"Auditoría Interna, el nuevo pilar de la Alta Dirección“

Instituto de Auditores Internos de Chile A.G.

SANTIAGO - CHILE clai2015

FLAI
FEDERACION LATINOAMERICANA DE AUDITORES INTERNOS

Interacción y Convergencia.
Gestión del Riesgo, Gobierno Corporativo, Cumplimiento y Auditoría Interna

Instituto de Auditores Internos de Chile

SANTIAGO - CHILE clai2015

FLAI
FEDERACION LATINOAMERICANA DE AUDITORES INTERNOS

Contexto Global Cambiante

- El mundo actual, en el que vivimos, cambia y se transforma a gran velocidad en forma permanente y esto será una constante en los próximos años

- Las empresas no pueden permanecer ajenas a estas circunstancias por lo que les resulta una necesidad acompañar esta inercia para permanecer, subsistir y crecer.

- En estas circunstancias **Auditoría** deberá tomar al cambio como una oportunidad de crecimiento, entendiéndolo como un desafío

Video

TI y el campo

FOCUS POINT !!

Oficiales de Cumplimiento.com

ISO 9001 Gestión de la Calidad

ISO 14001 Gestión Ambiental

OHSAS 18001 Gestión de seguridad y Salud Laboral

ISO 50001 Sistemas de Gestión Energética

PREVENCIÓN DE LAVADO DE DINERO Y FINANCIAMIENTO AL TERRORISMO

The Institute of Internal Auditors

NIIF

Normas Internacionales de información Financiera

Gobierno Corporativo

VITAL PARA LAS EMPRESAS

BASILEA III

RISK MANAGEMENT PROCESS

ASSESS RISK

IDENTIFY RISK

CONTROL RISK

REVIEW CONTROLS

FATCA

Required Elements

Mission

Core Principles

Definition

Standards

Code of Ethics

Implementation Guidance

Supplemental Guidance

Emerging Issues Guidance

Recommended Elements

IPPF

SARBANES-OXLEY ACT

CERO CORRUPCIÓN

100% DESARROLLO

ORGULLOSO DE SER UN AUDITOR INTERNO

www.theiia.org

FLAI

COSO 2013

FRAUD

Socios Estratégicos

Primer contacto de AI con GIR

Relevamiento de los procesos de Gestión de Riesgos incluyendo el análisis de riesgos de TI

Proceso Principal

- Identificación → Factores Riesgo
- Medición → Herr. Medición
- Monitoreo → Control Límites
- Mitigación → Plan de Acción

Procesos Anexos

- Relevar Fuentes de Información - Independiente
- Proceso de ABC de Metodologías
- Proceso de ABC de Límites
- Esquema Documental (Metodología / Evidencia)
- Sistemas de Información - Soporte

Retroalimentación

Convergencia

Auditoria Interna	SOX	GIR / Cumplimiento
Conocimiento del Negocio Identificación Procesos y Áreas	Scope de Información Financiera Identificación de Procesos y sus Dueños	Conocimiento del Negocio Identificación Procesos y responsable de la gestión
Prueba diseño y relevamiento Identificación de riesgos **(Entorno, Entidad, Procesos)** Clasificación de Riesgos (AMB) Matriz de Riesgos	Relevamientos Identificación de riesgos y controles **(ECL y Procesos)** Clasificación de Controles (ABC) Matrices de Riesgos y Controles.	Evaluar e Identificar riesgos **(Entorno, Entidad, Procesos)** Identificación y Clasificación de Eventos (ABC) Matriz de Riesgos
Planificación Anual de AI	Planificación del proyecto.	Planificación Anual
Pruebas de cumplimiento	Testeos y auto testeos	Medición Riesgo Residual
Metodología de revisión y generación de muestras	Metodología de revisión y generación de muestras	Metodología de revisión - Auto evaluaciones
Informes de Observaciones	Certificaciones con Incidencias	Reporta Eventos e Incidentes
Seguimiento de Observaciones	Remediación de Incidencias	Mejoras de Procesos

