**UNIVERSIDAD CENTRAL**

**AUDITORIA INFORMÁTICA Y FORENSE**

**(Taller De Seguridad Informática)**

**PRESENTADO POR:**

**EDGAR JAVIER VIJA SALINAS**

**PRESENTADO A:**

**DORA JANETH ALFONSO COMBITA**

**FACULTAD DE INGENIERÍA**

**U CENTRAL**

**BOGOTÁ 2013**

1. **Qué se entiende por seguridad informática.**

La seguridad informática, es el área de la [informática](http://es.wikipedia.org/wiki/Inform%C3%A1tica) que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

1. **Por qué consideran importante la seguridad de la información.**

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran. La infraestructura computacional: Es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y anticiparse en caso de fallas, planes de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

**Los usuarios**

Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los funcionarios y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

1. **Mencione y explique las fases o etapas que se deben tener en cuenta para tener una adecuada seguridad informática.**

La norma ISO 27001 determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información. Un sistema de gestión de este tipo, igual que las normas ISO 9001 o ISO 14001, está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

Las fases son las siguientes:

**La Fase de planificación:** esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad (la norma contiene un catálogo de 133 posibles controles).

**La Fase de implementación:** esta fase implica la realización de todo lo planificado en la fase anterior.

**La Fase de revisión:** el objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos “canales” y verificar si los resultados cumplen los objetivos establecidos.

**La Fase de mantenimiento y mejora:** el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

El ciclo de estas cuatro fases nunca termina, todas las actividades deben ser implementadas cíclicamente para mantener la eficacia del SGSI.

1. **Cuáles son las normas que se deben o pueden tener en cuenta y explíquelas, haga un cuadro comparativo para diferenciarlas destacando la finalidad de cada una de ellas.**

|  |  |
| --- | --- |
| Norma | Descripción |
| ISO 27001 | Norma para el manejo de seguridad de la información la cual se rige bajo otros estándares que garantizan la confidencialidad integridad y accesibilidad de la información |
| Estándar ISO 27001 | Buenas prácticas en objetivos de control y controles del SI |
| Estándar ISO 27002 | Guía de implementación SGSI |
| Estándar ISO 27003 | Especificación de métricas para determinar la eficacia del SGSI |
| Estándar ISO 27004 | Guía de técnicas de gestión de riesgo |
| Estándar ISO 27005 | Especificación de requisitos para acreditación de entidades de auditoria y certificación del SGSI |
| Estándar ISO 27006 | Guía de auditoria de SGSI |
| Estándar ISO 27007 | Guía de gestión de seguridad de la información para telecomunicaciones |
| Estándar ISO 27011 | Guía de continuidad del negocio en TIC |
| Estándar ISO 27031 | Guía de seguridad de Ciber seguridad |
| Estándar ISO 27032 | Guía de seguridad de redes |

1. **Realice una propuesta de auditoría para el área de seguridad informática.**

Con el fin de profundizar los conceptos vistos en clase quiero mostrar los aspectos más relevantes que se deben tener en cuenta a la hora de realzar una auditoria en un centro de cómputo este ejerció fue realzado el semestre pasado en la clase de auditoria de sistemas pongo en consideración el objetivo y auditoria realzada

**Objetivo**

Brindar conocimientos necesarios en el proceso de auditoría, en los centros de cómputo midiendo los recursos tecnológicos, en donde se identifiquen los problemas, deficiencias técnicas y se propongan soluciones para optimizar el centro de cómputo.

**Objetivos Específicos**

Evaluar los diferentes aspectos que involucran el buen funcionamiento de un centro de cómputo (Infraestructura, entorno, equipo y otros).

Evaluar la efectividad administrativa que desarrollan los responsables de centros de cómputos.

Verificar la red de distribución de los equipos.

Verificar si la selección de equipos y sistemas de computación es adecuada

**¿En Qué consiste la Auditoria a un Centro de Cómputo?**

Es la revisión exhaustiva, sistemática y global de todas las actividades y operaciones de un centro de cómputo, realizada por un equipo multidisciplinario de auditores, a fin de evaluar, en forma integral, el uso adecuado de sus sistemas computacionales, periféricos y equipos de apoyo para el procesamiento de información de la empresa, así como el desarrollo correcto de las funciones de sus áreas, personal y usuarios.

