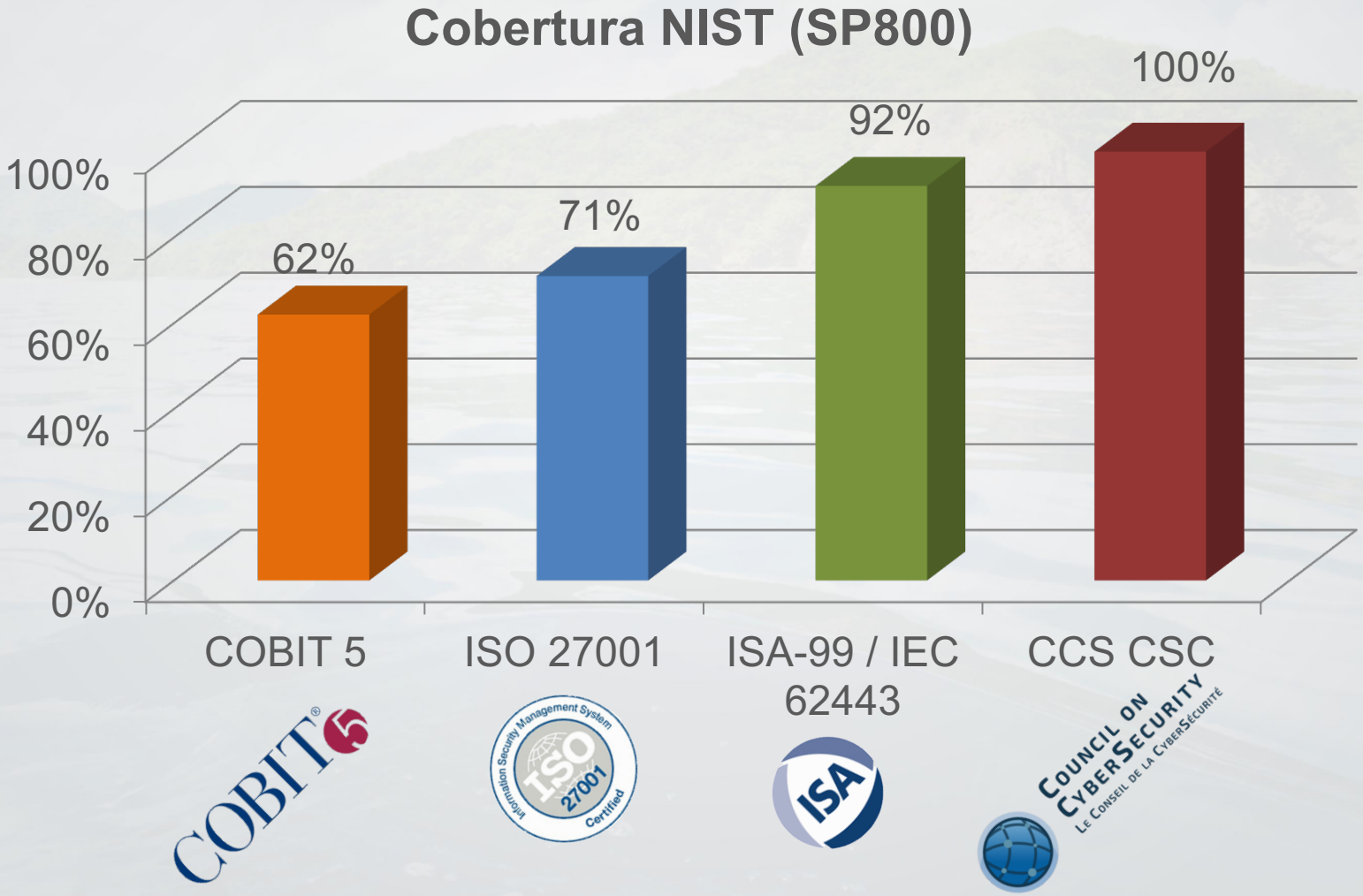
NIST
National Institute of Standards and Technology

ISA

COUNCIL ON CYBERSECURITY
LE CONSEIL DE LA CYBERSÉCURITÉ

XXI GLAIN COSTA RICA 2017

¿Qué framework usamos? ¿Por qué?



Estadística elaborada por el autor.

¿Qué framework usamos? ¿Por qué?

- A pesar de que ISACA también recomienda NIST (*), debemos tener en consideración que cada entidad es un caso particular y tenemos que evaluar:
  - ¿Cuáles son los requisitos legales?
  - ¿Cuáles son los requisitos contractuales?
  - ¿Qué beneficios le gustaría obtener?
  - ¿Cuáles son los objetivos que desearía lograr?

(*) https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Implementing-the-NIST-Cybersecurity-Framework.aspx

¿Cómo implementamos el framework?