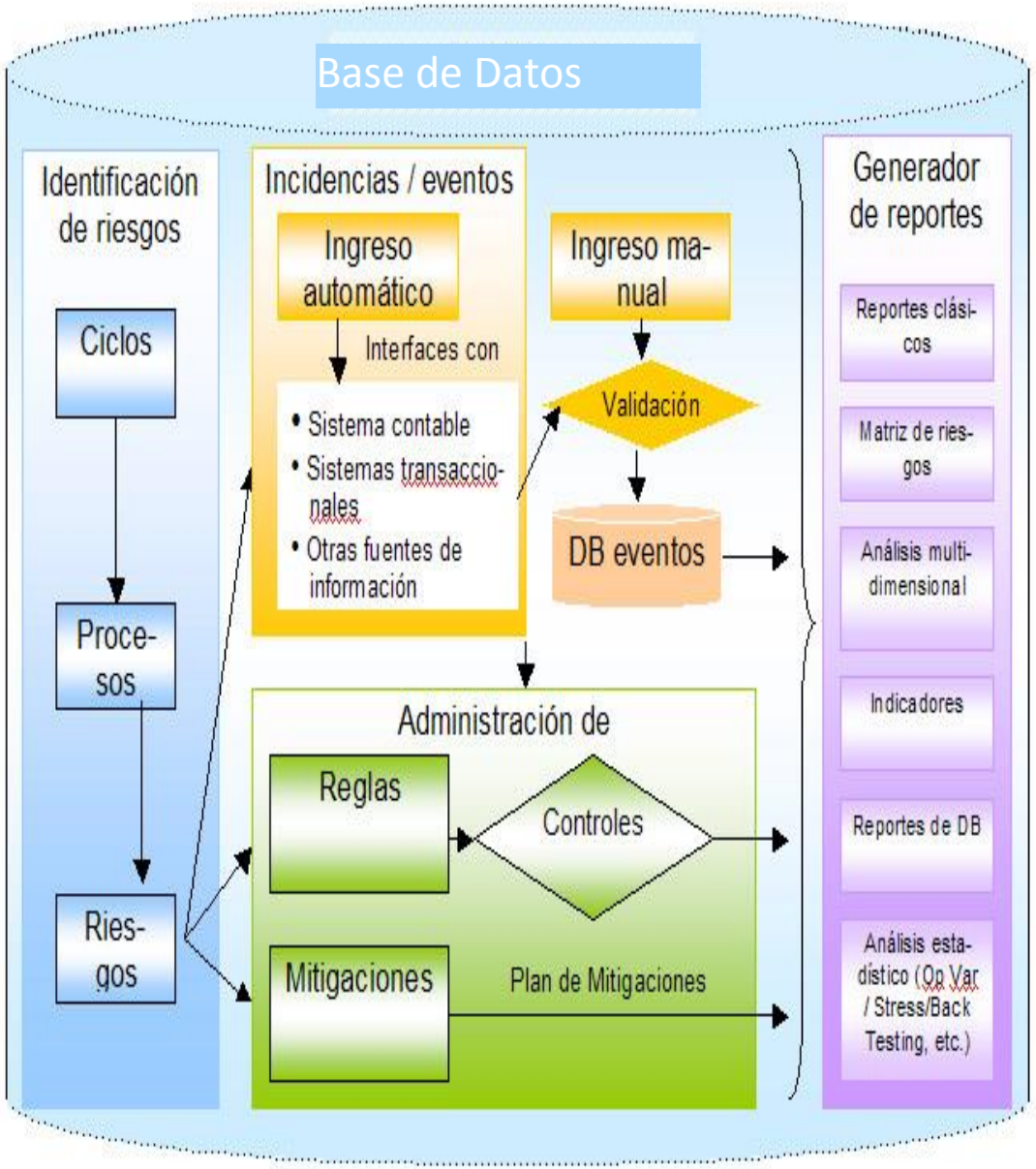
Implementación de normas y procedimientos de Gestión de Riesgos

- Acta de creación por Directorio del Comité
- Reglamenta el Comité de Gestión
- Política Marco de GR y Manuales según Riesgo
- Misiones y Funciones
- Diseño de metodología de Pruebas de Estrés Integral
- Supervisión, control y seguimiento de planes correctivos o Contingencia

Mapa Integral de Riesgos y Controles

Herramienta para administración y gestión.

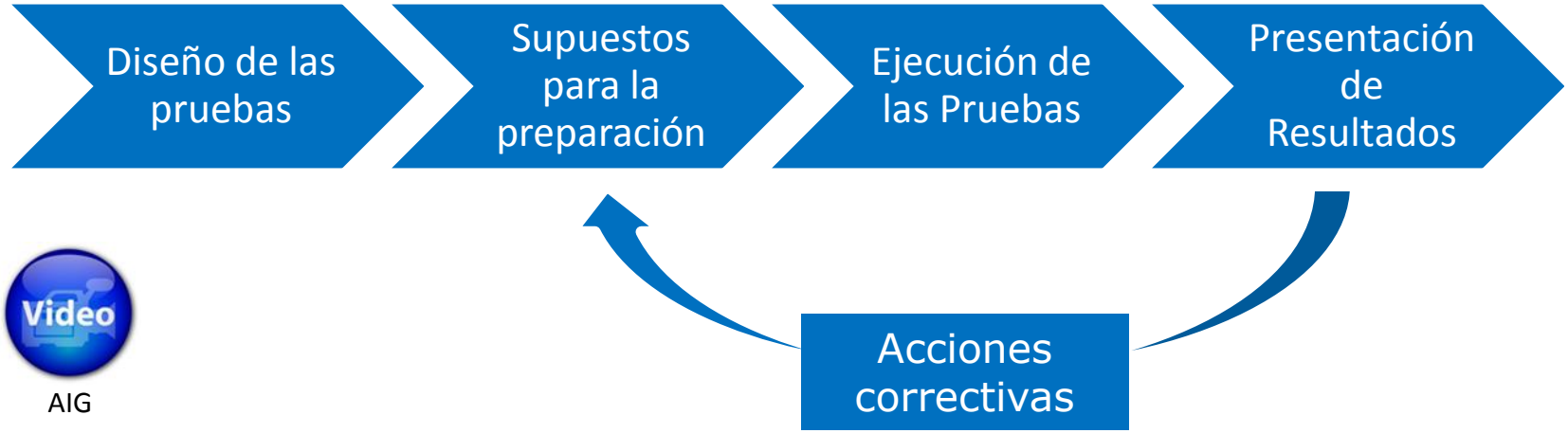
Funcionalidades
Generación de una base de riesgos.
Asociación a procesos y productos.
Relación con controles mitigantes.
Estimación de impacto y ocurrencia.
Incorporación de planes de mitigación.
Generación de indicadores.
Relación con Normas y Políticas.
Administración Testeos y Auto-testeos.
Obtención de Reportes de Gestión.
Obtención de Reportes de Incidencias.
Planes de Acción y Seguimiento.
Emisión de Certificaciones.
Estandarización de Narrativos.



