




### LISTA DE COTEJO

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA		NOMBRE DEL CURSO: <u>AVANCE INFORMATICA</u> UNIDAD: <u>I</u>		
NOMBRE DEL DOCENTE: ROSARIO CARVAJAL HERNÁNDEZ		FIRMA DEL DOCENTE		
DATOS GENERALES DEL PROCESO DE EVALUACION				
NOMBRE DEL ALUMNO: <u>TEOBAL DIAZ EMMANUEL DE JESUS</u>	No. DE CONTROL: <u>22140521</u>	FIRMA DEL ALUMNO: 		
PRODUCTO: <u>INFOGRAFIA</u>	FECHA: <u>20/09/2024</u>	PERIODO ESCOLAR: <u>AGO - DIC 2024</u>		
INSTRUCCIONES DE APLICACION				
Revisar las actividades que se solicitan y marque con una X en los apartados "SI" cuando la evidencia se cumple; en caso contrario marque "NO". En la columna "OBSERVACIONES" escriba indicaciones que puedan ayudar al alumno a saber cuáles son las condiciones no cumplidas, si fuese necesario.				
VALOR DEL REACTIVO	CARACTERÍSTICA A CUMPLIR (REACTIVO)	CUMPLE		OBSERVACIONES
		SI	NO	
5	Material a utilizar: Se apegó a los criterios previamente establecidos.	X		
5	Creatividad: Plasmó los temas con ingenio.	X		
0	Originalidad: El producto es único.	X		
5	Contiene todos los temas relacionados a la unidad.	X		
5	Claridad y Estructura: Se da a entender el tema que se está tratando.	X		
0	Responsabilidad: Entregó el producto en la fecha y hora señalada.	X		
20%	CALIFICACION	20%		

### LISTA DE COTEJO

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA		NOMBRE DEL CURSO: <u>AUDITORIA INFORMATICA</u> UNIDAD: <u>I</u>		
NOMBRE DEL DOCENTE: ROSARIO CARVAJAL HERNÁNDEZ		FIRMA DEL DOCENTE		
DATOS GENERALES DEL PROCESO DE EVALUACION				
NOMBRE DEL ALUMNO: <u>ROBAL QAZ</u> <u>EMMANUEL DE JESUS</u>	No. DE CONTROL: <u>22140 521</u>	FIRMA DEL ALUMNO: 		
PRODUCTO: <u>POSTER</u>	FECHA: <u>20/09/2024</u>	PERIODO ESCOLAR: <u>AUG-DIC 2024.</u>		
INSTRUCCIONES DE APLICACION				
Revisar las actividades que se solicitan y marque con una X en los apartados "SI" cuando la evidencia se cumple; en caso contrario marque "NO". En la columna "OBSERVACIONES" escriba indicaciones que puedan ayudar al alumno a saber cuáles son las condiciones no cumplidas, si fuese necesario.				
VALOR DEL REACTIVO	CARACTERÍSTICA A CUMPLIR (REACTIVO)	CUMPLE		OBSERVACIONES
		SI	NO	
10	Material a utilizar: Se apegó a los criterios previamente establecidos.	X		
0	Creatividad: Plasmó los temas con ingenio.	X		
0	Originalidad: El producto es único.	X		
10	Contiene todos los temas relacionados a la unidad.	X		
10	Claridad y Estructura: Se da a entender el tema que se está tratando.	X		
0	Responsabilidad: Entregó el producto en la fecha y hora señalada.	X		
30/1.	<b>CALIFICACION</b>	30/1.		

