AUDITORÍA INFORMÁTICA

TÉCNICAS DE AUDITORÍA INFORMÁTICA

Presentado a:

Ing. Elizabeth Granados Pemberty

Preserntado por:

Erwin Daza Rendón

Edwin Caldón

Javier Ignacio Caicedo S. Cod.

Alejandra María Narváez C.

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Popayán, Marzo de 2.007

CUESTIONARIO

Ejercicio 1:

Le damos un cordial saludo. El presente cuestionario es con el fin de identificar sus aptitudes en el área de auditoría, y las ponga en práctica en nuestra empresa Kuky´s Ltda. dedicada a prestar servicios de salud a personas afiliadas al Sisbén. Le solicitamos su colaboración para diligenciarlo, si usted tiene conocimientos previos en el área de auditoría informática. Lea detenidamente las instrucciones para responder a cada pregunta y responda con la mayor sinceridad posible.

Instrucciones

Al momento de diligenciar el cuestionario debe tener en cuenta que: en algunas preguntas usted debe explicar su respuesta, para ello hay destinadas unas líneas debajo de dichas preguntas; y otras en las cuales debes simplemente marcar con una X su respuesta.

De orden personal

¿Cuáles son sus expectativas económicas?

( ) $ 1’000.000
( ) $ 1’200.000
( ) $ 3’000.000
Otro $_____

¿Tiene familiares o conocidos trabajando en esta empresa?

Si ____
No ____

¿Cuál es su nivel de empatía?

Alto ____
Medio ____
Bajo ____

¿En qué orden realiza la auditoría a las diferentes áreas de la empresa?

_____
_____
_____
_____
_____

¿Cuáles son las personas que usted considera deben entrevistarse dentro de la empresa para la auditoría?

_____
_____
_____
_____

Asumiendo que encuentra irregularidades en la empresa y es amenazado para que no reporte esta situación en el informe ¿Cómo actuaría al respecto?

_____
_____
_____
_____

¿Cree usted que tiene la capacidad de trabajar en grupo?

Siempre ____
No siempre ____
Ocasionalmente ____

Dé un ejemplo de diplomacia en el trabajo.

_____
_____
_____
_____
_____

¿Cuáles considera usted son las 3 características más importantes que debe tener un auditor?

_____
_____
_____
_____
_____

¿Practica usted algún deporte?

Si _____ ¿Cual? _____

No _____

¿Con quién convive en su hogar?

_____
_____

¿Tiene personas a su cargo?

Si _____ ¿Quienes? _____

De orden laboral

¿Qué experiencia tiene usted como auditor informático? ¿Cuál?

_____
_____
_____
_____
_____

¿Tiene experiencia en el manejo en el área financiera de una empresa?

Si ____ ¿Cuál empresa? _____

¿Conoce usted esta empresa y su comportamiento? Explique. Si la respuesta es no conteste la siguiente pregunta:

¿Cuánto tiempo considera necesitar para conocer el funcionamiento de la empresa?

- 1 semana _____
- 2 semanas ____
- 1 mes _____
- Otro. ¿Cuanto? _____

¿Cuáles son los estándares que usted sigue para realizar la auditoría?

_____
_____
_____

¿Qué otros estudios ha realizado?

_____
_____
_____

De orden técnico

¿Qué son las TIC's?

_____
_____
_____

Mencione 3 DBMS

_____
_____
_____

¿Qué sistemas operativos maneja?

_____
_____
_____

Considera que su formación es investigativa o técnica. Explique

_____
_____
_____

¿Qué lenguajes de programación maneja?

_____
_____
_____

¿Qué idiomas maneja?

Inglés _____. Lo lee ___ %. Lo escribe ____ %. Lo habla ___ %.
Francés _____.Lo lee ___ %. Lo escribe ____ %. Lo habla ___ %.
Otro _____. Lo lee ___ %. Lo escribe ____ %. Lo habla ___ %.

De habilidad

¿Hasta donde entra un perro en un bosque?

_____
_____
_____

¿Por qué las tapas de las alcantarillas son redondas?

_____
_____
_____

Agradecemos su colaboración y atención prestada al presente cuestionario. Los resultados los podrás ver a partir de 20 de Marzo de 2007 en la dirección www.unicauca.edu.co/~jicaicedo/resultados
Cuestionario realizado por: Kuky´s Ltda.