Auditoría, crítica del Modelo de GIR

Evaluación de la metodología.

- Desafío las premisas / supuestos
- Validar el soporte de los escenarios
- Analizar los resultados
- Informar aspectos relevantes y/o acuerdos de mejora



Video

AIG

Oficial de Cumplimiento

2005 Comité de Basilea
“Cumplimiento y su función “

“Riesgo de sanciones legales o reglamentarias, pérdidas financieras materiales o pérdida reputacional que se pueden sufrir, como consecuencia de la falta de cumplimiento de leyes, reglamentos, normas, estándares y códigos de conducta”

Video

El cumplimiento será eficaz en una cultura corporativa que hace hincapié en estándares de “honestidad e integridad”

Toshiba

Características de la función

- ✓ **Independiente (recursos suficientes y responsabilidades específicas).**
- ✓ **Sujetos a revisión periódica por Auditoria Interna**
- ✓ **Flexible (tamaño, naturaleza, extensión, complejidad organizativa)**
- ✓ **Compatible con el marco regulatorio y legal**
- ✓ **Consistente (estrategia comercial, estructura y gestión de riesgos)**
- ✓ **Abarca temáticas diversas tales como:**
  - **Prevención de Lavado**
  - **Protección de Datos Personales**
  - **Protección de Usuarios Financieros**
  - **Otras regulaciones o leyes nacionales /internacionales**

CRM Regulatory Complience Management

04/2014 OSFI – Guía E-13

Actualiza y Alinea el marco de supervisión Con Gobierno Corporativo y Riesgo Operacional

El Marco CRM se define en función a:

- ✓ **Estructuras, Procesos y Controles claves**
- ✓ **Aplica a la organización, subsidiarias o filiales**
- ✓ **Útil para gestionar o mitigar el riesgo de cumplimiento**

Video

VW Calidad

Aspectos más salientes

- ✓ **Incluye una guía orientativa y estándares éticos**
- ✓ **Requiere de clara separación de las 3 líneas de defensa**
- ✓ **Respuesta a una legislación punitiva respecto de las organizaciones**

Modelo de "tres líneas de defensa"

Primera línea: Controles en origen.

Segunda línea: Controles de supervisión área independiente.

Tercera línea: Controles Entity Level.

Modelo recomendado por diversas organizaciones internacionales (ISACA, FSA, COSO, IIA, Comité Basilea, etc.)

Debe contar con procedimientos adecuados sobre la base del día a día. Incluye supervisión, seguimiento y prueba de aseguramiento de adhesión y eficacia

Debe poseer metodología de monitoreo independiente y procedimientos de prueba. Apunta a identificar patrones, temáticas o tendencias que indican debilidad.

Auditoría Interna independiente que valida la eficacia y adhesión al Marco RCM en base a riesgos, en forma regular y con rotación de énfasis. Aplica al nivel 1 y 2.

COSO 2013

Componentes	Principios	Buenas Prácticas
Ambiente de Control	1. Demostrar compromiso con integridad y valores éticos 2. Ejercitar la supervisión de manera responsable 3. Establecer estructura, autoridad y responsabilidad 4. Demostrar compromiso por ser competente 5. Reforzar la responsabilidad	**Gobierno Corporativo**
Evaluación de Riesgos	6. Definir objetivos adecuados 7. Identificar y analizar riesgos 8. Evaluar el riesgo de fraude 9. Identificar y analizar cambios significativos	**Gestión Integral de Riesgos**
Actividades de Control	10. Seleccionar e Implementar actividades de control 11. Seleccionar e implementar controles generales sobre TI 12. Formalizar a través de políticas y procedimientos	**3 Líneas de Defensa**
Información y Comunicaciones	13. Usar información relevante 14. Comunicar internamente 15. Comunicar externamente	**Cumplimiento**
Actividades de supervisión	16. Desarrollar evaluaciones propias o separadas 17. Evaluar y Comunicar deficiencias	**Auditoría y Supervisión Continua**

Puntos de interés : 78

Nuevos Desafíos …

Mayor importancia de la Planificación Estratégica

Cambio de paradigma o segmentación de temáticas

Comprensión de riesgos inherentes. Identificación de controles claves y validación de su efectividad.

Enfocados en el negocio. Entrenados en nuevos riesgos (estratégico- tecnológicos – fraude – reputacional)

Mejor comunicación. Liderar. Consultoría. Alinear con inteligencia el esfuerzo del control

Vuelve a cuestionar el modelo de AI.

Cuento con recursos adecuados para sortear nuevos desafíos ?

