ESTRUCTURA DE LA AUDITORIA BASADA EN COBIT

Objetivo: Establecer los pasos ha seguir y los entregables de una auditoría basada en COBIT

1) SITUACION ACTUAL DE LA EMPRESA

- Misión
- Visión
- Entorno general de la empresa

2) SELECCIÓN DE RECURSOS DE TI

- Recursos de Hardware
- Recursos de software
- Aplicaciones
- Software en general
- Recursos de comunicaciones
- Recursos Humanos
- Recursos de infraestructura

3) ANALISIS DE RIESGOS DE TI

MATRIZ DE EVALUACION DE RIESGOS

Recurso	Amenaza	Vulnerabilidad	Control Existente	Impacto	Probabilidad	Nivel de Riesgo	Recomendación
Servidores y PC	Mal uso de recursos	El documento de políticas de TI no cuenta con un proceso de revisión definido.	El documento actual de políticas no actualizado.	Bajo	Media	Bajo	Establecer un procedimiento de actualización periódica del documento.
Servidores y PC	Acceso no autorizado a información confidencial	El documento de políticas de TI no cuenta con un proceso de revisión definido.	El documento actual de políticas no actualizado.	Bajo	Media	Bajo	Establecer un procedimiento de actualización periódica del documento.
Equipos de conexión de red	Mal uso de recursos	El documento de políticas de TI no cuenta con un proceso de revisión definido.	El documento actual de políticas no actualizado.	Medio	Media	Medio	Establecer un procedimiento de actualización periódica del documento.
Servidores y PC	Mal uso de recursos y acceso no autorizado	No existe un documento específico de políticas de seguridad de TI.	Ninguno	Alto	Media	Medio	Definir un documento de políticas de seguridad para TI.
Equipos de conexión de red	Mal uso de recursos	No existe un documento específico de políticas de seguridad de TI.	Ninguno	Alto	Media	Medio	Definir un documento de políticas de seguridad para TI.

Recurso	Amenaza	Vulnerabilidad	Control Existente	Impacto	Probabilidad	Nivel de Riesgo	Recomendación
Enlaces Ultima Milla	Ataque a la red y mal uso de recursos	No existe un procedimiento formal para reportar los incidentes de seguridad por los canales de administración apropiados tan pronto como sea posible.	Reportes informales.	Alto	Baja	Bajo	Establecer un procedimiento de formal para reportar incidentes de seguridad.
PC	Carga de software malicioso	No existe un procedimiento para verificar todos los boletines de advertencia e informativos con respecto al uso de software malicioso.	Se define usuarios con perfil limitado.	Bajo	Media	Bajo	Verificar periódicamente los boletines y dar a conocer a los usuarios.

4) PLAN DE AUDITORIA

- Alcance
- Objetivos de la auditoría
- Identificación de los Dominios, Procesos y objetivos de control Cobit aplicables

OBJETIVOS DE CONTROL COBIT-CRITERIOS Y RECURSOS TI AFECTADOS

DOMINIO	PROCESO		Criterios de Información							Recursos de TI				
			Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Recursos	Sist. Aplicación	Tecnología	Instalaciones	Datos
Planificación y Organización	PO4	Definición de la Organización y Relaciones de TI.	P	S						X				
	PO6	Comunicación de la Dirección y Aspiraciones Gerenciales.	P				S			X				
	PO8	Asegurar de cumplimiento de requerimientos externos.	P					P	S	X	X			X
	PO9	Evaluación de Riesgos.	S	S	P	P	P	S	S	X	X	X	X	X
Adquisición e Implementación	AI3	Adquirir y mantener la arquitectura tecnológica	P	P	S						X			
Entrega de Servicios y Soporte	DS2	Administrar servicios de terceros	P	P	S	S	S	S	S	X	X	X	X	X
	DS4	Asegurar continuidad de servicio	P	S			P			X	X	X	X	X
	DS5	Garantizar la seguridad de sistemas			P	P	S	S	S	X	X	X	X	X
	DS9.	Administración de la Configuración.	P				S		S		X	X		X
	DS11	Administración de Datos				P			P					X