Ejercicio 2:

La empresa Kuky´s Ltda. tiene como objeto hacer galletas para la exportación.

Actualmente, se ha podido observar que varias irregularidades se han ido presentando con el manejo que se realiza a la información.

Se han encontrado inconsistencias en los datos, pérdida de información, los backup no se pueden recuperar porque el programa no los accede, etc...

¿Usted como auditor informático de Kuky´s, que funciones tendría con respecto al problema que se está presentando?

Solución:

Al tener la función de auditor informático en Kuky´s Ltda. Es mí deber controlar y verificar que los sistemas de información realicen sus tareas de manera eficiente. De lo contrario es necesario iniciar un análisis y detectar las posibles causas del problema, para así hacer las respectivas sugerencias.

El análisis debe realizarse a todas las partes que tienen acceso a la información, ya sean software, hardware y personal de la empresa.
Es importante seguir minuciosamente el manejo de la información, la manera en que se adquiere la información, su procesamiento, su almacenamiento y su seguridad.

Realizar y entregar un informe final, manteniendo manteniendo niveles de confidencialidad adecuados.

ENTREVISTA

PRESENTACIÓN

Hoy 9 de marzo de 2007, nos encontramos con el señor _____, graduado de la _____ como _____, quien ahora se desempeña como docente _____.

El propósito de esta entrevista es conocer su proceso de preparación de clases.

CUERPO

1. ¿Considera usted necesario realizar una preparación anticipada de cada clase, por qué?

Como docente es una de las actividades que debemos realizar, las diferentes temáticas que se manejan en un curso se deben preparar.

2. ¿Cuánto tiempo dedica a la preparación de una clase?

Depende de la temática y del curso al que se le va a dictar la clase, generalmente cuando los cursos o los temas son nuevos, implican mayor cantidad de tiempo, muchas veces cuando la temática es nueva por 2 horas de clase se pueden llegar a necesitar 6 u 8 horas de preparación, pero cuando la temática ya es conocida, esos tiempos se pueden ir reduciendo considerablemente.

3. ¿Desde cuándo viene realizando la preparación de sus clases?

4. ¿La preparación de una clase debe hacerse minuciosamente o basta con tener claros los temas principales, por qué?

5. ¿El proceso de preparación de la clase es igual para todas las materias?

6. ¿Piensa que es posible que sus alumnos noten la diferencia entre una clase preparada y una clase improvisada, por qué?

7. ¿Lleva una documentación organizada de sus clases, por qué?

8. ¿Considera que esta documentación es importante?

9. ¿Cuáles son las partes principales en el desarrollo de una de sus clases?

10. ¿Si por alguna circunstancia debe dar una clase improvisadamente, a qué herramientas recurre, o prefiere no desarrollar la clase, por qué?

CIERRE

Agradecemos mucho su atención y el tiempo dedicado a esta entrevista.

LISTA DE CHEQUEO

Lista de chequeo para verificar el proceso de administración de las salas de computo del Programa de Ingeniería de Sistemas (PIS)

Sujetos de control	*Si*	*No*
Las Salas de Informática están bajo la responsabilidad legal del Coordinador del PIS		
Las Salas de Informática están ubicadas en instalaciones adecuadas		
Las Salas de Informática están administradas por un Tecnólogo de Sistemas vinculado al PIS		
El Coordinador del PIS y el Administrador son los únicos autorizados para poseer llaves de acceso a las Salas de Informática		
Los profesores adscritos al PIS poseen llaves de acceso a las Salas de Informática		
Los estudiantes adscritos al PIS pueden portar y manejar llaves de acceso a las Salas de Informática		
El Administrador es el único autorizado para realizar instalaciones y/o actualizaciones de Hardware y de Software en los equipos		
Los profesores adscritos al PIS pueden realizar instalaciones y/o actualizaciones de Software en los equipos		
El Administrador es el encargado de controlar el acceso y uso de los equipos de cómputo por parte de los usuarios		
El Administrador informa al Coordinador del PIS sobre los inconvenientes que pudieran suscitarse entre los usuarios de las Salas de Informática		
Sólo estudiantes adscritos al PIS utilizan los equipos de la Salas de Informática		
Los usuarios (profesores y estudiantes adscritos al PIS) pueden consumir alimentos o bebidas en las Salas de Informática		
El usuario que requiere uso continuo de un equipo de las Salas de Informática o en horarios adicionales presenta una solicitud escrita al Coordinador del PIS indicando el horario y equipo a utilizar además presenta una copia de la autorización al Administrador		
El Administrador asigna horarios de acceso a los computadores por parte de los estudiantes para la realización de las prácticas, consultas y trabajos de las diferentes materias académicas en las que están matriculados		
El Administrador controla el acceso y la correcta utilización de los		

