Auditoría Continua:
Mejores Prácticas y Caso Real

Julio R. Jolly Moore – *Socio*, BDO

&

Gerardo Alcarraz – *Coordinador de Auditoría Informática*, Banco de la República Oriental de Uruguay

CLAIN 2010

Congreso Latinoamericano de Auditoría Interna y Evaluación de Riesgos

Ciudad de Panamá

Mayo 2010

Agenda

Auditoría Continua: Mejores Prácticas y Caso Real

- Introducción
- Antecedentes de Auditoría Continua
- Definiciones - ¿Qué es Auditoría Continua?
- Nuevo Enfoque de Auditoría Interna
- Pasos para aplicar Auditoría Continua
- Cobit dentro del proceso de Auditoría Continua
- Caso Práctico
- Conclusiones

INTRODUCCIÓN

Auditoría Continua: Mejores Prácticas y Caso Real

ANTECEDENTES

Auditoría Continua: Mejores Prácticas y Caso Real

Antecedentes

- El proceso de “auditoría continua” surgió alrededor de 1989 mediante los esfuerzos de Vasarhelyi y Halper para medir y analizar el proceso de facturación en la empresa internacional AT&T.
- Se enforon al proceso de auditar extensas bases de datos, para establecer estándares y comparar las operaciones contra los mismos y emitir alarmas cuando sea necesario.

Fuente: Vasarhelyi, M.A. and Halper, F. B., 1991, The Continuous Audit of Online Systems, Auditing: A Journal of Practice and Theory

Antecedentes

- Algunas organizaciones y entidades que han identificado Auditoría Continua como una tendencia de alto beneficio:
  - American Institute of Certified Public Accountants (AICPA) - http://www.aicpa.org/
  - Canadian Institute of Chartered Accountants (AICPA/CICA) http://www.cica.ca/
  - Instituto de Auditores Internos (http://www.theiia.org)

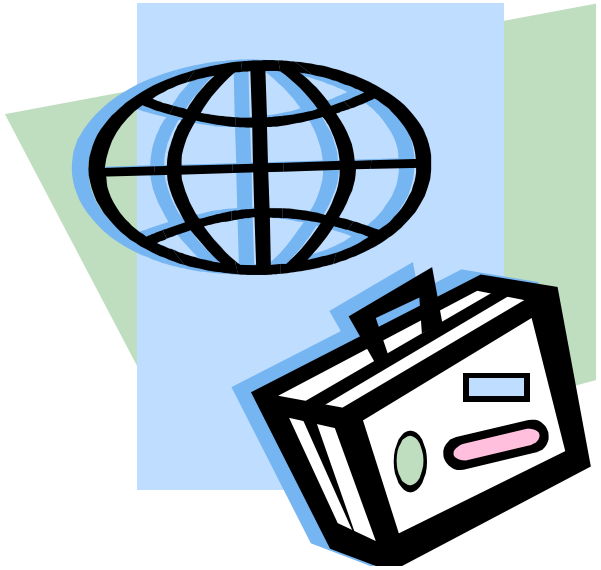
DEFINICIONES

Auditoría Continua: Mejores Prácticas y Caso Real

Definiciones

- “Método automatizado utilizado para realizar evaluaciones de controles y riesgos con mayor frecuencia”

Global Technology Audit Guide (GTAG) Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment,



Definiciones

- “Es un proceso o metodología que habilita a un auditor independiente a proporcionar aseguramiento formal sobre un tema, utilizando una serie de reportes de auditoría emitidos simultáneamente, o poco después, de la ocurrencia de un evento relacionado con dicho tema”

Continuous Auditing: An Operational Model for Internal Auditors – Mohammed Abdolmohammadi y Ahmad Sharbatouglie.

Definiciones

- Auditoría Continua **NO ES** …
- ***Monitoreo Continuo*** – Es una actividad que es responsabilidad de la Alta Dirección, dedicado a asegurar el funcionamiento de los procesos de negocio de acuerdo a sus políticas internas.

Definiciones

- Auditoría Continua **NO ES** …
- ***Aseguramiento Continuo*** – Es un conjunto de los trabajos de Auditoría Interna, en combinación con el monitoreo continuo de la Alta Dirección.

NUEVO ENFOQUE DE AUDITORÍA

Auditoría Continua: Mejores Prácticas y Caso Real

Evolución

ETAPAS	ENFOQUE TRADICIONAL	ENFOQUE AUDITORÍA CONTINUA
Planeación	Establecer el objetivo y alcance de la auditoría	**Establecer el objetivo y alcance de la auditoría**, *e identificar fuentes de datos, describir los atributos de la información y establecer formatos del análisis e informes.*
Trabajo en Campo	Realizar pruebas y documentar resultados.	Obtener y **realizar pruebas** a los datos identificados durante la planeación según la frecuencia deseada. Investigar, dar seguimiento a cualquier excepción y **documentar resultados**.
Informes	Discutir resultados y presentar informe luego de finalizar la auditoría.	Identificar las razones de las diferencias, dar prioridad a los hallazgos y **presentar un informe con los resultados** y recomendaciones de manera *continua*

Evolución

EFECTIVIDAD DE LOS CONTROLES

- Enfoque tradicional
  - Se asume que la efectividad de los controles aumenta después de los resultados y recomendaciones de cada auditoría.
  - Sin embargo, reduce con el pasar del tiempo hasta los resultados de la siguiente auditoría.

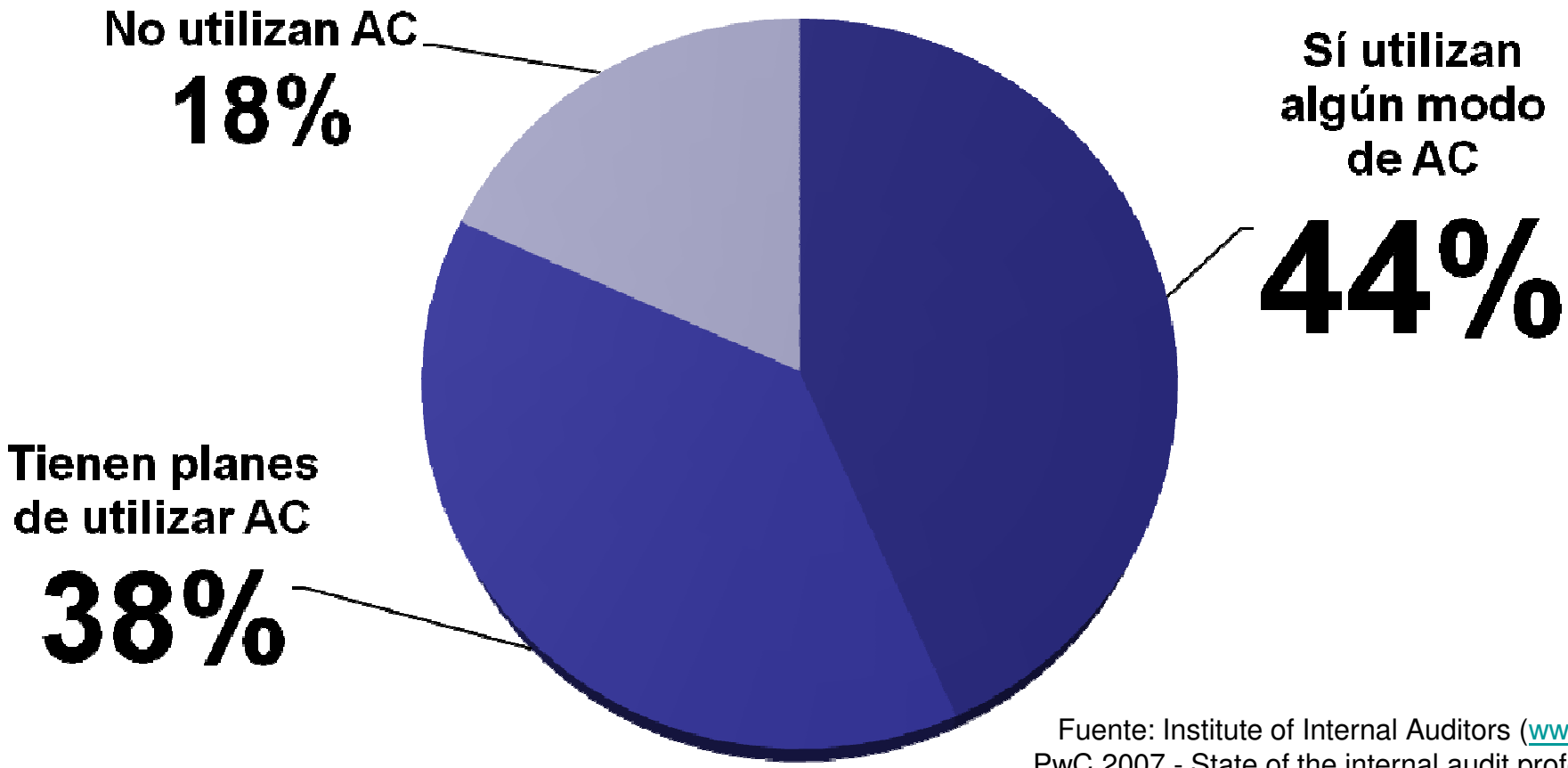
Evolución

EFECTIVIDAD DE LOS CONTROLES

- Enfoque Auditoría Continua
  - La efectividad de los controles se mantiene a niveles aceptables dado que se están probando de manera continua y reportando los resultados con la ocurrencia de un evento o poco después del mismo.

