ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

CENTRO DE EDUCACION CONTINUA

DIPLOMADO EN AUDITORIA INFORMATICA

III PROMOCIÓN

TEMA

"INFRAESTRUCTURA FISICA DE TI BASADOS EN LA NORMA ISO 27002:2005"

AUTORA

ING. SAYNE COLOBON CASTILLO

AÑO

2011

INDICE

CAPITULO 1

1. INTRODUCCIÓN

1.1 Investigación Preliminar

La Universidad de Guayaquil, fue fundada en 1867, se encuentra ubicada en la zona norte de la ciudad de Guayaquil en la ciudadela universitaria, cercana al puente 5 de junio, junto al parque Guayaquil, en la intersección de la Av. Kennedy y la Av. Delta.

El Congreso Nacional de esa época, presidido por Pedro Carbo decreto la fundación de la Junta Universitaria del Guayas, que se instala el primero de Diciembre y que tiene el privilegio de otorgar grados y títulos, por lo que se considera ésta la fecha de la fundación de la Universidad de Guayaquil. La primera Facultad en instalarse fue la de Jurisprudencia en 1868.

Actualmente la Universidad está llevando a cabo Reformas Académicas y Administrativas, e impulsando el estudio de nuevas carreras.

Así como la Carrera de Ingeniería de sistemas fue creada para formar profesionales en las ciencias de la Informática, altamente calificados en el ámbito tecnológico con sólidos valores éticos y morales.

Actualmente la carrera cuenta con 6 laboratorios de computación y dos más en desarrollo, cada uno posee 30 computadores, para uso de los estudiantes desde las 7:00 hasta las 22:00; en ellos se dictan clases de programación, cisco, seminarios de graduación e investigación para las diferentes materias dictadas en la misma.

Para esta auditoría se realizo varias entrevistas a las siguientes personas:

NOMBRES	CARGO
Ing. Fernando Castro	Vicedirector de la Institución
Ing. Alfonso Guijarro	Coordinador de Hardware
Ing. Jorge Medina	Coordinador de Software
C.P.A Marcos Bejar.	Coordinador Administrativo

1.1. Objetivo

Realizar una evaluación constructiva y objetiva a los procesos de Seguridades en Infraestructura de TI con el fin de determinar la situación actual del Departamento Técnico Informático de la institución

1.2. Alcance

Evaluar en forma integral los procesos de Seguridades en Infraestructura Física de TI por el período comprendido del 01 de Enero de 2010 al 30 de Junio de 2010. Verificando, examinando y reportando sobre el cumplimiento, la adecuación, efectividad del sistema de control interno y el

cumplimiento con las políticas y procedimientos establecidos por la institución para el Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales.

CAPITULO 2

2. FUNDAMENTOS

2.1. Reseña Norma ISO 27002

Este estándar se deriva del británico BS 7799, y fue adoptado por la Organización Internacional de Estandarización (ISO) en el año 2000. Hoy en día es conocida mundialmente como el más completo estándar de seguridad de la información. **ISO** define un conjunto completo de controles de seguridad de la información que incluye las mejores prácticas, que se pueden aplicar a organizaciones de todos los tamaños y sectores.
Es una guía de seguridad que puede ser adoptada por cualquier organización, tenga o no ningún interés en obtener la certificación.

ISO/IEC 27002:2005.- Cuenta con 115 Página
A partir del 1 de Julio del 2007 se la conoce con este nombre, manteniendo el 2005 como año de creación. Establece pautas y los principios generales para iniciar, poner, mantener, y mejorar a la gerencia de la seguridad de la información en una organización. Los objetivos contorneados proporcionan la dirección general en las metas comúnmente aceptadas de la gerencia de la seguridad de la información. ISO/IEC 27002:2005 contiene las mejores prácticas de los objetivos y de los controle de la gerencia de la seguridad de la información en las siguientes áreas:

- Política de la seguridad.
- Aspectos organizativos de la seguridad de la información.
- Gestión de activo.
- Seguridad ligada a los recursos humanos.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Gestión de incidentes en la seguridad de la información.
- Gestión de la continuidad del negocio.
- Cumplimiento.

ISO/IEC 27002:2005 se piensa como una base común y guía práctica para desarrollar estándares de organización de la seguridad y prácticas de gerencia

eficaces de la seguridad, y ayudar a construir confianza en actividades internas de la organización.

2.2. JUSTIFICATIVO

La realización de una auditoría al departamento técnico Informático de la Carrera de Ingeniería de Sistemas Computacionales basada en la norma ISO 27002:2005 proporciona a sus directivos los siguientes beneficios:

- Un análisis de la situación actual del departamento.
- Conocer que se puede llegar a tener un departamento más seguro y consciente de sus riesgos.
- Conocer las posibles mejoras en seguridad de información basados en las mejores prácticas.
- Contar con un documento de apoyo para mejorar los controles existentes e implementar nuevos en la medida que se considere necesario.

Cabe indicar que esta norma no permite una certificación ya que no es una norma basada en gestión sino en controles.

CAPITULO 3

3. MARCO GENERAL DE INSTITUCIÓN

3.1. Misión

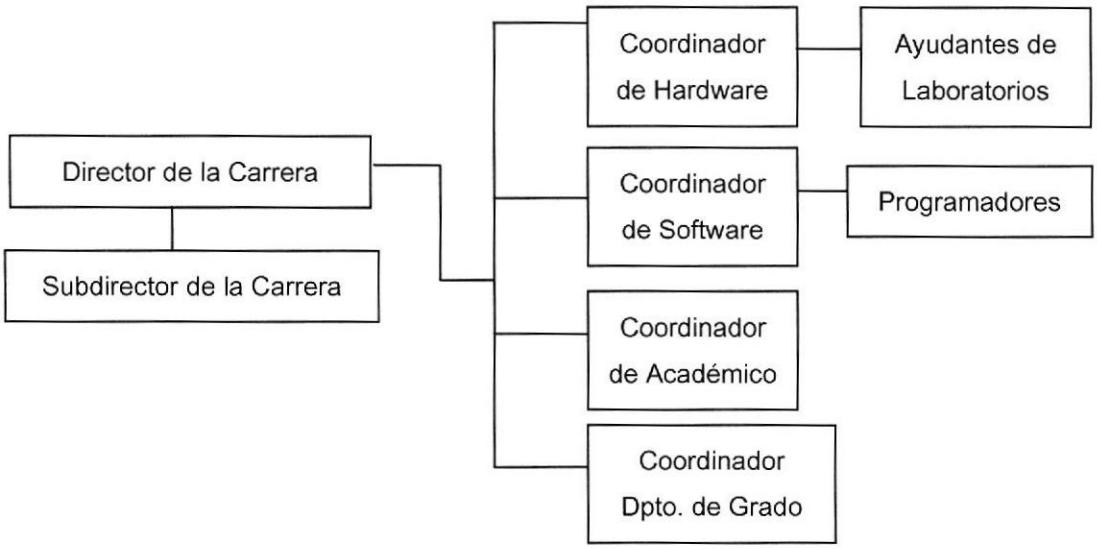
Formar profesionales, en las ciencias de la Informática, altamente calificados en el ámbito académico, científico, tecnológico, humanista y cultural, con sólidos valores éticos y morales; capaces de investigar e innovar para dar soluciones a los problemas y necesidades presentes y futuras del país.

3.2. Visión

La Carrera de Ingeniería en Sistemas Computacionales, es una institución educativa de nivel superior cuya visión es convertirse en una carrera líder en la formación de profesionales comprometidos con la sociedad que se proyectará como un conjunto de conocimientos, técnicas, procedimientos, metodologías y convenios; tal que permita cultivar y fomentar la investigación técnico-científica, desarrollar habilidades que posibiliten la aplicación de los elementos anteriores al servicio de otras áreas del conocimiento, profesiones y de nuestra realidad nacional e intercambio institucional.

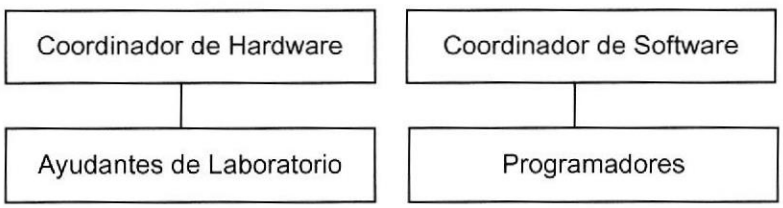
La carrera estará sustentada con un plan de estudio flexible, con una comunidad académica innovadora e investigadora, personal administrativo idóneo, estructura física confortable y funcional.

3.3. Estructura Institucional



NOMBRES	CARGO
Ing. Juan Chanabá Alcócer	Director de la Institución
Ing. Fernando Castro	Vicedirector de la Institución
Ing. Alfonso Guijarro	Coordinador de Hardware
Ing. Jorge Medina	Coordinador de Software
C.P.A Marcos Bejar.	Coordinador Administrativo
Ing. Michael Vásquez	Coordinador Académico
Ing. Patiño	Coordinador de Dpto. Grado

3.4. Estructura del Área de TI



CAPITULO 4

4. PROPUESTA DE AUDITORIA

En la propuesta presentada a las autoridades de la Carrera de Ingeniería de Sistemas Computacionales (CISC) de la Universidad de Guayaquil, se detallan los puntos a tratar en la auditoria, los mismos que fueron revisados y aceptados.
La propuesta se encuentra en el anexo 6.1

CAPITULO 5

5. DESARROLLO DE AUDITORIA

5.1. Acuerdo de Confidencialidad

Se realizo un documento en el cual se detalla un convenio establecido entre la institución a auditar y la persona que realiza dicha auditoria.
Para lo cual revisar el anexo 6.2

5.2. Memorándum de Planificación

Se realizo un documento en el cual se detalla un convenio establecido entre el representante de la institución a auditar y la persona que realiza dicha auditoria.
Para lo cual revisar el anexo 6.3

5.3. Carta de Inicio de Auditoria

Se realizo un documento en el cual se detalla un convenio establecido entre la institución a auditar y la persona que realiza dicha auditoria.
Para lo cual revisar el anexo 6.5

5.4. Acta de Reunión de Inicio

En este documento se indica los temas tratados en la primera reunión con las personas involucradas en la auditoria.
Para lo cual revisar el anexo 6.6

5.5. Programa de Auditoria

Se utilizo el siguiente programa de auditoría para esta institución:

ACTIVIDAD	FECHA DE INICIO	FECHA FINAL
Reunión de Inicio	2/Septiembre/2010	
Entendimiento de los Procesos, identificación de riesgos	20/Septiembre/2010	24/Septiembre/2010
Trabajo en Campo	1/Octubre/2010	14/Diciembre/2010
Reunión de Aclaración Final	28/Octubre/2010	10/Noviembre/2010
Borrador del Informe de Auditoria	11/Enero/2011	14/Enero/2011
Reunión de Cierre	2/Febrero/2011	8/Febrero/2011
Emisión del Informe definitivo	12/Abril/2011	26/Abril/2011

5.6. Evaluación del área de sistemas en base a la propuesta

Luego de realizar una evaluación al departamento técnico de la carrera de Ingeniería de Sistemas Computacionales en base a la propuesta, se encontró lo siguiente:

Política de Seguridad de Información

HECHO	OBSERVACION	EVIDENCIA	RIESGO	OPRTUNIDADES DE MEJORA	DOMINIO	CONTROL
No existe política de Seguridad de la información ni documento de la misma.	El coordinador de hardware como el subdirector conocen los beneficios de contar con una política de seguridad de información pero no se ha tomado alguna medida para realizar la misma por falta de respaldo del directorio.	No	Alto nivel de exposición y utilización de la información. Falta de concienciación del personal de la institución.	➢ Contar con una política de seguridad de información para la institución, lo cual es necesaria y urgente, la misma de ser debidamente aprobada por los niveles superiores de la misma. ➢ Dar a conocer a todos y cada una de las personas que trabajan en la institución. ➢ Una vez definida la política y fomentada la misma debe ser revisada de manera periódica para su actualización	Política de Seguridad de la Información	5.1.1 Documento de política de seguridad de Información . 5.1.2. Revisión de la política de seguridad de la información .