### LISTA DE COTEJO

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA		NOMBRE DEL CURSO: <u>AVANCE</u> <u>INFORMÁTICA</u> UNIDAD: <u>I</u>		
NOMBRE DEL DOCENTE: ROSARIO CARVAJAL HERNÁNDEZ		FIRMA DEL DOCENTE		
DATOS GENERALES DEL PROCESO DE EVALUACION				
NOMBRE DEL ALUMNO: <u>TEOBALDÍAS</u> <u>EMMANUEL DE JESÚS</u>	No. DE CONTROL: <u>22240524</u>	FIRMA DEL ALUMNO: 		
PRODUCTO: <u>AVANCE DE PROJ.</u>	FECHA: <u>20/09/2024</u>	PERIODO ESCOLAR: <u>Ago - Dic 2024</u>		
INSTRUCCIONES DE APLICACIÓN				
Revisar las actividades que se solicitan y marque con una X en los apartados "SI" cuando la evidencia se cumple; en caso contrario marque "NO". En la columna "OBSERVACIONES" escriba indicaciones que puedan ayudar al alumno a saber cuáles son las condiciones no cumplidas, si fuese necesario.				
VALOR DEL REACTIVO	CARACTERÍSTICA A CUMPLIR (REACTIVO)	CUMPLE		OBSERVACIONES
		SI	NO	
<u>10</u>	Material a utilizar: Se apegó a los criterios previamente establecidos.	<u>X</u>		
<u>10</u>	Creatividad: Plasmó los temas con ingenio.	<u>X</u>		
<u>5</u>	Originalidad: El producto es único.	<u>X</u>		
<u>10</u>	Contiene todos los temas relacionados a la unidad.	<u>X</u>		
<u>10</u>	Claridad y Estructura: Se da a entender el tema que se está tratando.	<u>X</u>		
<u>5</u>	Responsabilidad: Entregó el producto en la fecha y hora señalada.	<u>X</u>		
<u>50%</u>	<b>CALIFICACIÓN</b>	<u>50%</u>		



# TERMINOLOGÍA DE AUDITORÍA EN INFORMÁTICA

## ¿QUÉ ES UNA AUDITORÍA?

La auditoría es una opinión profesional basada en procedimientos diseñados para obtener información, con el objetivo de evaluar si esta refleja adecuadamente la realidad y cumple con las expectativas asignadas, es decir, su fiabilidad.

La palabra proviene del latín "auditorius," que se relaciona con "auditor," o "el que tiene la virtud de oír."



## AUDITORÍA INFORMÁTICA

La auditoría en informática consiste en revisar y evaluar los controles, sistemas y procedimientos relacionados con el uso de equipos de cómputo. Su objetivo es asegurar la eficiencia y seguridad en el procesamiento de la información dentro de una organización, con el fin de mejorar su uso de manera más confiable y segura.

## TIPOS DE AUDITORÍA

- Financiera
- Operacional
- Sistemas
- Fiscal
- Administrativa
- Calidad
- Social
- Informática**

## MARCOS Y CERTIFICACIONES

### COSO

EL **Committee of Sponsoring Organizations of the Treadway Commission**, es un marco que proporciona directrices para la gestión de riesgos y el control interno.

Se centra en mejorar la efectividad de los procesos de gestión y la integridad financiera.



### ISACA

La **Information Systems Audit and Control Association**, es una organización profesional que ofrece marcos, estándares y certificaciones para la auditoría, control y seguridad de la información.

Promueve buenas prácticas en la gobernanza de TI.



### COBIT

El **Control Objectives for Information and Related Technologies**, es un marco desarrollado por ISACA que proporciona un conjunto de buenas prácticas para la gestión y gobernanza de la tecnología de la información.

Facilita la alineación de TI con los objetivos empresariales.



### CISA

El **Certified Information Systems Auditor**, es una certificación ofrecida por ISACA que valida la experiencia en auditoría de sistemas de información, control y seguridad.

Acredita a los profesionales en la evaluación y mejora de la infraestructura de TI de las organizaciones.



# TÉCNICAS Y HERRAMIENTAS

## HERRAMIENTAS

Son programas o software específicos que facilitan la realización de auditorías, permitiendo ejecutar tareas concretas de manera más eficiente.



## TÉCNICAS

Son métodos o enfoques que se emplean para llevar a cabo el proceso de auditoría. Involucran procedimientos y estrategias para analizar información y evaluar sistemas.