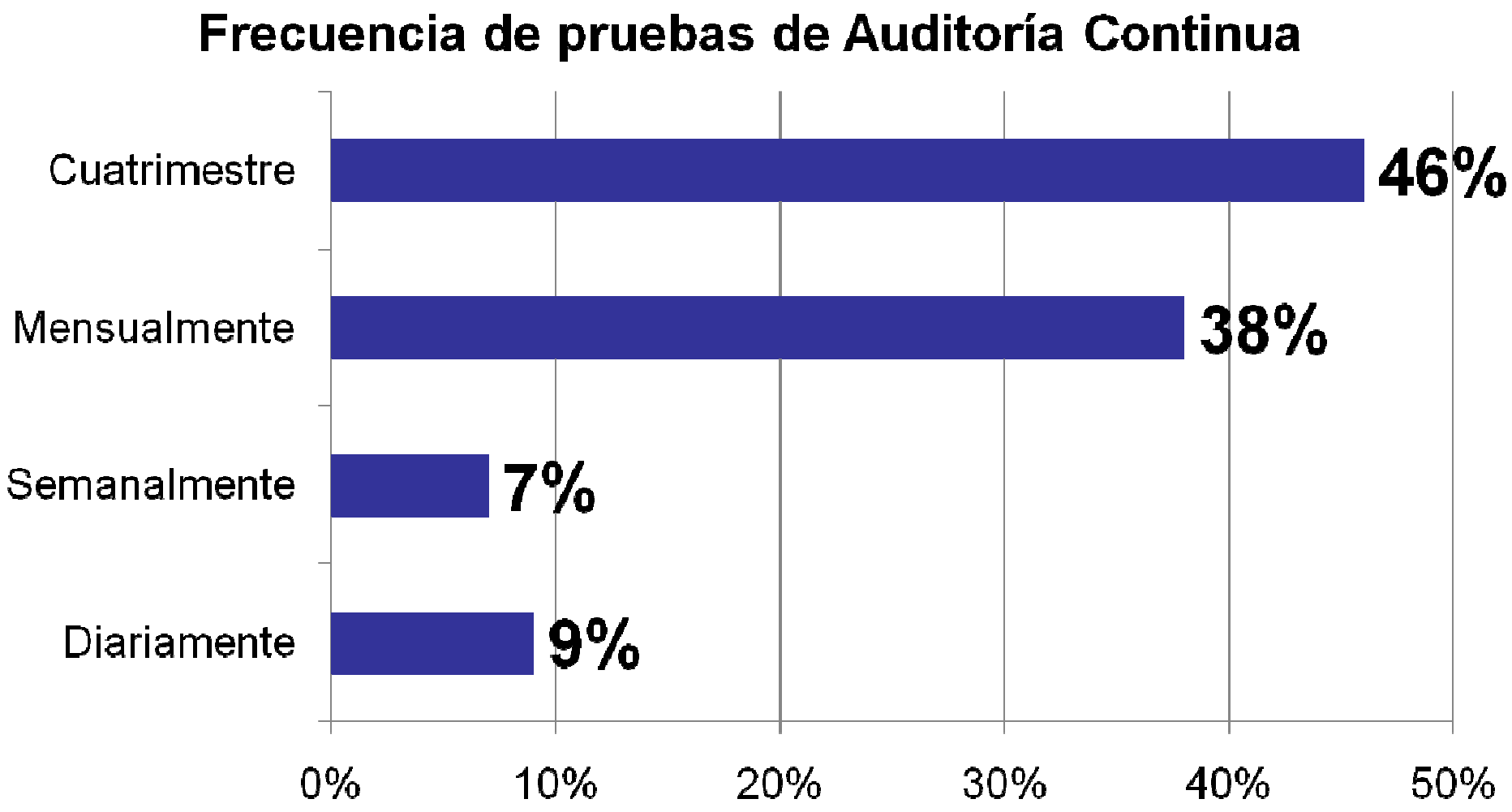
Auditoría Continua

Utiliza algún método de Auditoría Continua en sus operaciones de auditoría?



Fuente: Institute of Internal Auditors (www.theiia.org)
PwC 2007 - State of the internal audit profession study

Auditoría Continua



Fuente: Institute of Internal Auditors (www.theiia.org)
PwC 2007 - State of the internal audit profession study

PASOS DE IMPLEMENTACION

Auditoría Continua: Mejores Prácticas y Caso Real

Pasos de implementación

Entendimiento del Negocio | Identificar Riesgos y Controles | Planificación de la Auditoría | Ejecución de la Auditoría Continua | Evaluar Resultados y Emitir Reporte

ENTENDIMIENTO DEL NEGOCIO

Actividades

- Conocer la Estructura Organizacional y ubicaciones importantes
- Evaluar los planes estratégicos vigentes
- Identificar y comprender las unidades de negocio y/o procesos críticos
- Evaluar el entorno de Tecnología de Información que soporta los unidades de negocio y/o procesos críticos

Pasos de implementación

Entendimiento del Negocio | **Identificar Riesgos y Controles** | Planificación de la Auditoría | Ejecución de la Auditoría Continua | Evaluar Resultados y Emitir Reporte

IDENTIFICAR RIESGOS Y CONTROLES

Actividades

- Seleccionar las unidades de negocio y/o procesos críticos que deben evaluarse
- Revisar métricas de riesgo y categorización
- Revisar los controles claves existentes para mitigar los riesgos significativos
- Seleccionar riesgos y controles a ser considerados en el proceso de Auditoría Continua

Ejemplo – Categoría de Riesgos

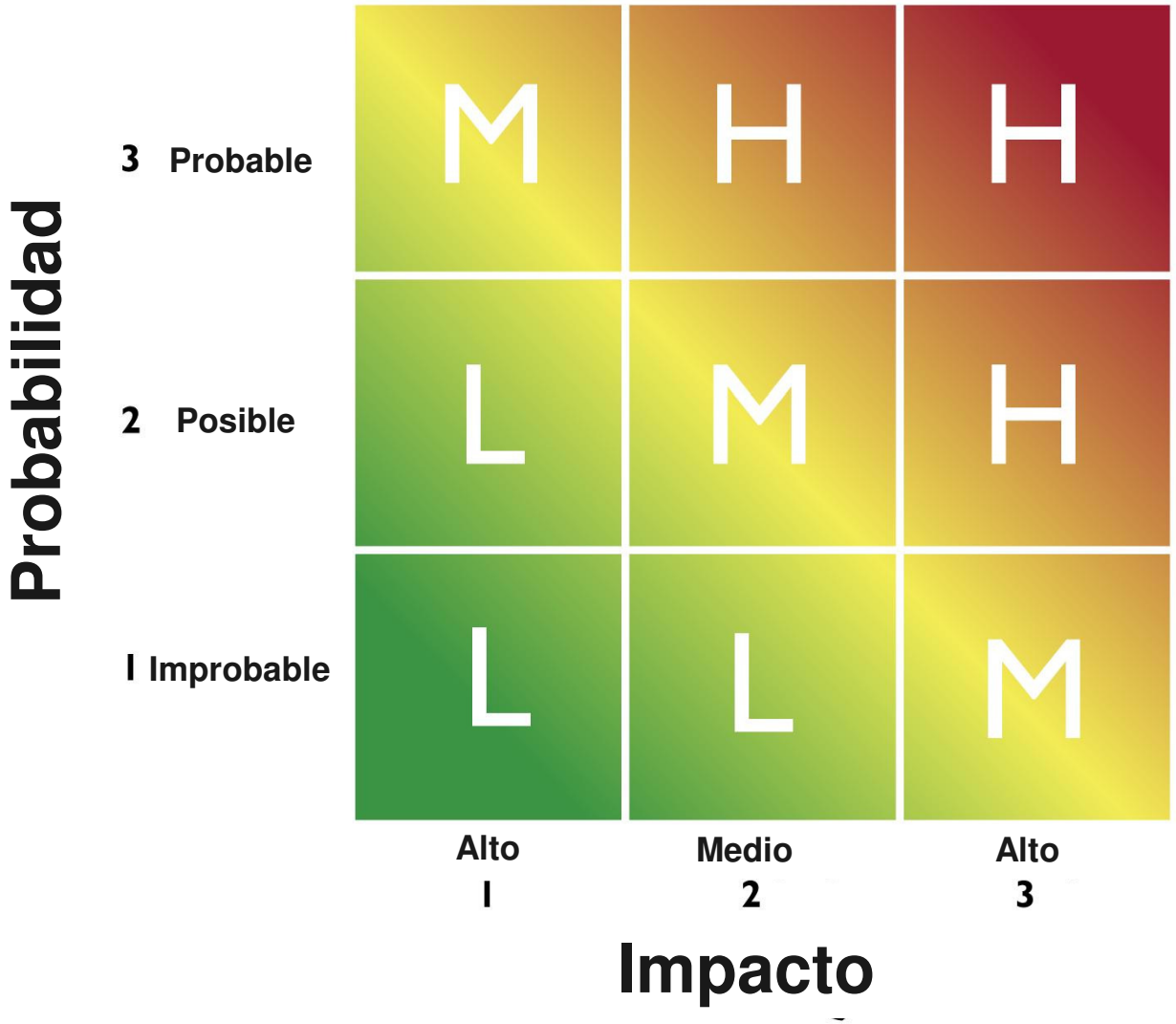
Ejemplos de consideraciones de métricas y categorización de riesgos

Estratégico	**Operativo**	**Cumplimiento**	**Financieros**
Riesgos relacionados con la implementación de estrategias de negocio equivocadas.	Riesgos relacionados a la operación diaria del negocio.	Riesgos relacionados a violar legislaciones relevantes y obligaciones contractuales.	Riesgos relacionados a gestionar, controlar y reportar riesgos financieros.

Ejemplo – Priorizar riesgos

Alta	Los riesgos en esta categoría son significantes en consecuencias y amenazan la habilidad de la organización para cumplir sus objetivos estratégicos y son de alta probabilidad de ocurrencia.
Medio	Los riesgos en esta categoría pueden tener altas consecuencias pero son menos probables de que ocurran. Alternativamente, pueden tener bajas consecuencias pero con más probabilidad de ocurrencia.
Bajo	El riesgo en esta categoría tendrá consecuencias limitadas para que la organización cumpla sus objetivos estratégicos y son poco probables de que ocurran.

Ejemplo – Mapa de Riesgos



Escala de Categorización

Impacto:
El impacto a las operaciones del negocio y la habilidad de cumplir con los objetivos estratégicos.

