ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Centro de Educación Continua

"Auditoría de Controles Generales de TI"

TESIS

Previa culminación del:

DIPLOMADO DE AUDITORIA INFORMATICA

Presentado por:

Ing. Freddy Villavicencio B.

Guayaquil – Ecuador

2011

ESPOL
Escuela Superior Politécnica del Litoral

ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Centro de Educación Continua

"Auditoría de Controles Generales de TI"

TESIS

Previa culminación del:

DIPLOMADO DE AUDITORIA INFORMATICA

Presentado por:

Ing. Freddy Villavicencio B.

Guayaquil – Ecuador

2011

INDICE

INFORME DEL PROYECTO 2

Objetivo del Proyecto 2

Alcance del Proyecto 2

Metodología 2

Equipo de Trabajo 2

Observaciones Adicionales 3

PLAN Y PROGRAMA 3

Investigación preliminar 3

Evaluación de Riesgos 7

Objetivos de Auditoría 13

Áreas o componentes a auditar 13

Alcance de la Auditoría 13

Herramientas 13

Programa de Auditoría 14

INFORME DE AUDITORIA 18

INFORME DEL PROYECTO

Objetivo del Proyecto

El objetivo del presente proyecto, es el de utilizar los conocimientos adquiridos durante el Diplomado de Auditoría Informática, realizando un trabajo de auditoría en una Empresa; de manera tal, que el trabajo de auditoría sirva a dicha Empresa, para mejorar el control interno en sus tecnologías de la información.

Alcance del Proyecto

El alcance del presente proyecto es verificar si se han implementado los controles necesarios en la gestión de las tecnologías de la información, de manera tal, que garanticen de manera razonable la integridad, confidencialidad y disponibilidad de la información.

Para lo cual, se realizaran reuniones con el personal del Departamento de TI para conocer los procesos que llevan a cabo, se les solicitara documentación de dichos procesos, y de ameritar el caso, se revisara asuntos específicos en el sistema informático más importante de la Empresa.

Metodología

Para realizar el presente trabajo, se tomara como referencia el marco COBIT 4.1, y la metodología a utilizar será:

- Levantamiento de Información.
- Evaluación de Riesgos.
- Elaborar Programa de Auditoría.
- Ejecutar Programa de Auditoría.
- Elaborar borrador de Informe de Auditoría.
- Presentar borrador de Informe de Auditoría a los Auditados.
- Presentación de Informe de Auditoría al Gerente General.

Equipo de Trabajo

El trabajo de Auditoría será realizado por el Ing. Freddy Villavicencio Bermúdez.

Observaciones Adicionales

No hay observaciones adicionales.

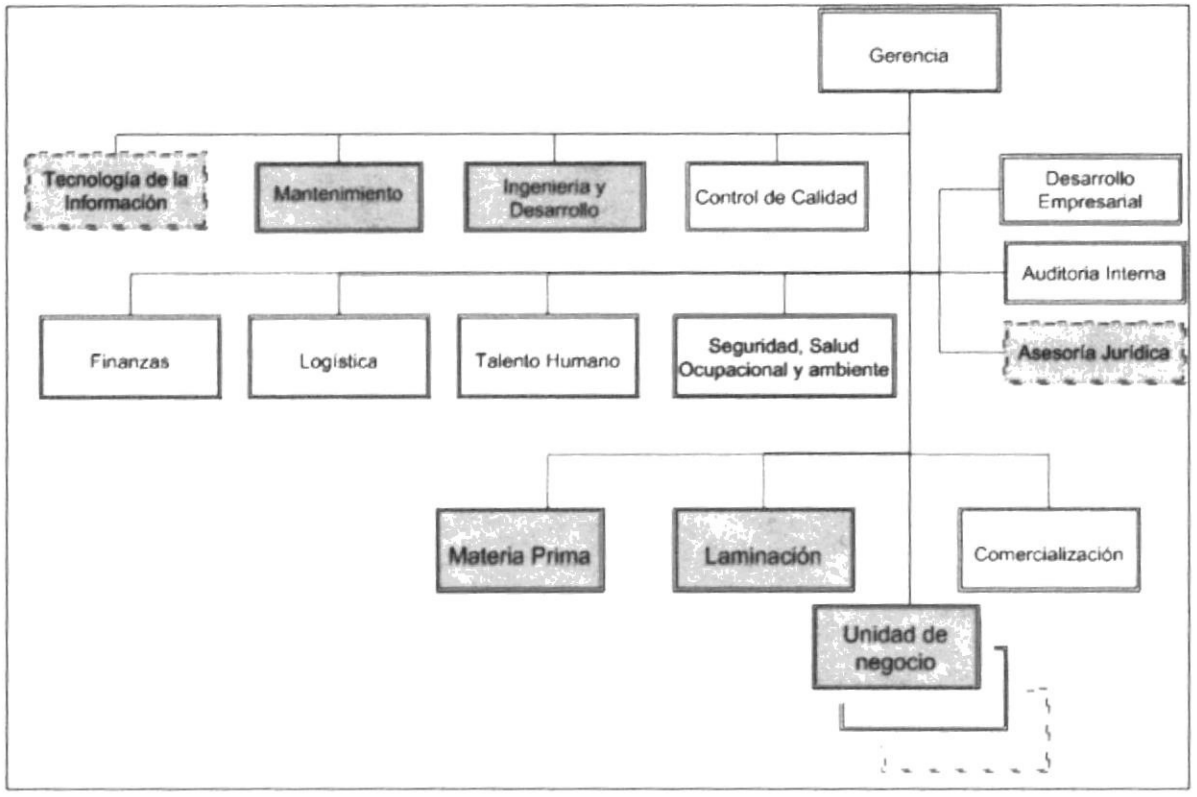
PLAN Y PROGRAMA

Investigación preliminar

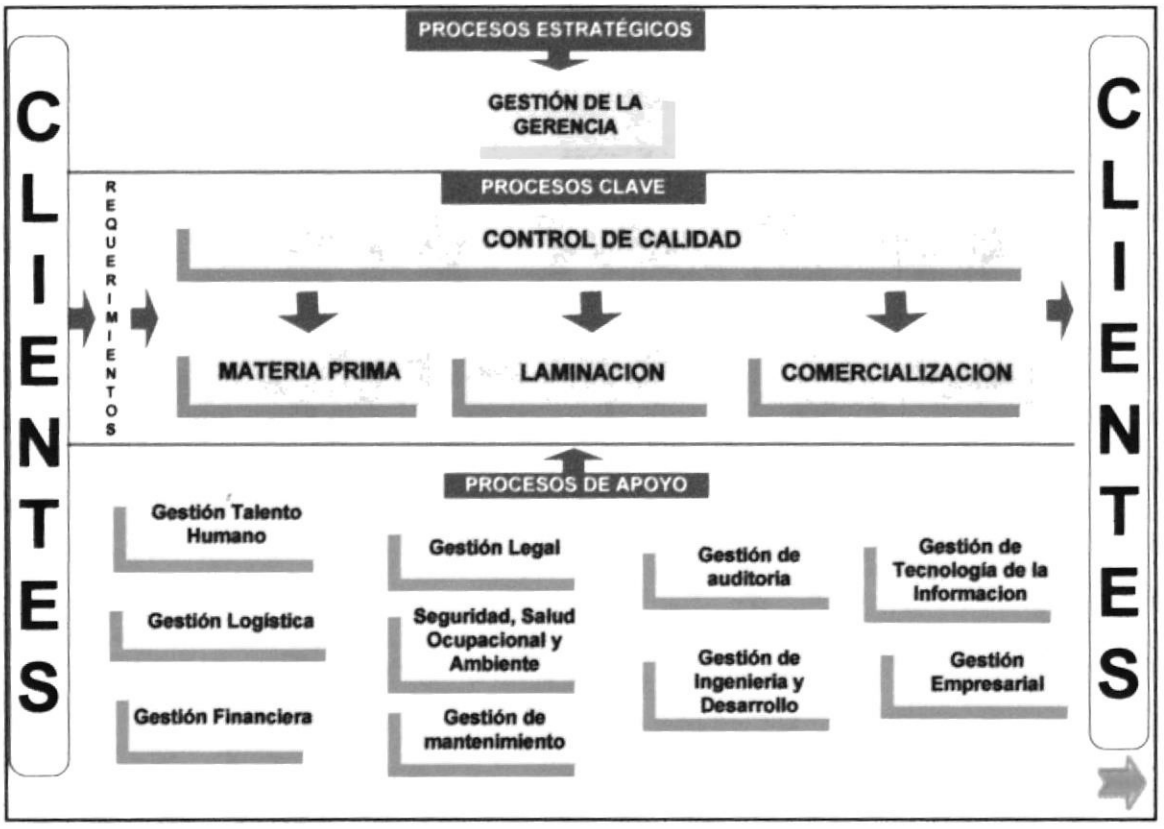
Como parte de una Corporación, la empresa Aceros del Ecuador (ACE), fue fundada en los años 60. Es una Empresa Ecuatoriana que fabrica varillas de acero para la construcción. Su matriz y planta industrial se encuentran en la ciudad de Guayaquil. También cuenta con sucursales en las ciudades de Quito y Cuenca.