- Descripción de herramientas, documentos, estándares, directrices, etc

5) PUESTA EN MARCHA DE LA AUDITORIA

- Por cada objetivo de control de COBIT identificar los factores de riesgo

DOMINIO: PLANEACION Y ORGANIZACIÓN	
PO4 Definición de la organización y de las relaciones de TI	
Para conocer si las responsabilidades de seguridad están definidas, entendidas y asignadas apropiadamente.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
PO4.6 Responsabilidad por la seguridad lógica y física La Gerencia deberá asignar formalmente la responsabilidad de la seguridad lógica y física de los activos de información de la organización a un Gerente de seguridad de la información, quien reportará a la alta gerencia. Como mínimo, la responsabilidad de la Gerencia de seguridad deberá establecerse a todos los niveles de la organización para manejar los problemas generales de seguridad en la organización. En caso necesario, deberán asignarse responsabilidades gerenciales de seguridad adicionales a niveles específicos con el fin de resolver los problemas de seguridad relacionados con ellos.	➢ No existirán procedimientos definidos para el manejo de acciones en caso de problemas de seguridad. ➢ Falta de planes de contingencia específicos para el manejo de incidentes de seguridad.

DOMINIO: ADQUISICION E IMPLEMENTACION	
AI3 Adquisición y Mantenimiento de la Infraestructura Tecnológica	
Se refiere a la seguridad apropiada para la infraestructura tecnológica (hardware y software) que tiene que ver con la actualización, mantenimiento y adquisición.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
AI3.2 Mantenimiento preventivo para hardware La Gerencia de la función de servicios de información deberá agendar o programar el mantenimiento rutinario y periódico del hardware con el fin de reducir la frecuencia y el impacto de fallas de rendimiento.	➢ Daño permanente de los equipos. ➢ Fallo en el servicio en caso de daños de equipos de interconexión. ➢ Incremento de gastos por reparación de equipos. ➢ Usuarios insatisfechos.

- Elaboración de matriz de pruebas para cada objetivo de control

DOMINIO: PLANEACION Y ORGANIZACIÓN		
PO4 Definición de la organización y de las relaciones de TI		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
PO4.6 Responsabilidad por la seguridad lógica y física La Gerencia deberá asignar formalmente la responsabilidad de la seguridad lógica y física de los activos de información de la organización a un Gerente de seguridad de la información, quien reportará a la alta gerencia. Como mínimo, la responsabilidad de la Gerencia de seguridad deberá establecerse a todos los niveles de la organización para manejar los problemas generales de seguridad en la organización. En caso necesario, deberán asignarse responsabilidades gerenciales de seguridad adicionales a niveles específicos con el fin de resolver los problemas de seguridad relacionados con ellos.	*Evaluación de controles:* Existen políticas que determinen los roles y responsabilidades para todo el personal dentro de la organización con respecto a sistemas de información, control interno y seguridad. La Gerencia ha asignado formalmente la responsabilidad a lo largo de toda la organización para la formulación de políticas y procedimientos de control interno y seguridad (tanto lógicos como físicos) a un oficial de seguridad. El oficial de seguridad de la información comprende adecuadamente sus funciones y responsabilidades y si éstas han mostrado consistencia con respecto a la política de seguridad de la información de la organización. Las políticas de seguridad de la organización definen claramente las responsabilidades sobre la seguridad de la información que cada propietario de los activos (por ejemplo, usuarios, administración y administradores de seguridad) debe llevar a cabo.	Revisión del documento de descripción de funciones. Entrevista al Gerente de TI.

DOMINIO: ADQUISICION E IMPLEMENTACION		
AI3 Adquisición y Mantenimiento de la Infraestructura Tecnológica		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
AI3.2 Mantenimiento preventivo para hardware La Gerencia de la función de servicios de información deberá agendar o programar el mantenimiento rutinario y periódico del hardware con el fin de reducir la frecuencia y el impacto de fallas de rendimiento.	*Evaluación de controles:* Existen políticas y procedimientos para el mantenimiento preventivo de hardware (tanto el operado por la función de servicios de información como por las funciones de los usuarios afectados) para reducir la frecuencia y el impacto de las fallas de desempeño Se cumple con los pasos y la frecuencia de mantenimiento preventivo prescritos por el proveedor para cada dispositivo de hardware operado por la función de servicios de información y los usuarios afectados se adhieren a ellos. *Probando que:* El calendario de mantenimiento preventivo asegura que el mantenimiento de hardware programado no tendrá ningún impacto negativo sobre aplicaciones críticas o sensitivas. El mantenimiento programado asegura que no ha sido planeado para períodos pico de carga de trabajo y que la función de servicios de información y las operaciones de los grupos de usuarios afectados son suficientemente flexibles para adaptar el mantenimiento preventivo rutinario planeado. Los programas operativos de servicios de información aseguran que existen las preparaciones adecuadas para manejar anticipadamente los tiempos muertos de hardware ocasionados por mantenimiento no programado.	Entrevista al Gerente de TI. Revisión del Contrato de Mantenimiento de Hardware.