Probabilidad:
Posibilidad de que el evento ocurra en 1 a 3 años

Ejemplo – Escala de categorización

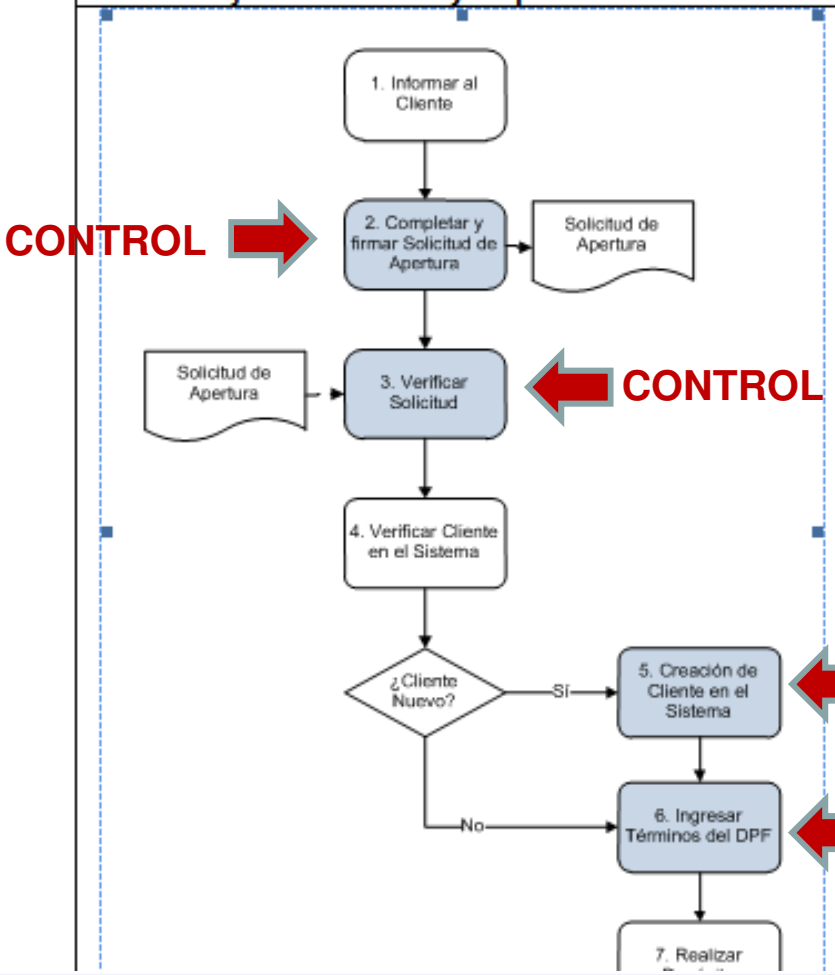
Impacto El impacto a las operaciones del negocio y su habilidad para cumplir objetivos estratégicos.	
Bajo	Bajo impacto a las operaciones y la habilidad para cumplir con los objetivos estratégicos.
Moderado	Impacto considerable a las operaciones y la habilidad para cumplir con los objetivos estratégicos.
Alto	Alto impacto a las operaciones y la habilidad para cumplir con los objetivos estratégicos.
Probabilidad Posibilidad de que el evento ocurra en los siguientes 1 a 3 años	
Baja	Baja probabilidad de que ocurra en los siguientes 1 - 3 años.
Media	Probabilidad media de que ocurra en los siguientes 1 - 3 años.
Alta	Alta probabilidad de que ocurra en los siguientes 1 - 3 años.

Ejemplo – Narrativas y Diagramas de Proceso

Proceso: Apertura de Cuenta

Diagramas de Flujo y Narrativas

Flujo de Procesos y Mapa de Controles



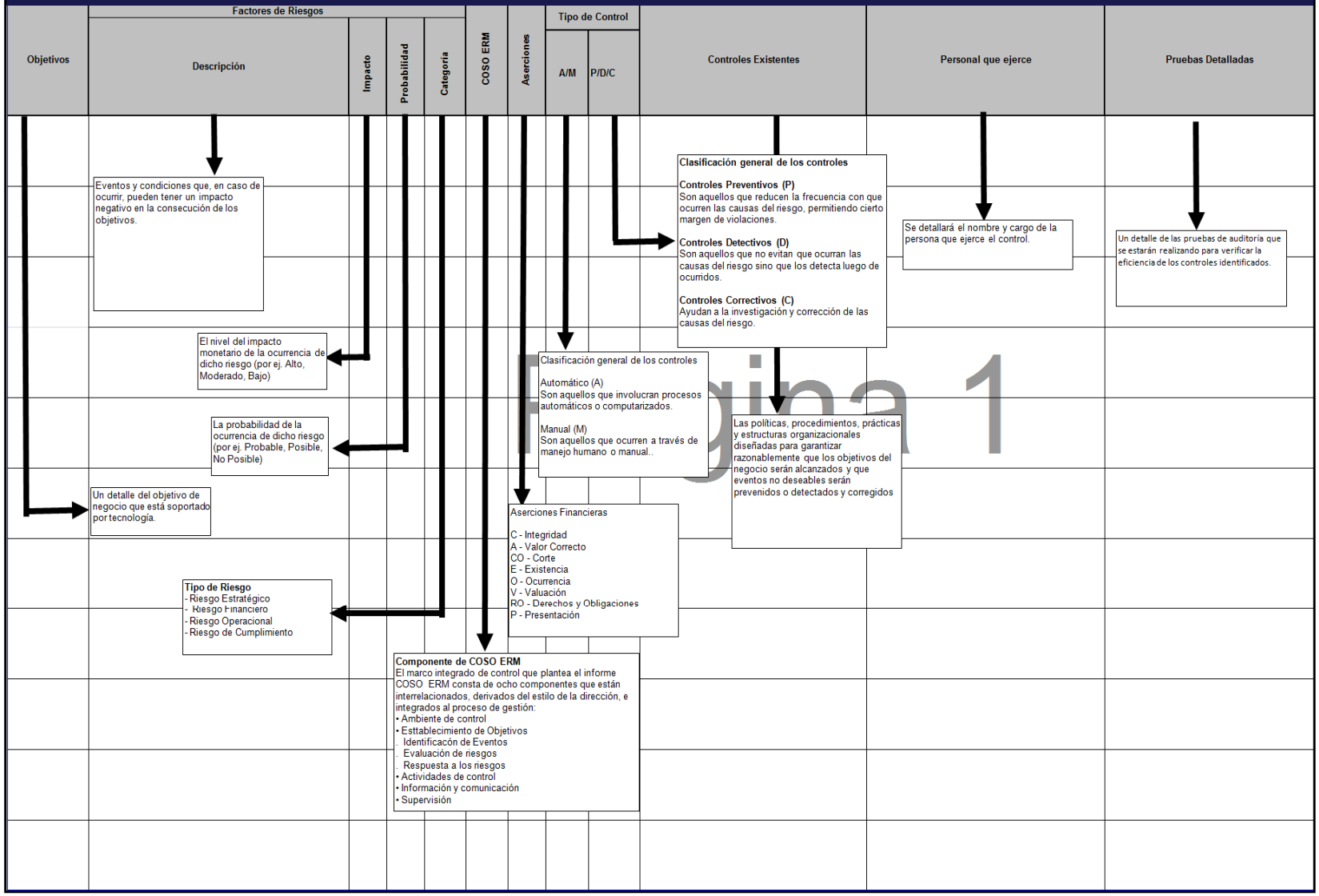
Descripción

1. **Informar al Cliente:** El oficial orienta al interesado sobre los beneficios y le explica sobre los documentos requeridos.
2. **Completar Solicitud de Apertura:** El cliente completa la solicitud de apertura y entrega la información requerida de acuerdo al listado de requisitos.
3. **Verificar Solicitud:** La Gerente de recibe la solicitud de apertura y verifica que la misma cumpla con todos los requisitos y documentación de respaldo.
4. **Verificar Cliente en el Sistema:** El oficial verifica si el interesado existe en el sistema.
5. **Creación de Cliente en el Sistema:** Si el cliente no existe en el sistema, el oficial lo ingresa colocando toda la información y datos referente a la apertura.
6. **Ingresar Términos:** El oficial apertura la cuenta de ahorro a plazo fijo de acuerdo a término y condiciones establecidas.
7. **Realizar Depósito:** En caso de los Ahorro a Plazo Fijo se envía al cliente a depositar a la caja. Si el depósito es mayor a B/

Ejemplo

Modelo General de Matriz de Riesgos y Controles

Modelo General de Matriz de Riesgos y Controles



Pasos de implementación

Entendimiento del Negocio | Identificar Riesgos y Controles | **Planificación de la Auditoría** | Ejecución de la Auditoría Continua | Evaluar Resultados y Emitir Reporte

PLANIFICACIÓN DE LA AUDITORÍA CONTINUA

Actividades

- Determinar el nivel de automatización de los controles claves
- Identificar y comprender si los controles claves están basados en datos de los Sistemas de Información (SI)
- Conocer y comprender las fuentes de datos de los SI
- Evaluar las herramientas y competencias del personal de Auditoría Interna para realizar las pruebas de Auditoría Continua
- Definir los objetivos de la Auditoría Continua
- Obtener la aprobación del Comité de Auditoría, Alta Dirección y/o Junta Directiva

Pasos de implementación

Entendimiento del Negocio | Identificar Riesgos y Controles | **Planificación de la Auditoría** | Ejecución de la Auditoría Continua | Evaluar Resultados y Emitir Reporte

PLANIFICACIÓN DE LA AUDITORÍA CONTINUA - *Continuación*

Actividades

- Determinar el nivel en que la Administración ha implementado monitoreo continuo
- Considerar el área de Tecnología de la Información (TI) durante todo el proceso
- Determinar el alcance y nivel de frecuencia de las pruebas
- Establecer fuentes de información para realizar las pruebas
- Asegurar tener los accesos requeridos a dichas fuentes de información
- Determinar confiabilidad de los datos

Pasos de implementación

Entendimiento del Negocio | Identificar Riesgos y Controles | Planificación de la Auditoría | **Ejecución de la Auditoría Continua** | Evaluar Resultados y Emitir Reporte

EJECUCIÓN DE LA AUDITORÍA CONTINUA

Actividades

- Realizar pruebas sobre los controles identificados
- Identificar desviaciones o deficiencias en los controles identificados
- Investigar las razones de las deficiencias identificadas

Pasos de implementación

Entendimiento del Negocio | Identificar Riesgos y Controles | Planificación de la Auditoría | Diseño de la Auditoría Continua | **Evaluar Resultados y Emitir Reporte**