La principal materia prima para la fabricación de varillas de acero, es la chatarra, por lo que ACE compra dicha materia prima a chatarreros y empresas con lotes de chatarra; siendo esta actividad, junto con las ventas y despachos de varillas, los procesos claves de esta empresa.

La empresa ACE está organizada de la siguiente manera:



En la siguiente imagen se puede observar que la compra de materia prima y la comercialización son parte de los procesos claves de la Empresa.



La Empresa cuenta con un Departamento de Tecnología de la Información, que está estructurado de la siguiente manera:

- Jefe de TI
    - Asistente Técnico.
    - Especialista de Redes.
    - Especialista de Aplicativos.
    - Especialista de Base de Datos.

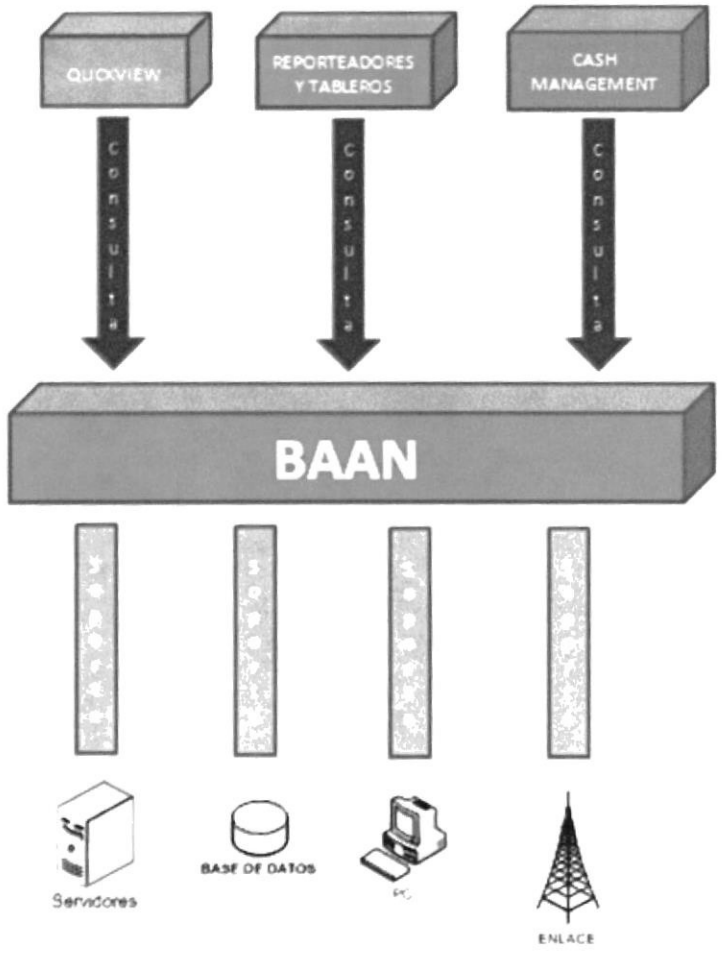
A continuación, se presenta un resumen del inventario de las tecnologías de la información de la Empresa ACE.

Activo de Información	Descripción	Importancia
Sistemas de Información		
Baan	Sistema ERP que soporta las operaciones de la Empresa.	Alta
Qlick View	Reporteador a Nivel Gerencial para tener una visión del estado de la Empresa.	Alta
Adams	Sistema para la Administración del Recurso Humano.	Media
Reporteadores y Tableros	Reporteadores desarrollados por el Departamento de TI para las diferentes Gerencias.	Alta
Cash Management	Aplicación Web de los bancos para realizar consultas y pagos a Proveedores Online	Alta
Balance Score Card	Control de cumplimiento de metas a nivel de compañía, empleados y proceso.	Media
9000 Doc	Descripción de los Procesos de la Empresa.	Baja
Tecnología de Información		
Servidores (10)	Base de Datos, Aplicaciones, Internet, Antivirus, Correo, BSC, Relojes Biométricos.	Alta
Enlaces	A bases de datos, internet, video conferencia, otros.	Alta
Computadores (225)	Para el uso de Trabajadores	Alta
Redes (Física e inalámbricas)	Comunicación	Alta

Los reporteadores y tableros gerenciales son desarrollados por el Departamento de TI, utilizando PowerBuilder y Oracle.

El sistema BAAN ERP fue comprado a la compañía Novatech, e implementado en Junio del 2008. Es el sistema de información más importante de la Empresa, ya que el mismo soporta las operaciones. En dicho sistema, se registran las ventas, compras, contabilidad, pagos, etc.

Los otros sistemas que tienen una importancia alta, dependen de la información que se genera en el BAAN. A continuación, se observa una gráfica de cómo el inventario de TI interactúa con el sistema BAAN:


QUICKVIEW
REPORTEADORES Y TABLEROS
CASH MANAGEMENT
consulta
consulta
consulta
BAAN
Servidores
BASE DE DATOS
ENLACE

Evaluación de Riesgos

1. Objetivo

El objetivo de la Evaluación de Riesgos, es identificar los riesgos generados por aquellas debilidades detectadas durante el levantamiento de información; valorar el impacto sobre los objetivos y continuidad del negocio y orientar la auditoria hacia los riesgos más importantes.

2. Calificación del riesgo

Para determinar si un riesgo identificado es alto, medio o bajo, se utilizan los siguientes criterios:

- *Frecuencia:*
  Se refiere a la frecuencia con la que sucede o se manifiesta la debilidad identificada.

- *Materialidad:*
  Se refiere al perjuicio económico que puede ocasionar el riesgo identificado.

- *Impacto:*
  Se refiere al impacto que tiene el riesgo, sobre el logro de objetivos y la continuidad del negocio. Se obtiene multiplicando la frecuencia y la materialidad. A continuación, se presenta los rangos de impacto, para calificar los riesgos:

Nivel	Rango
Alto	6 - 9
Medio	3 - 5
Bajo	1 - 2

3. Matriz de Evaluación de Riesgos

Sec	Debilidad	Riesgo	Frecuencia	Materialidad	Impacto	Nivel de Riesgo
Seguridad de TI						
1	No existen políticas de seguridad de la información, tampoco nada que haga referencia a la seguridad informática.	Riesgo de accesos indebidos en los activos de información, ocasionando pérdidas económicas por fraudes, e incluso riesgo de afectar la continuidad del negocio.	3	3	9	ALTO
2	No existe un Sistema de Gestión de Seguridad de la Información (SGSI), que permita la preservación de la confidencialidad, integridad y disponibilidad de la información en todas sus formas (digital, escrita y verbal).	1. Fraudes, debido a permisos indebidos en el sistema BAAN ERP, ya que los mismos son asignados por los Usuarios Claves a Usuarios Finales del mismo proceso. 2. Que la seguridad de la información sea considerada como un aspecto exclusivo de la Jefatura de Tecnología de la Información de ACE y no extender dicha responsabilidad a todas las áreas de la Empresa. 3. Que la Gerencia General no conciba a la Seguridad de la Información como un área estratégica del negocio; por lo tanto, la estrategia de seguridad de la información no va a ser compatible con la estrategia del negocio. 4. Que no se informe a los niveles directivos, los problemas críticos relacionados con la seguridad de la información.	3	2	6	ALTO