## SEGURIDAD Y PROTECCIÓN DE DATOS

**Backups y Copias:** Estrategia para crear y verificar copias de seguridad de datos críticos.

**Borrado Definitivo:** Proceso para eliminar datos de forma que no puedan ser recuperados.



## ANÁLISIS Y RECUPERACIÓN DE DATOS

**Software de Recuperación de Archivos Borrados:** Herramientas para restaurar archivos eliminados.

**Análisis de Memoria RAM:** Examen del contenido de la memoria para identificar procesos y datos activos.

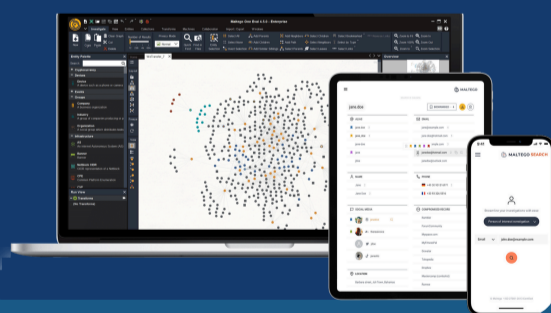
## MONITOREO Y BÚSQUEDA DE INFORMACIÓN

**Software de Búsqueda:** Herramientas para localizar información específica en sistemas y bases de datos.

**Búsqueda de Mails, Historial, Chats:** Localización y análisis de correos electrónicos y registros de comunicación.



## HERRAMIENTAS FORENSES Y DE INTELIGENCIA



**Encase Forensic:** Herramienta forense para análisis de dispositivos de almacenamiento.

**CondorLinux:** Distribución de Linux con herramientas forenses.

**Maltego:** Herramienta de análisis de relaciones e inteligencia.

## DOCUMENTACIÓN Y VERIFICACIÓN

**Impresiones:** Análisis de documentos impresos relevantes para auditorías.



## FUENTES

[1] M. PATTINI Y E. DEL PESO, AUDITORÍA INFORMÁTICA - UN ENFOQUE PRÁCTICO, 2A ED. RAMA: ALFAOMEGA.

[2] J. A. EUCENIQUE GARCÍA, AUDITORÍA EN INFORMÁTICA. MC GRAW HILL.



ROL Y RESPONSABILIDADES DEL

# AUDITOR INFORMÁTICO

## Auditoría Informática

La auditoría informática es un **análisis crítico** de los **sistemas de información** que usa la empresa con el objetivo de **evaluar la eficiencia** de los mismos. También **comprueba** que los sistemas de recopilación y uso de la información cumplan con la normativa vigente y que la gestión de los recursos informáticos sea adecuada y contribuya a la eficiencia de la organización.

## Responsabilidades del Auditor

**Elabora el cronograma de auditorías, Analiza la situación actual de los sistemas y procesos, Controla y verifica el funcionamiento de los sistemas informáticos, Detecta los riesgos, Diseña soluciones y Propone** nuevas estrategias para mejorar los sistemas informáticos.

## Importancia

La auditoría informática es esencial para **proteger** los datos sensibles, **garantizar** el cumplimiento normativo y **mejorar** los controles internos. Además, **ayuda** a las organizaciones a estar preparadas ante incidentes y fomenta una cultura de seguridad entre los empleados.

## Riesgos

La auditoría depende de herramientas tecnológicas que no son infalibles y está sujeta a errores humanos, lo que podría llevar a conclusiones incorrectas. Por lo tanto, es fundamental gestionar estos riesgos para maximizar los beneficios de la auditoría informática.

## Rol del Auditor

El auditor informático es el **profesional encargado de evaluar** los **procesos** relacionados con las tecnologías de la **información** de la empresa, así como su infraestructura tecnológica, para asegurarse de que se ajustan a su actividad principal y ofrecer soluciones viables para los problemas detectados.