				ajustándose a los nuevos procedimiento de la institución según su propia evolución		

Gestión de Activos

HECHO	OBSERVACION	EVIDENCIA	RIESGO	OPRTUNIDADES DE MEJORA	DOMINIO	CONTROL
Responsabilidad de activos	Se cuenta con una persona que lleva un control de los equipos de computación que existen en la institución y el movimiento de los mismos(bodeguero)	Si	Bajo	➢ Contar con otra persona alterna que adquiera el conocimiento y responsabilidad que tiene el actual.	Gestión de Activos	7.1.2 Propiedad de los activos
Inventario interno.	Se cuenta con un inventario general que se maneja en la oficina central de la universidad, pero la institución maneja un inventario interno de equipos hecho en Excel, actualizado cada 3	Si	Perdida del documento	➢ Contar con un sistema de inventario de equipos, que se actualice de manera automática para que permita tomar decisiones oportunas en caso de ser necesario.	Gestión de Activos	7.1.1 Inventario de Activos

	meses					
Etiquetado de equipos	Todos los equipos de computación que existen en la institución están identificados en base a la función de cada uno. Ver anexo 6.10	Si	Quiten el etiquetado	➢ Contar con etiquetas estandarizadas en la cual incluyan código y departamento al que pertenecen.	Gestión de Activos	7.1.1. Inventario de Activos
Utilización correcta de los activos	No se cuenta con reglas documentadas ni divulgadas que regulen el uso aceptable de la información, equipos, dispositivos móviles dentro o fuera de la institución.	No	Alto riesgo de pérdida de equipos y divulgación información importante de la institución	➢ Contar con reglas documentadas del uso adecuado de los equipos e información existente en la institución. ➢ Dar a conocer a todas las personas que laboren en la institución, estudiantes, proveedores.	Gestión de Activos	7.1.3. Uso aceptable de los activos.
Clasificación de la información	No se cuenta con una clasificación de la información.	No	Alto riesgo de que información confidencial e importante no cuente con la protección necesaria.	➢ Contar con una clasificación de la información para conocer la necesidad, protección y uso de la misma. ➢ Esta clasificación	Gestión de Activos	7.2.1 Directrices de clasificación 7.2.2 Etiquetado y

				debe ser conocida por las personas que laboran en la institución.		manipulación de la información

Seguridad Física y del Entorno

HECHO	OBSERVACION	EVIDENCIA	RIESGO	OPRTUNIDADES DE MEJORA	DOMINIO	CONTROL
No se cuenta con controles de ingreso para el departamento técnico informático.	Cuando una persona ingresa se le consulta en que se la puede ayudar o con quien desea hablar aunque no se lleva un control de ingreso a la misma.	No	Alto	➢ Contar con un registro de las personas que ingresan y salen del departamento técnico informático, en la cual indiquen hora de llegada, salida, persona a quien visito.	Seguridad Física y del Entorno	9.1.2 Controles Físicos de Entrada
➢ Se cuenta con dos puertas de entradas y salidas de la institución. ➢ La oficina del coordinador de hardware también funciona	➢ Solo se utiliza una puerta para ingresar y salir de la institución, la cual es utilizada por los colaboradores, estudiantes, personas	Si	Alto	➢ Contar con una salida de emergencia, señalizada y darla a conocer a las personas que laboran, visitan o estudian en la institución. ➢ Contar con un	Seguridad Física y del Entorno	9.1.3 Seguridad de oficinas, despachos e instalaciones. 9.1.6 Áreas de acceso público y de carga y descarga.

como área de servidores. ➢ Se cuenta con una puerta de entrada y salida del departamento técnico de la institución. Ver anexo 6.9	externas, vehículos y proveedores. ➢ Contar con un área designada a los servidores con adecuada ventilación. ➢ Falta una división adecuada del departamento técnico informático. ➢ Las puertas se abren de manera manual.			área designada a los servidores con adecuada ventilación. ➢ Contar con una puerta automática o de brazo para el ingreso al departamento técnico informático.		
➢ Existe un documento de control de ingreso y salida para las personas que ingresan caminando a la institución y que llevan un equipo de computación.	Este control se lleva a cabo siempre y cuando el equipo este a la vista; cuando la persona va a salir se revisa que coincida con los datos tomados anteriormente. Ver anexo 8 El documento antes	Si	Baja	➢ Mejorar la revisión de las personas que ingresan o salen de la institución especialmente las que llevan mochila.	Seguridad Física y del Entorno.	9.1.2 Controles Físicos de Entrada.

	mencionado es entregado y custodiado por el Coordinador Administrativo, guardado por un año. También se lleva un control del personal administrativo y docentes, cualquier otra persona pasa sin registro alguno ya que se considera estudiante.					
Seguro de los equipos de computación por pérdida o sustracción.	➢ Los equipos de computación cuentan con un seguro, en caso de pérdida deben ser reemplazados en su totalidad por la aseguradora. (El documento físico de este contrato se encuentra guardado en la administración	No	El riesgo es bajo ya que este seguro se lleva a cabo en su totalidad.	➢ Contar con una copia del seguro de los equipos en la dirección de la institución.	Seguridad física y del entorno.	9.2.1 Instalación y protección de los equipos.

	central de la institución),					
Extintores de incendio	Se cuenta con un extintor de incendio en cada laboratorio y en el departamento técnico informático. Ver anexo 6.11	Si	El riesgo en Medio ya que no se tiene conocimiento del contenido pero el mantenimiento si se lo realiza en la fecha indicada.	➢ Contar con extintores con polvo químico seco.	Seguridad física y del entorno.	9.2.1 Instalación y protección de los equipos.
Mantenimiento de los equipos de computación	El mantenimiento de los equipos es realizado por una empresa externa, la misma que realiza esta tarea dos veces al año.	No	El riesgo de daños en los equipos en bajo ya que el mantenimiento se lo realiza de manera puntual.	➢ Contar con controles formales que permitan que permitan asegurar un grado de confianza, satisfacción y desempeño que brinda el hardware. ➢ Contar con un procedimiento interno para la medición de la calidad de servicios contratados (mantenimiento)	Seguridad física y del entorno.	9.2.4 Mantenimiento de los equipos
Los equipos son utilizados fuera de la institución	Cuando un equipo va a ser utilizado fuera de la	No	El riesgo de pérdida o daño del equipo es	➢ No aplica	Seguridad física y del entorno.	9.2.5 Seguridad de los equipos

	institución se lleva un documento en el cual se detalla el nombre de la persona encargada, serie, número de equipos, destino. Este documento es firmado por el Coordinador de Hardware y el Coordinador Administrativo.		bajo ya que se cuenta con un documento de respaldo que garantiza la devolución de los mismos.			fuera de la institución
Cableado de datos	▪ Se cuenta con un cableado de datos que pasa por la parte superior de las paredes sobre rejillas de acero. Ver anexo 6.12. ▪ Se cuenta con dos Rack de comunicaciones en el cual el cableado no se encuentra totalmente ordenado, además no	Si	El riesgo es medio ya que para alcanzar los cables debe utilizar una escalera.	➢ Contar con aplicación de normas para cableado estructurado. ➢ Contar con un cableado en el rack ordenado que facilite la utilización del mismo. ➢ Contar con un etiquetado del cableado para facilitar la resolución de inconvenientes.	Seguridad física y del entorno.	9.2.3 Seguridad del cableado.

	existe identificación de los mismos.					
Cableado Eléctrico	Se cuenta con un cableado eléctrico que pasa por rejillas de acero en la parte superior de las paredes, está debidamente etiquetado y polarizado, dentro de tubos de pvc. Ver anexo 6.12	Si	El riesgo es medio ya que para alcanzar los cables debe utilizar una escalera.	➢ Contar con aplicación de normas para cableado eléctrico.	Seguridad física y del entorno.	9.2.3 Seguridad del cableado.

Control de Acceso

HECHO	OBSERVACION	EVIDENCIA	RIESGO	OPRTUNIDADES DE MEJORA	DOMINIO	CONTROL
Documento de política de control de acceso.	No se cuenta con una política para el control del acceso de los usuarios a la información existe en la institución. Ni documentación de la misma.	No	El riesgo es Alto por cuanto las personas que laboran en la institución desconocen la debida utilización de la información	➢ Contar con una política de control de acceso documentada y aprobada por los directivos de la institución. ➢ Dar a conocer a todos y cada una de las personas que trabajan en la	Control de acceso	11.1.1 Política de control de acceso

			que se maneja.	institución. ➢ Revisar y actualizar la política de control de acceso en base a los cambios en la institución.		
Gestión de acceso de usuario	Se cuenta con una persona encargada de administrar el acceso de los usuarios a la información, pero no existe un procedimiento formal para el mismo.	No	El riesgo es Alto por cuanto la persona que se encarga de esto es el coordinador de hardware.	➢ Contar con regla de control de acceso definidas por los propietarios de las aplicaciones existentes. ➢ Contar con un administrador de seguridad que aplique reglas de control de acceso.	Control de Acceso	11.2.2 Gestión de privilegios de usuarios
Contraseñas de ingreso a los equipos.	No se cuenta con una política de contraseñas para los usuarios existentes y nuevos pero de manera informal se indica las características, manejo y seguridad de la misma.	No	El riesgo es medio, ya que se procura que los usuarios tengan una contraseña segura.	➢ Contar con una política formal y documentada de creación de contraseñas, la misma que debe ser fomentada en la institución.	Control de acceso	11.2.3 Gestión de contraseña de usuarios.
Acuerdo de confidencialidad	No se cuenta con un acuerdo de	No	El riesgo es Alto, ya que	➢ Contar con un acuerdo de	Control de Acceso	11.2.4 Revisión de

	confidencialidad a la información que se maneja de la institución		las personas desconocen la importancia de la información que manejan.	confidencialidad, el mismo que debe ser firmado por todos las personas que laboran en la institución.		derecho de usuario
Acceso a la red	Se cuenta con bloqueo de ingreso a la red a nivel de los puertos de los switch existentes en del departamento técnico informático de la institución.	Si (se realizo una prueba con una portátil)	El riesgo es Bajo porque el nivel de seguridad es alto.	➢ Contar con equipos de back-up con los mismos parámetros de los principales.	Control de Acceso	11.4.6 Control de conexión a la red

OTROS HALLAZGOS.

Además de encontrar lo antes mencionado, se pudo observar lo siguiente que a pesar de no estar en nuestro alcance se pone a consideración:

- Las personas encargadas de la vigilancia interna de la institución, son los conserjes los mismo que cuales no cuentan con capacitación requerida para realizar este trabajo, ellos reportan semanalmente los acontecimientos suscitados a Coordinador Administrativo.

- El personal de la institución no cuenta con una capacitación en caso de que suceda una emergencia o desastre natural, lo cual ha sido propuesto por el coordinador de hardware sin tener resultados positivos hasta el momento que se realizo esta auditoría.

- Las personas que laboran en el Dpto. Técnico informático tienen botellas llenas de liquido cerca de los equipo de computación lo cual puede ocasionar accidentes.

- No se cuenta con un antivirus robusto.
- En la actualidad los respaldos de la información se los realiza en cds los mismos que son realizados cada semestre y se custodian en la oficina del director de la institución.

- Actualmente la estructura del Departamento técnico es limitada para atender y mejorar las necesidades tecnológicas del negocio, y satisfacer sus demandas de corto y mediano plazo, identificándose una actitud de resignación de parte de los usuarios internos ya que no posee un personal estable con el cual contar.

- Las personas que ayudan en los 6 laboratorios son pasantes quienes son alumnos de la carrera que están cursando el cuarto semestre en adelante los cuales son capacitados por el coordinador de hardware, para dar soporte y manejar los laboratorios. Ellos realizan esta labor por 3 meses, lo cual impide implementar una nueva estructura de funcionamiento del área por el corto tiempo de existencia del personal.