Sec	Debilidad	Riesgo	Frecuencia	Materialidad	Impacto	Nivel de Riesgo
3	Usuarios Claves han asignado las restricciones en los diferentes módulos del sistema. Dichos Usuarios Claves, tienen opciones para crear, modificar o eliminar accesos en el sistema BAAN. Gerente General indica que Auditoria Interna a reportado varios accesos indebidos en el sistema.	Accesos indebidos en el sistema, que pueden provocar fraudes.	3	3	9	ALTO
4	La puerta de entrada y las paredes interiores del Centro de Cómputo son de vidrio. En la entrada, existe un dispositivo para ingresar una clave de acceso; sin embargo, se observa que el mismo no se utiliza. También se observa que existen ventanas al exterior, que dan a un parqueadero.	Que personas no autorizadas, ingresen al Centro de Cómputo, y afecten la información de la Empresa y su disponibilidad, causando pérdidas económicas.	3	3	9	ALTO

Sec	Debilidad	Riesgo	Frecuencia	Materialidad	Impacto	Nivel de Riesgo
Operaciones de TI						
5	No existe evidencia de que se monitoree la capacidad de la infraestructura de TI (comunicaciones y servidores); sin embargo, personal de TI manifiesta que si se realiza. Se observa que se disponen de herramientas para monitorear la capacidad; sin embargo, en el caso de los servidores no permite obtener datos históricos para realizar proyecciones.	No disponibilidad de los sistemas de información debido a la falta de capacidad de la infraestructura, lo que afectaría la continuidad del negocio y produciría perdidas económicas.	2	3	6	ALTO
6	Las aplicaciones se desarrollan directamente sobre la base de datos. Es decir, que el ambiente de desarrollo y pruebas no está separado del ambiente de producción.	Que se inserte, modifique o elimine información de la base de datos, para cometer fraudes o afectar la continuidad del negocio.	3	3	9	ALTO

Sec	Debilidad	Riesgo	Frecuencia	Materialidad	Impacto	Nivel de Riesgo
7	Los requerimientos de Usuarios Finales son registrados en el sistema de HelpDesck, por el personal de TI, quienes manifiestan que no siempre ingresan todos, o los ingresan días después.	Que se afecten los indicadores de desempeño concerniente a la atencion de requerimiento de Usuarios Finales, al ingresar tiempos de solución errados.	2	1	2	BAJO
8	No existen políticas, procedimientos y funciones de manera formal, que obliguen a la ejecución de controles en la gestión de TI. Sin embargo, se está en proceso de formalizarlos. Jefe de TI presenta borradores recientemente creados.	Riesgo de errores o fraudes que afecten a la continuidad del negocio o que produzcan perdidas económicas importantes.	3	3	9	ALTO
Continuidad del Negocio						
9	No existen planes de continuidad del negocio. Sin embargo, si se sacan copias de base de datos y aplicaciones.	Que la continuidad del negocio se vea afectada, por la falta de respuesta oportuna ante un evento de desastre.	3	3	9	ALTO

Sec	Debilidad	Riesgo	Frecuencia	Materialidad	Impacto	Nivel de Riesgo
10	Los respaldos de base de datos son almacenados en el baño de la oficina del Jefe de TI, el cual es utilizado como bodega. Estos respaldos se encuentran junto al lavamanos, el cual presente humedad por el reciente uso.	Que los respaldos sufran daños, por lo que existe el riesgo de que no puedan ser utilizados ante un evento de desastre, afectando la continuidad del negocio.	3	3	9	ALTO

Objetivos de Auditoría

Atendiendo la preocupación manifestada por el Gerente General de la Empresa, sobre los accesos indebidos reportados por Auditoría Interna, el objetivo de la presente auditoría, es el verificar que se han implementado los controles necesarios en la gestión de las tecnologías de la información de la Empresa, de manera tal, que garanticen de manera razonable la integridad, confidencialidad y disponibilidad de la información.

Áreas o componentes a auditar

El área a auditar será el Departamento de Tecnología de la Información.

Alcance de la Auditoría

El alcance de la presente auditoría, es verificar si se han implementado los controles necesarios en la gestión de las tecnologías de la información, de manera tal, que garanticen de manera razonable la integridad, confidencialidad y disponibilidad de la información.

Para lo cual, se realizaran reuniones con el personal del Departamento de TI para conocer los procesos que llevan a cabo, se les solicitara documentación de dichos procesos, y de ameritar el caso, se revisara asuntos específicos en el sistema informático más importante de la Empresa.

Herramientas

Los programas a utilizar para la presente auditoría son:

- Word 2007/2010: Procesador de Texto.
- Excel 2007/2010: Hoja de Cálculo.
- PDF Creator : Creación de archivos PDF.
- BAAN ERP : Sistema ERP utilizado por la Empresa.
- SQL PLUS : Consultas a la Base de Datos.

Programa de Auditoría

Acogiendo la preocupación del Gerente General, sobre los accesos indebidos reportados por Auditoría Interna, el objetivo es evaluar los controles generales implementados en la gestión de las tecnologías de la información de la Empresa, para verificar si se garantiza de manera razonable la integridad, confidencialidad y disponibilidad de la información. Se toma como marco referencial COBIT 4.1.

No.	Descripción
	Planear y Organizar
PO2 – Definir la arquitectura de la Información.	
	Solicitar a Jefe de TI, políticas y procedimientos de seguridad, referentes a la integridad de los datos en medios digitales.
	Revisar que en la red interna, no se encuentre compartida información sensible.
	Revisar si existe un esquema de clasificación de datos.
PO8 –Administrar la Calidad.	
	Obtener el documento formal de los estándares de codificación de software. Verificar si en el último desarrollo se ha cumplido con el estándar de codificación.
	Revisar si se mantiene un diccionario de datos para el desarrollo y mantenimiento de los sistemas informáticos.
	Obtener evidencia de que los resultados de pruebas de implementaciones o cambios de sistemas informáticos son aceptados por Usuarios finales.
PO9 –Evaluar y Administrar los riesgos de TI.	
	Solicitar a Jefe de TI, las evaluaciones de riesgo sobre los activos de información de la Empresa.
	Evaluar que la Evaluación de Riesgo se ha realizado sobre los activos críticos de TI, los mismos que afectan a la Continuidad del Negocio.
	Solicitar a Jefe de TI, los Planes de Acción en respuesta a la Evaluación de Riesgos y evaluar que el mismo se mantiene y monitorea.
	Evaluar los controles implementados para mitigar los riesgos identificados en la

No.	Descripción
	evaluación.
	Adquirir e Implementar
AI2 – Adquirir y Mantener Software Aplicativo.	
	Solicitar a Jefe de TI, procedimiento para la compra de software.
	Solicitar a Jefe de TI, el procedimiento para las customizaciones del Baan (cambios), tanto para controles y funcionales.
	Solicitar a Jefe de TI, los procedimientos para administrar la seguridad de las aplicaciones (asignación de permisos, nuevos usuarios, eliminación de usuarios).
	Solicitar a Jefe de Talento Humano, listado de las personas que han salido durante el 2011, y verificar que sus usuarios están desactivados.
	Verificar que se ejecutan procedimientos para que el ambiente de pruebas sea igual al ambiente de producción, durante la etapa de pruebas.
	Verificar que el ambiente de desarrollo y pruebas, está separado del ambiente de producción. Monitorear las conexiones a la base de datos y verificar que no existen conexiones a través de herramientas de desarrollo.
AI4 – Facilitar la operación y el uso.	
	Solicitar a Jefe de TI, los manuales del sistema BAAN.
	Solicitar a Jefe de TI, el Plan de Entrenamiento Inicial para Usuarios Finales BAAN.
	Evaluar el soporte a Usuarios (helpdesk): • Revisar si se categorizan los problemas, según prioridad. • Revisar si se lleva una bitácora de los problemas, que incluya la hora en la que se presentan y la hora en la que se resuelven. • Verificar que el tiempo de solución, sea incluido en los indicadores de desempeño. • Revisar si se sacan datos estadísticos, para identificar donde se presentan la mayor cantidad de problemas.