Mirada holística y convergente

GIR - GC

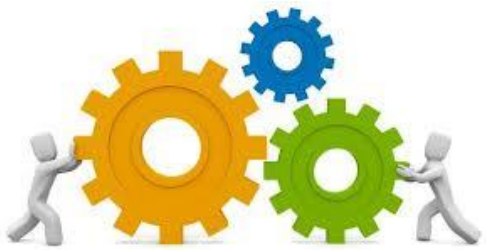
Video

Fraude IT

Desarrollo Tablero de Monitoreo del Comité

Por donde empiezo??

- Auditores conocedores del negocio, contexto y estrategia, así como de los riesgos claves y puntos críticos de control que los mitigan.



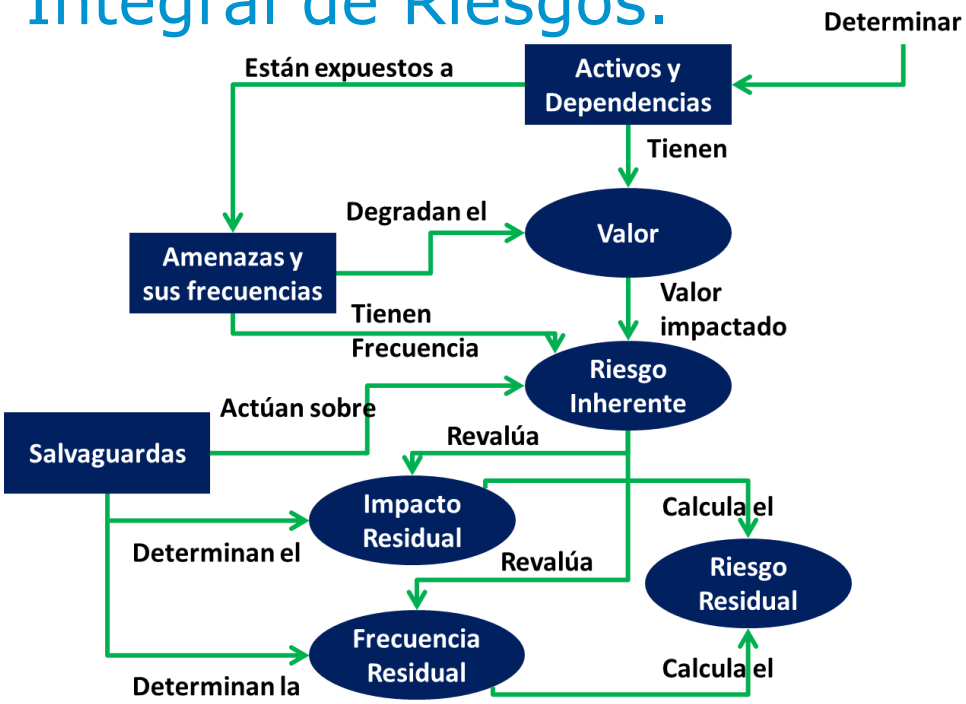
- Análisis de datos frecuentes y automatizados.
- Detecta anomalías con indicadores / tendencias / debilidades de control y riesgos emergentes.

- Implementación un sistema de auditoria continua:
  - ✓ Definir los Objetivos de la Auditoria, con acuerdo de la Dirección.
  - ✓ Uso y acceso a datos mediante herramientas de análisis.
  - ✓ Evaluación continua de riesgos, basada en matriz.
  - ✓ Evaluación con foco en Controles Claves.
  - ✓ Informar y gestionar resultados.
  - ✓ Generar Indicadores (propios o convergentes)
  - ✓ Ponderar e implementar Panel de Monitoreo

Hacia dónde vamos …

Continuar apoyando el desarrollo de una adecuada y efectiva Gestión Integral de Riesgos.

Monitorear la Gestión de riesgos, su interrelación con procesos de negocios y sus riesgos, evaluando el grado de adhesión al control.



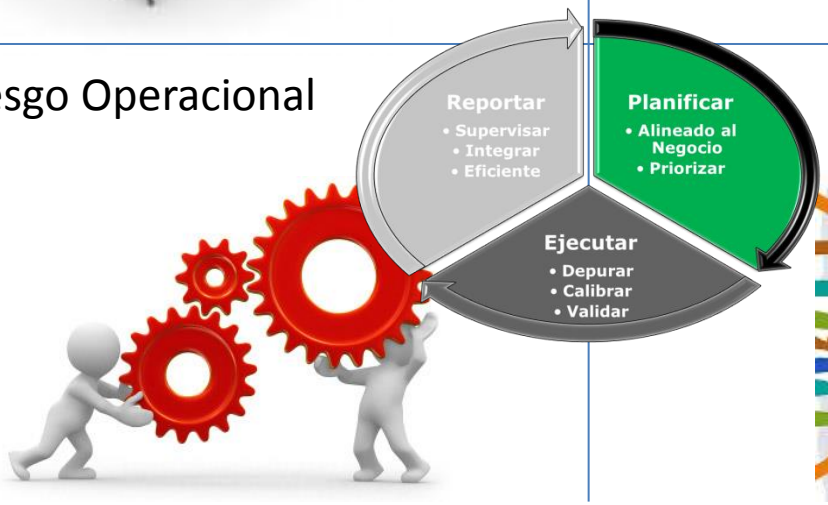
Validar que se dé tratamiento en Comité y/o Alta Dirección. Asegurar que los riesgos se gestionan y se retroalimenta el Plan de Continuidad del Negocio ….