computadores por parte de los estudiantes en los horarios designados		
El Administrador lleva un control del funcionamiento de cada computador instalado en las salas de informática		
El Administrador realiza mantenimiento preventivo del total de equipos instalados en las salas de informática		
El Administrador presenta informes periódicos de los mantenimientos preventivos y correctivos que se realicen a los equipos de las salas de informática junto con reportes de estadísticas de utilización de los equipos por parte de los usuarios, y demás informes que sean requeridos por la Coordinación del Programa		
Se presenta alguna clase de desorden alguno en las Salas de Informática por parte de los usuarios		
Las personas no adscritas al PIS son autorizadas por el Administrador de las salas para el uso de los equipos de cómputo		
En caso de alta demanda de los equipos de las Salas de Informática, el Administrador establece y divulga un tiempo de uso máximo permitido cada usuario		
El Administrador sanciona al usuario que realice actividades delictivas, como por ejemplo uso de programas que violen la seguridad de otros sistemas, con la suspensión definitiva del servicio		
El Administrador sanciona al usuario que usa los equipos para utilizar juegos y/o navegar en páginas con contenido pornográfico, con la suspensión del servicio por un periodo de tiempo		
El usuario puede desarmar, destapar o instalar hardware adicional a un equipo		
En el caso de que el usuario requiera instalar hardware adicional a un equipo deberá hacerlo el Administrador con previa solicitud		
El Administrador hace llamados de atención a los estudiantes que hagan mal uso de los computadores o en general de cualquier equipo o recurso que ellos utilizan en sus actividades académicas o cualquier acción que vaya en contra del "Reglamento de Usos y Cuidados de las Salas de Informática"		
El Administrador informa por escrito al Coordinador del Programa para que se tomen las sanciones pertinentes, en caso de reincidencia en una mala acción, por parte de algún usuario de las salas		

_____

Administrador Salas Informática
PIS - FIET

SOFTWARE DE INDAGACIÓN EN AUDITORÍA INFORMÁTICA

A pesar de ser una técnica muy nueva en la Auditoria Informática, su utilización es de gran ayuda para las empresas, debido a los beneficios que se obtienen:

Reducción de licenciamiento del software y costos de mantenimiento
Mejora y efectividad en servicios de escritorio
Reducción de riesgos de incumplimiento asociados a acuerdos de licencia y términos de contrato
Generación de planes más completos y exactos
Reducción de costos de inventarios, manuales y reportes

De acuerdo a la investigación realizada, en el siguiente vínculo encontramos el sitio Web de la empresa **Novel Inc.** que ofrece un software gratuito para realizar Auditorias Informáticas:

http://www.novell.com/products/zenworks/assetmanagement/eval.html

Este software se denomina: **ZENworks Asset Management**, que ya se encuentra disponible en su versión 7.5 y funciona en plataformas Windows, Unix, Mac y Linux.

Como ya se mencionó, el nombre de la empresa que lo ofrece es: **Novel Inc.**

ZENworks Asset Management, es una herramienta muy potente que presenta las siguientes **características**, entre las cuales encontramos áreas que maneja, operaciones que permite y resultados que presenta:

11. Generación de reportes
    1. Reportes Web que incluye opciones gráficas
    2. Historial y análisis de recursos
    3. Alertas vía e-mail por condiciones críticas o cambios en los recursos
12. Descubrimiento, reconocimiento e inventario
    1. Descubrimiento de la red basado en dispositivos IP
    2. Reconocimiento automático de miles de productos de acuerdo a un conocimiento base
    3. Reconocimiento de software, hardware y dispositivos de red
    4. Reconocimiento de productos locales, privados y productos legales
    5. Sin límite de campos de usuarios definidos para colección de datos
    6. Colección de datos de usuarios
13. Operaciones
    1. Integración de clientes
    2. Procesos de inventarios personalizado
    3. Flexibilidad de opciones (cliente, login-script y políticas del sistema)
    4. Múltiples opciones de calendarización