NIST ofrece una metodología basada en fases y categorías:

http://www.stickman.com.au/services/transformation/nist-cyber-security-framework/

¿Cómo implementamos el framework?

- No solo cómo, sino quién debe participar:

¿Cómo implementamos el framework?

FASES	CATEGORÍA	IMPLEMENTACIÓN DEL FRAMEWORK NIST			POST IMPLEMENTACIÓN	
		1ª Línea de Defensa	2ª Línea de Defensa	3ª Línea de Defensa	Auditoría	Auditoría Continua
IDENTIFICAR	Gestión de Activos	Identificar y clasificar procesos de negocio, activos, riesgos y controles, basados en la estrategia de negocio y apetito de riesgos.		Asesorar y acompañar en el proceso de identificación.	Asegurar la actualización periódica basándose en eventos significativos	Alertas de altas o modificaciones de activos, riesgos o controles.
	Ambiente de Negocios					
	Gobernabilidad					
	Evaluación de Riesgos					
	Estrategia de GIR					
	Disponibilidad					

¿Cómo implementamos el framework?

FASES	CATEGORÍA	IMPLEMENTACIÓN DEL FRAMEWORK NIST			POST IMPLEMENTACIÓN	
		1ª Línea de Defensa	2ª Línea de Defensa	3ª Línea de Defensa	Auditoría	Auditoría Continua
PROTEGER	Gestión del control de acceso	Establecer políticas, normas, procedimientos y estándares acordes a los riesgos identificados. La segunda línea de defensa lo implementará y la tercera validará su eficiencia y efectividad.			Validar los cambios en forma periódica.	Alertas de cambios en las directivas de seguridad. Monitoreo de gestión, disponibilidad, etc.
	Aseguramiento y Capacitación					
	Seguridad de los Datos					
	Protección de la información					
	Mantenimiento					
	Tecnología de protección					

¿Cómo implementamos el framework?

FASES	CATEGORÍA	IMPLEMENTACIÓN DEL FRAMEWORK NIST			POST IMPLEMENTACIÓN	
		1ª Línea de Defensa	2ª Línea de Defensa	3ª Línea de Defensa	Auditoría	Auditoría Continua
DETECTAR	Anomalías y Eventos	Establecer procedimientos detección, identificación, clasificación y resolución de incidentes. Periódicamente se deben actualizar los riesgos y controles.			Verificar los incidentes críticos y que los mismos impacten en sus procesos.	Pistas de incidentes con tipologías, clasificaciones y riesgos asociados.
	Seguridad de supervisión continua					
	Procesos de detección					

¿Cómo implementamos el framework?

FASES	CATEGORÍA	IMPLEMENTACIÓN DEL FRAMEWORK NIST			POST IMPLEMENTACIÓN	
		1ª Línea de Defensa	2ª Línea de Defensa	3ª Línea de Defensa	Auditoría	Auditoría Continua
RESPONDER	Planificación de la respuesta	Definir la normativa interna para cada categoría.	Estratificar los incidentes ya registrados y establecer distintos planes de acción según su clasificación.	Acompañar y validar las definiciones basados en los riesgos identificados en las distintas fases.	Verificar que los incidentes se encuentren gestionados según los planes establecidos y que los mismos se encuentren actualizados.	Mediciones de tiempos de respuestas ante incidentes según su taxonomía.
	Comunicaciones					
	Análisis					
	Mitigación					
	Mejoras					

¿Cómo implementamos el framework?

FASES	CATEGORÍA	IMPLEMENTACIÓN DEL FRAMEWORK NIST			POST IMPLEMENTACIÓN	
		1º Línea de Defensa	2ª Línea de Defensa	3ª Línea de Defensa	Auditoría	Auditoría Continua
RECUPERAR	Planificación de recuperación	Definir la normativa interna para cada categoría.	Establecer distintos planes de acción según los incidentes estratificados.	Acompañar y validar las definiciones basados en los riesgos identificados en las distintas fases.	Verificar que las mejoras implementadas mitiguen los riesgos generados por nuevos incidentes y que actualice la fase de identificación.	Mediciones de tiempos de recuperación ante incidentes según su taxonomía.
	Mejoras					
	Comunicaciones					

¿Cuál es el resultado esperado? ¿Qué rol debe tomar el auditor interno?