- No cuentan con un plan de contingencia.

5.7 Reporte de Auditoria

A continuación se detalla el reporte de la auditoría efectuada en la institución:

INFORME DE AUDITORIA INFORMATICA

Institución Auditada:

Carrera de Ingeniería de Sistemas de la Universidad de Guayaquil

Departamento Auditado

Departamento Técnico Informático

Objetivos:

Realizar una evaluación constructiva y objetiva a los procesos de: Seguridades en Infraestructura de TI con el fin de determinar el grado de eficiencia, eficacia y efectividad que se manejan los recursos físicos, técnicos, tecnológicos, relaciones con terceros (outsourcing), y lo adecuado de sus procesos.

Alcance de la Auditoria:

Evaluar en forma integral los procesos de Seguridades en Infraestructura Física de TI por el período entre el 01 de Enero de 2010 al 30 de Junio de 2010, verificando, examinando y reportando sobre el cumplimiento la adecuación y efectividad del sistema de control interno y el cumplimiento con las políticas y procedimientos establecidos por la institución.

Metodología Utilizada:

Para realizar esta auditoría se utilizo lo siguientes:

- Se utilizo los dominios de Política de Seguridad de la Información, Gestión de Activos, Seguridad Física y ambiental, Control de Acceso; de la norma ISO 27002:2005.
- Se utilizo la herramienta de entrevistas y observación al personal que labora en el departamento técnico informático, oficinas administrativas de la institución auditada.
- Se utilizo la herramienta de observación en el departamento técnico informático, laboratorios de computación y pasillos.

Hallazgos y Sugerencias
Basados a la propuesta de auditoría se encontró lo siguiente:

Política de Seguridad de Información
Hallazgos

1. No se cuenta con una política de seguridad de la información en la institución, lo cual conlleva a un alto nivel de exposición y utilización de la información.

La norma indica:

La dirección debería establecer una política clara y en línea con los objetivos del negocio, demostrar su apoyo y compromiso con la seguridad de la información mediante la publicación y mantenimiento de esta política de seguridad de la información para toda la organización.

Sugerencias

1. Contar con una política de seguridad de información para la institución, lo cual es necesaria y urgente, la misma de ser debidamente aprobada por el director de la institución.

2. Dar a conocer esta política a todos y cada una de las personas que trabajan en la institución.

3. Una vez definida la política y fomentada la misma debe ser revisada de manera periódica para su actualización ajustándose a los nuevos procedimiento de la institución según su propia evolución

Gestión de Activos
Hallazgos

1. Se cuenta con una persona que lleva un control de los equipos de computación que existen en la institución y el movimiento de los mismos.
2. Se cuenta con un inventario general que se maneja en la oficina central de la universidad, pero la institución maneja un inventario interno de equipos hecho en Excel, actualizado cada 3 meses.
3. Todos los equipos de computación que existen en la institución están identificados en base a la función de cada uno.
4. No se cuenta con reglas documentadas ni divulgadas que regulen el uso aceptable de la información, equipos, dispositivos móviles dentro o fuera de la institución.
5. No se cuenta con una clasificación de la información.

La norma indica:

Todos los activos deberían estar justificados y tener asignado un propietario, el cual debe ser responsable de la adecuada protección del activo asignado.
Se debe elaborar y mantener un inventario de activos de información, mostrando el propietario del activo y los detalles del activos (Ej.: ubicación, no. serie, etc.).
Se debería identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.

Sugerencias

1. Contar con otra persona alterna que adquiera el conocimiento y responsabilidad que tiene el actual.
2. Contar con un sistema de inventario de equipos, que se actualice de manera automática para que permita tomar decisiones oportunas en caso de ser necesario.
3. Contar con etiquetas estandarizadas en la cual incluyan código y departamento al que pertenecen.
4. Contar con reglas documentadas del uso adecuado de los equipos e información existente en la institución.
5. Dar a conocer las reglas del uso adecuado de los activos a todas las personas que laboran en la institución, estudiantes, proveedores.
6. Contar con una clasificación de la información para conocer la necesidad, protección y uso de la misma.
7. Esta clasificación debe ser conocida por las personas que laboran en la institución.

Seguridad Física y Ambiental
Hallazgos

1. No se cuenta con controles de ingreso para el departamento técnico informático.
2. Se cuenta con una puerta manual de ingreso al departamento técnico informático.
3. Se cuenta con una oficina que funciona como cuarto de servidores y puesto de trabajo del coordinador de hardware.
4. Se cuenta con dos entradas a la institución pero se utiliza una como entrada del personal que labora en la institución, estudiantes, proveedores.
5. No existe piso falso en el cuarto de servidores.
6. Se cuenta con mantenimiento de los equipos por parte de un proveedor externo dos veces al año.

7. Se cuenta con un control y documentación de los equipos ingresados por estudiantes y al salir se verifica que los datos del equipo saliente coincidan con los datos tomados anteriormente, este documento es entregado al Coordinador Administrativo quien custodia dicho documento por 1 año.
8. Se cuenta cuentan con un seguro para los equipos de computación de la institución en caso de pérdida o sustracción, los cuales deben ser reemplazados en su totalidad por la aseguradora. (El documento físico de este contrato se encuentra guardado en la administración central de la institución).
9. En el departamento técnico informático y en cada laboratorio existe un extintor de incendio, al cual se le da mantenimiento cada 11 meses como lo indica la fecha de caducidad del producto, pero no se conoce su contenido.
10. Se cuenta con un cableado de datos que pasa por la parte superior de las paredes sobre rejillas de acero.
11. Se cuenta con dos Rack de comunicaciones en el cual el cableado no se encuentra totalmente ordenado, además no existe identificación de los mismos.
12. Se cuenta con un cableado eléctrico que pasa por rejillas de acero en la parte superior de las paredes, está debidamente etiquetado y polarizado, dentro de tubos de Pvc.

La norma indica:

Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización.
Evitar la pérdida, daño, robo o puesta en peligro de los activos e interrupción de las actividades de la organización.

Sugerencias

1. Contar con un registro de las personas que ingresan y salen del departamento técnico informático, en la cual indiquen hora de llegada, salida, persona a quien visito.
2. Contar con una puerta automática para el ingreso y salida del departamento técnico informático.
3. Contar con una mejor distribución del departamento técnico informático.
4. Contar con salidas de emergencia en la institución debidamente señalizadas y dar a conocer la existencia de las mismas a todas y cada una de las personas que laboran, visitan o estudian en la institución.
5. Contar con piso falso adecuado para el cuarto donde se encuentran los servidores.

6. Contar con un procedimiento interno para la medición de la calidad de servicios contratados (mantenimiento).

7. Mejorar la revisión de las personas que ingresan o salen de la institución especialmente las que llevan mochila.

8. Contar con una copia del seguro de los equipos en la dirección de la institución.

9. Contar con extintores que contengan polvo químico seco que es el indicado para rociar en equipos de computación.

10. Contar con aplicación de normas para cableado estructurado.

11. Contar con un etiquetado del cableado para facilitar la resolución de inconvenientes.
12. Contar con un cableado en el rack más organizado que facilite la utilización del mismo.
13. Contar con aplicación de normas para cableado eléctrico.

Control de Acceso
Hallazgos

1. No se cuenta con una política de control de acceso a la información. Ni documentación de una existida.
2. Se cuenta con una persona encargada de administrar el acceso de los usuarios a la información, pero no existe un procedimiento formal para el mismo.
3. No se cuenta con una política de contraseñas para los usuarios existentes y nuevos pero de manera informal se indica las características, manejo y seguridad de la misma.
4. No se cuenta con un acuerdo de confidencialidad a la información que se maneja de la institución.
5. Se cuenta con bloqueo de ingreso a la red a nivel de los puertos de los switch existentes en del departamento técnico informático de la institución.

La norma indica

Se deberían controlar los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad.
Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la institución.

Sugerencias

1. Contar con una política de acceso a la información, la misma debe ser documentada y dada a conocer a todos y cada una de las personas que laboran en la institución.
2. Contar con regla de control de acceso definidas por los propietarios de las aplicaciones existentes.
3. Contar con una política formal y documentada de creación de contraseñas, la misma que debe ser fomentada en la institución.
4. Contar con un acuerdo de confidencialidad, el mismo que debe ser firmado por todos las personas que laboran en la institución.
5. Contar con un administrador de seguridad que aplique reglas de control de acceso.
6. Contar con equipos de comunicación back-up con los mismos parámetros de los principales.

Conclusiones:

Se considera esta auditoría como aceptable ya que con ella se dio a conocer las vulnerabilidades y fortalezas que tiene el Departamento Técnico Informático, espero que la misma aporte oportunidades de mejoras para alcanzar las metas de la institución.

Ing. Sayne Colobón Castillo
Auditor de Sistemas

CAPITULO 6

6.1 PROPUESTA DE AUDITORIA

ANEXOS No 1

[redacted]

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

"Impulsando la Sociedad del Conocimiento"

CEC-A-085-2010

Guayaquil, 27 de julio del 2010

Ingeniero
Fernando Castro
Subdirector de la Carrera de Ingeniería de Sistemas
Universidad de Guayaquil
Presente

15745
Fernanda Cano C.

Estimado Ingeniero.:

El Centro de Educación Continua de la ESPOL (CEC) ofrece distintos cursos y programas de post-grado atendiendo las necesidades de los profesionales y del sector empresarial de nuestro País.

Cada uno de nuestros programas busca los mejores resultados en el aprendizaje mediante la aplicación de los conocimientos adquiridos en proyectos que son desarrollados en empresas que deseen brindar su aporte en la formación de nuestros profesionales y beneficiarse de los resultados de los proyectos.

En este contexto, uno de nuestros participantes del Diplomado de Auditoria Informática ha seleccionado el Departamento Técnico de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil, para el desarrollo de su proyecto final para lo cual requerimos su aceptación formal.

El proyecto es el siguiente:

TEMA: Infraestructura Física de TI basados en la Norma ISO 27002

Objetivos.- Realizar una evaluación constructiva y objetiva a los procesos de: Infraestructura Física de TI con el fin de determinar el grado de seguridad, riesgos y controles con que se manejan los recursos físicos técnicos, tecnológicos, relaciones con terceros (outsourcing), y lo adecuado de sus procesos.

Alcance Del Proyecto:
Evaluar los procesos de TI e Infraestructura Física de TI del primer semestre del 2010, verificando, examinando y reportando sobre la adecuación y cumplimiento con las políticas y procedimientos de TI establecidos por la compañía.

La revisión comprenderá lo siguiente:

POLITICA DE LA SEGURIDAD

- Política de seguridad de la información
- Documento de política de seguridad de la información
- Revisión de la política de seguridad de la información

Centro de Educación Continua
Guayaquil Ecuador

GUAYAQUIL: CAMPUS PROSPERINA KM. 30.5 VIA PERIMETRAL * CASILLA 09-01-5863 * TELEF.: 2269269 FAX (593-4) 854629
SAMBORONDÓN: MALECON 100 Y LOJA, BLOQUE A, OFICINA 104 TELEF.: 2830488 - 2830489
QUITO: AV. 6 DE DICIEMBRE 3355 y LEON ALFARO ED. TORRE BLANCA 2DO PISO * TELEFONOS: 256615 - 561999

6.2 Acuerdo de Confidencialidad

ANEXO No. 2

ACUERDO DE CONFIDENCIALIDAD

La suscrita del presente compromiso se compromete a mantener la confidencialidad con relación a toda la documentación accesible por su condición de auditora y declara que está de acuerdo con lo siguiente:

- Entender, apoyar y cumplir con la política, estándares y procedimientos de seguridad que gobiernan la protección de los activos de información.