5. Inventarios de escaneos por demanda en tiempo real de dispositivos específicos
6. Actualización automática de produtos

14. Rastreando Licencias
    1. Cuentas automatizadas para nuevas contrataciones
15. Conciliación
    1. Conciliación entre contrataciones y productos descubiertos
    2. Inventario de software enlazado con contrataciones e instalación
16. Gestión de recursos software
    1. Gestión de estandarización del software
    2. Reportes que integran licencias, instalación y uso de los datos
    3. Colección software de usuarios definidos para reportes
17. Utilización de software
    1. Reportes de máquina local, servidor y utilización de aplicaciones Web
    2. Rastreo de aplicaciones en tiempo real
    3. Identificación de poco uso, ó uso frecuente de las aplicaciones
    4. Información de usuario y dispositivo que maneja
18. Gestión de contratos
    1. Evaluación de todos los tipos de contratos, y términos/condiciones claves
    2. Grabación y notificación de datos claves en los contratos

ANÁLISIS DE UN LOG DE EVENTOS

A continuación se presenta un Log de eventos en el cual se registran usuarios y acciones que ellos realizan en un cajero automático del banco "dineros calientes".
Por medio del Log de eventos se pretende determinar que usuarios están utilizando de forma errónea el cajero. Para este caso en particular se registrarán 5 usuarios. A continuación se presenta un posible esquema que refleja lo anteriormente dicho:

Log_dineros_calientes

Fecha (día/mes/año)	Hora (hora/minuto/segundo)	Acción realizada
09/03/07	18:00:23	Usuario 1 ingresa su tarjeta al cajero. Inmediatamente es registrado en el Log y reconocido por el cajero
09/03/07	18:00:28	El cajero pide al usuario que ingrese su contraseña. El usuario efectivamente la escribe
09/03/07	18:00:32	Se despliega automáticamente las opciones (consulta, retiro, cambio de clave). El usuario procede a consultar su saldo
09/03/07	18:00:34	Se despliega automáticamente las opciones (cuenta ahorros, cuenta corriente). El usuario accede a la cuenta ahorros
09/03/07	18:00:35	Efectivamente el cajero muestra su saldo en la cuenta ahorros, por medio de un recibo
09/03/07	18:00:40	El usuario retira su recibo
09/03/07	18:00:40	El cajero automáticamente cierra la sesión de ese usuario, y se queda en modo de escucha hasta que vuelvan a introducir una tarjeta
XXXXXXXX	XXXXXXXXXXXXXX	XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
09/03/07	19:32:17	Usuario 2 ingresa su tarjeta al cajero. Inmediatamente es registrado en el Log y reconocido por el cajero
09/03/07	19:32:22	El cajero pide al usuario que ingrese su contraseña. El usuario efectivamente la escribe
09/03/07	19:32:27	Se despliega automáticamente las opciones (consulta, retiro, cambio de clave).

		El usuario procede a retirar dinero
09/03/07	19:32:29	Se despliega automáticamente las opciones (cuenta ahorros, cuenta corriente). El usuario accede a la cuenta ahorros
09/03/07	19:32:33	El cajero muestra las diferentes cantidades de dinero disponibles que se pueden realizar: (300.000, 200.000, 100.000, 50.000, 10.000)
09/03/07	19:32:37	El usuario ejecuta la acción de retirar 300.000
09/03/07	19:32:42	El cajero retira 300.000 de la cuenta ahorros del Usuario 2, entrega el dinero y genera un recibo por la transacción hecha
09/03/07	19:32:45	El usuario retira el dinero y el recibo
09/03/07	19:32:46	El cajero automáticamente cierra la sesión de ese usuario, y se queda en modo de escucha hasta que vuelvan a introducir una tarjeta
XXXXXXXX	XXXXXXXXXXXXXX	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
09/0307	20:59:50	Usuario 3 ingresa su tarjeta al cajero. Inmediatamente es registrado en el Log y reconocido por el cajero
09/0307	20:59:55	El cajero pide al usuario que ingrese su contraseña. El usuario efectivamente la escribe
09/03/07	21:00:00	Se despliega automáticamente las opciones (consulta, retiro, cambio de clave). El usuario procede a retirar dinero
09/03/07	21:00:02	Se despliega automáticamente las opciones (cuenta ahorros, cuenta corriente). El usuario accede a la cuenta ahorros
09/03/07	21:00:06	El cajero muestra las diferentes cantidades de dinero disponibles que se pueden realizar: (300.000, 200.000, 100.000, 50.000, 10.000)
09/03/07	21:00:10	El usuario ejecuta la acción de retirar 100.000
09/03/07	21:00:11	El cajero le responde al usuario con el siguiente mensaje: “Señor usuario, el dinero que usted solicita retirar supera el saldo disponible en su cuenta de ahorros. Usted dispone de 95.000 en esa cuenta”
09/03/07	21:00:21	El cajero automáticamente cierra la sesión de ese usuario, y se queda en modo de escucha hasta que vuelvan a introducir una tarjeta
XXXXXXXX	XXXXXXXXXXXXXX	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