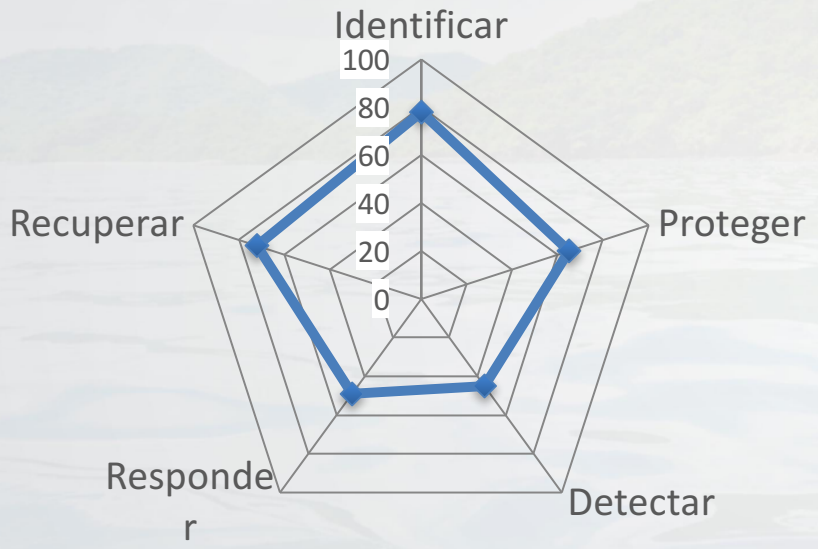
¿Cuál es el resultado esperado? ¿Qué rol debe tomar el auditor interno?

	PUNTOS FUERTES		PUNTOS DÉBILES	
DE ORIGEN INTERNO	Proceso de **identificación**.	76%	Inconvenientes con **permisos sobre BD**.	83%
	Tenemos un buen **ambiente de control** interno.	56%	Controles de **DLP** no son fuertes.	74%
	Tenemos una buena **capacitación** del personal.	34%	**Accesos incompatibles** a las aplicaciones.	59%
	Cumplimiento **normas internacionales**.	28%	**Plan estratégico** de seguridad inefectivo e ineficiente.	49%
DE ORIGEN EXTERNO	Controles **perimétricos** satisfactorios.	67%	Software **antivirus desactualizado**.	89%
	Ciber ataques durante el último año.	44%	El **pentest** no nos arroja las amenazas.	72%
	Phishing durante el último año.	39%	**Reglas de firewall** escasas o excesivas.	63%
	Controles sobre la **actividad terciarizad**	12%	No contamos con **IDS e IPS**.	31%

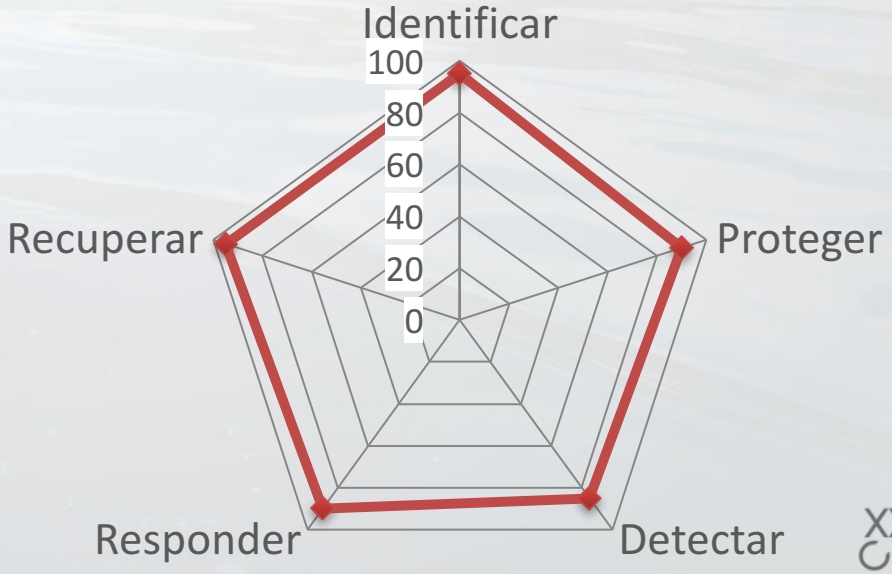
Estadística según encuesta.

¿Cuál es el resultado esperado? ¿Qué rol debe tomar el auditor interno?