No.	Descripción
	Verificar que se tenga formalizado el alcance de los Usuarios Clave, ya sea a través de políticas o disposición.
AI6 – Administrar Cambios.	
	Solicitar a Jefe de TI, procedimientos para los cambios de aplicaciones.
	Revisar que las customizaciones de BAAN, hayan sido aprobadas por el dueño del proceso.
	Verificar que en los procedimientos de cambios, se considere el cierre de los mismos y la actualización de manuales y procedimientos.
Entregar y dar soporte	
DS1 – Definir y administrar los niveles de servicio.	
	Verificar si se tiene identificado los servicios que presta el Departamento de TI a la empresa, a través de un Catálogo de servicios.
	Revisar que en el Catálogo de Servicios exista la definición del servicio, características, requerimiento del negocio y fuente de financiamiento para los SLAs y OLAs.
	Evaluar que los SLA'S cubren los procesos críticos de TI.
	Solicitar a Jefe de TI, las evaluaciones periódicas de cumplimiento de los SLAs y OLAs, tanto de Clientes Interno y Proveedores.
DS2 – Administrar los servicios de terceros.	
	Solicitar a Jefe de TI, evidencia de que se han mitigado los riesgos de la habilidad de los Proveedores para la entrega del servicio.
	Solicitar a Jefe de TI, los acuerdos de Confidencialidad con Novatech, Akros y Telconet. En caso de que no los tenga, revisar los contratos con dichas compañías, para verificar si existen cláusulas de acuerdos de confidencialidad.
DS3 – Administrar el desempeño y la capacidad.	
	Obtener evidencia de que se monitorea la capacidad de las comunicaciones (redes) y uso de servidores (cpu, memoria, espacio en disco).

No.	Descripción
DS4 – Garantizar la continuidad del servicio.	
	Solicitar a Jefe de TI, el Plan de Continuidad (Plan de Contingencia, Plan de Recuperación).
	Revisar que en los Planes de Continuidad, se detallan roles, procedimientos, procesos de comunicación, enfoque de pruebas.
	Evaluar la prueba periódica de los Planes de Contingencia y Recuperación.
	Verificar que se sacan respaldos periódicos de la base de datos.
DS5 – Garantizar la seguridad de los sistemas.	
	Revisar que no existen Usuarios Genéricos en el Sistema BAAN y su Base de Datos.
	Solicitar a Jefe de TI, procedimientos para la Administración de Cuentas de Usuarios.
DS9 – Administrar la configuración.	
	Verificar si se mantienen registros de las configuraciones actuales de la infraestructura de TI.
DS12 – Administración del ambiente físico.	
	Verificar que existen restricciones de acceso al Centro de Cómputo.
	Verificar que se mantiene un registro de los accesos al Centro de Cómputo.
	Verificar que se han implementado equipos de monitoreo ambiental para la temperatura, humedad, fuego.
Monitorear y Evaluar	
ME1 – Monitorear y Evaluar el desempeño de TI.	
	Evaluar los KPI'S del Departamento de TI, y determinar si son los apropiados.
	Revisar si se han ingresado a tiempo los KPI'S.

INFORME DE AUDITORIA

Informe de Auditoría

Auditoría de Sistemas a los controles generales de las Tecnologías de la Información de ACE S.A.

Septiembre 28, 2011

INFORME DE AUDITORIA

Ing.
Fernando Herrera C.
Gerente de ACE S.A.

De acuerdo con lo acordado con Usted, hemos realizado una Auditoría de Sistemas a los controles generales de las Tecnologías de la Información de ACE S.A., vigentes a Septiembre del 2011; con el propósito de evaluar si dichos controles garantizan de manera razonable la integridad, confidencialidad y disponibilidad de la información de la Empresa.

Nuestro trabajo se realizó en base al marco referencial COBIT 4.1, que se refiere a los controles para la información y la tecnología relacionada; y aplicando Normas de Auditoría de Sistemas de Información, promulgadas por la Asociación para el Control y Auditoría de los Sistemas de Información (ISACA) y Normas Internacionales de Auditoría y Aseguramiento (NIAA), vigentes en el Ecuador. Estas normas requieren entre otras cosas, el diseño y desarrollo de pruebas de auditoría apropiadas, para cumplir con el objetivo de la misma; incluyendo la obtención de evidencia suficiente y competente, para sustentar nuestros hallazgos.

La responsabilidad de mantener controles adecuados en las Tecnologías de la Información de ACE, corresponde al Jefe de Tecnología de la Información. La responsabilidad del Auditor Informático, consiste en revelar aspectos relevantes observados durante su examen.

I. Alcance

El alcance de nuestra revisión, consistió en:

a) Levantamiento de información sobre la estructura de las Tecnologías de la Información y sus procesos.

b) Evaluar políticas y procedimientos vigentes del Departamento de Tecnología de la Información de ACE.

c) Evaluar políticas y procedimientos de seguridad de la información.

d) Revisar la evaluación de Riesgos sobre los activos de Tecnología de la Información, y sus planes de acción.

e) Evaluar los procesos de desarrollo, pruebas, cambios e implementación de aplicativos.

f) Evaluar la administración del desempeño y capacidad de la infraestructura de TI.

g) Evaluar la gestión de soporte a los Usuarios.

h) Evaluar la seguridad de la información que se comparte en la red interna.

i) Evaluar las seguridades del Centro de Cómputo, donde se encuentran servidores y demás dispositivos que permiten la disponibilidad de los sistemas de información.

j) Revisar que los Usuarios de BAAN y de Base de Datos de ex trabajadores, estén desactivados.

k) Evaluar los indicadores de desempeño del Departamento de Tecnología de la Información, que se encuentran registrados en el sistema Strategy Link.

l) Evaluar el Plan de Continuidad de Tecnología de la Información.

II. Niveles de riesgo de los hallazgos de auditoría

Los hallazgos de auditoría informados como oportunidades de mejora, se clasifican en cuatro categorías de riesgo, en base a las buenas prácticas de una adecuada Administración del Riesgo. Estas categorías de riesgo buscan apoyar a la Alta Gerencia en la identificación de los riesgos y en la priorización e implantación de las recomendaciones de Auditoría. A continuación presentamos un cuadro, en donde se describe en que situaciones se considera cada categoría de riesgo:

CATEGORIA	DESCRIPCION DEL RIESGO	ACCION
ALTO (A)	• Ha ocurrido o hay peligro directo que un evento pueda ocasionar paralización temporal o definitiva del negocio. • Tanto los incumplimientos de normativas legales e internas como buenas prácticas y las deficiencias en el control interno hallados son de seria importancia. • Las actividades de esta categoría incluyen posibilidad de daños catastróficos y críticos, fraudes o pérdidas humanas, pérdidas financieras altas , afectaciones a la información confidencial de la Empresa y litigios legales	• Estos riesgos son tan significativos para la entidad que requieren la atención inmediata de la Gerencia y la máxima prioridad en buscar una solución. • La Empresa debe considerar la posibilidad de eliminar o modificar las actividades que tienen luego de aplicar todas las estrategias de gestión de riesgo razonable.
MODERAMENTE ALTO (MA)	• Ha ocurrido o hay peligro directo de actos fraudulentos o ilegales • La Empresa puede ser objeto de litigios. • Puede ocasionar daños personales graves, daños materiales importantes, pérdida financiera considerable y/o publicidad negativa para la organización.	• La materialidad de estos riesgos es de tal importancia para la entidad que se requiere la pronta atención de la Gerencia para determinar las contingencias existentes a la fecha y acordar un catálogo de medidas y acciones que logre una rápida resolución de los riesgos identificados y ofrezca la seguridad de que no se volverá a incurrir en las mismas en el futuro. • Se aconseja aplicar estrategias proactivas de gestión de riesgos para reducir el riesgo. La Empresa debe considerar la manera de modificar o eliminar los riesgos inaceptables.
MODERADO (M)	• Puede ocasionar daños personales menores, daños materiales, pérdida financiera y/o publicidad negativa para la organización.	• Las actividades de esta categoría contienen algún nivel de riesgo que probablemente no suceda. La Empresa debe considerar qué se podría hacer para gestionar el riesgo y evitar resultados negativos.
BAJO (B)	• El peligro representa una amenaza mínima a la seguridad y normal funcionamiento de la organización. • El riesgo relacionado con las actividades auditadas no presenta actualmente materialidad pero puede llegar a presentarla cuando se incrementen dichas actividades.	• Las actividades de esta categoría contienen un riesgo mínimo que probablemente no suceda. La Empresa puede continuar con estas actividades, de acuerdo con lo planificado. • Estos riesgos no necesariamente requieren atención inmediata, pero la Gerencia debe estar atenta a la solución de los mismos para mejorar el sistema de control interno

III. Conclusión

En nuestra opinión, los controles y procesos implementados en las Tecnologías de la Información de ACE S.A., ***no garantizan*** la integridad, confidencialidad y disponibilidad de la información de la Empresa; debido a que: Las seguridades del Centro de Cómputo son muy deficientes; no existen planes de contingencia y recuperación en el caso de ocurrencia de eventos de desastres; el ambiente de desarrollo y pruebas no está separado del ambiente de producción, y otras debilidades, que detallamos en los *Anexos 1 al 6,* adjuntos.