- A No mantener la información entregada como confidencial de manera reservada, mantenerla protegida del acceso de terceros, con el fin de no permitir su conocimiento o manejo por parte de personas no autorizadas.

- A no permitir la copia o reproducción total o parcial de los documentos e información obtenidos en esta auditoría, que no necesite conocer.

- Manifiesta y reconoce que conoce en su totalidad el contenido del presente compromiso, y que comprende a cabalidad el alcance y las obligaciones tanto directas como subsecuentes que del mismo se derivan, en consecuencia y aceptación de lo cual lo suscribe

Ing. Sayne Colobón
Auditora de Sistemas
CI. 0802124115

6.3 Memorándum de Planificación

ANEXO No. 3

PROYECTO DE AUDITORIA	MEMORANDUM DE PLANIFICACIÓN	
	NOMBRE DE LA EMPRESA:	CARRERA DE INGENIERIA DE SISTEMAS COMPUTACIONALES
	NOMBRE DEL PROYECTO:	Auditoria de Seguridades en la Infraestructura Física de TI basados en la Norma ISO 27002

1. INTRODUCCIÓN

De conformidad con las conversaciones previas efectuadas con el Ing. Fernando Castro representando a LA CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL, realizaremos una Auditoria de Seguridades en la Infraestructura Física de TI basada en la Norma ISO 27002.

2. OBJETIVO GENERAL

Realizar una evaluación constructiva y objetiva a los procesos de: Seguridades en la Infraestructura de TI con el fin de determinar el grado de eficiencia, eficacia y efectividad con que se manejan los recursos físicos, técnicos, tecnológicos, relaciones con terceros (outsourcing), y lo adecuado de sus procesos.

3. OBJETIVO ESPECÍFICOS

3.1 Validar la existencia de una Política de Seguridad de la información.
- 3.1.1 Solicitud de Documentación de la política de seguridad de la información
- 3.1.2 Revisión y evaluación de Documentación de la política de seguridad de la información.

3.2 Verificar la Gestión de los activos
- 3.2.1 Verificar las responsabilidades de los usuarios
- 3.2.2 Verificar la clasificación de la información

3.3 Verificar la Seguridad Física y Ambiental
- 3.3.1 Validar las Áreas Seguras.
- 3.3.2 Validar la Seguridad de los equipos

3.4 Validar el Control De Accesos
- 3.4.1 Verificación de Requerimientos de negocio para el control de accesos
- 3.4.2 Verificación de Administración de accesos de usuarios
- 3.4.3 Verificación de la responsabilidad de los usuarios
- 3.4.4 Validación de Control del acceso de red

4. ALCANCE DE LA AUDITORIA

Evaluar en forma integral los procesos de Seguridades en la Infraestructura Física de TI por el período entre el 01 de Enero de 2010 al 30 de Junio de 2010, verificando, examinando y reportando sobre el cumplimiento la adecuación y efectividad del sistema de control interno y el cumplimiento con las políticas y procedimientos establecidos por la compañía.

5. CRONOGRAMA DE ACTIVIDADES CLAVE DEL PROCESO DE AUDITORIA

ACTIVIDAD	FECHA DE INICIO	FECHA FINAL
Reunión de Inicio	2/Septiembre/2010	
Entendimiento de los Procesos, identificación de riesgos	20/Septiembre/2010	24/Septiembre/2010
Trabajo en Campo	1/Octubre/2010	14/Diciembre/2010
Reunión de Aclaración Final	28/Octubre/2010	10/Noviembre/2010
Borrador del Informe de Auditoria	11/Enero/2011	14/Enero/2011
Reunión de Cierre	2/Febrero/2011	8/Febrero/2011
Emisión del Informe definitivo	12/Abril/2011	26/Abril/2011

6. DOCUMENTOS A SOLICITAR

Políticas, estándares, normas y procedimientos.
Plan de sistemas.
Planes de seguridad y continuidad
Contratos, pólizas de seguros.
Organigrama y manual de funciones.
Registros
Entrevistas
Archivos

7. MIEMBROS DEL EQUIPO DE AUDITORIA

Ing. Sayne Colobón Castillo Telf.: 094033186

7. Preocupaciones o asuntos de interes de los representantes de carrera de ingeniería de sistemas computacionales

El Subdirector de CARRERA DE INGENIERIA DE SISTEMAS COMPUTACIONALES me comentó que desea que se les realice la evaluación basado en los siguientes puntos:

POLITICA DE SEGURIDAD

- Política de seguridad de la información
- Documento de política de seguridad de la información
- Revisión de la policía de seguridad de la información

GESTION DE ACTIVOS

- Responsabilidad por los activos
- Clasificación de la información

SEGURIDAD FISICA Y AMBIENTAL

- Áreas Seguras
- Equipo de seguridad

CONTROL DE ACCESOS

• Requerimientos de negocio para el control de acceso • Administración de accesos de usuarios • Registro de Usuarios • Responsabilidad de los usuarios • Control de acceso a la red
9. POSIBLES LIMITACIONES
Se perciben limitaciones de evaluaciones en sitio en horario laboral.
10. OTROS ASUNTOS IMPORTANTES
Ninguno.

ELABORADO POR:	Ing. Sayne Colobón	**FECHA:**	22/Septiembre/2010	**FIRMA:**	
REVISADO POR:	Ing. Fernando Castro	**FECHA:**	23/Septiembre/2010	**FIRMA:**	
AUTORIZADO POR:	Ing. Fernando Castro	**FECHA:**	24/Septiembre/2010	**FIRMA:**	

6.4 Carta de Aceptación de Auditoria

ANEXO No. 4

Universidad de Guayaquil
Facultad de Ciencias Matemática y Físicas
Carrera de Ingeniería en Sistemas Computacionales

Guayaquil, Septiembre 14 del 2010
Ofic. N° 113-2010-SUB-CISC

Máster
Julia Bravo
Directora
Centro de Educación Continua – CEC
En su despacho.-

Ref: Infraestructura Física de TI basados en Norma ISO

Por medio del presente, comunico a usted, que el proyecto presentado por la Ing. Sayne Colobon Castillo, con tema: **Infraestructura Física de TI basados en Norma ISO 27002**, a ser realizado en la Carrera de Sistemas Computacionales de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Guayaquil, tengo a bien indicar que nuestra institución le concede los permisos de acceso a las dependencias de nuestra Carrera con la supervisión de los responsables de cada una de las áreas, para el desarrollo del tema antes mencionado.

Atentamente,

ING.FERNANDO CASTRO AGUILAR, M.Sc
SUBDIRECTOR

C.c.: Archivo
FCA/Rosa

CEC - C
2010

6.5 Acta de Inicio de Auditoria

ANEXO No. 5

Guayaquil 17 de Septiembre 2010

Ing. Fernando Castro
Subdirector de la Carrera de Ingeniería de Sistemas Computacionales
En su despacho

El presente es para informarle que, de acuerdo con nuestro Proyecto de Auditoria, iniciaremos la revisión de auditoría en el Departamento Técnico Informático, a partir del 1 de Octubre del 2010
Para realizar una evaluación constructiva y objetiva a los procesos de: Seguridades en Infraestructura de TI con el fin de determinar el grado de eficiencia, eficacia con que se manejan los recursos físicos, técnicos, tecnológicos, relaciones con terceros (outsourcing), y lo adecuado de sus procesos.

La auditoria está planificada en tres etapas, como sigue:

Etapa 1. Consiste en conocer mediante una entrevista con el jefe de área o encargado de la misma, las actividades y procesos que llevan a cabo.
En esta etapa se evaluará el cumplimiento a los procedimientos autorizados y se podrán definir aquellos procesos o actividades que no se están llevando a cabo o se llevan de forma distinta al procedimiento, procesos o actividades.
Asimismo esta etapa nos sirve para determinar los procesos o actividades que realmente son susceptibles de auditar.

Etapa 2. Realización de la Auditoria. Una vez determinados los procesos o actividades susceptibles de auditar, presentaremos un plan de trabajo y el requerimiento de información necesario para llevar a cabo la revisión de los mismos

Etapa 3. Presentación de Resultados. En esta etapa presentamos los resultados obtenidos de mi revisión, así como las propuestas de solución o de implementación de nuevos mecanismos para mejorar los procesos o actividades revisados. Antes de emitir cualquier reporte de manera oficial, nuestras conclusiones siempre serán comentadas el Auditado.

Atentamente;

Ing. Sayne Colobón Castillo
Auditor de Sistemas

7.6 Acta de Reunión de Inicio

ANEXO No. 6

PROYECTO DE AUDITORIA	REUNIÓN DE INICIO DE AUDITORÍA	
	Empresa:	**CARRERA DE INGENIERIA DE SISTEMAS COMPUTACIONALES**
	Nombre del Proyecto:	**AUDITORIA DE SEGURIDADES EN INFRAESTRUCTURA FÍSICA DE TI BASADOS EN LA NORMA ISO 27002**

I. ASISTENTES	
NOMBRE	**PUESTO**
Ing. Fernando Castro	Subdirector
Ing. Alfonso Guijarro	Coordinador de Hardware
Ing.	Coordinador de Software
Ing. Sayne Colobón	Auditor de Sistemas

II. PUNTOS COMENTADOS			
Propósito y Alcance	x	**Comunicación de Hallazgos**	
Ubicación Física	x	**Reunión de Revisión del Informe**	
Auditor Asignado	x	**Evaluación del Informe**	
Fecha de Inicio y Duración	x	**Proceso de Acciones Correctivas**	

III. COMENTARIOS DEL CLIENTE			
Manifestó puntos específicos que desea sean incluidos en la revisión	Si	☐	No ☒
DESCRIPCIÓN:			
Descritos en el Memorándum			
Señaló algún problema en específico que requiere sea evaluado	Si	☐	No ☒
DESCRIPCIÓN:			

Elaboro	Ing. Sayne Colobón	Fecha:		Iniciales:	SC

6.7 Documento de las funciones del personal de departamento técnico informático

ANEXO No. 7

FUNCIONES

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES
Coordinador de Hardware
Versión 2010

Descripción

El Coordinador de Hardware es el responsable por el buen funcionamiento de los equipos informáticos, sistemas de redes y comunicaciones de la Carrera incluyendo el área administrativa y laboratorios. Así como la coordinación de las actividades del equipo de trabajo compuesto por Administrador de Red, Ayudantes de Laboratorio y Pasantes.

Perfil

El Coordinador requiere un conocimiento alto de hardware y mantenimiento de equipos y redes, así como técnicas y mecanismos de seguridad física y lógica, entre las características técnicas necesarias para ocupar este cargo tenemos:

- Conocimientos avanzados de Hardware de equipos informáticos.
- Conocimientos avanzados de instalación, administración y mantenimiento de Sistemas Operativos para equipos de Escritorio y Servidores: Windows 2000, Windows XP, Windows Seven, RedHat, CentOs, Fedora, entre otros.
- Conocimientos avanzado de instalación y optimización de cableado estructurado.
- Conocimientos avanzados de instalación, configuración, administración y protección de redes informáticas.
- Conocimientos avanzados de instalación, configuración y administración de equipos de seguridad y acceso físico, y su integración con sistemas

informáticos: sensores biométricos, cámaras CCTV, sensores de movimiento, entre otros.

- Conocimientos avanzados de instalación, configuración y administración de equipos de seguridad lógica para redes informáticas: firewall, ruteadores, entre otros.
- Conocimiento avanzado de administración y optimización de Servidores de Bases de Datos: Oracle, SQL Server, MySql, PostGreSQL, entre otros.
- Conocimientos de seguridad física de las áreas de trabajo y seguridad industrial.