EVALUAR RESULTADOS Y EMITIR REPORTES

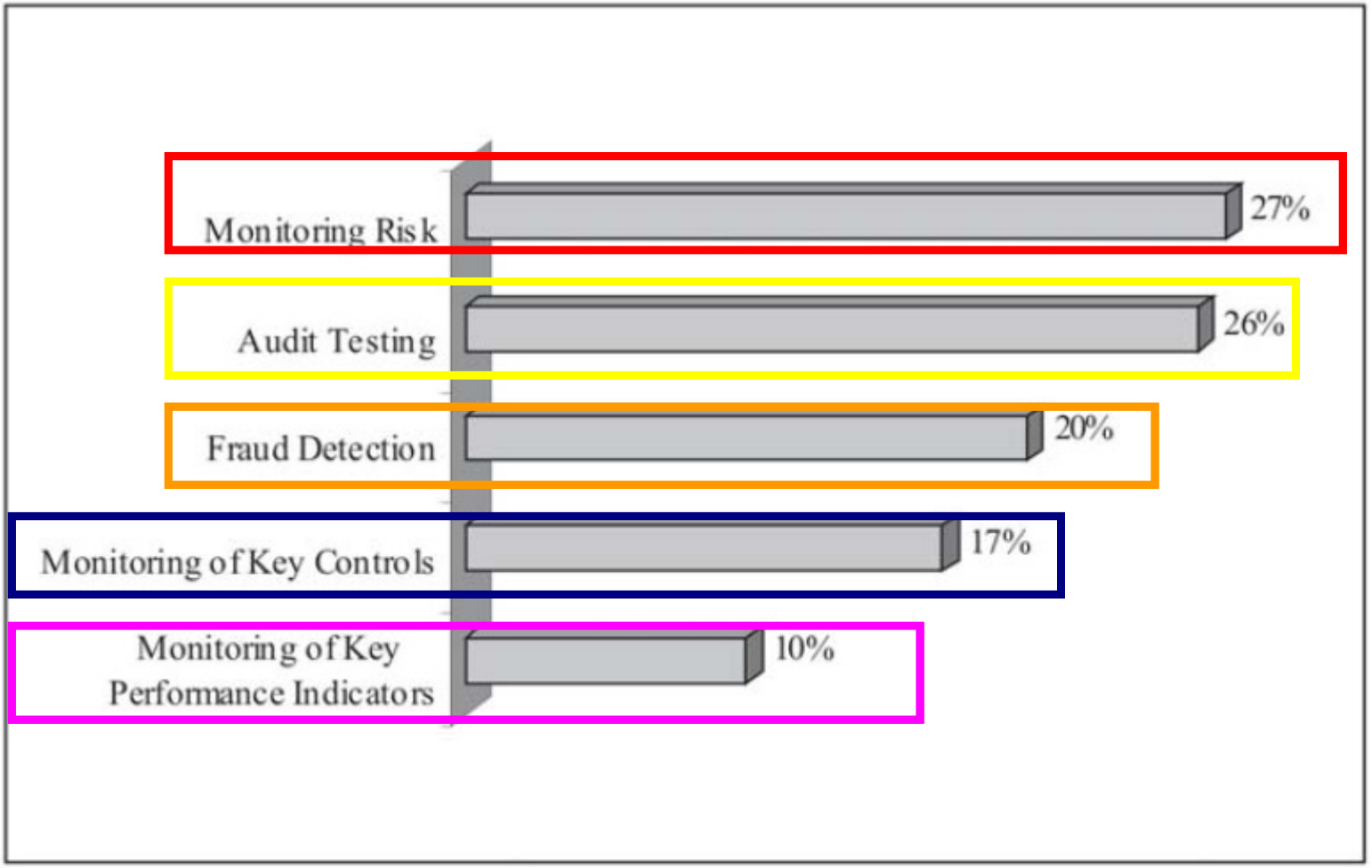
Actividades

- Establecer niveles de prioridad sobre los resultados
- Preparar recomendaciones y emitir informes
- Re-evaluar y actualizar (de ser necesario) el diseño de las pruebas de Auditoría Continua

COBIT EN EL PROCESO DE AUDITORÍA CONTINUA

Auditoría Continua: Mejores Prácticas y Caso Real

Lo que nos preocupa en Auditoría Continua…



Graph 1 – Continuous auditing and monitoring uses

Source: 2006 State of the Internal Audit Profession Study, PricewaterhouseCoopers.

En el mundo de TI …COBIT

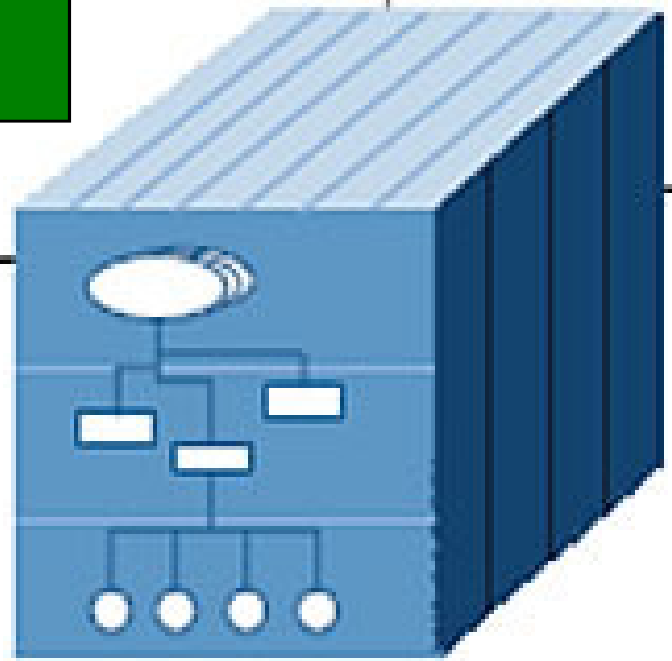
- **Algunas cuestiones…**
  - ¿Podemos identificar riesgos por medio de COBIT?
  - ¿Tenemos forma de monitorearlos?
  - ¿Podemos identificar controles clave?
  - ¿Podemos diseñar pruebas de auditoria?
  - ¿Podemos detectar fraudes?
  - ¿Podemos monitorear indicadores de desempeño?

COBIT ES UNA GRAN CAJA DE SORPRESAS

COBIT

REQUERIMIENTOS DEL NEGOCIO

CRITERIOS DE INFORMACION
EFECTIVIDAD
EFICIENCIA
CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD
CUMPLIMIENTO
CONFIABILIDAD



PROCESOS DE TI
DOMINIOS
PROCESOS
ACTIVIDADES

RECURSOS DE TI
PERSONAS
APLICACIONES
INFRAESTRUCTURA
INFORMACION

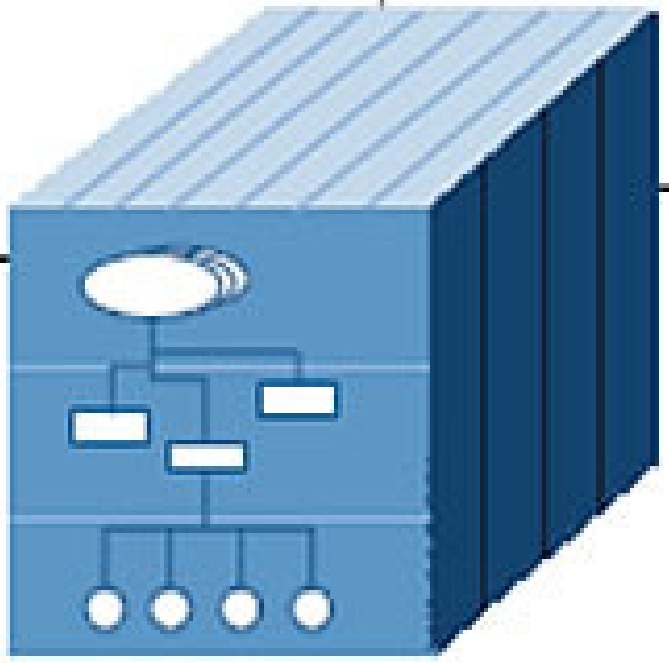
COBIT

REQUERIMIENTOS DEL NEGOCIO

CRITERIOS DE INFORMACION
EFECTIVIDAD
EFICIENCIA
CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD
CUMPLIMIENTO
CONFIABILIDAD

RIESGOS DE NEGOCIO

PROCESOS DE TI
DOMINIOS
PROCESOS
ACTIVIDADES



RECURSOS DE TI
PERSONAS
APLICACIONES
INFRAESTRUCTURA
INFORMACION

Enfoque de Riesgo en TI

Pasaje de requerimientos de Información a enfoque de riesgos

CRITERIO	DEFINICION COBIT
EFECTIVIDAD EFICIENCIA	La información sea relevante y pertinente a los procesos del negocio, y se brinde de una manera oportuna, correcta, consistente y utilizable, optimizando los recursos.
CONFIDENCIALIDAD	Protección de información sensitiva contra revelación no autorizada
INTEGRIDAD	La precisión y completitud de la información, así como con su validez
DISPONIBILIDAD	La información esté disponible cuando sea requerida por los procesos del negocio
CUMPLIMIENTO	Cumplir leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios
CONFIABILIDAD	Brindar información apropiada para que la gerencia administre la entidad y ejercite responsabilidades fiduciarias y de gobierno

Pasaje de requerimientos de Información a enfoque de riesgos

CRITERIO	DEFINICION COBIT	DEFINICION RIESGO
EFECTIVIDAD EFICIENCIA	La información sea relevante y pertinente a los procesos del negocio, y se brinde de una manera oportuna, correcta, consistente y utilizable, optimizando los recursos.	La Tecnología de Información no cubre las expectativas de Negocio en términos de Efectividad y Eficiencia
CONFIDENCIALIDAD	Protección de información sensitiva contra revelación no autorizada	La información contenida en los Sistemas puede ser accedida por personas no autorizadas
INTEGRIDAD	La precisión y completitud de la información, así como con su validez	La información contenida en los Sistemas puede ser modificada o alterada sin autorización
DISPONIBILIDAD	La información esté disponible cuando sea requerida por los procesos del negocio	No se dispone de los Sistemas de información o Infraestructura para operar adecuadamente los Procesos de Negocio
CUMPLIMIENTO	Cumplir leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios	Incumplimiento de Leyes, Regulaciones y Contratos
CONFIABILIDAD	Brindar información apropiada para que la gerencia administre la entidad y ejercite responsabilidades fiduciarias y de gobierno	La información suministrada no es apropiada y la Gerencia no puede asumir las responsabilidades fiduciarias y de gobierno.

