TECNOSERVICE CR

Gerencia estratégica de TI

La Auditoria desde el punto de Vista del Auditor como del Auditado

Perfil de un Auditor

- Ser imparcial, sincero y honesto
- Entender el concepto de confidencialidad
- Tener la mente abierta
- Ser diplomático
- Ser firme, no negociar
- Ser muy observador
- Comprender las situaciones
- Capacidad de adaptación
- Orientación hacia la consecución de los logros
- Alcanzar conclusiones basadas en razonamientos lógicos
- Estar seguro de sí mismo
- Ser objetivo

El Auditor busca...

Actitud participativa del auditado para que:

Suministre información clara y concreta.
Asuma una posición abierta.
Sea Honesto
Se sienta bien.

El Auditor No Busca…
Busque fallas.
Caza brujas.
Busque violaciones de procedimientos.

TECNOSERVICE
Gerencia estratégica de TI

Puntos Vitales en una Auditoria de Sistemas

- Continuidad del Negocio DRP
- Seguridad de la Información
- Madurez Tecnológica
- Licenciamiento Riesgo Operativo
- Cuarto Servidores Procedimientos y acondicionamiento
- Procedimientos de Control de Cambios S.I
- Usuarios y documentación de accesos

Puntos Vitales en una Auditoria de Sistemas

- Contratos
- Diagramas de Red
- Diagramas de interconexión de Sistemas
- Versiones de Servidores
- Estudio de Vulnerabilidades de la red

Informe de Auditoria

Objetivo

Aplicación de algunos procedimientos de auditoría en el Área de Tecnología de la Información de la Entidad, como parte integral del proceso de auditoría de los estados financieros para el año que terminó el 30 de setiembre de 2017.

Alcance

Para un mejor desempeño de este compromiso, algunos supuestos básicos se consideraron en este documento:

- Diagnóstico de alto nivel del ambiente computacional:
  - Windows Server 2012 Standard, SQL Server 2005, POS Hovisys.
- Evaluación del diseño e implementación de los controles del ambiente computacional, antes indicados para pruebas que respondan a riesgos de TI identificados, los cuales son relevantes para la Auditoría en los siguientes perfiles:
  - Seguridad de Acceso.
  - Centro de datos y operaciones de Red.
  - Cambios en los sistemas.
- Seguimiento al informe de GRA-CA del año 2016.
- Emisión de informe de GRA-CA del año 2017.

Descripción metodológica

En Deloitte lideramos las mejores prácticas de auditoría de tecnología de la información. Tenemos una metodología completa y rigurosamente probada que ha asegurado la entrega exitosa de un servicio de talla mundial. La metodología asegura:

- Un enfoque que integra el control corporativo, los objetivos del negocio, la administración del riesgo y el cumplimiento.
- Un enfoque de consultoría diseñado para crear sinergia entre nuestro equipo de auditoría interna y la Entidad.
- Recursos enfocados en áreas de alto riesgo y oportunidad.

Informe de Auditoria

- Un enfoque proactivo que señala a la administración asuntos de riesgos potenciales antes de que se conviertan en problemas.

El concepto clave de la metodología de Deloitte para la auditoría de controles de Tecnología de Información es obtener una comprensión del riesgo tecnológico asociado, para permitir un enfoque en las áreas de importancia para el negocio.

El proceso de evaluación del riesgo de Deloitte permite a las organizaciones valorar y manejar los riesgos del negocio a cada nivel de la operación, clarifica los objetivos del negocio, identifica los riesgos que pueden impedir el logro de esos objetivos, permiten la administración de esos riesgos y valora si la exposición del riesgo es aceptable.

La práctica de Deloitte responde a una oportunidad de determinar los factores de riesgo presentes en el ambiente computacional en nuestros clientes, considerando los siguientes aspectos:

Valoración de la exposición: Identifica los riesgos del negocio, analiza el impacto del riesgo en la organización y valora la efectividad de los controles.

Implementación de controles: Verifica los controles efectivos y confiables implantados por nuestros clientes para mitigar el riesgo determinado.

Administración del riesgo: Monitorea y evalúa el rendimiento de los controles y los ambientes de riesgo para determinar si los niveles de exposición son aceptables.

Informe de Auditoria

Indicaciones generales

En Deloitte lideramos las mejores prácticas de auditoría de tecnología de la información. Tenemos una metodología completa y rigurosamente probada que ha asegurado la entrega exitosa de un servicio de talla mundial. La metodología asegura:

Las oportunidades de mejora descritas en las páginas siguientes están clasificadas de acuerdo con la metodología de Deloitte, definida con base en el riesgo que representan para los recursos tecnológicos (datos, aplicaciones, plataforma tecnológica, instalaciones físicas y personal). Adicionalmente, se presenta el mapa de riesgo el cual resume la relación entre el impacto para la organización y la probabilidad de ocurrencia de eventos que comprometan la efectividad, eficiencia, confidencialidad, integridad, disponibilidad y cumplimiento de los controles implementados.

Informe de Auditoria

Los niveles de clasificación se describen a continuación:

Categorías de Riesgos

Alto (A)	Representa una deficiencia sgnificativa en los controles relacionados con la tecnología e información. Deberá ser atendido lo antes posible.
Medio (M)	Representa una deficiencia en los controles relacionados con tecnología e información. Deberá ser atendido durante los siguientes 30-180 días.
Bajo (B)	Representa una desviación en los controles relacionados con tecnología e información. Deberá ser atendido de acuerdo con la disponibilidad de tiempo de los recursos asignados por la Entidad.

Informe de Auditoria

Conclusiones de la revisión de los controles

A continuación se detallan a manera de resumen general, las oportunidades de mejora identificadas con una clasificación de nivel de riesgo segregado en tres categorías alto (A), medio (M) y bajo (B), esto para que constituya una herramienta para la priorización de los esfuerzos.

Oportunidad de mejora	Nivel de riesgo		
	Alto	Medio	Bajo
1. Bitácoras de auditoría		●	
2. Versión SQL Server		●	
3. Plan Estratégico de Tecnologías de Información		●	
4. Acceso al Xp_cmdshell		●	
5. Roles Sysadmin SQL Server			●
6. Usuarios Sistemas de información			●
7. Parámetros de contraseñas			●
8. Continuidad de negocio y contingencias informáticas			●

TECNOSERVICE CR

Gerencia estratégica de TI

Jonathan Matamoros

Director Tecnológico

+506 6010 2090 Tecnoservice Costa Rica www.tecnoservicecr.com