Las labores del Coordinador de Hardware los llevan a tratar directamente con diferentes tipos de personas, por lo que la persona que ocupe el cargo debe contar con las siguientes características personales:

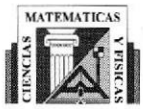
- Buenas relaciones interpersonales.
- Pulcritud.
- Proactividad.
- Manejo de equipos de trabajo.
- Manejo de proyectos, y tiempos de entrega
- Conocimientos de investigación de operaciones.
- Conocimientos de psicología laboral.
- Conocimientos de redacción de informes técnicos

Actividades

El Coordinador de Hardware debe cumplir con las siguientes actividades:

- Elaborar el Plan Estratégico del Departamento Técnico Informático de la Carrera.
- Elaborar el Plan de Seguridad, Contingencias y Desastres para preservar la continuidad de las operaciones de la Carrera.
- Colaborar en la planificación y desarrollo de eventos técnicos y científicos de la Carrera y la Facultad.
- Preparar y presentar informes de factibilidad técnica de hardware, equipos de comunicación y de redes, solicitados por Dirección y Subdirección de la Carrera.
- Reunirse periódicamente con el personal a su cargo para determinar tareas y establecer cronogramas de trabajo.
- Recibir y procesar los informes de equipos con problemas detectados por los Ayudantes de Laboratorio o Pasantes.
- Establecer y actualizar periódicamente las políticas y procedimientos de seguridad de acceso y control físico del Departamento Técnico Informático.
- Establecer y actualizar periódicamente las políticas y procedimientos de seguridad de acceso lógico a los equipos y sistemas de la Carrera.

- Establecer, actualizar periódicamente y publicar las políticas de préstamos de equipos informáticos a estudiantes y docentes de la Carrera.
- Coordinar con el equipo de trabajo las responsabilidades para la administración, configuración, envío de información y respaldo de bases de datos de la Carrera.
- Coordinar con el equipo de trabajo la ayuda que requiera el personal de Secretaría durante los procesos de matriculación de Semestre y Preuniversitario.
- Monitorizar el acceso a los recursos informáticos de la Carrera: Bases de Datos, Internet; para la detectar e impedir el uso no apropiado de los mismos.
- Mantener bajo su resguardo los discos originales de Instalación del Software de la Carrera y controlar las copias de los mismos necesarias para su respectiva instalación en los laboratorios y área administrativa.
- Mantener bajo su resguardo los respaldos de las aplicaciones y bases de datos de la Carrera.
- Mantener bajo su resguardo los inventarios actualizados de equipos informáticos y mobiliario de laboratorios y áreas administrativas.
- Informar al administrador del edificio (con copia a Dirección) de la entrada y salida de equipos que sean utilizados para préstamos.
- Informar al administrador del edificio (con copia a Dirección) de la entrada y salida de equipos para su reparación en el CAS.
- Establecer los parámetros técnicos físicos para los productos de Tesis o Seminario de Graduación que vayan a ser implantados en la Carrera.
- Interactuar con el Coordinador de Software para definir la agenda de trabajo de ambas áreas logrando una sinergia en los procesos técnicos administrativos.
- Presentar a la Dirección de la Carrera el informe mensual y anual de actividades realizadas, cabe indicar que debe enviarse una copia de este informe al Jefe de Personal de la Universidad.



UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES
Coordinador de Software
Versión 2010

Descripción

El Coordinador de Software es el responsable por la planificación, administración y control en el desarrollo del software de la Carrera.

Entre sus responsabilidades se incluye la administración y control de los recursos humanos e informáticos con los que cuenta la Carrera para el diseño, programación e implementación de aplicaciones propias.

Perfil

El Coordinador requiere un alto conocimiento de software y herramientas de desarrollo, así como técnicas y procedimientos para brindar a las aplicaciones un nivel alto de seguridad de acceso y disponibilidad, entre las características técnicas necesarias para ocupar este cargo tenemos:

- Conocimientos avanzados de ingeniería de software, y desarrollo de aplicaciones de escritorio y Web.
- Conocimientos avanzados de diseño y optimización de Bases de Datos.
- Conocimientos avanzados de seguridad informática y encriptación de datos.
- Manejo avanzado de herramientas de desarrollo de aplicaciones propietarias: Microsoft Visual Studio 6.0 y .Net, Microsoft FoxPro, Microsoft SQL Reporting Services, entre otras.
- Manejo avanzado de herramientas de desarrollo de aplicaciones de código abierto: NetBeans, JDeveloper, Eclipse, entre otras.
- Conocimientos avanzados de herramientas de diseño propietarias y de código abierto para aplicaciones Web y de escritorio: Microsoft Expression, Adobe Flash, Adobe DreamWeaver, Adobe Fireworks, entre otras.
- Conocimientos avanzados de Servidores de aplicaciones propietarios y de código abierto: Internet Information Server, JBoss, Apache, GlassFish, entre otros.

- Conocimientos avanzados de instalación, administración y mantenimiento de Sistemas Operativos para equipos de Escritorio y Servidores: Windows 2000, Windows XP, Windows Seven, RedHat, CentOs, Fedora, entre otros.
- Conocimiento avanzado de administración y optimización de Servidores de Bases de Datos: Oracle, SQL Server, MySql, PostGreSQL, entre otros.
- Conocimientos de seguridad física de las áreas de trabajo y seguridad industrial.

El Coordinador de Software debe contar con las siguientes características dentro del perfil administrativo:

- Manejo de proyectos, y tiempos de entrega.
- Conocimientos de investigación de operaciones.
- Conocimientos de redacción de informes técnicos

Las labores del Coordinador de Software los llevan a tratar directamente con diferentes tipos de personas, por lo que la persona que ocupe el cargo debe contar con las siguientes características personales:

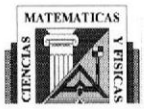
- Buenas relaciones interpersonales.
- Pulcritud.
- Proactividad.
- Manejo de equipos de trabajo.
- Conocimientos de psicología laboral.

Actividades

El Coordinador de Software debe cumplir con las siguientes actividades:

- Colaborar junto con el Coordinador de Hardware en el diseño e implementación del Plan Estratégico del Departamento Técnico Informático de la Carrera.
- Colaborar activamente en el Plan de Seguridad, Contingencias y Desastres para preservar la continuidad de las operaciones de la Carrera.
- Colaborar en la planificación y desarrollo de eventos técnicos y científicos de la Carrera y la Facultad.
- Preparar y presentar informes de factibilidad técnica de software, desarrollado localmente o adquirido a terceros, solicitados por Dirección y Subdirección de la Carrera.
- Reunirse periódicamente con el personal a su cargo para determinar tareas y establecer cronogramas de trabajo.
- Establecer y actualizar periódicamente las políticas y procedimientos para el desarrollo de aplicaciones y productos informáticos de la Carrera.

- Coordinar con el equipo de trabajo las responsabilidades para la administración, configuración, envío de información y respaldo de bases de datos de la Carrera.
- Coordinar con el equipo de trabajo la ayuda que requiera el personal de Secretaría durante los procesos de matriculación de Semestre y Preuniversitario.
- Realizar pruebas de control de calidad de los productos desarrollados en la Carrera.
- Establecer los parámetros técnicos de software para los productos de Tesis o Seminario de Graduación que vayan a ser implantados en la Carrera.
- Revisar, analizar y probar nuevas tecnologías que mejoren la calidad o seguridad del software desarrollado por la Carrera
- Interactuar con el Coordinador de Hardware para definir la agenda de trabajo de ambas áreas logrando una sinergia en los procesos técnicos administrativos.
- Presentar a la Dirección de la Carrera el informe mensual y anual de actividades realizadas, cabe indicar que debe enviarse una copia de este informe al Jefe de Personal de la Universidad.



UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES
Ayudante de laboratorio
Versión 2010

Descripción

Los ayudantes son personas dedicadas al control, administración y actualización de los recursos disponibles para estudiantes y docentes en los laboratorios de cómputo de la Carrera, así como el grupo de *pasantes* que esté a su cargo.

El cargo está orientado a Egresados o Estudiantes del último nivel de la Carrera de Ingeniería en Sistemas Computacionales, los mismos que deben contar con conocimientos básicos de hardware y software que les permitan brindar un servicio rápido y eficiente.

Perfil

El ayudante de laboratorio requiere un conocimiento medio-alto de hardware y mantenimiento de equipos y redes, entre las características técnicas necesarias para ocupar este cargo tenemos:

- Manejo de utilitarios básicos: Microsoft Office, Open Office.
- Conocimiento básico de hardware de computadores: Ensamblaje, configuración de BIOS, instalación y configuración de hardware incluyendo impresoras y escáner.
- Conocimiento básico de software de computadores: Instalación, actualización, configuración de programas.
- Instalación, manejo y configuración de sistemas operativos: Windows 2000, Windows XP, Windows Seven, Windows Server, RedHat, CentOS, Ubuntu.
- Conocimiento de redes computacionales: instalación, configuración de dispositivos, ensamblado de cables y conectores.

Las labores del ayudante los llevan a tratar directamente con docentes y estudiantes, así como el manejo de los pasantes que tenga asignados, por lo que la persona que ocupe el cargo debe contar con las siguientes características personales:

- Buenas relaciones interpersonales.
- Pulcritud.
- Proactividad.

- Trabajo en equipo.

Actividades diarias

Los ayudantes deben cumplir con las siguientes actividades:

- Coordinar con los pasantes las actividades del día, incluyendo las tareas asignadas por el Administrador de la Red o Coordinador de Hardware.
- Dejar constancia del estado del laboratorio asignado, a la entrada y a la salida.
- Revisar la bitácora del laboratorio, y reportar cualquier anomalía con respecto a equipos o mobiliario.
- Permitir el acceso a los laboratorios únicamente a los estudiantes matriculados en el Semestre o en Preuniversitario.
- No permitir el ingreso al laboratorio con alimentos o bebidas a ninguna persona sin excepción.
- Llevar un registro de los estudiantes que son atendidos en el laboratorio asignado.
- Dar soporte técnico a los estudiantes.
- Controlar del uso que los estudiantes den a los equipos computacionales, considerando que está prohibido abrir el computador, instalar software o hardware no autorizado, cambiar componentes de un computador a otro; así también, está prohibido el acceso a páginas pornográficas, redes sociales (MySpace, Facebook, Hi5, etc.), mensajería instantánea (Messenger, ILoveIM, etc.) o juegos en red (Travian, WildGuns, X-Wars, ManagerZone, etc.).
- Reportar el o los equipos que tengan problemas y que requieran del servicio técnico autorizado, que no puedan ser reparados en los laboratorios.
- Mantener, en la medida de lo posible, actualizados los programas de antivirus, dependiendo de la carga de trabajo del laboratorio.
- Reportar la presencia de personas ajenas a la institución, que demuestren actitudes sospechosas.
- Reportar a los estudiantes que sean encontrados jugando dentro del laboratorio.
- Dar soporte técnico al docente que tenga clases asignadas en el laboratorio, cabe indicar que el cargo es "*Ayudante de Laboratorio*" no "*Ayudante del profesor*".
- Archivar de manera ordenada los documentos concernientes al laboratorio: informes, órdenes de entrega-recepción, memos, solicitudes de préstamo de equipos, entre otros.
- Coordinar con el personal de servicio la limpieza del laboratorio.

Actividades mensuales

Las siguientes actividades deben realizarse por lo menos una vez a la semana:

- Confirmar y actualizar los inventarios del laboratorio, que incluyen los equipos computacionales, periféricos y mobiliario.

Actividades semestrales

Las siguientes actividades deben realizarse previo al inicio de cada semestre:

- Confirmar y actualizar los inventarios de equipos y mobiliarios asignados al laboratorio.
- Presentar un informe de equipos enviados para reparación, y el estado actual de los mismos.
- Formatear los equipos y prepararlos para el inicio de actividades del semestre.
- Coordinar con el Administrador de la Red o Coordinador de Hardware, los requerimientos de software de los docentes para su respectiva instalación, previo al inicio de clases.