## Fuentes

[1] "Características de un auditor informático | Blog UE". Universidad Europea. Accedido el 22 de septiembre de 2024. [En línea]. Disponible: <https://universidadeuropea.com/blog/caracteristicas-auditor-informatico/#:~:text=El%20auditor%20informático%20debe%20dominar,SOX,%20COBIT%20y%20COSO>.



# INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA

## PROYECTO

**ASIGNATURA: AUDITORÍA INFORMÁTICA**

**DOCENTE: ROSARIO CARVAJAL HERNÁNDEZ**

**ALUMNOS: EMMANUEL DE JESÚS TEOBAL DÍAZ**

**MONSERRAT PUCHETA CONCHI**

**SILVANA TIARÉ ROMÁN SANTIAGO**

**LUIS ALEXIS LUCHO HERNÁNDEZ**

**CARRERA: INGENIERÍA EN INFORMÁTICA**

**GRADO Y GRUPO: 510-A**

**FECHA: 24/09/2024**



---

# **INTRODUCCIÓN**



---

# ÍNDICE

## Contenido

1.1 ESTUDIO INICIAL DEL ENTORNO AUDITABLE.....	111
1.2 objetivos.....	112
(se pega lo de classroom).....	<b>¡Error! Marcador no definido.</b>
1.2.1 Objetivo general.....	112
1.2.2 objetivos específicos1.3 PLAN Y PROGRAMA DE AUDITORÍA.....	112
1.3.1 TAREAS.....	<b>¡Error! Marcador no definido.</b>
1.3.2 CALENDARIO.....	<b>¡Error! Marcador no definido.</b>
1.3.3 RESPONSABLES.....	<b>¡Error! Marcador no definido.</b>
1.3.4 ORGANIGRAMA.....	<b>¡Error! Marcador no definido.</b>
1.4 INSTRUMENTOS PARA MEDIR EL NIVEL DE APLICACIÓN DE LA NORMATIVIDAD.	115
1.4.1 Personal.....	115



# CAPITULO I

---

## 1.1 ESTUDIO INICIAL DEL ENTORNO AUDITABLE.

EL "Cyber Joya" es un establecimiento ubicado en Calle 5 de mayo y Iturbide, Hoja de Maíz, 95110 Tierra Blanca, Ver; México, Laborando de lunes a viernes con horario de 7:00 am – 10:30pm, Sábado y Domingo de 9:00am – 5:00pm, Cyber Joya Ofrece Centrado de copiado, papelería, Soluciones por internet, donde los usuarios pueden acceder a equipos informáticos y servicios de Internet, generalmente pagando por tiempo de uso. Cyber Joya ofrece impresiones, escaneos, y en algunos casos, pequeños servicios de reparación de computadoras.

El Cyber Joya depende de un conjunto de computadoras conectadas a internet, una infraestructura de red (routers, switches), y posiblemente servidores para gestionar sesiones y el acceso a recursos compartidos.

La auditoría informática se realiza por las siguientes razones:

- Protección de datos de usuarios, Aunque los usuarios utilizan los equipos temporalmente, es crucial asegurar que la información que manejan (contraseñas, documentos, cuentas de correo) no se quede almacenada en los equipos ni sea vulnerable a ataques o robo de datos.

Dependiendo de la jurisdicción, puede haber normativas de privacidad y protección de datos personales (como el RGPD en Europa), que el negocio debe cumplir.

Dado que los equipos están conectados a Internet de manera constante y que múltiples usuarios acceden a estos recursos, existe un riesgo elevado de ataques informáticos, como malware, ransomware, o accesos no autorizados.

Cyber Joya debe asegurar que su infraestructura informática (hardware, software, redes) funcione correctamente y esté disponible para los usuarios, ya que fallos constantes impactan la continuidad del negocio.

Es importante verificar que todo el software utilizado en las computadoras del cyber esté correctamente licenciado para evitar problemas legales por el uso de software pirata.