		X
10/03/07	10:15:52	Usuario 4 ingresa su tarjeta al cajero. Inmediatamente es registrado en el Log y reconocido por el cajero
10/03/07	10:15:57	El cajero pide al usuario que ingrese su contraseña
10/03/07	10:16:10	El usuario efectivamente escribe su contraseña
10/03/07	10:16:11	El cajero responde al usuario: "Su contraseña es inválida"
10/03/07	10:16:20	El usuario nuevamente escribe su contraseña
10/03/07	10:16:21	El cajero responde al usuario: "Su contraseña es inválida"
10/03/07	10:16:30	El usuario vuelve y digita una contraseña
10/03/07	10:16:31	El cajero procede a bloquear la tarjeta del Usuario 4 y a registrar todo este historial en el Log
XXXXXXXX	XXXXXXXXXXXXXX	XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
10/03/07	11:40:44	Usuario 5 ingresa su tarjeta al cajero. Inmediatamente es registrado en el Log y reconocido por el cajero
10/03/07	11:40:49	El cajero pide al usuario que ingrese su contraseña
10/03/07	11:40:58	El usuario ingresa su contraseña
10/03/07	11:40:59	Se despliega automáticamente las opciones (consulta, retiro, cambio de clave).
	11:41:11	El usuario procede a retirar dinero
	11:41:12	Se despliega automáticamente las opciones (cuenta ahorros, cuenta corriente).
	11:41:20	El usuario accede a la cuenta de ahorros
	11:41:21	El cajero muestra las diferentes cantidades de dinero disponibles que se pueden realizar: (300.000, 200.000, 100.000, 50.000, 10.000)
	11:41:30	El usuario ejecuta la acción de retirar 300.000
	11:41:40	El cajero retira 300.000 de la cuenta ahorros del Usuario 5, entrega el dinero y genera un recibo por la transacción hecha
	11:41:45	El usuario retira el dinero y el recibo
	11:41:46	El cajero automáticamente cierra la sesión de ese usuario, y se queda en modo de escucha hasta que vuelvan a introducir una tarjeta

	11:42:05	Usuario 5 ingresa su tarjeta al cajero. Inmediatamente es registrado en el Log y reconocido por el cajero
	11:42:09	El cajero pide al usuario que ingrese su contraseña
	11:42:15	El usuario ingresa su contraseña
	11:42:16	Se despliega automáticamente las opciones (consulta, retiro, cambio de clave).
	11:42:20	El usuario procede a retirar dinero
	11:42:21	Se despliega automáticamente las opciones (cuenta ahorros, cuenta corriente).
	11:42:25	El usuario accede a la cuenta de ahorros
	11:42:26	El cajero muestra las diferentes cantidades de dinero disponibles que se pueden realizar: (300.000, 200.000, 100.000, 50.000, 10.000)
	11:42:35	El usuario ejecuta la acción de retirar 200.000
	11:42:45	El cajero retira 200.000 de la cuenta ahorros del Usuario 5, entrega el dinero y genera un recibo por la transacción hecha
	11:42:49	El usuario retira el dinero y el recibo
	11:42:50	El cajero automáticamente cierra la sesión de ese usuario, y se queda en modo de escucha hasta que vuelvan a introducir una tarjeta

La tabla anterior es la interpretación del Log de eventos que registra todos los pasos que los usuarios hacen a la hora de interactuar con el cajero automático del banco “Dineros Calientes”.

El Log en realidad, es un archivo que contiene la información cifrada por cuestiones de seguridad de la información