Actividades no periódicas

Las siguientes actividades deben realizarse previo al inicio de cada semestre:

- Colaborar con las actividades de Dirección, Coordinación Académica y Secretaría que hayan sido coordinadas con el departamento técnico.
- Colaborar con la recepción, revisión e inventario interno de equipos tecnológicos nuevos adquiridos por la Universidad o directamente por la Carrera.
- Entregar y Recibir los equipos que hayan sido reportados cono dañados y que sean retirados o devueltos por el CAS de la Universidad. Esto incluye revisar el estado del bien, números de serie e inventario. Cabe indicar que toda entrada o salida de equipo(s) debe ser respaldada por la respectiva "*Solicitud de Entrada-Salida*", aprobada por el Administrador del Edificio y con conocimiento de Dirección.
- Colaborar con los estudiantes y docentes durante la realización de Ferias tecnológicas o Casas Abiertas.

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES
Programador
Versión 2010

Descripción

Los programadores son personas dedicadas al diseño, desarrollo, implementación e implantación de aplicaciones informáticas propias, así como la prueba e implantación de nuevos programas que ayuden al desarrollo tecnológico de la Carrera.

El cargo está orientado a Graduados de la Carrera de Ingeniería en Sistemas Computacionales, los mismos que deben contar con conocimientos avanzados de Desarrollo de Aplicaciones de Escritorio y Aplicaciones Web.

Perfil

El ayudante de laboratorio requiere un conocimiento medio-alto de hardware y mantenimiento de equipos y redes, entre las características técnicas necesarias para ocupar este cargo tenemos:

- Conocimientos de Ingeniería de Software, y los diferentes paradigmas del ciclo de vida de los sistemas.
- Conocimientos de Bases de Datos: diseño, implementación y optimización.
- Conocimiento de Herramientas Informáticas propietarias para Desarrollo, por ejemplo: Visual Basic, VisualFox
- Conocimientos de Herramientas de Código Abierto para Desarrollo, por ejemplo: JDeveloper, Eclipse, NetBeans.
- Conocimientos medios de Herramientas de Administración de Bases de Datos.
- Conocimiento y administración de Servidores de Aplicaciones Web: Internet Information Server, Apache, JBoss, GlassFish, entre otros.
- Conocimiento de Componentes para desarrollo con herramientas propietarias.
- Conocimiento de Frameworks para desarrollo Web: JQuery, Prototype, entre otros.
- Conocimiento medio de software de computadores: Instalación, actualización, configuración de programas.

- Instalación, manejo y configuración de Sistemas Operativos: Windows 2000, Windows XP, Windows Seven, Windows Server, RedHat, CentOS, Ubuntu.

Las labores del programador los llevan a tratar directamente con diferentes tipos de personas, desde usuarios "novatos" hasta avanzados, por lo que la persona que ocupe el cargo debe contar con las siguientes características personales:

- Buenas relaciones interpersonales.
- Pulcritud.
- Proactividad.
- Trabajo en equipo.

Actividades

El programador debe cumplir con las siguientes actividades:

- Coordinar con el Líder de Proyecto las actividades diarias a cumplir relacionadas con el calendario de actividades y entrega de avances en el desarrollo y pruebas de programas.
- Colaborar con las labores de respaldo de Bases de Datos, en coordinación con el Líder de Proyecto y Coordinador de Software.
- Colaborar con el diseño y actualización de estándares y procedimientos para: desarrollo de sistemas, inventarios de software, administración de la red para los sistemas informáticos, soporte a usuario y respaldos de información.
- Colaborar con la administración y soporte técnico de software de los usuarios de la red administrativa: Dirección, Coordinación Académica y Secretaría.
- Ayudar en el cumplimiento de las políticas de seguridad establecidas para la salvaguarda de la información crítica de la Carrera.
- Colaborar en el mantenimiento del sitio Web de la Carrera.
- Colaborar en recuperación de información, análisis y compilación de reportes solicitados por los diversos departamentos de la Institución.
- Analizar periódicamente la situación actual de los procesos administrativos, informáticos y no informáticos, con la finalidad de sugerir soluciones que permitan optimizar dichos procesos, para que se acoplen a los estándares establecidos para estos fines.
- Colaborar con las actividades de Dirección, Coordinación Académica y Secretaría que hayan sido coordinadas con el departamento técnico.
- Colaborar con la recepción, revisión e inventario interno de equipos tecnológicos nuevos adquiridos por la Universidad o directamente por la Carrera.

6.8 Documento de Control de Equipos

ANEXO No. 8

Universidad de Guayaquil
Facultad de Ciencias Matemáticas y Físicas
Carrera de Ingeniería en Sistemas Computacionales

CONTROL DE EQUIPOS PARA:

PROFESOR, ESTUDIANTE Y PERSONAL NO DOCENTE

☐ ☑ ☐

FECHA : 3 - Ene - 2010

PARA : **Ing. Juan Chanabá Alcócer, M.Sc – Director**

DEL ALUMNO : Isaac Baldeón Garcia

Por medio de la presente, solicito se me permita el ingreso del siguiente equipo; cuyas características son:

Equipo y / o Componentes	Marca	Serie	Modelo / Tipo	Laboratorio o Aula	Nombre del Profesor
Case	—	R5695	Torre		

HORA DE INGRESO: 5:00 PM

FECHA DE SALIDA: 3/01/2011 HORA DE SALIDA: 20:00

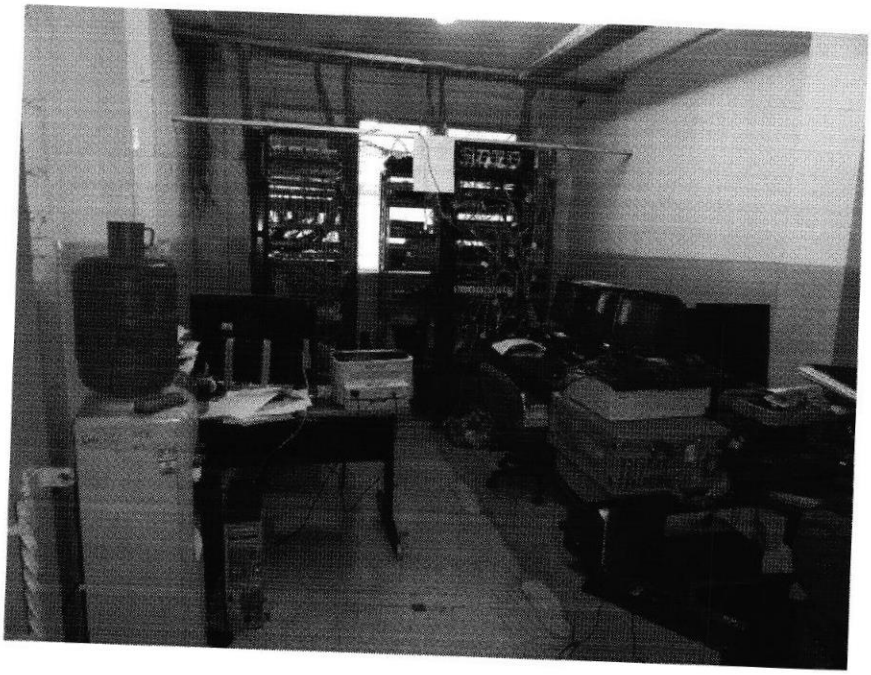
(f.) Isaac Baldeón G.
Nº Cedula 0922490385 - 1
Código Estudiantil 2000 2

REVISADO POR
Guardián de Turno

NOTA: Al presentar la solicitud, la persona debe de adjuntar un documento que lo identifique, sea está la Cédula de Identidad o el Carné Estudiantil al guardián de turno, la misma que será devuelta al salir con el equipo. Cada persona se hace responsable de su equipo al ingresar al edificio de la Carrera.