Durante nuestra auditoría, observamos que el Departamento de Tecnología de la Información, lleva a cabo un plan de mejora en sus procesos; sin embargo, consideramos que por los riesgos existentes, se debe dar prioridad a aquellos controles y procesos que garanticen la continuidad del negocio.

Queremos agradecer al personal del Departamento de Tecnología de la Información, por la colaboración brindada durante nuestro trabajo.

Atentamente,

Ing. Freddy Villavicencio
Auditor Informático

cc: File

INDICE

Descripción	Anexo No.
a. Debilidades en la gestión de la Seguridad de la Información	1
• Falta de un Sistema de Gestión de Seguridad de la Información.	
• Falta de Políticas de Seguridad de la Información.	
• Falta de Acuerdos de Confidencialidad.	
• Debilidades en las seguridades del Centro de Cómputo.	
• Debilidades en la seguridad de la información en la red.	
• Inadecuado almacenamiento de los respaldos de Base de Datos.	
• Existencia de Usuarios Genéricos en el sistema BAAN.	
• Usuarios Activos de personas que ya no laboran en la Empresa.	
• Falta de un esquema de clasificación de datos.	
b. Debilidades en la gestión de riesgos	2
• Falta de Evaluación de Riesgos.	
c. Debilidades en la administración de los servicios de TI	3
• Falta de Catálogo de Servicios.	
• Debilidades en el registro de problemas.	
• Debilidades en el monitoreo de la capacidad de la infraestructura.	
• Falta de registros de configuración de hardware y software.	
d. Debilidades en la gestión de Aplicativos	4
• Debilidades en el desarrollo de aplicativos.	
• Debilidades en el alcance de responsabilidad de los Usuarios Claves.	
• Ambiente de pruebas diferente al ambiente de producción.	

INDICE

Descripción	Anexo No.
• Falta de control de los cambios.	
e. **Debilidades en Planes de Continuidad**	5
• Falta de un Plan de Continuidad del Negocio.	
f. **Debilidades en Indicadores de Desempeño (KPI'S)**	6
• Debilidades en los indicadores de desempeño del Departamento de Tecnología de la Información.	

* * * *

REF.	RIESGO	1. DEBILIDADES EN LA GESTION DE LA SEGURIDAD DE LA INFORMACION
1.1	A	**FALTA DE UN SISTEMADE GESTION DE SEGURIDAD DE LA INFORMACION** ACE no cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI), que permita la preservación de la confidencialidad, integridad y disponibilidad de la información en todas sus formas (digital, escrita y verbal). Un adecuado SGSI, protege la información de una serie de amenazas; y evita que las mismas, afecten la continuidad del negocio y el logro de objetivos. Actualmente, solo se gestiona la seguridad dela información que es procesada a través de los sistemas computacionales; gestión que es compartida entre el Departamento de Tecnología de la Información y los Usuarios Claves de los diferentes procesos. Debido a esta situación, existen el riesgo de: 1. Fraudes, debido a permisos indebidos en el sistema BAAN ERP, ya que los mismos son asignados por los Usuarios Claves a Usuarios Finales del mismo proceso. 2. Que la seguridad de la información sea considerada como un aspecto exclusivo de la Jefatura de Tecnología de la Información de ACE y no extender dicha responsabilidad a todas las áreas de la Empresa. 3. Que la Gerencia General no conciba a la Seguridad de la Información como un área estratégica del negocio; por lo tanto, la estrategia de seguridad de la información no va a ser compatible con la estrategia del negocio. 4. Que no se informe a los niveles directivos, los problemas críticos relacionados conla seguridad de la información. **COMENTARIO DELJEFE DE TECNOLOGIA DE LA INFORMACION** Me parece que está bien, y de hecho dentro de la consultoría que he solicitado, se está contemplando esto. **RECOMENDACION** **Responsables:Gerencia General yDepartamento de Tecnología de la Información** Por la cantidad y complejidad de los procesos, por los recursos informáticos que son utilizados por varios Usuarios y por la aplicación de buenas prácticas de Gobierno Corporativo; se recomienda implementar un Sistema de Gestión de la Seguridad de la Información en ACE; en base a los estándares generalmente aceptados(ISO 27001 y 27002).

REF.	RIESGO	1. DEBILIDADES EN LA GESTION DE LA SEGURIDAD DE LA INFORMACION
1.2	MA	**FALTA DE POLITICIAS DE SEGURIDAD DE LA INFORMACION** Observamos que no existe ninguna política que se refiera a la seguridad de la información, ya sea esta digital, escrita o verbal. Una política de seguridad de la información, incluye la seguridad informática (digital), la cual cubre varios aspectos como la información que se almacena en medios digitales, uso de dispositivos móviles, restricciones durante el desarrollo de aplicaciones, seguridad de contraseñas, restricciones de usuarios, comunicaciones, entre otros. La seguridad informática se gestiona en base al juicio del personal del Departamento de Tecnología de la Información, y no en base a los requerimientos de seguridad de la Empresa. Las políticas de seguridad informática deben ser parte de las políticas de seguridad de la información, y deben sustentarse en una evaluación de riesgos,para identificarcuáles son las amenazas y vulnerabilidades a los que se exponen los activos de información de ACEy la tecnología que soporta su procesamiento. **COMENTARIO DEL JEFE DE TECNOLOGIA DE LA INFORMACION** La consultoría nos va ayudar bastante en esta situación, que incluye la validación del borrador de la política. Una vez aprobada la vamos aplicar. **RECOMENDACION** **Responsables: Departamentos de Tecnología de la Información y Desarrollo Empresarial** Se recomiendadesarrollar y poner a consideración de la Gerencia General, una Política de Seguridad de la Información basada en estándares de general aceptación, considerando principalmente los riesgos a los que enfrenta la entidad y los controles que deben implementarse para asegurar la integridad, disponibilidad y confidencialidad de la información administrada.
1.3	MA	**FALTA DE ACUERDOS DE CONFIDENCIALIDAD** No se realizan acuerdos de confidencialidad de la información de la Empresa, con Proveedores ni conTrabajadores de ACE. Los acuerdos de confidencialidad, ayudan a garantizar que la información crítica del negocio se mantenga de manera confidencial. **COMENTARIO DEL JEFEDE TECNOLOGIA DE LA INFORMACION** No existe, y se va a implementar en coordinación con Asesoría Jurídica.

REF.	RIESGO	1. DEBILIDADES EN LA GESTION DE LA SEGURIDAD DE LA INFORMACION
		RECOMENDACION **Responsable:Departamento de Tecnología de la Información** Que se implementen políticas, en la cuales se indique la obligatoriedad de la firma de Acuerdos de Confidencialidad, tanto con Proveedores como con Trabajadores de ACE.
1.4	A	**DEBILIDADES EN LAS SEGURIDADES DEL CENTRO DE COMPUTO** El 30 de Agosto del 2011, realizamos una visita al Centro de Cómputo de ACE, donde se encuentran los servidores y demás dispositivos que permiten la disponibilidad de los sistemas informáticos, y observamos debilidades críticas en la seguridad de dicho Centro, que mencionamos a continuación: 1. No existen mecanismos que restrinja el acceso al Centro de Cómputo, de personas no autorizadas. Actualmente, existe colocado un dispositivo en la puerta de acceso a dicho Centro, para ingresar con contraseña; sin embargo, el mismo estáinactivo. 2. La puerta de acceso al Centro de Cómputo, y paredes interiores son de vidrio; por tal motivo, existe el riesgo de que personas no autorizadas pueden acceder con facilidad a dichoCentro de Cómputo. 3. Debido a que el techo del Centro de Cómputo y el techado exterior que da al parqueadero del Bloque B, utilizan cielo raso, existe el riesgo de que personas no autorizadas y/o ajenas a la Empresa, ingresen por esta vía al Centro de Cómputo. 4. El Centro de Cómputo cuenta con ventanas que dan al parqueadero del Bloque B. Durante nuestra revisión, observamos que una de ellas estaba abierta, quedando expuestos los servidores y demás equipos. 5. Los dos extintores que se encuentran en las afueras del Centro de Cómputo, están caducados desde el 12 de Agosto del 2011; motivo por el cual, durante un incendio podrían no funcionar correctamente. 6. No existen mecanismos automáticos que permitan extinguir un incendio en horarios no laborables. 7. Existen cables de electricidad y equipos de redes en el piso, que no cuentan con algún orden ni protección. 8. El cajetín en el cual se encuentran los cables de red y de fibra óptica, se encuentran abiertos y sin ninguna protección.