- Recolección de documentación: manuales, procedimientos, funciones

6) RESULTADOS DE LA APLICACIÓN DE LA AUDITORIA

- Cuadros de evaluación para cada uno de los objetivos de COBIT

EVALUACIÓN DE PRUEBAS PO4.10

DOMINIO: PLANEACION Y ORGANIZACIÓN				
PO4 Definición de la organización y de las relaciones de TI				
PO4.10 Segregación de funciones				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Existen políticas y procedimientos que describan las prácticas de supervisión para asegurar que las funciones y responsabilidades sean ejercidas apropiadamente y que todo el personal cuente con suficiente autoridad y recursos para llevar a cabo sus funciones y responsabilidades. Existe una segregación de funciones entre los siguientes pares de unidades: - desarrollo y mantenimiento de sistemas - desarrollo y operaciones de sistemas - desarrollo/mantenimiento de sistemas y seguridad de la información. - operaciones y control de datos - operaciones y usuarios - operaciones y seguridad de la información *Probando que:* Las descripciones de los puestos de trabajo tienen claramente delimitada tanto la autoridad como la responsabilidad. La naturaleza y el alcance de la suficiencia de la segregación de funciones deseada y de las limitaciones de funciones dentro de TI.	Revisión del documento Descripción de Funciones del Departamento de Sistemas. Entrevista al Gerente de TI.	EFECTIVO	Descripción de Funciones del Personal del Departamento de TI.	

EVALUACIÓN DE PRUEBAS PO4.6

DOMINIO: PLANEACION Y ORGANIZACIÓN				
PO4 Definición de la organización y de las relaciones de TI				
PO4.6 Responsabilidad por la seguridad lógica y física				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Existen políticas que determinen los roles y responsabilidades para todo el personal dentro de la organización con respecto a sistemas de información, control interno y seguridad. La Gerencia ha asignado formalmente la responsabilidad a lo largo de toda la organización para la formulación de políticas y procedimientos de control interno y seguridad (tanto lógicos como físicos) a un oficial de seguridad. El oficial de seguridad de la información comprende adecuadamente sus funciones y responsabilidades y si éstas han mostrado consistencia con respecto a la política de seguridad de la información de la organización. Las políticas de seguridad de la organización definen claramente las responsabilidades sobre la seguridad de la información que cada propietario de los activos (por ejemplo, usuarios, administración y administradores de seguridad) debe llevar a cabo. *Probando que:* El personal de seguridad revisa los sistemas operativos y los sistemas de aplicación esenciales.	Revisión del documento de descripción de funciones. Entrevista al Gerente de TI.	NO EFECTIVO	Descripción de Funciones del Personal del Departamento de TI.	No existen documentos específicos sobre responsabilidades de seguridad, pero se entiende que la responsabilidad la tiene el Gerente de TI.

- Análisis de resultados

ANÁLISIS DE RESULTADOS

En base a la evaluación de las pruebas efectuadas sobre la gestión de la seguridad en redes se determinó que el 43% de los objetivos de control detallados cumplen con las condiciones necesarias para su efectivo cumplimiento. A continuación se detalla el funcionamiento actual de estos controles:

PO4.10 Segregación de funciones

Actualmente, existen los documentos que especifican las funciones a realizarse por el personal del Departamento y su nivel de responsabilidad en cada una de ellas, esto es, por el Gerente y Subgerente de T.I. Sin embargo en la entrevista realizada el Gerente de T.I. recalca que por el límite de personal del Departamento (2 personas), todas las funciones son conocidas por el personal, y los dos están en capacidad de realizar todas las tareas si es necesario.

7) INFORME FINAL DE AUDITORIA

- Carta de entrega del informe
- Alcance
- Objetivos
- Listado de objetivos de control con:
  - Observación
  - Riesgo
  - Recomendación

PO9.3 Identificación de Riesgos

Observación:

No existe procedimiento específico para la identificación de riesgos de TI, solamente se maneja una evaluación de los riesgos en base al criterio de los empleados del Área de TI según los objetivos del negocio.

Riesgo:

Al no identificarse los riesgos de TI no se consideran las posibles amenazas, vulnerabilidades, y consecuencias a las que esta expuesto el negocio, por lo tanto no es posible medir el impacto y pérdidas económicas de un ataque o falla de un recurso crítico.

Recomendación:

Definir procedimientos para identificar los recursos críticos y riesgos potenciales sobre éstos. Asegurarse del cumplimiento de los mismos y verificar que estén acorde con los objetivos del negocio.