Panel para Comité y/o Alta Dirección

Riesgo Estratégico

Riesgo Reputacional

Riesgo Operacional



Riesgo Cumplimiento

Mapa Riesgos Divisiones y Regiones

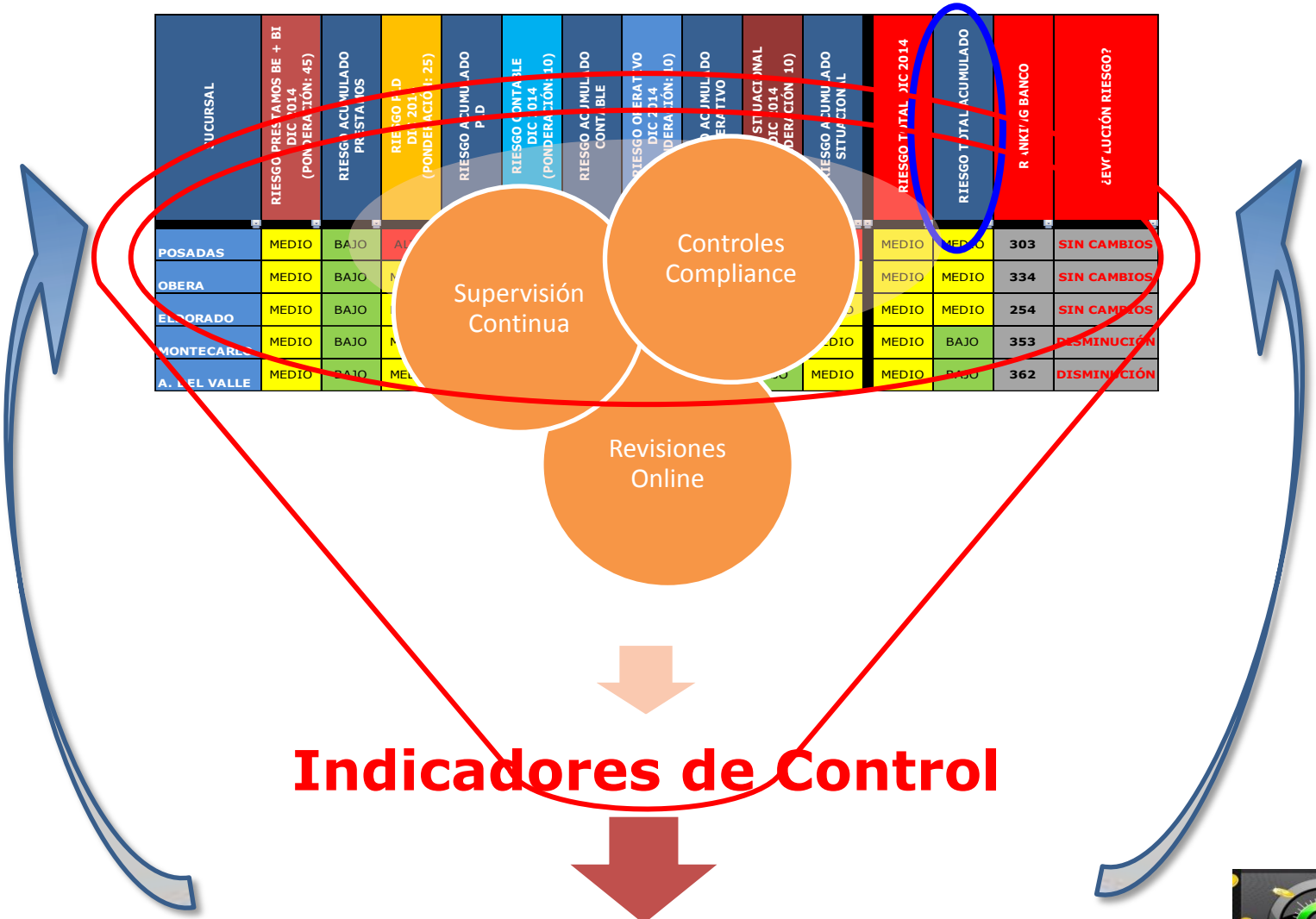
Diseño Modelo:

DIVISIÓN/REGIÓN	SUCURSALES CON RIESGO ACUMULADO ALTO Y MEDIO ALTO				SUCURSALES CON RIESGO ACUMULADO MEDIO				SUCURSALES CON RIESGO ACUMULADO MEDIO BAJO Y BAJO				TOTAL SUCURSALES
	CANT. SUC.	% SOBRE TOTAL SUC REGIÓN	RANKING BCO	EVOLUCIÓN CANTIDAD SUC A y MA	CANT. SUC.	% SOBRE TOTAL SUC REGIÓN	RANKING BCO	EVOLUCIÓN CANTIDAD SUC M	CANT. SUC.	% SOBRE TOTAL SUC REGIÓN	RANKING BCO	EVOLUCIÓN CANTIDAD SUC MB y B	
Metro Norte	1	7%	9	↓	6	43%	6	=	7	50%	7	↑	14
Metro Sur	3	14%	8	=	9	43%	6	↓	9	43%	9	↑	21
Microcentro	1	6%	10	↓	11	65%	1	↓	5	29%	11	↑	17
TOTAL AMBA	5	10%	6	↓	26	50%	2	↓	21	40%	6	↑	52
Salta	2	7%	9	↓	6	20%	11	↑	22	73%	4	↑	30
Total SALTA	2	7%	7	↓	6	20%	7	↑	22	73%	3	↑	30
Jujuy	0	0%	14	=	1	7%	14	=	14	93%	1	=	15
Total JUJUY	0	0%	9	=	1	7%	8	=	14	93%	1	=	15