REF.	RIESGO	1. DEBILIDADES EN LA GESTION DE LA SEGURIDAD DE LA INFORMACION
		9. Existe un servidor, cuyo CPU se encuentra abierto, por lo que está expuesto a gran cantidadde polvo y suciedad existente en dicho Centro. 10. En las paredes se observan huellas de humedad. Las debilidades antes expuestas, representan un riesgo para la continuidad del negocio, ya que se compromete la integridad, confidencialidad y disponibilidad de la información de ACE. ***Ver Anexo 1-A.*** **COMENTARIO DEL JEFEDE TECNOLOGIA DE LA INFORMACION** La suciedad del Centro de Cómputo se debe a un trabajo que realizó el Departamento de Mantenimiento y Adecuaciones en el cielo raso, y no dejaron limpio después de terminar el mismo. Ya les solicité que limpien el Centro de Cómputo y que sellen las ventanas. También se hizo una solicitud a la empresa Akros, para que se instalen canaletas en el Centro de Cómputo. **RECOMENDACION** **Responsable:Departamento de Tecnología de la Información** Que se implementen mejoras en la seguridad del Centro de Cómputo, tal como lo establecenlas normas y estándares de seguridad de la información, generalmente aceptados.
1.5	**MA**	**DEBILIDADES EN LA SEGURIDAD DE LA INFORMACION EN LA RED** En la red interna de ACE, se encuentra sin ninguna seguridad y disponible, información y recursos sensibles de la Empresa; tales como: Balances Generales, datos de producción y proyectos, instaladores de BAAN, herramientas para el desarrollo de aplicaciones, entre otros. ***Ver Anexo 1-B.*** Esto se debe, a que no existen políticas y procedimientos que permitan garantizar la seguridad de la información almacenada en medios digitales. **COMENTARIO DEL JEFEDE TECNOLOGIA DE LA INFORMACION** Se revisara todos los equipos en donde exista información compartida. Se identificará la necesidad de copias en dispositivos externos y documentar los Usuarios que lo requieran con la debida aprobación de sus Jefes y los equipos que lo puedan hacer; y luego a proceder a deshabilitar de los equipos esa facilidad.

REF.	RIESGO	1. DEBILIDADES EN LA GESTION DE LA SEGURIDAD DE LA INFORMACION
		RECOMENDACION **Responsable:Departamento de Tecnología de la Información** Que se implementen políticas y procedimientos formales de seguridad, para proteger la información que se encuentra en medios digitales.
1.6	**A**	**INADECUADO ALMACENAMIENTO DE RESPALDOS DE BASE DE DATOS** Observamos quelos respaldos de las bases de datos, son almacenados en el baño de la oficina delJefe de Tecnología de la Información, junto al lavamanos. Es decir, que se almacenan de manera inapropiada y en un lugar inseguro; por lo que existe el riesgo de que dichos respaldos sufran daños, sean sustraídos o usados indebidamente, poniendo en riesgo la continuidad del negocio ante un evento de desastre. ***Ver Anexo 1-C.*** **COMENTARIO DEL JEFEDE TECNOLOGIA DE LA INFORMACION** El baño solo se utiliza como bodega; ya solicité al Jefe de Mantenimiento y Adecuaciones, para que el baño se lo adecúe como bodega con todas las seguridades. **RECOMENDACION** **Responsable:Departamento de Tecnología de la Información** Que se almacenen los respaldos enlugares adecuados, que garanticen la seguridad y disponibilidad de dichos respaldos, ante un evento de desastre.
1.7	**MA**	**EXISTENCIA DE USUARIOS GENERICOS EN EL SISTEMA BAAN** Observamos que existen 11 Usuarios Genéricos en el sistema BAAN de ANDEC y 49 en la base de datos. Dichos Usuarios no se refieren a ninguna persona y en algunos casos, estos son utilizados por distintas personas. De los Usuarios de Base de Datos, 43 (88%) tienen contraseñas con un nivel de seguridad muy débil. El mantener usuarios genéricos debilita la estructura del control interno puesto que no existe un responsable específico de estos usuarios; adicionalmente, en caso de existir accesos no autorizados se dificulta el proceso de identificación oportuno de quien ejecutó dichos accesos. ***Ver Anexo 1-D.*** Debido a esta situación, existe el riesgo de que personas mal intencionadas descifren fácilmente las contraseñas de estos Usuarios y accedan al sistema BAAN o a su base de datos, afectando la integridad, confidencialidad, confiabilidad y disponibilidad de la información de ACE.

REF.	RIESGO	1. DEBILIDADES EN LA GESTION DE LA SEGURIDAD DE LA INFORMACION
		COMENTARIO DEL JEFEDE TECNOLOGIA DE LA INFORMACION Esto se corregirá de manera inmediata. **RECOMENDACION** **Responsable:Departamento de Tecnología de la Información** Desarrollar e implementar una política que controle que cada Usuario cuente con un identificador único que pueda ser reconocido por los sistemas de información, y que cada identificador de usuario corresponderá a una persona física; por lo tanto, esta persona es la única autorizada a utilizarlo; sin embargo, como excepción a la política y de manera autorizada por la Jefaturade Tecnología de la Información, se podrá definir y utilizarse Usuarios Genéricos siempre y cuando exista un responsable de este usuario,al que se le imputará la responsabilidad de todas las operaciones realizadas, independientemente de la persona física que lo haya ejecutado.
1.8	A	**USUARIOS ACTIVOS DE EX TRABAJADORES DE LA EMPRESA** Aún se encuentran activos, los Usuarios de acceso al sistema BAAN, de 11 personas de los 44 ex Trabajadores que fueron separados de la Empresa durante el año 2011 (25%). También, observamos que existen12 Usuarios activos de la Base de Datos, de personal que fue separado de la Empresa, durante los años 2010 y 2011. ***Ver Anexo 1-E.*** **COMENTARIO DEL JEFEDE TECNOLOGIA DE LA INFORMACION** En Base de Datos esto ya fue solucionado hace poco. **COMENTARIO DEL ADMINISTRADOR DEL BAAN** Esto sucede porque en ocasiones el Departamento de Talento Humano no envía un correo indicando que una persona ha dejado de laborar en la Empresa. En este caso, no se nos informó sobre estos Usuarios. **RECOMENDACIONES** **Responsables:Departamento de Tecnología de la Información y Gerencia de Talento Humano** 1. Que se desactiven los accesos de los Usuarios reportados. 2. Que se implementen políticas y procedimientos para que la Gerencia de Talento Humano informe al Departamento de Tecnología de la Información sobre las personas que son separadas de la Empresa, de tal forma que se desactiven sus accesos a los sistemas de información, de manera oportuna.

REF.	RIESGO	1. DEBILIDADES EN LA GESTION DE LA SEGURIDAD DE LA INFORMACION
1.9	M	**FALTA DE UN ESQUEMA DE CLASIFICACION DE DATOS** En ACE no se maneja un Esquema de Clasificación de Datos que permita identificar que información es pública, confidencial o secreta. Un esquema de clasificación de datos incluye detalles acerca de la propiedad de los datos, la definición de los niveles de seguridad, controles de protección, requerimientos de retención y destrucción de datos y sirve como base, para aplicar controles de acceso, archivo o cifrado. Debido a esta situación, existe el riesgo de que la integridad, confidencialidad y disponibilidad de la información se vea afectada. **COMENTARIO DEL JEFEDE TECNOLOGIA DE LA INFORMACION** Esto será uno de los puntos que se tratarán con la consultoría externa. **RECOMENDACION** **Responsables:Gerencia General y Departamento de Tecnología de la Información** Que se implementen políticas y procedimientos para la utilización de un Esquema de Datos;de manera tal, que se maneje la información de la Empresa, en base a su criticidad.