6.9 Fotos Dpto. Técnico Informático

ANEXO No. 9

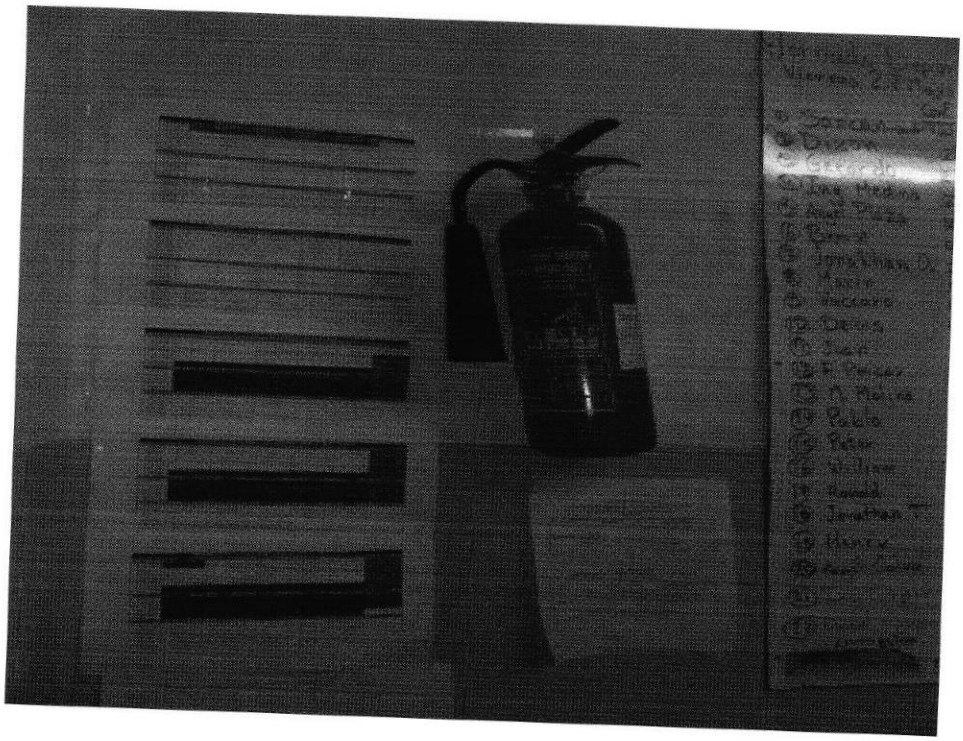


6.10 Etiquetado De Equipos

ANEXO No. 10

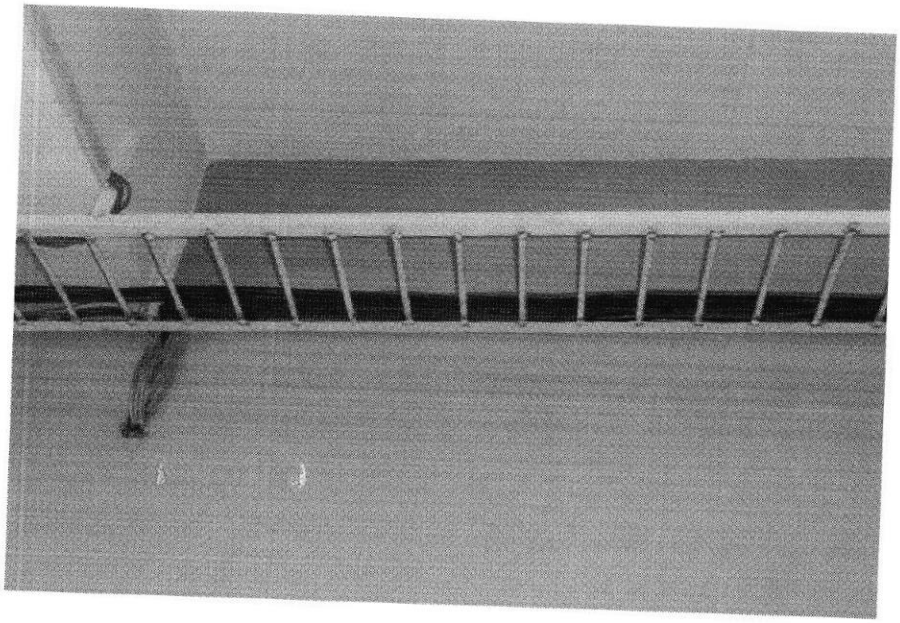
6.11 Foto Extintores

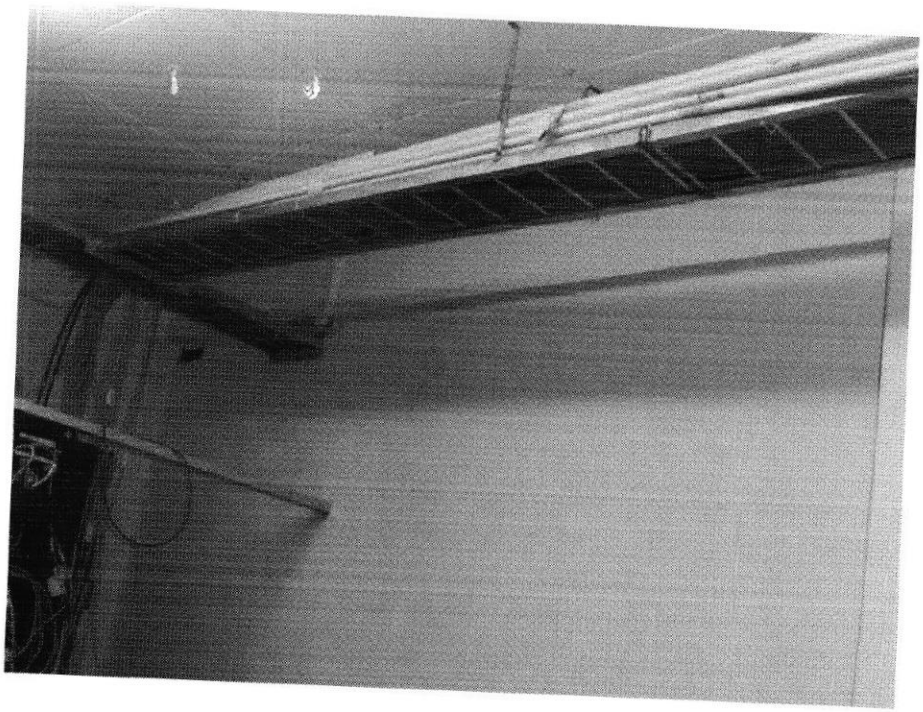
ANEXO No. 11

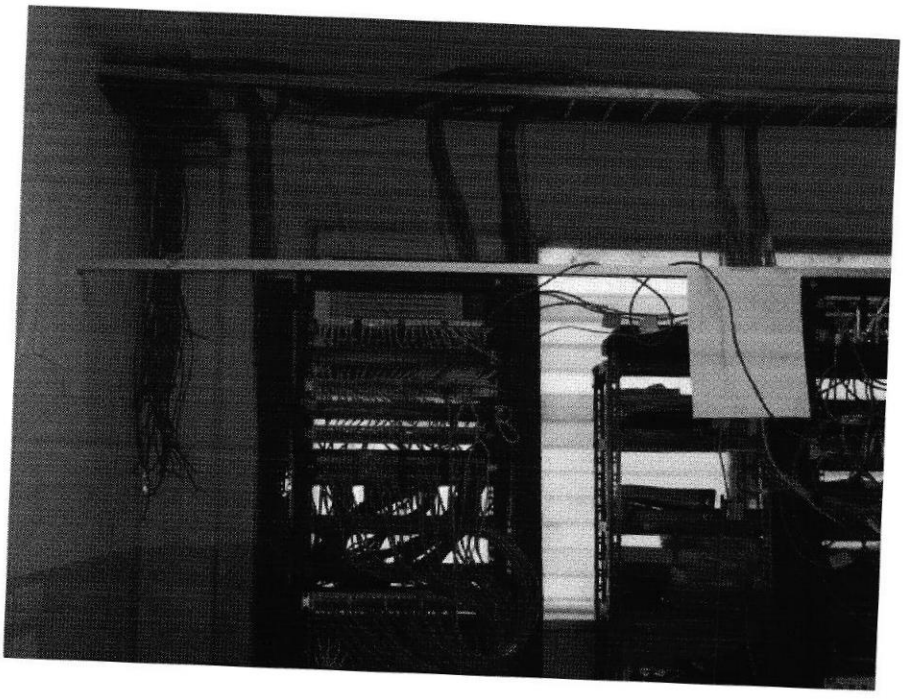


6.12 Foto del Cableado

ANEXO No. 12

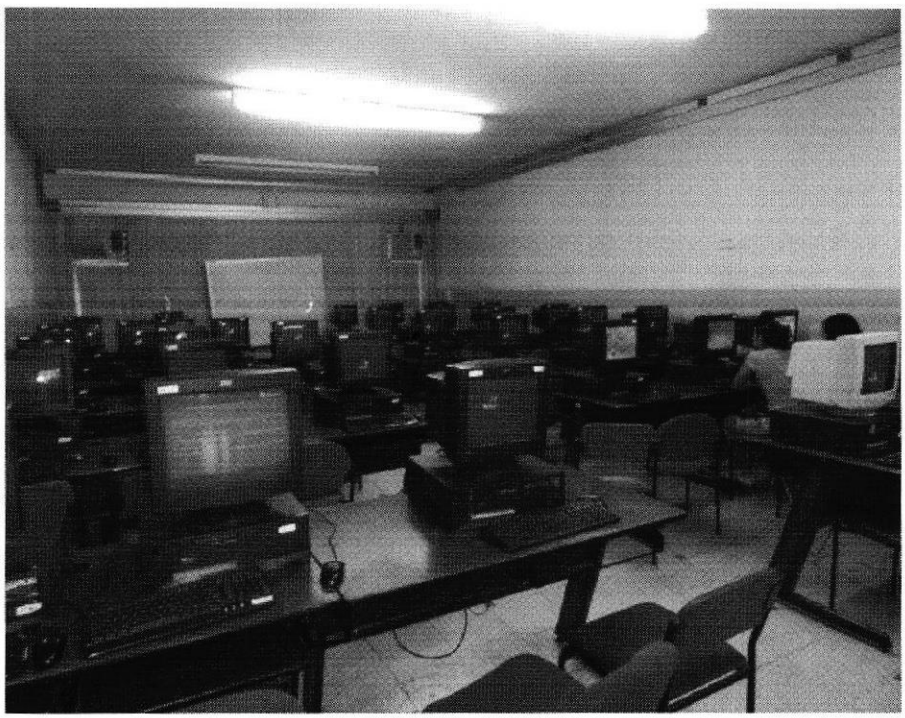






6.13 Foto de los Laboratorios

ANEXO No. 13



CUESTIONARIO DE ENTREVISTA

Cliente		Teléfonos		Web Site	
Entrevistador es)		Dirección			
Fecha y duración					
Horario de atención					

Entrevistados

Nombre	Cargo	Teléfono	Ext	Celular	Correo
1					
2.-					
3.-					
4.-					
5.-					

1. ORGANIZACIONAL

1.1. Distribución física y geográfica (Anexo 1.1)

Locación	Actividad	Dirección	Piso	# pc / departamentos	# Empleados	Observaciones

Locación	Actividad	Dirección	Piso	# pc / departamentos	# Empleados	Observaciones

1.2. Estructura Organizacional

Pregunta	Respuesta	Observaciones
¿Existe un organigrama organizacional?	☐ Sí ☐ No	No tiene un documento que respalde

2. TECNOLÓGICO

2.1. Tendido eléctrico

Pregunta	Respuesta	Observaciones
¿Han experimentado constantes problemas de daño de equipos por fallas eléctricas, variaciones de voltaje?	☐ Sí ☐ No	
¿Posee un tendido eléctrico exclusivo para sus equipos informáticos? Si la respuesta es **si** continúe	☐ Sí ☐ No	# puntos de luz (en base a pc's): •

con sgte. pregunta		Documentación del tendido eléctrico : ☐ Sí ☐ No Proveedor: •
¿Las tomas para los equipos de computación están señalizadas y polarizadas?	☐ Sí ☐ No	

2.2. Cableado

Pregunta	Respuesta	Observaciones
¿Existe cableado estructurado de servicio para:	Voz ☐ Sí ☐ No # Puntos: _____ Datos ☐ Sí ☐ No # Puntos: _____ Video ☐ Sí ☐ No # Puntos: _____	Documentación ☐ Sí ☐ No Desglose ☐ Sí ☐ No Mapeo de los puntos ☐ Sí ☐ No Listado de los puntos de cableado ☐ Sí ☐ No Dispositivos de cableado: •
¿Está certificado este cableado?	☐ Sí ☐ No	Fecha: Norma: Empresa: Documentación ☐ Sí ☐ No
El cableado fue implementado por:	Empresa:	Fecha:

Servicios inalámbricos	Dispositivos de cableado: o Nombres: •) o Nombre:

2.3. Equipos (PC + periféricos) Anexo 2.3 y 2.3a

Pregunta	Respuesta	Observaciones
¿Existe registro de inventario de las estaciones de trabajo, impresoras?	☐ Sí ☐ No	Nivel de detalle Básico ☒ Completo ☐ Proveedor de mantenimiento de equipos: Fecha de último mantenimiento: Frecuencia de mantenimiento:. Cada 3 meses Horarios de mantenimiento preferido:.
¿Mapa de distribución de estaciones de trabajo?	☐ Sí ☐ No	Formato del documento: Word
¿Documentación de SO y aplicaciones de escritorio instaladas por usuarios?	☐ Sí ☐ No	Nivel de detalle Básico ☐ Completo ☐ Depende del trabajo que realice el usuario
¿Existe registro de impresoras?	☐ Sí ☐ No	# imp. Matriciales: # imp. Láser: # imp. inyección:

Pregunta	Respuesta	Observaciones
¿Tienen centros de impresión?	☐ Sí ☐ No	Ubicación:

2.4. Servidores (Anexo 2.4)

Servidor	Detalle / Servicio	Observaciones
Nombre: S.O.: Marca y Modelo:	**Roles:** Controlador de Dominio. ☐ _____ DNS ☐ DHCP ☐ WINS ☐ Acceso Remoto ☐ Archivos ☐ _____ _____ Impresión ☐ _____ _____ Intranet ☐ _____	Ubicación: Doc. Instalación y config. ☐ Responsable:

Servidor	Detalle / Servicio	Observaciones
	_____ Correo ☐ Base de Datos ☐ _____ Aplicaciones ☐ _____ _____ Antivirus ☐ _____ _____ Respaldos ☐ _____ _____ Proxy de Internet ☐ _____ Faxes ☐ _____ _____ Firewall ☐ _____	
Nombre: S.O.:	**Roles:** Controlador de Dominio. ☐ Es el PDC porque es un Windows NT DNS ☐ DHCP ☐ WINS ☐	Ubicación:

Servidor	Detalle / Servicio	Observaciones
Marca y Modelo:	Acceso Remoto ☐ Archivos ☐ Instaladores, BD de Access, Fuentes y ejecutables de S.I., drivers Impresión ☐ _____ Intranet ☐ _____ _____ Correo ☐ _____ _____ Base de Datos ☐ Aplicaciones ☐ _____ _____ Antivirus ☐ _____ _____ Respaldos ☐ _____ _____ Proxy de Internet ☐ _____ __	Doc. Instalación y config. ☐ Responsable:

Servidor	Detalle / Servicio	Observaciones
	Faxes ☐ Desarrollo ☐	
1) Nombre: S.O.: Marca y Modelo:	**Roles:** Controlador de Dominio. ☐ DNS ☐ DHCP ☐ WINS ☐ Acceso Remoto ☐ Archivos ☐ Impresión ☐ Intranet ☐ Correo ☐ Base de Datos ☐	Ubicación: Doc. Instalación y config. ☐ Responsable:

Servidor	Detalle / Servicio	Observaciones
	Aplicaciones ☐ Antivirus ☐ Respaldos ☐ Proxy de Internet ☐ Faxes ☐	
2) Nombre: S.O.: Marca y Modelo:	**Roles:** Controlador de Dominio. ☐ DNS ☐ DHCP ☐ WINS ☐ Acceso Remoto ☐ Archivos ☐	Ubicación: Doc. Instalación y config. ☐ Responsable:

Servidor	Detalle / Servicio	Observaciones
	Impresión ☐ Intranet ☐ Correo ☐ Base de Datos ☐ Aplicaciones ☐ Antivirus ☐ Respaldos ☐ Proxy de Internet ☐ Faxes ☐	

Servidor	Detalle / Servicio	Observaciones
	_____ _____	
3) Nombre: S.O.: Marca y Modelo:	**Roles:** Controlador de Dominio. ☐ _____ DNS ☐ DHCP ☐ WINS ☐ Acceso Remoto ☐ Archivos ☐ _____ _____ Impresión ☐ _____ _____ Intranet ☐ _____ _____ Correo ☐ _____ _____ Base de Datos ☐ _____ Aplicaciones ☐ _____	Ubicación: Doc. Instalación y config. ☐ Responsable:

Servidor	Detalle / Servicio	Observaciones
	Antivirus ☐ Respaldos ☐ Proxy de Internet ☐ Faxes ☐	

2.5. Inventario de licencias (Anexo 2.5)

Pregunta	Respuesta	Observaciones
¿Existen un inventario de licencias?	☐ Sí ☐ No	
¿Los programas que utilizan están licenciados? • Estaciones de trabajo o Sistemas operativos	☐ Sí ☐ No	

Pregunta	Respuesta	Observaciones
○ Aplicaciones de escritorio (Office) ○ Antivirus cliente ○ Aplicaciones de diseño (Autocad, Adobe, Visio) ○ Aplicaciones de desarrollo (visual, cristal) ○ Aplicaciones de proyectos (Project) ○ Aplicaciones de control remoto ○ Utilitarios • Servidores ○ Sistemas operativos ○ De Correo ○ De Bases de Datos ○ De Internet y Firewall ○ Intranet Corporativa ○ Manejador de proyectos ○ Aplicaciones de gestión ○ Antivirus corporativo ○ Antispam corporativo (Microsoft Antispyware)	☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No	

Pregunta	Respuesta	Observaciones
o De Respaldos		

2.6. Internet ()

Pregunta	Respuesta	Observaciones
¿Tienen Página Web? Dirección:	☐ Sí ☐ No Documentación: ☐ Sí ☐ No	Fecha en que se publico el sitio : _____ Fecha de última modificación: _____ Administración y mantenimiento del sitio: Personal TI ☐ Tercerizado ☐ Compañía: _____ Contacto principal: _____
¿Tienen un dominio?	☐ Sí ☐ No Documentación: ☐ Sí ☐ No	Proveedor dominio: • Administración y mantenimiento del dominio: Personal TI ☐ Tercerizado ☐

		Compañía: _____ Contacto principal: _____
Sevicio de Alojamiento	☐ Sí ☐ No Documentación: ☐ Sí ☐ No	

2.7. Inventario de software, drivers, manuales

- Los cd's de instalación de los programas, drivers y manuales de se administran en esta oficina principal.

Pregunta	Respuesta	Observaciones
¿Existen un registro de inventario físico de drivers? • de las estaciones de trabajo • de los servidores	☐ Sí ☐ No ☐ Sí ☐ No	
¿Existe un registro de inventario de medios de instalación originales de los programas? • de las estaciones de trabajo • de los servidores	☐ Sí ☐ No ☐ Sí ☐ No	
¿Existen un registro de inventario de manuales de		

componentes? • de las estaciones de trabajo • de los servidores	☐ Sí ☐ No ☐ Sí ☐ No	
¿Tienen un lugar específico para almacenar estas componentes?	☐ Sí ☐ No	

2.8. Inventario de partes y piezas

Pregunta	Respuesta	Observaciones
¿Existen un registro de inventario de partes y piezas de estaciones de trabajo y de servidores que estén fuera de uso, pero que pueden ser reutilizadas?	☐ Sí ☐ No	
¿Tienen un lugar específico para almacenar estas partes y piezas? Ubicación actual:	☐ Sí ☐ No	

2.9. Inventario de equipos de protección (UPS, reguladores) Anexo 2.12

Pregunta	Respuesta	Observaciones
¿Existen un registro de inventario de reguladores y UPS?	☐ Sí ☐ No	Mapa de ubicación de UPS y reguladores ☐ Sí ☐ No Fecha de último mantenimiento: •
¿Todos los equipos están protegidos con reguladores?	☐ Sí ☐ No	
¿Todos los equipos están protegidos con UPS?	☐ Sí ☐ No	

3. Gerencia de Sistemas

3.1. Administración de la función de Informática

Pregunta	Respuesta	Observaciones
Conoce la misión, visión y los objetivos de la empresa	☐ Sí ☐ No	Documentación: ☐ Por medio de una presentación.
Realizan planes estratégicos para el área de TI	☐ Sí ☐ No	Documentación: ☐
¿Tienen un departamento que administre y realice las funciones de TI?	☐ Sí ☐ No	No. de integrantes: • _____ • _____ • _____
¿Existe un documento que detalle las funciones del personal de TI?	☐ Sí ☐ No	Documentación ☐
Se realizan evaluaciones al personal de TI	☐ Sí ☐ No	
Disponen de Presupuesto para el área de TI	☐ Sí ☐ No	Documentación ☐

Manejan parámetros de medición de los productos y servicios del área de TI	☐ Sí ☐ No	Documentación ☐
Se realizan capacitaciones del personal de TI	☐ Sí ☐ No	Frecuencia ☐

3.2. Asegurar integración con responsables de los procesos de negocio. Dirección y niveles ejecutivos

Pregunta	Respuesta	Observaciones
Se realiza un seguimiento de las funciones de TI	☐ Sí ☐ No	A quien reporta?
La comunicación entre el área de TI y los niveles directivos existe	☐ Sí ☐ No	
Las funciones de TI apoyan los procesos de toma de decisiones	☐ Sí ☐ No	
Los planes de TI están alineados con el plan de negocio	☐ Sí ☐ No	

3.3. Estandarizar y aplicar el Ciclo de Desarrollo e Implantación de Sistemas de Información

Pregunta	Respuesta	Observaciones
Disponen de una metodología el desarrollo de sistemas de información	☐ Sí ☐ No	Documentación ☐

El personal de desarrollo es capacitado para desarrollar los sistemas de información de la empresa	☐ Sí ☐ No	
Realizan actualizaciones a los sistemas de información	☐ Sí ☐ No	
Los sistemas de información en desarrollo buscan alinearse con los planes estratégicos del área.	☐ Sí ☐ No	

3.4. Redes y Servicios de Comunicación electrónica

Pregunta	Respuesta	Observaciones
Planifican en la implementación, configuración e instalación de los servicios y productos del área	☐ Sí ☐ No	Documentación ☐
Existen manuales de procedimientos para apoyar la operación de las Redes y Servicios	☐ Sí ☐ No	
El personal de TI es capacitado para administrar las Redes y Servicios	☐ Sí ☐ No	
La administración de los equipos y software se definió y está documentada.	☐ Sí ☐ No	

3.5. Mantenimiento (preventivo /correctivo)

Pregunta	Respuesta	Observaciones
Políticas de mantenimiento de hardware • Mainframes • Servidores • Estaciones de trabajo • Portátiles • Impresoras • Equipos de protección • Equipos de comunicaciones	☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No	Documentación ☐
Políticas de mantenimiento de software • Lenguajes de programación • Utilitarios de oficina • Sistemas operativos • Bases de datos • Herramientas CASE • Herramientas de diseño • Aplicaciones de servidores	☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No	Documentación ☐

Pregunta	Respuesta	Observaciones
	☐ Sí ☐ No ☐ Sí ☐ No	
Políticas de mantenimiento de los equipos de telecomunicación • Antivirus • Monitoreo de redes • Cortafuegos • Sistemas detectores de intrusos	☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No	Documentación ☐ .
Políticas de creación y mantenimiento de documentación del área • Contratos • Solicitud de servicios a proveedores • Garantías • Cartas de confidencialidad • Estándares	☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No ☐ Sí ☐ No	Documentación ☐
¿Manejan actualmente alguna política de respaldos?	☐ Sí ☐ No	Documentación ☐

Pregunta	Respuesta	Observaciones
Políticas de almacenamiento de la data empresarial	☐ Sí ☐ No	Documentación ☐
Políticas de redistribución y mudanza de puestos de trabajo	☐ Sí ☐ No	Documentación ☐

3.6. Seguridad

Pregunta	Respuesta	Observaciones
Políticas de seguridad		Documentación ☐
• Lógica	☐ Sí ☐ No	
• Administrativa	☐ Sí ☐ No	
• Física	☐ Sí ☐ No	
• De la Información		
• De los Sistemas de Información	☐ Sí ☐ No	
• Redes		
• Internet	☐ Sí ☐ No	
• De uso de aplicaciones		

Pregunta	Respuesta	Observaciones
	☐ Sí ☐ No ☐ Sí ☐ No	
Planes de contingencia	☐ Sí ☐ No	Documentación ☐
Planes de recuperación ante desastres	☐ Sí ☐ No	Documentación ☐

3.7. Administración tecnológica de hardware

Pregunta	Respuesta	Observaciones
Planes de renovación tecnológica de hardware	☐ Sí ☐ No	Documentación ☐
Justifican económicamente, funcional y tecnológicamente la adquisición de SW	☐ Sí ☐ No	Documentación ☐
Políticas de selección y evaluación de proveedores	☐ Sí ☐ No	Documentación ☐
Políticas de negociación de la compra	☐ Sí ☐ No	Documentación ☐

Pregunta	Respuesta	Observaciones
Políticas de instalación, operación y seguridad de HW	☐ Sí ☐ No	Documentación ☐

3.8. Administración tecnológica de software

Pregunta	Respuesta	Observaciones
Planes de renovación tecnológica de software	☐ Sí ☐ No	Documentación ☐ •
Justifican económicamente, funcional y tecnológicamente la adquisición de SW	☐ Sí ☐ No	Documentación ☐
Políticas de selección y evaluación de proveedores	☐ Sí ☐ No	Documentación ☐
Políticas de negociación de la compra	☐ Sí ☐ No	Documentación ☐
Políticas de instalación, operación y seguridad de SW	☐ Sí ☐ No	Documentación ☐

3.9. Investigación y adquisición de tecnologías emergentes

Pregunta	Respuesta	Observaciones
Evaluación de necesidades del negocio	☐ Sí ☐ No	Documentación ☐
Estudios de mercado	☐ Sí ☐ No	Documentación ☐
Manejan proyectos de benchmarking por clase de tecnología	☐ Sí ☐ No	Documentación ☐
Evaluación de tecnologías requeridas	☐ Sí ☐ No	Documentación ☐
Evaluación y selección	☐ Sí ☐ No	Documentación ☐
Metodologías de adquisición, compra, liberación a producción	☐ Sí ☐ No	Documentación ☐

3.10. Estandarización de productos y servicios de informática(HW, SW, Telecomunicaciones,etc)

Pregunta	Respuesta	Observaciones
Los usuarios finales reciben o han recibido capacitación acerca del uso de las herramientas ofimáticas		Frecuencia:

Pregunta	Respuesta	Observaciones

• Familiariación de equipos
• Sistemas operativos
• Office
  o Word
  o Excel´
  o Power Point
  o Outlook
  o Project
	☐ Sí ☐ No
	☐ Sí ☐ No
	
	☐ Sí ☐ No
	☐ Sí ☐ No
	☐ Sí ☐ No
	☐ Sí ☐ No
	☐ Sí ☐ No	

El personal de TI ha sido capacitado	☐ Sí ☐ No	Frecuencia _____ Tópicos de capacitaciones • _____ • _____ • _____ • _____

8. **BIBLIOGRAFIA**

Norma ISO/IEC 27002:2005

http://iso27002.wiki.zoho.com/ISO-27002.html

http://www.iso27000.es/download/ControlesISO27002-2005.pdf