Situación Actual

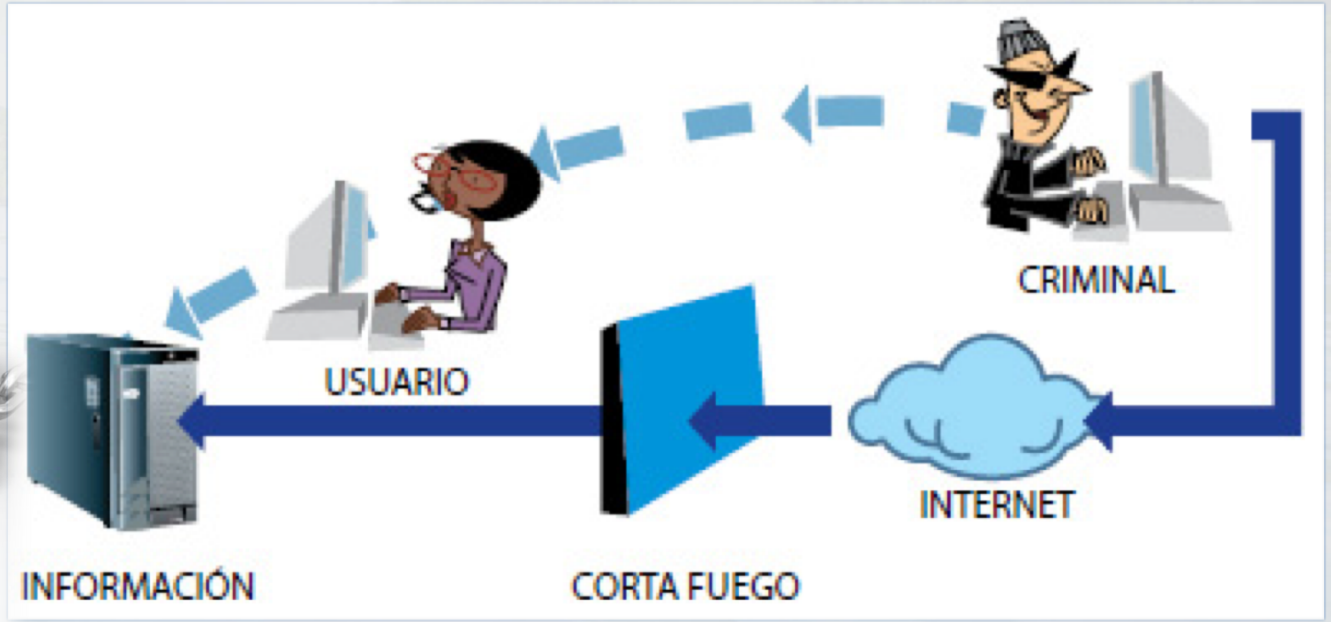


Situación Deseable

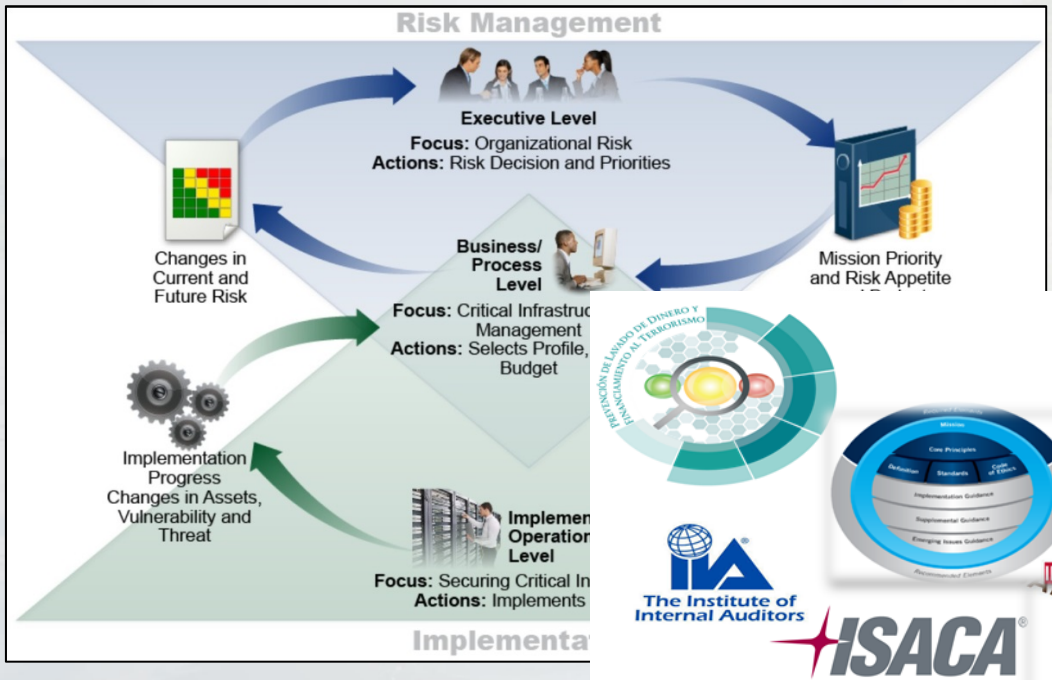


Estadística según encuesta.

¿Cuál es el resultado esperado? ¿Qué rol debe tomar el auditor interno?



¿Cuál es el resultado esperado? ¿Qué rol debe tomar el auditor interno?



La seguridad se hace entre responsab

Auditor Especialista en Gestión Integral de Riesgos.

Gabriel Alderete

Banco Macro S. A. - Argentina

Contacto: gabrielalderete@macro.com.ar

Muchas gracias por su atención…