Una metodología usando COBIT

IDENTIFICAR RIESGOS DE NEGOCIO

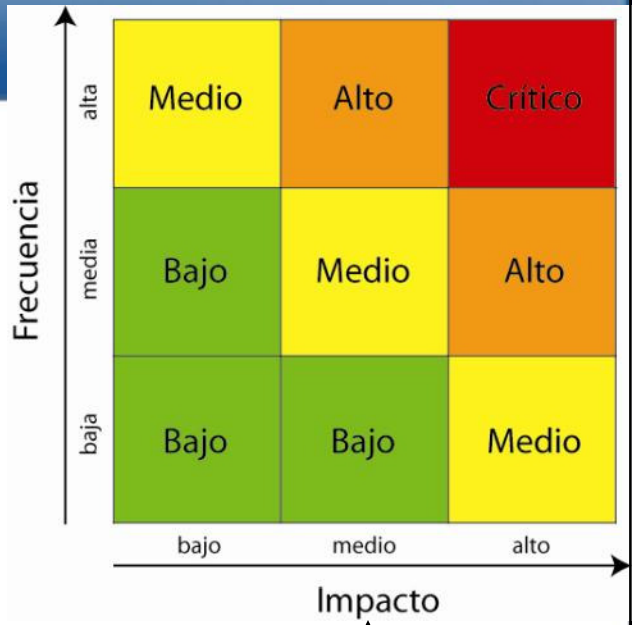
PRIORIZAR RIESGOS DE NEGOCIO

IDENTIFICAR PROCESOS DE TI

IDENTIFICAR RIESGOS DE PROCESOS DE TI

VALORACION Y EVALUACION DE CONTROLES

MATRIZ DE RIESGOS



Identificar los riesgos de negocio

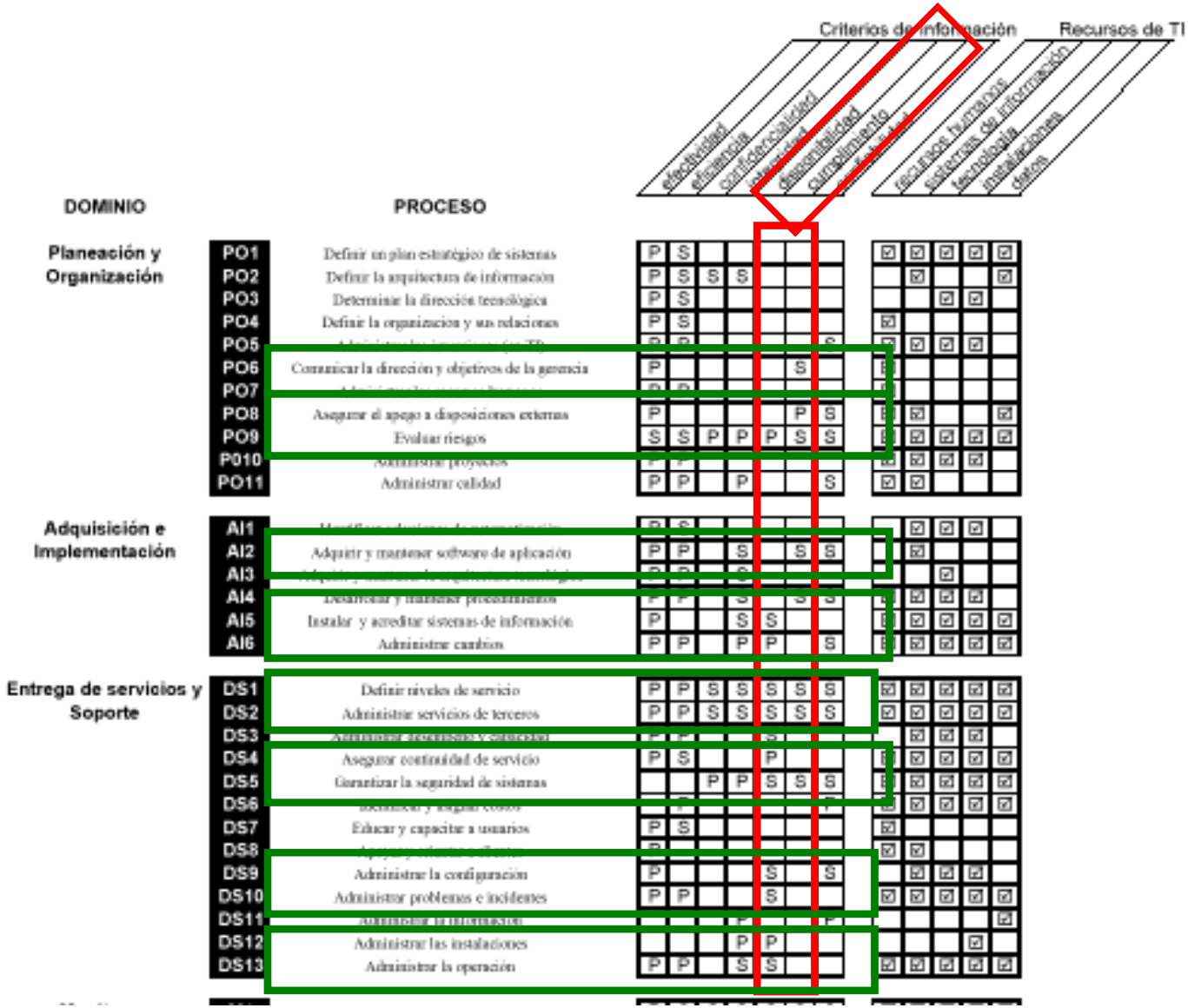
EFICIENCIA - EFICACIA	La Tecnología de Información no cubre las expectativas de Negocio en términos de Efectividad y Eficiencia
CONFIDENCIALIDAD	La información contenida en los Sistemas puede ser accedida por personas no autorizadas
INTEGRIDAD	La información contenida en los Sistemas puede ser modificada o alterada sin autorización
DISPONIBILIDAD	No se dispone de los Sistemas de información o Infraestructura para operar adecuadamente los Procesos de Negocio
CUMPLIMIENTO	Incumplimiento de Leyes, Regulaciones y Contratos
CONFIABILIDAD	La información suministrada por los Sistemas no es apropiada y la Gerencia no puede asumir las responsabilidades de gobierno

Priorizar los riesgos de negocio

DISPONIBILIDAD	No se dispone de los Sistemas de información o Infraestructura para operar adecuadamente los Procesos de Negocio
CUMPLIMIENTO	Incumplimiento de Leyes, Regulaciones y Contratos
INTEGRIDAD	La información contenida en los Sistemas puede ser modificada o alterada sin autorización
EFICIENCIA - EFICACIA	La Tecnología de Información no cubre las expectativas de Negocio en términos de Efectividad y Eficiencia
CONFIDENCIALIDAD	La información contenida en los Sistemas puede ser accedida por personas no autorizadas
CONFIABILIDAD	La información suministrada por los Sistemas no es apropiada y la Gerencia no puede asumir las responsabilidades de gobierno

Identifico los Procesos COBIT afectados

TABLA RESUMEN



Identifico los Procesos COBIT afectados

DISPONIBILIDAD	PROCESOS DE TI	CUMPLIMIENTO
	PO6 Comunicar las aspiraciones y la dirección de la gerencia	S
P	PO9 Evaluar y administrar los riesgos de TI	S
S	AI3 Adquirir y mantener la infraestructura tecnológica	
S	AI4 Facilitar la operación y el uso	S
	AI5 Adquirir recursos de TI	S
P	AI6 Administrar cambios	
S	AI7 Instalar y acreditar soluciones y cambios	
S	DS1 Definir y administrar niveles de servicio	S
S	DS2 Administrar los servicios de terceros	S
S	DS3 Administrar el desempeño y la capacidad	
P	DS4 Garantizar la continuidad del servicio	
S	DS5 Garantizar la seguridad de los sistemas	S
S	DS9 Administrar la configuración	
S	DS10 Administración de problemas	
P	DS12 Administración del ambiente físico	
S	DS13 Administración de operaciones	

P = 4 S = 2

P = 2 S = 1

Identifico los Procesos COBIT afectados

DISPONIBILIDAD	PROCESOS DE TI	CUMPLIMIENTO
	PO6 Comunicar las aspiraciones y la dirección de la gerencia	1
4	PO9 Evaluar y administrar los riesgos de TI	1
2	AI3 Adquirir y mantener la infraestructura tecnológica	
2	AI4 Facilitar la operación y el uso	1
	AI5 Adquirir recursos de TI	1
4	AI6 Administrar cambios	
2	AI7 Instalar y acreditar soluciones y cambios	
2	DS1 Definir y administrar niveles de servicio	1
2	DS2 Administrar los servicios de terceros	1
2	DS3 Administrar el desempeño y la capacidad	
4	DS4 Garantizar la continuidad del servicio	
2	DS5 Garantizar la seguridad de los sistemas	1
2	DS9 Administrar la configuración	
2	DS10 Administración de problemas	
4	DS12 Administración del ambiente físico	
2	DS13 Administración de operaciones	

Identifico los Procesos COBIT afectados

SUMO VALORES DE CRITERIOS	PROCESOS DE TI	SELECCIÓN DE PROCESOS
1	PO6 Comunicar las aspiraciones y la dirección de la gerencia	
5	PO9 Evaluar y administrar los riesgos de TI	
2	AI3 Adquirir y mantener la infraestructura tecnológica	
3	AI4 Facilitar la operación y el uso	
1	AI5 Adquirir recursos de TI	
4	AI6 Administrar cambios	
2	AI7 Instalar y acreditar soluciones y cambios	
3	DS1 Definir y administrar niveles de servicio	
3	DS2 Administrar los servicios de terceros	
2	DS3 Administrar el desempeño y la capacidad	
4	DS4 Garantizar la continuidad del servicio	
3	DS5 Garantizar la seguridad de los sistemas	
2	DS9 Administrar la configuración	
2	DS10 Administración de problemas	
4	DS12 Administración del ambiente físico	
2	DS13 Administración de operaciones	

Identifico los Procesos COBIT afectados

ORDENO PROCESOS	PROCESOS DE TI	SELECCIÓN DE PROCESOS
5	PO9 Evaluar y administrar los riesgos de TI	
4	AI6 Administrar cambios	
4	DS4 Garantizar la continuidad del servicio	
4	DS12 Administración del ambiente físico	
3	AI4 Facilitar la operación y el uso	
3	DS1 Definir y administrar niveles de servicio	
3	DS2 Administrar los servicios de terceros	
3	DS5 Garantizar la seguridad de los sistemas	
2	AI3 Adquirir y mantener la infraestructura tecnológica	
2	AI7 Instalar y acreditar soluciones y cambios	
2	DS3 Administrar el desempeño y la capacidad	
2	DS9 Administrar la configuración	
2	DS10 Administración de problemas	
2	DS13 Administración de operaciones	
1	AI5 Adquirir recursos de TI	
1	PO6 Comunicar las aspiraciones y la dirección de la gerencia	