Asegurarse de que las herramientas usadas sean apropiadas para el negocio, incluyendo software de control de usuarios y gestión de tiempo.

---

Se necesita una auditoría para evaluar los mecanismos de control de accesos (por ejemplo, software de gestión de tiempo) y asegurar que se están registrando de manera adecuada las actividades de los usuarios, especialmente en casos de uso indebido o actividades ilícitas.

La auditoría informática ayuda a analizar si los equipos informáticos están funcionando de manera óptima y si los procesos de mantenimiento y actualización se están llevando a cabo de manera eficiente.

Un análisis puede identificar ineficiencias en el uso de los recursos tecnológicos y sugerir formas de reducir costos (energía, mantenimiento, renovación de equipos).

## **1.2 OBJETIVOS**

### **1.2.1 OBJETIVO GENERAL**

Aplicar auditorías y consultorías utilizando técnicas y herramientas para la evaluación de las áreas relacionadas con la informática en...

### **1.2.2 OBJETIVOS ESPECIFICOS**

1. Estudiar y analizar el entorno auditable de la empresa...
2. Realizar la planeación y el programa de auditoria
3. Determinar los instrumentos para medir el nivel de aplicación de la normatividad
4. Aplicar la normatividad a la auditoria informática
5. Realizar la auditoria de hardware.
6. Realizar la auditoria de redes
7. Realizar la auditoria en telecomunicaciones
8. Documentar los resultados obtenidos

### 1.3 PLAN Y PROGRAMA DE AUDITORÍA

#### Plan de Auditoría

<b>Objetivos de la Auditoría</b>	<ol style="list-style-type: none"><li>1. Valorar la situación actual de cada una de las áreas de la organización</li><li>2. Realizar una comparación de la situación actual de la organización con respecto a los requisitos de la norma ISO 9001:2000</li><li>3. Poder implementar un Sistema de Calidad basado en la norma ISO 9001:2000</li><li>4. Identificar las No conformidades encontradas en cada una de las áreas de la organización</li><li>5. Proponer acciones correctivas para las no conformidades</li></ol>
<b>Alcance de la Auditoría</b>	<p>Esta auditoría a diferencia de muchas, el auditor fue quien buscó al cliente y le ofreció los servicios de auditoría para posteriormente poder proponer un Sistema de Calidad basado en la norma ISO 9001:2000.</p> <p>Las áreas para auditar son las siguientes:</p> <ol style="list-style-type: none"><li>1. Establecimiento</li><li>2. Ventas</li><li>3. Administrativa<ul style="list-style-type: none"><li>• Herramientas de Software</li><li>• Mobiliario</li></ul></li><li>4. Operativa</li></ol> <p>Al finalizar la auditoría se le entregará al Departamento Administrativo el reporte del final que contiene;</p> <ul style="list-style-type: none"><li>• Plan de auditoría</li><li>• Documento de referencia (Norma ISO 9001:2000)</li><li>• Las observaciones obtenidas</li><li>• Las no conformidades detectadas</li><li>• La propuesta de acciones correctivas</li></ul>
<b>Personas Involucradas</b>	Emmanuel de Jesús Teobal Díaz Montserrat Pucheta Conchi Silvana Tiaré Román Santiago Luis Alexis Lucho Hernández
<b>Documentos Referencia</b>	Se tomará como documento de referencia la Norma ISO 9001:2000 NMX-CC-9001-IMNC-2000 (Se encuentra ampliamente desarrollado en el Capítulo II)
<b>Miembros Equipo Auditor</b>	La persona que realizará la auditoría es Montserrat Pucheta Conchi. Esta persona será encargada de elaborar el plan de auditoría, aplicar las listas de verificación y finalmente realizar el reporte final.