Ranking Divisiones:

División	Tucumán	Oeste	Córdoba	Patagonia	Amba	Santa Fe	Pcia Bs As	Salta	Nea	Jujuy
% SUC A / MA	43%	40%	27%	20%	10%	9%	7%	7%	3%	0%

Gestión del Ambiente de Control



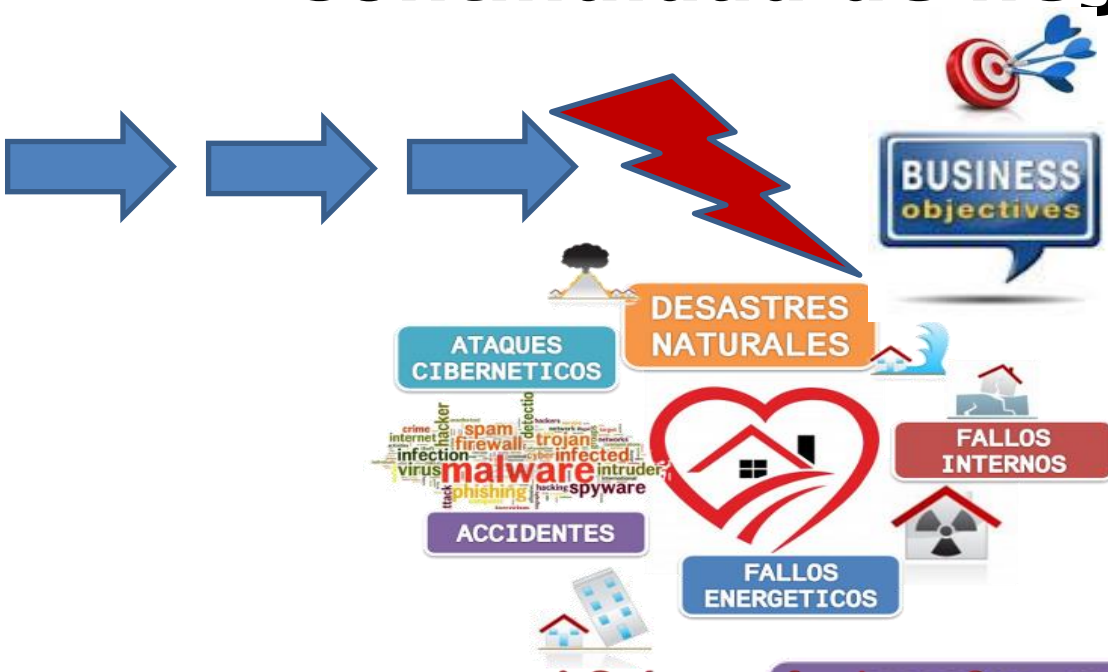
Gestión de la continuidad de negocio

Lo importante es estar preparados…

Pero cómo?

A través de un SISTEMA DE GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

Continuidad de negocio ??...



¿A Qué nos enfrentamos?