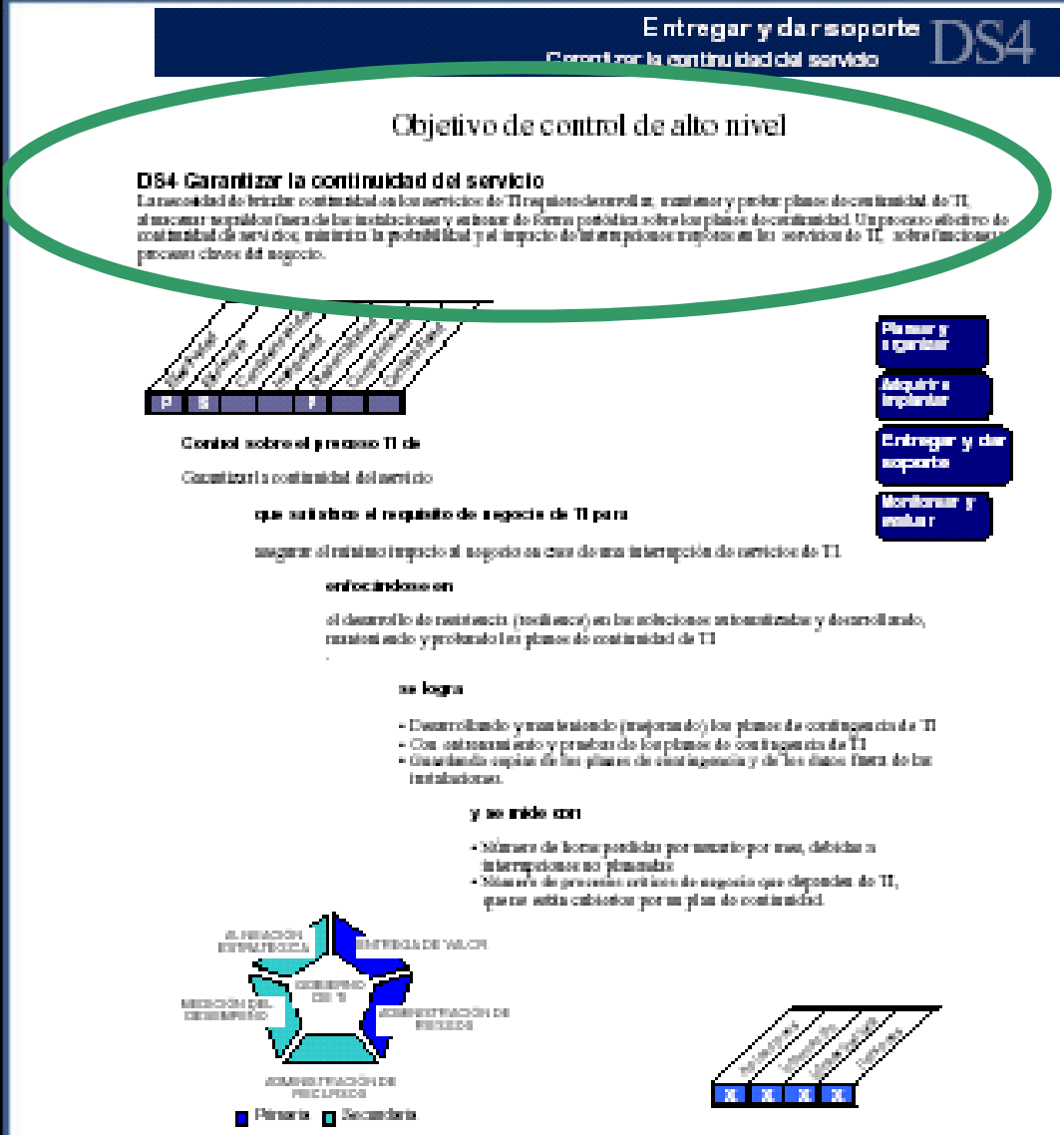
Identifico los Procesos COBIT afectados
Enfoque de riesgo

PROCESOS DE TI		DEFINICIÓN COBIT	DEFINICIÓN RIESGO
PO9	Evaluar y administrar los riesgos de TI	Analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de negocio	Los Riesgos de TI no son identificados, analizados, tratados y comunicados de manera adecuada
AI6	Administrar cambios	Controlar la evaluación de impacto, autorización e implantación de todos los cambios minimizando errores y detener la implantación de cambios no autorizados	Se producen interrupciones, alternaciones no autorizadas, errores y re-trabajos por cambios no controlados en los Sistemas de Información
DS4	Garantizar la continuidad del servicio	Asegurar el mínimo impacto al negocio en caso de una interrupción de servicios de TI	Los principales procesos de Negocio no pueden ser llevados adelante debido a una Interrupción en los sistemas o infraestructura
DS12	Administración del ambiente físico	Proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI contra acceso, daño o robo y minimizar las interrupciones de los servicios	Se producen interrupciones en los Servicios de TI debido a problemas físicos de los Equipos y/o Instalaciones

Identifico los Procesos COBIT afectados

PROCESOS DE TI		DEFINICIÓN RIESGO
PO9	Evaluar y administrar los riesgos de TI	Los Riesgos de TI no son identificados, analizados, tratados y comunicados de manera adecuada
AI6	Administrar cambios	Se producen interrupciones, alternaciones no autorizadas, errores y re-trabajos por Cambios no controlados en el Sistema de Información
DS4	Garantizar la continuidad del servicio	Los principales procesos de Negocio no pueden ser llevados adelante debido a una Interrupción en los sistemas
DS12	Administración del ambiente físico	Se producen interrupciones en los Servicios de TI debido a problemas físicos de los Equipos y/o Instalaciones

Identificación de Procesos y Objetivos de Control



DS4.1 Marco de trabajo de continuidad de TI

DS4.2 Planes de continuidad de TI

DS4.3 Recursos críticos de TI

DS4.4 Mantenimiento del plan de continuidad de TI

DS4.5 Pruebas del plan de continuidad de TI

DS4.6 Entrenamiento del plan de continuidad de TI

DS4.7 Distribución del plan de continuidad de TI

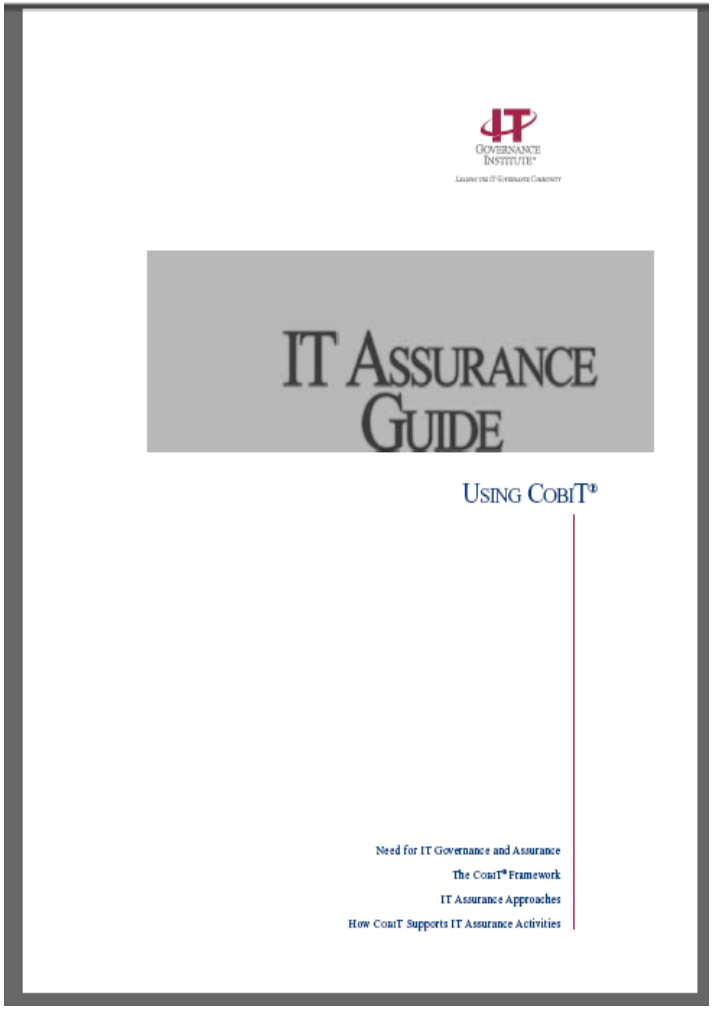
DS4.8 Recuperación y reanudación de los servicios de TI

DS4.9 Almacenamiento de respaldos fuera de las instalaciones

DS4.10 Revisión post-reanudación

Pruebas de Auditoria
Guias de Aseguramiento deTI

- Proveer una guía para utilizar en una variedad de actividades de aseguramiento (planificar, definir alcance y ejecutar).
- La guía está dirigida primariamente a profesionales de aseguramiento de TI, sin embargo, como todo el material de CobiT, puede ser utilizada por todas las partes relacionadas a TI, como profesionales de TI y consultores .



Estructura – Guías de Aseguramiento

Controles Clave

Beneficios para el negocio

Riesgos

DS4 Ensure Continuous Service (cont.)

Control Objective	Value Drivers	Risk Drivers
DS4.2 IT Continuity Plans Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.	• Continuous service across IT, addressing the requirements for critical IT resources • Defined and documented guidelines, roles and responsibilities • Achieved short- and long-range objectives supporting the organisation's objectives	• Failure to recover IT systems and services in a timely manner • Failure of alternative decision-making processes • Lack of required recovery resources • Failed communication to internal and external stakeholders

Test the Control Design

- Confirm that business continuity plans exist for all key business functions and processes.
- Review an appropriate sample of business continuity plans and confirm that each plan:
  - Is designed to establish the resilience, alternative processing and recovery capability in line with service commitments and availability targets
  - Defines roles and responsibilities
  - Includes communication processes
  - Defines the minimum acceptable recovery configuration
- Obtain the overall testing strategy for business continuity plans and evidence that tests are being executed with the agreed-upon frequency.
- Review the outcome of testing, and ensure that resulting actions are followed up.

Prueba de Controles

Identificación de riesgos

Dominio/Proceso	Objetivo de Control	Riesgos
DS4 Garantizar la continuidad del servicio	4.1 TI Marco de trabajo de continuidad	Prácticas insuficientes en materia de continuidad
		Continuidad de los servicios de TI no gestionadas correctamente
		Aumento de la dependencia en el personal clave
	4.2 Planes de continuidad de TI	Incapacidad de recuperar los sistemas y servicios de TI de manera oportuna
		Fallas en los procesos de toma de decisiones alternativos
		Falta de recuperación de los recursos necesarios
		Falta de comunicación con los stakeholders internos y externos
	4.3 Recursos críticos de TI	Recursos críticos de TI no disponibles
		Incremento en los costos en la gestión de la continuidad
		Determinación de las prioridades de recuperación de los servicios sin basarse en las necesidades del negocio

Valoración del riesgo
Indicadores

KPI

Indicadoresclave de desempeño

- Tiempo transcurrido entre las pruebas de cualquier elemento dado del plan de continuidad de TI
- Número de horas de capacitación por año de cada empleado relevante de TI
- % de componentes de infraestructura críticos con monitoreo de disponibilidad automatizado
- Frecuencia de revisión del plan de continuidad de TI

KGI

Indicadores clave de meta de procesos

- % de SLAs de disponibilidad que se cumplen
- # de procesos críticos del negocio que dependen de TI, no cubiertos por un plan de continuidad
- % de pruebas para lograr los objetivos de recuperación
- Frecuencia en la interrupción de servicios de sistemas críticos

Permiten brindar mejor información para identificar y valorar riesgos ayudando a ajustar los niveles de probabilidad y/o impacto.