<b>Idioma Auditoría</b>	El idioma utilizado será el español.
<b>Unidades Organizacionales Auditadas</b>	Las unidades organizacionales de Divulga a auditar son: <ol style="list-style-type: none"> <li>1. Establecimiento</li> <li>2. Administrativa</li> <li>3. Ventas <ol style="list-style-type: none"> <li>a. Herramientas de Software</li> <li>b. Mobiliario</li> </ol> </li> <li>4. Operativa</li> </ol>
<b>Fecha Estimada y duración de las actividades</b>	La fecha estimada para la aplicación de las listas de verificación será: <ol style="list-style-type: none"> <li>1. Establecimiento: octubre 16</li> <li>2. Administrativa: octubre 25</li> <li>3. Ventas: noviembre 08 <ol style="list-style-type: none"> <li>a. Programas Institucionales</li> <li>b. Programas Juveniles</li> </ol> </li> <li>4. Operativa: diciembre 06</li> </ol> <p>La duración de las actividades será no más de tres horas para cada área.</p>
<b>Programar las reuniones con la Administración</b>	Las reuniones con la administración serán dos, una al principio de la auditoría y otra al finalizar la misma.
<b>Requisitos de confidencialidad</b>	El establecimiento “Cyber Joya” ha solicitado un cuidado especial de la documentación sobre todo aquella que implica los procedimientos para la realización del servicio.
<b>Distribución del informe de auditoría y fecha de emisión</b>	La entrega del reporte final estará estimada para principios de agosto. El reporte incluye las no conformidades detectadas, así como también la propuesta a las acciones correctivas.

---

## 1.4 INSTRUMENTOS PARA MEDIR EL NIVEL DE APLICACIÓN DE LA NORMATIVIDAD.

### 1.4.1 Personal

Preguntas	SI	NO	N/A
¿Existe personal con conocimiento y experiencia suficiente que organiza el trabajo para que resulte lo más eficaz posible?			
¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?			
¿Se aprueban por personal autorizado las solicitudes de nuevas aplicaciones?			
¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?			
¿Existen procedimientos adecuados para mantener la documentación al día?			
¿Tienen manuales todas las aplicaciones?			
¿Existen controles que garanticen el uso adecuado de discos y cintas?			
¿Existen procedimientos adecuados para conectarse y desconectarse de los equipos remotos?			
¿Se aprueban los programas nuevos y los que se revisan antes de ponerlos en funcionamiento?			
¿Revisan y evalúan los departamentos de usuario los resultados de las pruebas finales dando su aprobación antes de poner en funcionamiento las aplicaciones?			
Al poner en funcionamiento nuevas aplicaciones o versiones actualizada ¿funcionan en paralelo las existentes durante un cierto tiempo?			

### 1.4.1 Administración

PREGUNTAS	SI	NO	N/A
¿Existe un informe técnico en el que se justifique la adquisición del equipo, software y servicios de computación, incluyendo un estudio costo-beneficio?			
¿Existe un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación?			
¿Han elaborado un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios computacionales?			
¿Se cuenta con software de oficina?			
¿Se han efectuado las acciones necesarias para una mayor participación de proveedores?			
¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica?			
¿El acceso al centro de cómputo cuenta con las seguridades necesarias para reservar el ingreso al personal autorizado?			
¿Se han implantado claves o password para garantizar operación de consola y equipo central (mainframe), a personal autorizado?			
¿Se han formulado políticas respecto a seguridad, privacidad y protección de las facilidades de procesamiento ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación?			
¿Se mantiene un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos?			
¿Los operadores del equipo central están entrenados para recuperar o restaurar información en caso de destrucción de archivos?			