REF.	RIESGO	2. DEBILIDADES EN LA GESTION DE RIESGOS
2.1	MA	**FALTA DE EVALUACION DE RIESGOS** No se realizan Evaluaciones de Riesgos periódicas sobre los activos y recursos de TI. Una evaluación de riesgos permite identificar aquellos eventos que pueden afectar la infraestructura de las tecnologías de la información de la Empresa, y permite establecer planes de acción para mitigar los riesgos que comprometan la integridad, confidencialidad y disponibilidad de la información. Debido a la falta de evaluaciones de riesgo, la infraestructura de las tecnologías de la información puede estar expuesta a eventos que afecten a la información y continuidad de la Empresa. **COMENTARIO DELJEFEDE TECNOLOGIA DE LA INFORMACION** En base a esta observación, solicité a una empresa consultora, para que me ayude en temas de seguridad y plan de continuidad. Estoy realizando las entrevistas a Proveedores. **RECOMENDACION** **Responsable**: **Jefe de Tecnología de la Información** 1. Implementar políticas y procedimientos para realizar Evaluaciones de Riesgos periódicas sobre los activos de TI. 2. Presentar al Gerente General, planes de acción sobre los riesgos identificados, para su aprobación e implementación.

REF.	RIESGO	3. DEBILIDADES EN LA ADMINISTRACION DE LOS SERVICIOS DE TI
3.1	M	**FALTA DE CATALOGO DE SERVICIOS** El Departamento de Tecnología de la Información, no cuenta con un catálogo de los servicios que presta a la Empresa. El tener identificado los servicios de TI de manera formal, permite establecer las definiciones, características, y requerimientos del negocio sobre dichos servicios; tales como la seguridad, disponibilidad, desempeño, capacidad de crecimiento, métricas cualitativas y cuantitativas, entre otros; ayudando de esta manera a alinear los servicios de TI con los objetivos de la Empresa. **COMENTARIO DEL JEFE DE TECNOLOGIA DE LA INFORMACION** Actualmente tenemos los servicios de manera informal. No se ha realizado un análisis en base a una metodología establecida, que nos permita identificar las necesidades de la empresa. **RECOMENDACIONES** **Responsable**: **Jefe de Tecnología de la Información** 1. Formalizar la entrega de los servicios que presta el Departamento de Tecnología de la Información, a través de un Catálogo de Servicios, en base a estándares generalmente aceptados. 2. Incluir en los KPI'S del Departamento de Tecnología de la Información, las métricas establecidas para los servicios.
3.2	B	**DEBILIDADES EN EL REGISTRO DE PROBLEMAS** Los diferentes problemas que reportan los Usuarios Finales, son registrados por el Departamento de Tecnología de la Información, en un programa informático que permite controlar el número de problemas reportados, tiempo de solución y la frecuencia. Sin embargo, el personal del Departamento de Tecnología de la Información, nos manifestó que en ocasiones, los problemas no se registran inmediatamente, sino tiempo después de que fueron reportados y/o solucionados. Debido a esta situación, existe el riesgo de que no se registren todos los problemas existentes, y/o que se registren tiempos de solución errados, afectando la efectividad de este sistema, para evaluar el desempeño y la tendencia de los problemas. **COMENTARIO DEL JEFE DE TECNOLOGIA DE LA INFORMACION** Actualmente disponemos de un sistema en su primera versión, en donde el Usuario Final, no es quien genera el requerimiento, motivo por el cual se generan las situaciones descritas. Se utilizará las bondades del nuevo sistema de mantenimiento, en donde el Usuario Final será quien ingrese el requerimiento, lo que permitirá realizar una mejor gestión.

REF.	RIESGO	3. DEBILIDADES EN LA ADMINISTRACION DE LOS SERVICIOS DE TI
		RECOMENDACION **Responsable**: **Jefe de Tecnología de la Información** Que se implemente un sistema informático para el registro de problemas, de manera tal, que sean los Usuarios Finales y no el Departamento de Tecnología de la Información, quienes registren los problemas.
3.3	MA	**DEBILIDADES EN EL MONITOREO DE LA CAPACIDAD DE LA INFRAESTRUCTURA** No existe evidencia de que se monitoree la capacidad de la infraestructura de las tecnologías de la información de la Empresa (redes, servidores, espacios en discos duros, etc). El Personal del Departamento de Tecnología de la Información, nos manifestaron que se monitorea la capacidad de las redes y servidores, pero no se documentan ni realizan informes al respecto. Tampoco existe un historial del uso de la infraestructura de TI, que permita realizar proyecciones sobre la capacidad y desempeño de dicha infraestructura. El monitoreo periódico de la capacidad de la infraestructura de TI, permite ejecutar planes de acción para prevenir la no disponibilidad de los sistemas de información, a causa de colapsos por capacidad. **COMENTARIO DEL JEFE DE TECNOLOGIA DE LA INFORMACION** Se realizarán los monitoreos de la infraestructura de las tecnologías de la información, exigiendo a cada Especialista de Sistemas, los informes periódicos. **RECOMENDACIONES** **Responsable**: **Jefe de Tecnología de la Información** 1. Que se implementen procedimientos formales para el monitoreo periódico de la capacidad de la infraestructura de TI, los mismos que deberán terminar en informes aprobados por el Jefe de Tecnología de la Información. 2. Implementar el registro del historial de la capacidad de la infraestructura de las tecnologías de la información, con el propósito de realizar predicciones y planes de acción oportunos.
3.4	M	**FALTA DE REGISTROS DE CONFIGURACION DE HARDWARE Y SOFTWARE** No se mantienen registros de las configuraciones que se utilizan en el hardware y software que soportan a los sistemas informáticos de la Empresa (BAAN, ADAM, Reporteadores, etc). El establecer y mantener un registro de las configuraciones, permite:

REF.	RIESGO	3. DEBILIDADES EN LA ADMINISTRACION DE LOS SERVICIOS DE TI

1. Detectar de manera oportuna, cambios no autorizados en las configuraciones del hardware y software; a través de monitoreos periódicos con las configuraciones actuales.

2. Disminuir el tiempo de recuperación después de la ocurrencia de un evento de desastre, porque se contaría con el registro actualizado de la configuración del hardware y software, después del desastre.

COMENTARIO DEL JEFE DE TECNOLOGIA DE LA INFORMACION

Se utilizará la computadora donde tenemos los drivers, para guardar las configuraciones de hardware y software e implementaremos un procedimiento que garantice el cumplimiento del mismo.

RECOMENDACIONES

Responsable: **Jefe de Tecnología de la Información**

1. Implementar y mantener actualizado un repositorio central, para el registro de las configuraciones de los sistemas de información y de la infraestructura que la soporta.

2. Incluir en los respaldos que se realizan a las base de datos y aplicativos de la Empresa, una copia del repositorio central de configuraciones.

REF.	RIESGO	4. DEBILIDADES EN LA GESTION DE APLICATIVOS
4.1	MA	**DEBILIDADES EN EL DESARROLLO DE APLICATIVOS** Observamos las siguientes debilidades en el proceso de desarrollo de aplicativos: 1. No existen estándares formales para el diseño, codificación y nomenclatura del código fuente, de las aplicaciones elaboradas por el personal del Departamento de Tecnología de la Información. El implementar estos estándares de manera formal, permite garantizar la calidad de las aplicaciones desarrolladas. **COMENTARIO DEL JEFE DE TECNOLOGÍA DE LA INFORMACIÓN** Es verdad, no tenemos estándares. **RECOMENDACION** **Responsable**: **Jefe de Tecnología de la Información** Que se implementen estándares formales para el desarrollo de las aplicaciones. 2. No existe un Diccionario de Datos, que permita identificar: Tablas, tipos de datos, definiciones de campos y relaciones, de las bases de datos, que contienen la información de la Empresa, y que pueda ser consultado durante el desarrollo o los cambios en aplicativos. Un Diccionario de Datos, fomenta un entendimiento común de los datos y previene la creación de datos incompatibles, ayudando a asegurar que los aplicativos desarrollados, muestren y procesen correctamente la información. **COMENTARIO DEL JEFE DE TECNOLOGÍA DE LA INFORMACIÓN** Vamos a trabajar en esta observación, como un proyecto de la documentación de los aplicativos desarrollados en ACE. **RECOMENDACION** **Responsable**: **Jefe de Tecnología de la Información** Que se implementen políticas y procedimientos para el uso y mantenimiento de un Diccionario de Datos. 3. El Personal del Departamento de Tecnología de la Información y los Pasantes, acceden a la base de datos en producción para el desarrollo de aplicaciones. Esta situación se da, porque no está separado el ambiente de desarrollo del ambiente de producción, existiendo el riesgo de que por error o irregularidad se inserte, modifique o elimine información de la base de datos.