Valoración del riesgo inherente Ejemplo

Indicadores clave de meta de procesos

- % de SLAs de disponibilidad que se cumplen
- # de procesos críticos del negocio que dependen de TI, no cubiertos por un plan de continuidad
- % de pruebas para lograr los objetivos de recuperación
- Frecuencia en la interrupción de servicios de sistemas críticos

Matriz de Riesgos

Impacto / Probabilidad	Probabilidad Baja (1)	Probabilidad Media (2)	Probabilidad Alta (3)
Impacto Alto (6)	6x1=6	6x2=12	6x3=18
Impacto Medio (3)	3x1=3	3x2=6	3x3=9
Impacto Bajo (1)	1x1=1	1x2=2	1x3=3

Indicadoresclave de desempeño

- Tiempo transcurrido entre las pruebas de cualquier elemento dado del plan de continuidad de TI
- Número de horas de capacitación por año de cada empleado relevante de TI
- % de componentes de infraestructura críticos con monitoreo de disponibilidad automatizado
- Frecuencia de revisión del plan de continuidad de TI

Estructura – Guías de Aseguramiento

DS4 Ensure Continuous Service (cont.)

Control Objective

DS4.2 IT Continuity Plans

Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.

Value Drivers

- Continuous service across IT, addressing the requirements for critical IT resources
- Defined and documented guidelines, roles and responsibilities
- Achieved short- and long-range objectives supporting the organisation's objectives

Risk Drivers

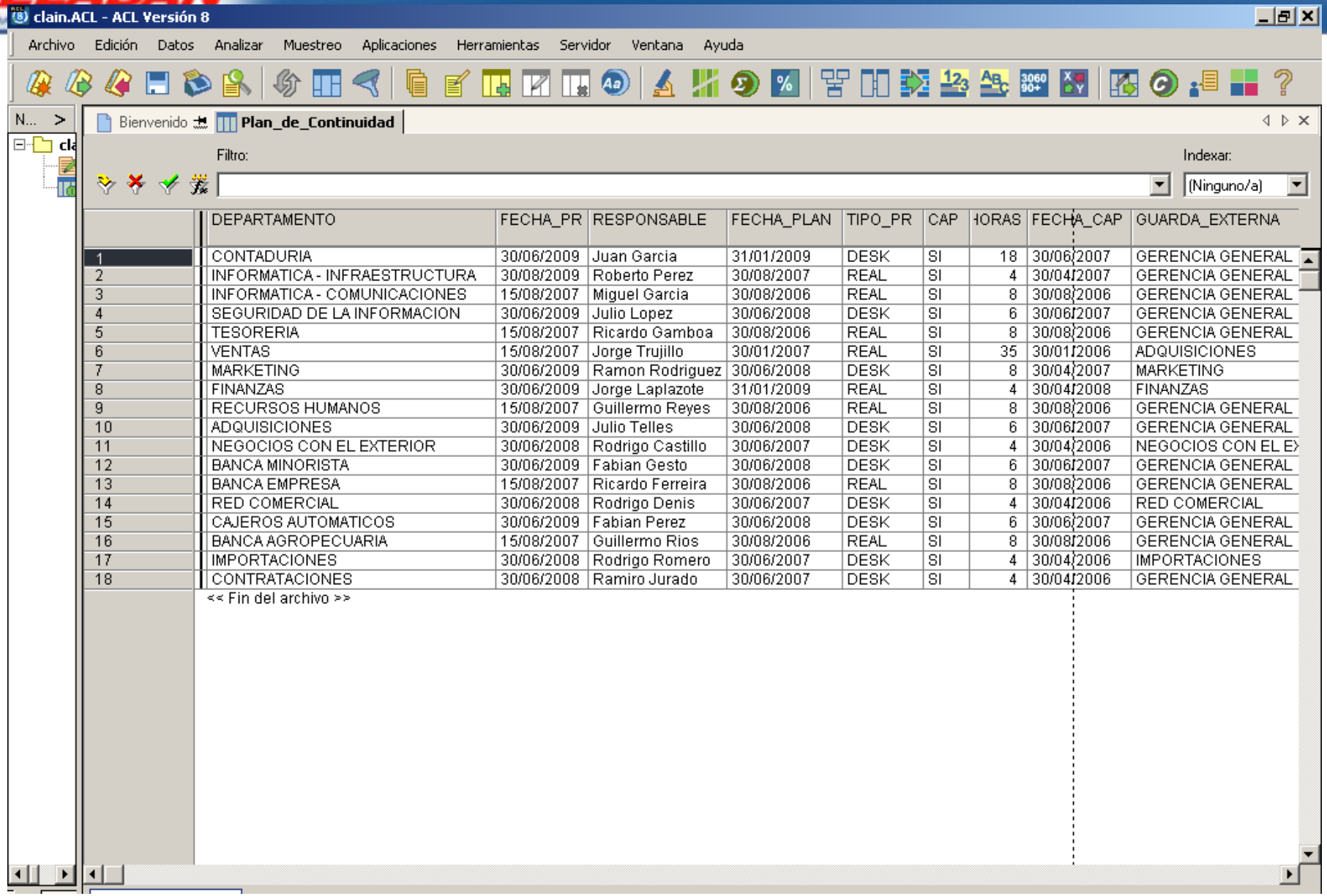
- Failure to recover IT systems and services in a timely manner
- Failure of alternative decision-making processes
- Lack of required recovery resources
- Failed communication to internal and external stakeholders

Test the Control Design

- Confirm that business continuity plans exist for all key business functions and processes.
- Review an appropriate sample of business continuity plans and confirm that each plan:
  - Is designed to establish the resilience, alternative processing and recovery capability in line with service commitments and availability targets
  - Defines roles and responsibilities
  - Includes communication processes
  - Defines the minimum acceptable recovery configuration
- Obtain the overall testing strategy for business continuity plans and evidence that tests are being executed with the agreed-upon frequency.
- Review the outcome of testing, and ensure that resulting actions are followed up.

Prueba de Controles → **Auditoría Continua**

Ejemplo – Planes de continuidad



	DEPARTAMENTO	FECHA_PR	RESPONSABLE	FECHA_PLAN	TIPO_PR	CAP	HORAS	FECHA_CAP	GUARDA_EXTERNA
1	CONTADURIA	30/06/2009	Juan Garcia	31/01/2009	DESK	SI	18	30/06/2007	GERENCIA GENERAL
2	INFORMATICA - INFRAESTRUCTURA	30/08/2009	Roberto Perez	30/08/2007	REAL	SI	4	30/04/2007	GERENCIA GENERAL
3	INFORMATICA - COMUNICACIONES	15/08/2007	Miguel Garcia	30/08/2006	REAL	SI	8	30/08/2006	GERENCIA GENERAL
4	SEGURIDAD DE LA INFORMACION	30/06/2009	Julio Lopez	30/06/2008	DESK	SI	6	30/06/2007	GERENCIA GENERAL
5	TESORERIA	15/08/2007	Ricardo Gamboa	30/08/2006	REAL	SI	8	30/08/2006	GERENCIA GENERAL
6	VENTAS	15/08/2007	Jorge Trujillo	30/01/2007	REAL	SI	35	30/01/2006	ADQUISICIONES
7	MARKETING	30/06/2009	Ramon Rodriguez	30/06/2008	DESK	SI	8	30/04/2007	MARKETING
8	FINANZAS	30/06/2009	Jorge Laplazote	31/01/2009	REAL	SI	4	30/04/2008	FINANZAS
9	RECURSOS HUMANOS	15/08/2007	Guillermo Reyes	30/08/2006	REAL	SI	8	30/08/2006	GERENCIA GENERAL
10	ADQUISICIONES	30/06/2009	Julio Telles	30/06/2008	DESK	SI	6	30/06/2007	GERENCIA GENERAL
11	NEGOCIOS CON EL EXTERIOR	30/06/2008	Rodrigo Castillo	30/06/2007	DESK	SI	4	30/04/2006	NEGOCIOS CON EL E
12	BANCA MINORISTA	30/06/2009	Fabian Gesto	30/06/2008	DESK	SI	6	30/06/2007	GERENCIA GENERAL
13	BANCA EMPRESA	15/08/2007	Ricardo Ferreira	30/08/2006	REAL	SI	8	30/08/2006	GERENCIA GENERAL
14	RED COMERCIAL	30/06/2008	Rodrigo Denis	30/06/2007	DESK	SI	4	30/04/2006	RED COMERCIAL
15	CAJEROS AUTOMATICOS	30/06/2009	Fabian Perez	30/06/2008	DESK	SI	6	30/06/2007	GERENCIA GENERAL
16	BANCA AGROPECUARIA	15/08/2007	Guillermo Rios	30/08/2006	REAL	SI	8	30/08/2006	GERENCIA GENERAL
17	IMPORTACIONES	30/06/2008	Rodrigo Romero	30/06/2007	DESK	SI	4	30/04/2006	IMPORTACIONES
18	CONTRATACIONES	30/06/2008	Ramiro Jurado	30/06/2007	DESK	SI	4	30/04/2006	GERENCIA GENERAL