¿Los backups son mayores de dos (padres e hijos) y se guardan en lugares seguros y adecuados, preferentemente en bóvedas de bancos?			
¿Se han implantado calendarios de operación a fin de establecer prioridades de proceso?			
¿Todas las actividades del Centro de Computo están normadas mediante manuales, instructivos, normas, reglamentos, etc.?			
¿Las instalaciones cuentan con sistema de alarma por presencia de fuego, humo, así como extintores de incendio, conexiones eléctricas seguras, entre otras?			
¿Se han instalado equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores pico, UPS, generadores de energía?			
¿Se han contratado pólizas de seguros para proteger la información, equipos, personal y todo riesgo que se produzca por casos fortuitos o mala operación?			
¿Se han Adquirido equipos de protección como supresores de pico, reguladores de voltaje y de ser posible UPS previo a la adquisición del equipo?			
¿Se establecen procedimientos para obtención de backups de paquetes y de archivos de datos?			
¿Se hacen revisiones periódicas y sorpresivas del contenido del disco para verificar la instalación de aplicaciones no relacionadas a la gestión de la empresa?			
¿Se mantiene programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos?			
Existen licencias			

## 1.4.2 Instalación

Pregunta	SI	NO	N/A
¿Se cuenta con instalación con tierra física para todos los equipos?			
¿La instalación eléctrica se realizó específicamente para el centro de cómputo?			
¿Se cuenta con otra Instalación dentro el centro de cómputo, diferente de la que alimenta a los equipos de cómputo?			
¿La Instalación es independiente para el centro de cómputo?			
¿La misma instalación con tierra física se ocupa en otras partes del edificio?			
¿La iluminación está alimentada de la misma acometida que los equipos?			
¿Las reactancias (balastos de las lámparas) están ubicadas dentro de la sala?			
¿Los ventiladores y aire acondicionado están conectados en la misma instalación de los equipos a la planta de emergencia?			
¿Los ventiladores y aire acondicionado están conectados en la misma instalación de los equipos a los no-break?			
¿Se cuenta con interruptores generales?			
¿Se cuenta con interruptores de emergencia en serie al interruptor general?			
¿Se cuenta con interruptores por secciones o aulas?			
¿Se tienen los interruptores rotulados adecuadamente?			
¿Se tienen protecciones contra corto circuito?			
¿Se tiene implementado algún tipo de equipo de energía auxiliar?			
¿Se cuenta con Planta de emergencia?			
¿Se tienen conectadas algunas lámparas del centro de cómputo a la planta de emergencia?			

¿Las instalaciones (aulas, cubículos y oficinas) fueron diseñadas o adaptadas específicamente para funcionar como un laboratorio de cómputo?			
¿Se tiene una distribución del espacio adecuada, de forma tal que facilite el trabajo y no existan distracciones?			
¿Existe suficiente espacio dentro de las instalaciones de forma que permita una circulación fluida?			
¿Existen lugares de acceso restringido?			
¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?			
¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de sensores?			
¿Existen señalizaciones adecuadas en las salidas de emergencia y se tienen establecidas rutas de evacuación?			
¿Se tienen medios adecuados para extinción de fuego en el centro de cómputo?			
¿Se cuenta con iluminación adecuada y con iluminación de emergencia en casos de contingencia?			
¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?			
¿Son funcionales los muebles instalados dentro del centro de cómputo: Discoteca, archiveros, mesas de trabajo, etc.?			
¿Existen prohibiciones para fumar, consumir alimentos y bebidas?			
¿Se cuenta con suficientes carteles en lugares visibles que recuerdan estas prohibiciones?			
¿Se limpian las instalaciones?			

### 1.4.3 Operación

PREGUNTAS	SI	NO	N/A
Existe un contrato de mantenimiento			
¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?			
¿Se lleva a cabo tal programa?			
¿Existen tiempos de respuesta y de compostura estipulados en los contratos?			
Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿Qué acciones correctivas se toman para ajustarlos a lo convenido?			
¿Existe plan de mantenimiento preventivo?			
¿Este plan es proporcionado por el proveedor?			
¿Se notifican las fallas?			
¿Se les da seguimiento?			
¿Tiene un plan logístico para dar soporte al producto software?			
¿Los requerimientos de mantenibilidad se incluyen en la actividad de Iniciación durante el Proceso de Adquisición (ISO 12207) y se evalúa durante el Proceso de Desarrollo?			
¿Las variaciones en el diseño son supervisadas durante el desarrollo para establecer su impacto sobre la mantenibilidad?			
¿Se realizan varios tipos de medidas para poder estimar la calidad del software?			
¿La mantenibilidad se tiene en cuenta antes de empezar a desarrollar?			