TENDENCIA NATURAL A MINIMIZAR LOS RIESGOS

DESPUES DE UN INCIDENTE CRITICO

EL PERSONAL CLAVE NO ESTABA DISPONIBLE

EL 50% DE LAS EMPRESAS SUSPENDIERON SUS OPERACIONES

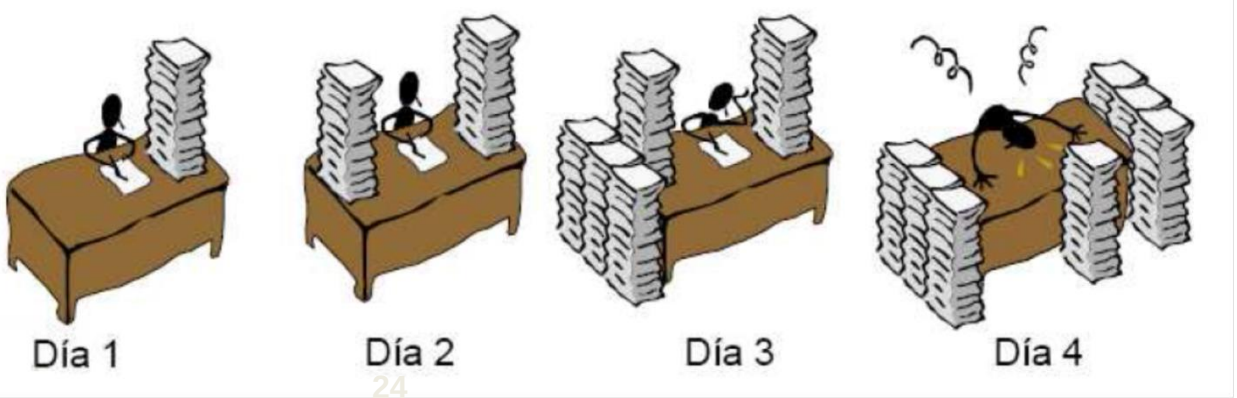
EL 10% RESTANTE CERRO SUS PUERTAS ANTES DE 2 AÑOS

Continuidad de negocio vs Continuidad de procesamiento

Objetivo de punto de recuperación — **RPO**

Tiempo objetivo de recuperación — **RTO**

4-24 horas	1-4 horas	0-1hora	0-1hora	1-4 horas	4-24 horas
▪ Copias de respaldo en cinta ▪ Envío de registros	▪ Copias de respaldo basadas en disco ▪ Imágenes instantáneas ▪ Replicación con demora ▪ Envío de registros	▪ Replicación de datos en espejo (mirroring)	▪ Clustering activo-activo	▪ Clustering activo-pasivo ▪ Hot standby	▪ Cold standby



AUDITORIA CONTINUA

Ejemplo de Tableros … Combina riesgo y Debilidades

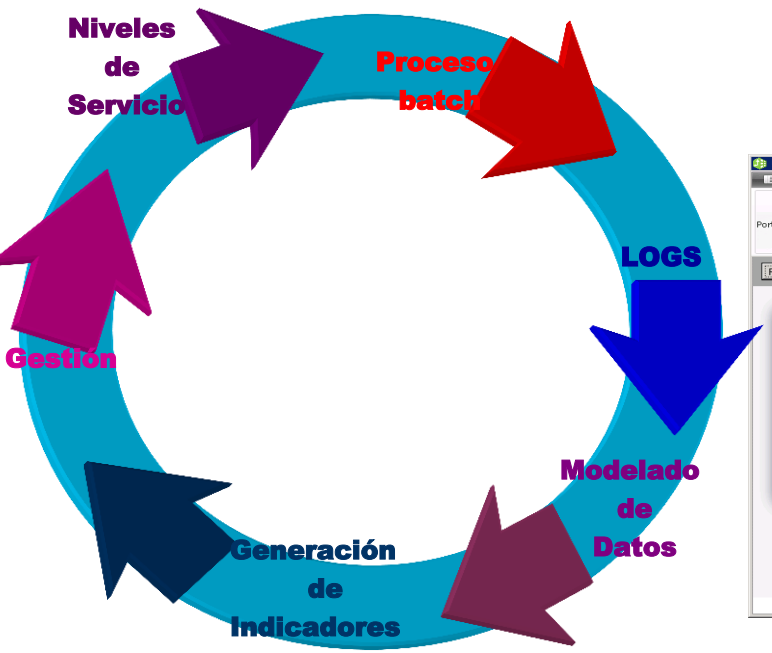
Satisfactorio	90% ≤ **AC** ≤ 100%
Aceptable	70% ≤ **AC** < 90%
Ajustado	40% ≤ **AC** < 70%
Sujeto a Mejora	15% ≤ **AC** < 40%
Insatisfactorio	0% ≤ **AC** < 15%