**Aspectos básicos para el buen funcionamiento de un centro de cómputo.**

Evaluación de Infraestructura.

Evaluación del entorno.

Evaluación de Mobiliario y equipo.

Evaluación del Recurso humano.

Evaluación del Hardware.

Evaluación del Software.

Evaluación de la Seguridad.

Evaluación de la Gestión administrativa.

**Evaluación de la Infraestructura**

Como primer paso se considera la evaluación de la infraestructura por ser la base donde se establece el funcionamiento principal del centro de cómputo, es decir: lo tangible como paredes, piso, techo e instalaciones eléctricas, su correspondiente mantenimiento y remodelaciones de la misma.

¿QUE SE REVISA DE ESTOS ASPECTOS?

QUE SE MIRA DE LOS PISOS

DEL TECHO

DE LAS INSTALACIONES

**Evaluación del entorno**

Es otro de los aspectos a evaluar que interviene directamente en el centro de cómputo, pues es de gran importancia para el buen funcionamiento de estos.

Para la evaluación del entorno se toma en consideración aspectos que intervienen directa o indirectamente en el desarrollo de las actividades, aunque estas no se puedan ver o tocar, pero si se pueden medir (calor, ruido), sentir (la ergonomía o comodidad, espacio físico, ubicación, condiciones ambiéntales, distribución del equipo de cómputo.

**Evaluación de Mobiliario y Equipo**

En cuanto a mobiliario y equipo, se avaluará los siguientes puntos:

Cantidad suficiente de equipo de cómputo, se están dejando de realizar actividades por falta de equipo de cómputo y recursos tecnológicos; o existen equipos de cómputo adicionales que sean reemplazados al ocurrir un daño.

HAY CRITERIOS PARA SABER CUAL ES LA CANTIDAD

La existencia de lugares específicos para guardar papelería, herramientas y otros.

Sobre quien recae la responsabilidad del mobiliario y/o equipo.

**Evaluación del Recurso Humano**

Para la evaluación del recurso humano, los aspectos a evaluar son los siguientes:

El proceso que se lleva acabo para seleccionar el personal administrativo del centro de cómputo y aula informática, las capacitaciones tanto a administradores como docentes, sugerencias del administrador, encargados e instructores para mejoramientos del centro de cómputo, como se lleva a cabo la supervisión del recurso humano, si son presentadas las sugerencias al director de la institución para su mejora, Si existe un sustituto para la realización de las funciones en caso de ausencia del personal, la realización de funciones adicionales del personal que labora en el centro de cómputo y aula de informática es realizada en horas laborales o no laborales y las políticas para sancionar la indisciplina.

**Evaluación del Hardware**

En cuanto a la evaluación del hardware los aspectos son:

El comprobante de la adquisición, cantidad y estado del equipo de cómputo y recurso tecnológico, así como la actualización. Además la proporción de los servicios de mantenimiento el tipo que se le proporciona y con qué frecuencia.

También si es adecuado a las necesidades de los usuarios el hardware, los problemas que se dan con mayor frecuencia, y el tiempo con que son resueltos

**Evaluación del Software**

Con este aspecto se evaluara:

El licenciamiento y facturación del software, su actualización, servicios de mantenimiento, tiempo en cual se da, los problemas relacionados con el congestionamiento de la información, así como la instalación innecesaria de programas, además si carecen de programas para la realización de alguna práctica, se toman en cuenta los problemas y el tiempo para ofrecerles la solución.

**Evaluación de la Seguridad**

Para evaluar la seguridad se toman los siguientes aspectos:

La vigilancia para salvaguardar los recursos tecnológicos como en las instalaciones, así como los controles preventivos y de riesgo supervisando actividades, claves de acceso a los sistemas, alarmas, políticas, salidas de emergencias y seguros. **“Ser Especifico Con Ejemplos, Fotos Del Debe Ser”**

Al realizar nuestra evaluación y auditoria al Centro de Cómputo como aspecto físico, lógico y de seguridad, necesitamos evaluar el espacio, los controles dentro y fuera del centro de cómputo, análisis del local, y sobre todo, la seguridad del local y los implementos con que cuenta.