<p>¿El desarrollador prepara un Plan de Mantenibilidad que establece prácticas específicas de mantenibilidad, así como recursos y secuencias relevantes de actividades?</p>			
<p>¿Durante el análisis de requerimientos, los siguientes aspectos que afectan a la mantenibilidad, son tomados en cuenta?</p> <ul style="list-style-type: none"> <li>➤ Identificación y definición de funciones, especialmente las opcionales.</li> <li>➤ Exactitud y organización lógica de los datos.</li> <li>➤ Los Interfaces (de máquina y de usuario).</li> <li>➤ Requerimientos de rendimiento.</li> <li>➤ Requerimientos impuestos por el entorno (presupuesto).</li> <li>➤ Granularidad (detalle) de los requerimientos y su impacto sobre la trazabilidad.</li> <li>➤ Énfasis del Plan de Aseguramiento de Calidad del Software (SQAP) en el cumplimiento de las normas de documentación.</li> </ul>			
<p>¿La transición del software consiste en una secuencia controlada y coordinada de acciones para trasladar un producto software desde la organización que inicialmente ha realizado el desarrollo a la encargada del mantenimiento?</p>			
<p>¿La responsabilidad del mantenimiento se transfiere a una organización distinta, se elabora un Plan de Transición?</p> <p>¿qué es lo que incluye este plan?</p> <ul style="list-style-type: none"> <li>➤ La transferencia de hardware, software, datos y experiencia desde el desarrollador al mantenedor.</li> <li>➤ Las tareas necesarias para que el mantenedor pueda implementar una estrategia de mantenimiento del software.</li> </ul>			
<p>¿El mantenedor a menudo se encuentra con un producto software con documentación?</p>			

¿Documentos como especificaciones, manuales de mantenimiento para programadores, manuales de usuario o guías de instalación pueden ser modificados o creados, si fuese necesario?			
El Plan de Mantenimiento es preparado por el mantenedor durante el desarrollo del software.			
¿Los elementos software reflejan la documentación de diseño?			
¿Los productos software fueron suficientemente probados y sus especificaciones cumplidas?			
¿Los informes de pruebas son correctos y las discrepancias entre resultados actuales y esperados han sido resueltas?			
¿La documentación de usuario cumple los estándares especificados?			
¿Los costes y calendarios se ajustan a los planes establecidos?			

#### 1.4.4 Seguridad

Preguntas	SI	NO	N/A
¿Existen medidas, controles, procedimientos, normas y estándares de seguridad?			
¿Existe un documento donde este especificado la relación de las funciones y obligaciones del personal?			
¿Existen procedimientos de notificación y gestión de incidencias?			
¿Existen procedimientos de realización de copias de seguridad y de recuperación de datos?			
¿Existe una relación del personal autorizado a conceder, alterar o anular el acceso sobre datos y recursos?			
¿Existe una relación de controles periódicos a realizar para verificar el cumplimiento del documento?			
¿Existen medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado?			
¿Existe una relación del personal autorizado a acceder a los locales donde se encuentren ubicados los sistemas que tratan datos personales?			
¿Existe una relación de personal autorizado a acceder a los soportes de datos?			
¿Existe un período máximo de vida de las contraseñas?			
¿Existe una relación de usuarios autorizados a acceder a los sistemas y que incluye los tipos de acceso permitidos?			
¿Hay dadas de alta en el sistema cuentas de usuario genéricas, es decir, utilizadas por más de una persona, no permitiendo por tanto la identificación de la persona física que las ha utilizado?			
¿En la práctica las personas que tienen atribuciones y privilegios dentro del sistema para conceder derechos de acceso son las autorizadas e incluidas en el Documento de Seguridad?			
¿El sistema de autenticación de usuarios guarda las contraseñas encriptadas?			