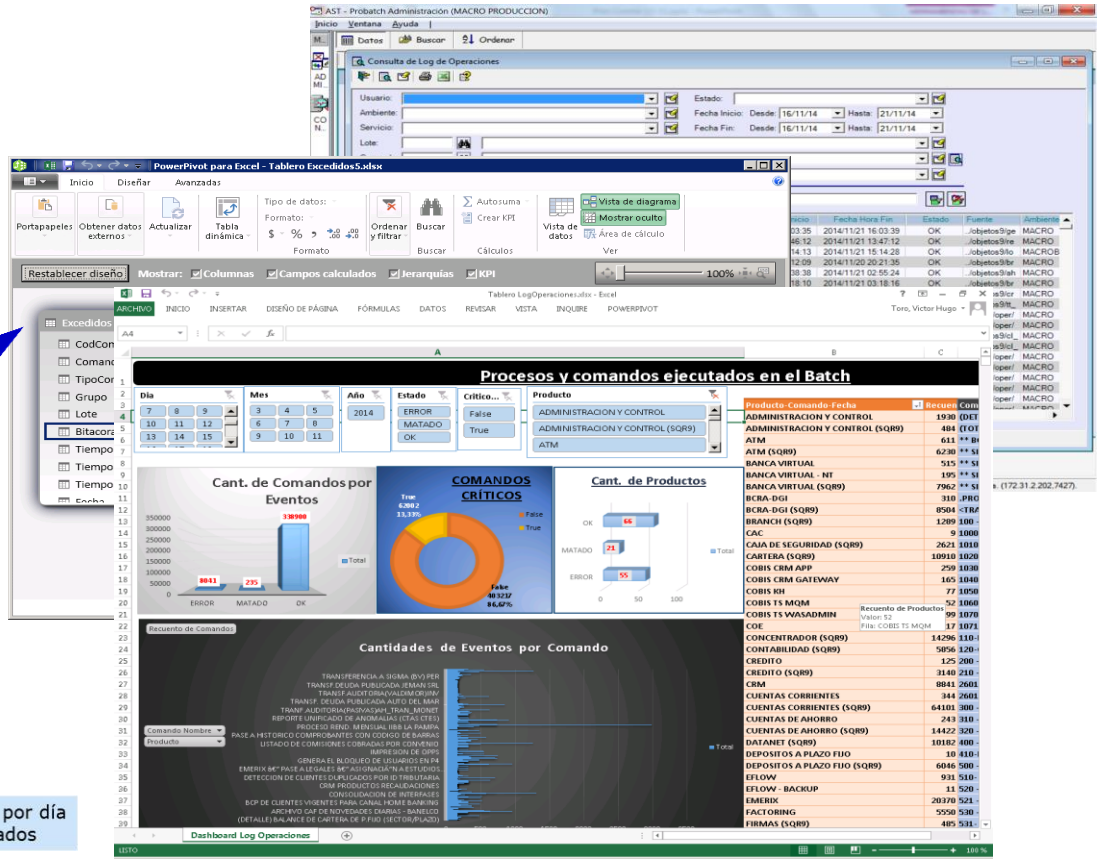
Riesgo Residual
[RI + (1-AC)] / 2

AMBIENTE DE CONTROL	RIESGO INHERENTE		
	Bajo	Medio	Alto
Satisfactorio			
Aceptable			
Ajustado			
Sujeto a Mejora			
Insatisfactorio			

Aproximaciones

Tableros en base a AUDITORIA CONTINUA





- ✓ Enfoque compartido con Alta Gerencia .
- ✓ Diseño dinámico = reportes + ágiles.
- ✓ Resolución de errores/cancelaciones claves.

- ✓ Disminución de tiempos excedidos.
- ✓ Tiempo de procesamiento (Ventana Horaria)

Resumiendo ….

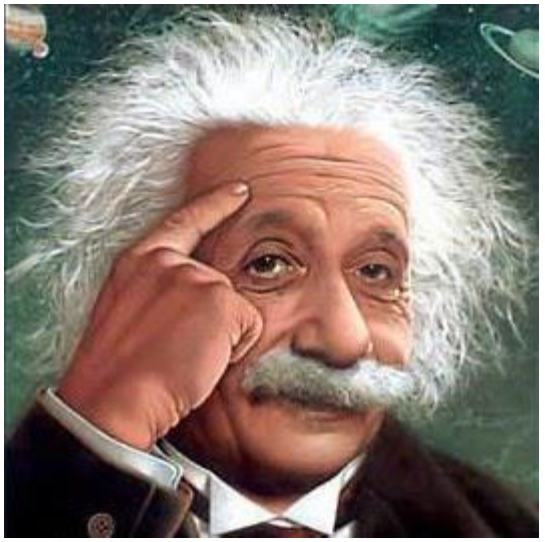
1. Conocer profundamente el Negocio; las normas que lo regulan y las buenas prácticas.
2. Contar con el Mapa de riesgos y controles convalidado por sus dueños
3. Generar una planificación convergente, alineada con los objetivos de la organización y basada en riesgos críticos y controles claves
4. Seleccionar indicadores que permitan medir el Ambiente de Control, alineados al Plan estratégico. Generar Panel de Medición vs. Objetivo Comercial
5. Recolectar, evaluar eventos, debilidades y repensar el mapa de Riesgos y Controles, revisar la eficacia de las pruebas de contingencia,

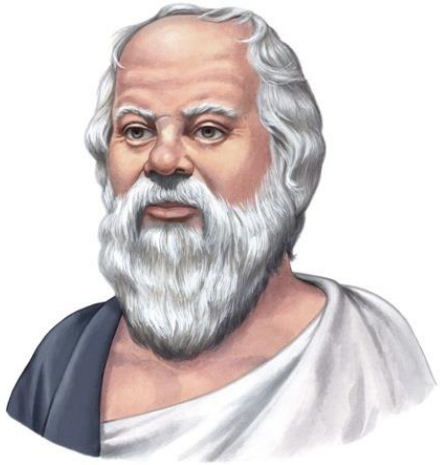
Conclusiones

- ✓ **Alta Dirección involucrada**
- ✓ **Contar con herramientas y recursos suficientes**
- ✓ **Converger y complementar, con independencia las 3 líneas de control**
- ✓ **Debatir y acordar la visión de control interno con socios estratégicos**
- ✓ **Generar espacios complementarios que garantice el Buen Gobierno Corporativo**
- ✓ **Diseñar Mapas de Aseguramiento y Evaluar la eficiencia de los controles**
- ✓ **Distinguir con claridad las Tres líneas de control**
- ✓ **Delinear Programas para fortalecer la Cultura “Ética, honestidad, integridad”**
- ✓ **Generar Valor. Transparencia / Mayor regulación**
- ✓ **Aportar un Tablero /Panel que permita medir la eficiencia del Control**

“Los problemas que tenemos no pueden ser resueltos pensando de la misma manera en que pensamos cuando los creamos”

Albert Einstein





“No puedo enseñar nada a nadie.
Sólo puedo hacerlos pensar”
Sócrates

Video

AS 6 Claves

Muchas Gracias !!!!!

Carmen Esther Estévez

carmenestevez@macro.com.ar