REF.	RIESGO	4. DEBILIDADES EN LA GESTION DE APLICATIVOS
		COMENTARIO DEL JEFE DE TECNOLOGÍA DE LA INFORMACIÓN Voy hablar con el Especialista de Aplicativos, para que oriente el desarrollo de aplicaciones en un ambiente de desarrollo y pruebas. **RECOMENDACIONES** **Responsable**: **Jefe de Tecnología de la Información** 1. Que el Administrador de Base de Datos, monitoree e informe periódicamente al Jefe de Tecnología de la Información, sobre accesos indebidos de Usuarios, a la base de datos en producción, para evitar el riesgo de fraudes o perdida de información de la base de datos. 2. Realizar las acciones necesarias para separar el ambiente de desarrollo del ambiente de producción.
4.2	MA	**DEBILIDADES EN EL ALCANCE DE RESPONSABILIDAD DE LOS USUARIOS CLAVES** No existen políticas y procedimientos, que delimiten las acciones y responsabilidades de los Usuarios Claves en el sistema BAAN. Durante la fase de implementación del BAAN, se nombraron Usuarios Claves para los diferentes procesos; dichos Usuarios eran responsables de las pruebas, solución de problemas y asignación de permisos a los Usuarios Finales; motivo por el cual, se les asignó permisos especiales en el sistema BAAN, con opción de insertar, modificar y eliminar datos en procesos que no les corresponde interactuar. Sin embargo, han pasado tres años desde que se implementó el BAAN, y los Usuarios Claves siguen realizando dichas funciones; entre las cuales constan, asignar los accesos en el sistema BAAN a los Usuarios Finales. **COMENTARIO DEL JEFE DE TECNOLOGIA DE LA INFORMACION** Voy a elaborar las políticas y procedimientos para que sean aprobadas por el Gerente General. **RECOMENDACIONES** **Responsable**: **Jefe de Tecnología de la Información** 1. Que se implementen políticas y procedimientos para delimitar el alcance y las funciones de los Usuarios Claves de ANDEC, en el sistema BAAN. 2. Que la administración de las seguridades del sistema BAAN, se centralice en el Departamento de Tecnología de la Información.

REF.	RIESGO	4. DEBILIDADES EN LA GESTION DE APLICATIVOS
4.3	MA	**AMBIENTE DE PRUEBAS DIFERENTE AL AMBIENTE DE PRODUCCION** No se han implementado controles para validar que el ambiente en el que se prueban los cambios a realizarse en el sistema BAAN (customizaciones), sea igual al ambiente en producción. Esta validación, permite asegurar que los cambios que se realizan en el sistema, funcionen de igual manera, tanto en el ambiente de pruebas como en el ambiente de producción; previniendo errores de procesamiento (confiabilidad) y/o la no disponibilidad de los recursos informáticos. Debido a esta situación, existe el riesgo de ocurrencia de situaciones similares a la ocurrida el 25 de Agosto del 2011, en la customización HDL076, que se refiere a la calificación de la chatarra; la cual fue solucionada, cambiando la parametrización del ambiente en producción de manera idéntica a la del ambiente de pruebas. **COMENTARIO DEL JEFE DE TECNOLOGIA DE LA INFORMACION** Se solicitará a Novatech una consultoría y capacitación sobre la generación correcta de un ambiente de pruebas. **RECOMENDACION** **Responsable**: **Jefe de Tecnología de la Información** Que se implementen políticas y procedimientos para el proceso de pruebas de los cambios que se realizan a los sistemas, con la finalidad de asegurar que el ambiente de pruebas sea igual al ambiente de producción.
4.4	MA	**FALTA DE CONTROL DE LOS CAMBIOS** No se han implementado controles para administrar los cambios que se realizan a los aplicativos (programas); tal como sucedió con el problema presentado en los equipos PDA utilizados por los Calificadores de chatarra, el 18 de Julio del 2011, el cual se debió a un cambio en la estructura de una tabla en la base de datos por parte de Novatech, sin considerar que esa estructura era utilizada por los PDA. Esta situación ocasionó que no se pudieran utilizar los PDA, por más de un mes. Debido a esta situación, existe el riesgo de que los cambios realizados en los aplicativos no funcionen correctamente, afectando la disponibilidad y confiabilidad de los sistemas de información. **COMENTARIO DEL JEFE DE TECNOLOGIA DE LA INFORMACION** Ya se solicitó a Novatech que las customizaciones que incluyan cambios de estructura de las tablas, sean comunicadas a ACE.

REF.	RIESGO	4. DEBILIDADES EN LA GESTION DE APLICATIVOS
		RECOMENDACION **Responsable**: **Jefe de Tecnología de la Información** Que se implementen políticas y procedimientos formales para administrar los cambios en aplicativos; de manera tal, que el impacto sobre la disponibilidad y confiabilidad de los sistemas de información sea mínimo.

REF.	RIESGO	5. DEBILIDADES EN PLANES DE CONTINUIDAD
5.1	A	**FALTA DE UN PLAN DE CONTINUIDAD DEL NEGOCIO** No existen Planes de Contingencia y de Recuperación del negocio, que indiquen "que hacer" en caso de ocurrencia de desastres (incendios, terremotos, explosiones, etc), que permitan garantizar la continuidad del negocio, durante y después de estos eventos. Debido a esta situación, existe un alto riesgo de que la Empresa no se recupere oportunamente ante un evento de desastre, afectando la disponibilidad de los sistemas informáticos y la continuidad del negocio. **COMENTARIO DEL JEFE DE TECNOLOGIA DE LA INFORMACION** Se han realizado diagnósticos de la plataforma, lo que nos va a permitir desarrollar los planes con el debido asesoramiento. **RECOMENDACION** **Responsable**: **Jefe de Tecnología de la Información** Que de manera URGENTE, se implemente en ACE, los Planes de Contingencia y de Recuperación, con el objetivo de asegurar la continuidad del negocio, durante y después de un evento de desastre.

REF.	RIESGO	6. DEBILIDADES EN INDICADORES DE DESEMPEÑO (KPI'S)
6.1	M	**DEBILIDADES EN LOS INDICADORES DE DESEMPEÑO DEL DEPARTAMENTO DE TI** Como parte de nuestra revisión, evaluamos los indicadores de desempeño del Departamento de Tecnología de la Información, que se encuentran registrados en el sistema Strategy Link. En dicha revisión, encontramos las siguientes situaciones: 1. Existen KPI`S que no tienen relación con el objetivo estratégico al que están vinculados o cuyas fórmulas son incoherentes.  2. Existen KPI`S en los cuales no se han registrado datos o están incompletos. Debido a las debilidades mencionadas, consideramos que los indicadores de desempeño de TI, no están acordes a los requerimientos del negocio, lo que podría afectar el logro de los objetivos de la Empresa. **COMENTARIO DEL JEFE DE TECNOLOGIA DE LA INFORMACION** Estoy de acuerdo, esto lo hablé con el Jefe de Desarrollo Empresarial, quien me indicó que no se podían cambiar, porque fueron establecidos de manera corporativa y están relacionados con los objetivos de la empresa. **RECOMENDACIONES** **Responsable**: **Gerencia de Tecnología de la Información y Departamento de Desarrollo Empresarial** 1. Que se revisen y actualicen los indicadores de desempeño del Departamento de Tecnología de la Información, tomando como referencia los estándares generalmente aceptados (COBIT / ITIL). 2. Que el Jefe de Desarrollo Empresarial, monitoree el ingreso y cumplimiento de las metas establecidas en cada indicador de desempeño del Departamento de Tecnología de la Información.