**En la Auditoria de Centro De Computo se deben tener en cuenta los siguientes ítems**

Política de Seguridad Física del Centro de Cómputo.

Control de Mantenimiento.

Control de Medios de Almacenamiento Masivo.

Evaluación de la configuración del sistema de cómputo.

Orden en el centro de cómputo.

**Política de Seguridad Física Centro de Cómputo**

Las Instalaciones deben ser adecuadas para asegurar el buen funcionamiento y la continuidad necesaria en las operaciones.

Deben existir políticas y procedimientos que describan los aspectos de seguridad física mínimos.

Se deben observar los siguientes puntos:

El acceso al centro del cómputo debe estar restringido por una puerta, la cual contará con una chapa adecuada de seguridad, o con un dispositivo electrónico de control de acceso.

Se deben tener dispositivos adecuados de detección de humo, así como aspersores de calor para la extinción de incendios, además de contar con extintores.

Se debe tener protección en los servidores para que no puedan ser desconectados accidental o intencionalmente y provocar así serios daños al equipo.

El personal operativo no debe permitir el acceso a personal ajeno al departamento

Debe existir un plan de contingencia que permita que los sistemas sigan funcionando en caso de algún siniestro; se sugiere la revisión del plan de contingencias para que contengan los siguientes controles:

**Control de Mantenimiento**

**Control de Medios de Almacenamiento Masivo**

Los dispositivos de almacenamiento representan, para cualquier centro de cómputo, archivo extremadamente importante, cuya pérdida parcial o total podría tener repercusiones muy seria.

**Evaluación de la Configuración del Sistema de Cómputo**

Los objetivos son evaluar la configuración actual, tomando en consideración las aplicaciones, y el nivel de uso del sistema.

Se tienen en cuenta los siguientes ítems:

Evaluar los posibles cambios en el hardware a fin de nivelar el sistema de cómputo con la carga de trabajo actual.

Evaluar las posibilidades de modificar el equipo para reducir el costo o el tiempo de proceso.

Evaluar la utilización de los diferentes dispositivos periféricos.

**Orden en el Centro de Cómputo**

Una dirección de informática bien administrada debe tener y observar reglas relativas al orden y cuidado de la sala de máquinas. Los dispositivos del sistema de cómputo y los archivos magnéticos pueden ser dañados si se manejan en forma inadecuada, lo que puede traducirse en pérdidas irreparables de información o en costos muy elevados en la reconstrucción de archivos.

**Evaluación de la Gestión Administrativa**

En cuanto a la evaluación de la gestión administrativa, esta va enfocada específicamente a los centros de cómputo y aulas informáticas, por ser estos de gran importancia en la actualidad. Para las instituciones educativas, además de verificar que estos cuenten con manuales de procedimiento, su elaboración, revisión y aplicación.

Así como el control de activos fijo tales como: equipo de cómputo, recursos tecnológicos y el control de cómo se lleva sobre estos, es decir, el préstamo, uso del equipo de cómputo, seguridad, inventario y mantenimiento.

También las limitantes y responsabilidades con las que cuenta el administrador, encargado e instructor para realizar las actividades adecuadamente.

**Herramientas para Efectuar la Auditoria a un Centro de Cómputo**

1) WinAudit 2.20: del tipo Freeware es un programa gratis que analiza al detalle todo el hardware y software de la PC.

2) Test My Hardware 2.1: del tipo Freeware este programa ofrece información al detalle de todos los componentes del hardware instalados en la PC.

3) CargaDrivers 1.0: del tipo Freeware este programa instala activa, desactiva y elimina drivers de la forma más sencilla.

4) AIDA32: del tipo Freeware es un programa gratis que analiza al detalle todo el hardware y software de la PC por categorías o áreas específicas.

5) SiSoftware Sandra 2002: del tipo Freeware es un Programa gratis que analiza al detalle todo el hardware y software de la PC por categorías o áreas específicas.

6) WashAndGo: del tipo Freeware este programa

Analiza, desactiva y elimina carpetas, archivos de la forma más sencilla.