<< Fin del archivo >>

Pasaje de Guías de Aseguramiento a un enfoque de auditoría continua

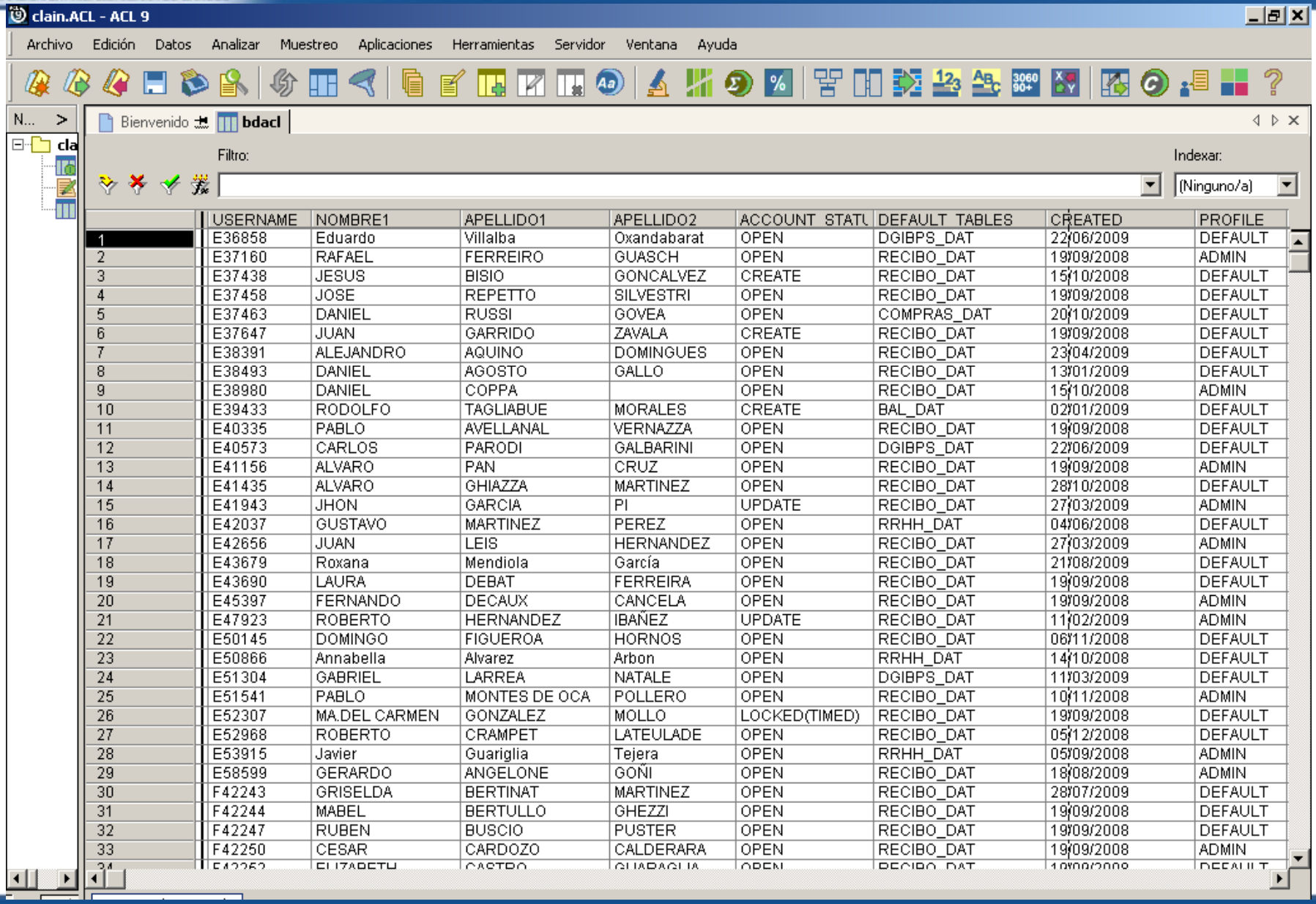
Pruebas de controles – Guías de Aseguramiento

- Revisar una muestra apropiada de planes de continuidad de negocio y confirmar que cada plan incluye :
- Definición de roles y responsabilidades.
- Incluir los procesos de comunicación
- Definición de una configuración mínima de configuración.
- Obtener evidencia de que los planes están siendo ejecutados con una frecuencia acordada.
- Revisar el resultado de las pruebas y asegurar que las acciones resultantes son seguidas y controladas.

Enfoque de Auditoría Continua

- Auditar que todas las áreas tienen un plan de continuidad.
- Auditar que los roles y responsables están actualizados.
- Auditar que los planes se actualizan con una periodicidad menor a un año.
- Auditar que las pruebas al plan se realizan con una periodicidad no mayor a un año.
- Auditar que se realizan por lo menos una prueba de la infraestructura tecnológica cada 6 meses.
- Auditar que los participantes hayan recibido capacitación y que la misma se actualiza cada 2 años.
- Auditar que los planes se guardan en un sitio externo.

Ejemplo – Acceso a BD



	USERNAME	NOMBRE1	APELLIDO1	APELLIDO2	ACCOUNT_STATU	DEFAULT_TABLES	CREATED	PROFILE
1	E36858	Eduardo	Villalba	Oxandabarat	OPEN	DGIBPS_DAT	22/06/2009	DEFAULT
2	E37160	RAFAEL	FERREIRO	GUASCH	OPEN	RECIBO_DAT	19/09/2008	ADMIN
3	E37438	JESUS	BISIO	GONCALVEZ	CREATE	RECIBO_DAT	15/10/2008	DEFAULT
4	E37458	JOSE	REPETTO	SILVESTRI	OPEN	RECIBO_DAT	19/09/2008	DEFAULT
5	E37463	DANIEL	RUSSI	GOVEA	OPEN	COMPRAS_DAT	20/10/2009	DEFAULT
6	E37647	JUAN	GARRIDO	ZAVALA	CREATE	RECIBO_DAT	19/09/2008	DEFAULT
7	E38391	ALEJANDRO	AQUINO	DOMINGUES	OPEN	RECIBO_DAT	23/04/2009	DEFAULT
8	E38493	DANIEL	AGOSTO	GALLO	OPEN	RECIBO_DAT	13/01/2009	DEFAULT
9	E38980	DANIEL	COPPA		OPEN	RECIBO_DAT	15/10/2008	ADMIN
10	E39433	RODOLFO	TAGLIABUE	MORALES	CREATE	BAL_DAT	02/01/2009	DEFAULT
11	E40335	PABLO	AVELLANAL	VERNAZZA	OPEN	RECIBO_DAT	19/09/2008	DEFAULT
12	E40573	CARLOS	PARODI	GALBARINI	OPEN	DGIBPS_DAT	22/06/2009	DEFAULT
13	E41156	ALVARO	PAN	CRUZ	OPEN	RECIBO_DAT	19/09/2008	ADMIN
14	E41435	ALVARO	GHIAZZA	MARTINEZ	OPEN	RECIBO_DAT	28/10/2008	DEFAULT
15	E41943	JHON	GARCIA	PI	UPDATE	RECIBO_DAT	27/03/2009	ADMIN
16	E42037	GUSTAVO	MARTINEZ	PEREZ	OPEN	RRHH_DAT	04/06/2008	DEFAULT
17	E42656	JUAN	LEIS	HERNANDEZ	OPEN	RECIBO_DAT	27/03/2009	ADMIN
18	E43679	Roxana	Mendiola	García	OPEN	RECIBO_DAT	21/08/2009	DEFAULT
19	E43690	LAURA	DEBAT	FERREIRA	OPEN	RECIBO_DAT	19/09/2008	DEFAULT
20	E45397	FERNANDO	DECAUX	CANCELA	OPEN	RECIBO_DAT	19/09/2008	ADMIN
21	E47923	ROBERTO	HERNANDEZ	IBAÑEZ	UPDATE	RECIBO_DAT	11/02/2009	ADMIN
22	E50145	DOMINGO	FIGUEROA	HORNOS	OPEN	RECIBO_DAT	06/11/2008	DEFAULT
23	E50866	Annabella	Alvarez	Arbon	OPEN	RRHH_DAT	14/10/2008	DEFAULT
24	E51304	GABRIEL	LARREA	NATALE	OPEN	DGIBPS_DAT	11/03/2009	DEFAULT
25	E51541	PABLO	MONTES DE OCA	POLLERO	OPEN	RECIBO_DAT	10/11/2008	ADMIN
26	E52307	MA.DEL CARMEN	GONZALEZ	MOLLO	LOCKED(TIMED)	RECIBO_DAT	19/09/2008	DEFAULT
27	E52968	ROBERTO	CRAMPET	LATEULADE	OPEN	RECIBO_DAT	05/12/2008	DEFAULT
28	E53915	Javier	Guariglia	Tejera	OPEN	RRHH_DAT	05/09/2008	ADMIN
29	E58599	GERARDO	ANGELONE	GOÑI	OPEN	RECIBO_DAT	18/08/2009	ADMIN
30	F42243	GRISELDA	BERTINAT	MARTINEZ	OPEN	RECIBO_DAT	28/07/2009	DEFAULT
31	F42244	MABEL	BERTULLO	GHEZZI	OPEN	RECIBO_DAT	19/09/2008	DEFAULT
32	F42247	RUBEN	BUSCIO	PUSTER	OPEN	RECIBO_DAT	19/09/2008	DEFAULT
33	F42250	CESAR	CARDOZO	CALDERARA	OPEN	RECIBO_DAT	19/09/2008	ADMIN
34	F42252	ELIZABETH	CASTRO	GUARAGLIA	OPEN	RECIBO_DAT	19/09/2008	DEFAULT

Enfoque de auditoría continua
Prevención y Detección de Fraudes

Pruebas de controles – Guías de Aseguramiento

- Existencia de procedimientos que aseguren que los perfiles de acceso están de acuerdo a las responsabilidades.
- Existencia de registros de todos los accesos al centro de procesamiento.
- Verificar que el acceso a información sensitiva está restringido a usuarios no autorizados.
- Verificar que existe entrenamiento de concientización a los usuarios a través de registro de entrenamiento.

Enfoque de Auditoría Continua

- Auditar que los usuarios con permisos especiales.
- Auditar que los usuarios con permiso de "Administradores" están asignados en función de la responsabilidad.
- Auditar los accesos en horarios inusuales.
- Auditar los registros o logs en forma periódica en busca de registro de intentos fallidos, usuarios que no acceden asiduamente, transacciones inusuales.

CASO PRÁCTICO

Auditoría Continua: Mejores Prácticas y Caso Real

Presentación de Caso Práctico

CONCLUSIONES

Auditoría Continua: Mejores Prácticas y Caso Real

Conclusiones

- Auditoría Continua es un método para evaluar la eficiencia de controles automatizados con mayor frecuencia, manteniendo así su nivel de eficiencia.
- Permite medir de manera concreta un aumento en el nivel de riesgo de la entidad, unidad de negocio y/o proceso.
- La Alta Gerencia recibe alertas simultáneamente o poco después de la ocurrencia de una falla/debilidad en un control.
- Mayor cobertura en la auditoría con la habilidad de hacer pruebas sobre el 100% de la población.
- Reducción de costos de auditoría.

GRACIAS

Auditoría Continua: Mejores Prácticas y Caso Real

Julio R. Jolly Moore

Socio

BDO Consulting

jjolly@bdo.com.pa

Gerardo Alcarraz

Coordinador de Auditoría Informática

Banco de la República Oriental de Uruguay

gerardo.alcarraz@brou.com.uy