Universidad Autónoma del Estado de México
Ingeniería en Computación

Administración de Recursos Informáticos

Unidad IV

PLAN DE SEGURIDAD PARA UNA UNIDAD INFORMÁTICA

M. En A. Silvia Edith Albarrán Trujillo

Septiembre 2015

fppt.com

Estructura de la Unidad de Aprendizaje

1. ANALIZAR LA MADUREZ DE UNA ORGANIZACIÓN MEDIANTE HERRAMIENTAS O MODELOS DE APOYO PARA ESTE PROPÓSITO

2. INDICAR LOS ASPECTOS QUE DEBEN CONSIDERARSE PARA ELABORAR UN ESTUDIO DE VIABILIDAD PARA LA COMPRA DE RECURSOS Y ANÁLISIS DE PROVEEDORES.

3. IDENTIFICAR ADMINISTRACIÓN DE UNA UNIDAD INFORMÁTICA.

4. ANALIZAR UN PLAN DE SEGURIDAD PARA UNA UNIDAD INFORMÁTICA.

5. CONOCERA EL ENFOQUE DE LA ADMISTRACION DE SERVICIOS EN TECNOLOGIAS DE LA INFORMACION (ITSM) Y DE LA BIBLIOTECA DE INFRAESTRUCTURA DE LAS TECNOLOGIAS DE LA INFORMACION (ITIL)

6. CONOCERÁ LA DIRECCIÓN/GESTIÓN/ADMINISTRACIÓN DE PROYECTOS MEDIANTE MODELOS DE BUENAS PRÁCTICAS

fppt.com

Propósito de la Unidad de Aprendizaje

- APLICARÁ SATISFACTORIAMENTE LOS PRINCIPIOS ADMINISTRATIVOS EN EL USO DE LOS RECURSOS INFORMÁTICOS DE UNA ENTIDAD, DE ACUERDO CON LAS CONDICIONES DE OPERACIÓN Y EL ENTORNO ECONÓMICO, TÉCNICO Y OPERATIVO EN QUE DEBA APLICARSE..
- IDENTIFICARÁ LAS BASES PARA LA ESPECIALIZACIÓN DE DIVERSAS ÁREAS AFINES DE DESARROLLO PROFESIONAL, TALES COMO LA SELECCIÓN Y EVALUACIÓN DEL DESEMPEÑO DEL PERSONAL TÉCNICO DE INFORMÁTICA, LA AUDITORIA INFORMÁTICA EN TODAS SUS VERTIENTES, LA PLANEACIÓN INFORMÁTICA Y LA SELECCIÓN DE EQUIPO Y PROGRAMAS DE CÓMPUTO, ENTRE OTRAS

fppt.com

Guión para el Uso de este Material

- La información de esta presentación contiene ideas generales que serán explicadas en la clase.
- Para ampliar la información que se presenta en esta presentación se incluye al final un apartado de bibliografía.
- La presente contiene sólo información de la unidad 4, Titulada: ANALIZAR UN PLAN DE SEGURIDAD PARA UNA UNIDAD INFORMÁTICA (Ámbitos de seguridad en instalaciones con recursos informáticos, Seguridad de las instalaciones, Seguridad del personal, Protección de los equipos, Seguridad de la información, Medidas preventivas en caso de desastres y características de cada una de ellas)
- Una vez concluida esta unidad el alumno tendrá familiaridad con las características y contenido de los Planes de Seguridad informática.

fppt.com

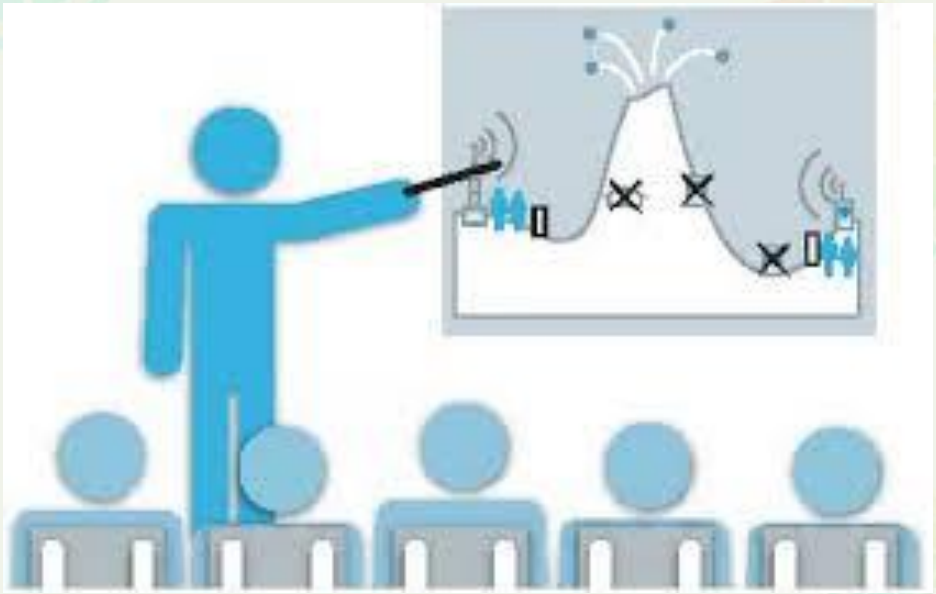
Contenido del material

1. Portada
2. Objetivo dela Unidad de Aprendizaje
3. Programa de la Unidad de Aprendizaje
4. Guión para uso de este material
5. Contenido del material
6. Objetivo de la Unidad IV
7. Seguridad
8. Seguridad en un Departamento de TI
9. Normas de Seguridad Informática
10. Políticas de Seguridad
11. Seguridad de Instalaciones
12. Seguridad Física
13. Seguridad de Personal
14. Protección de Equipos
15. Seguridad de la Información
16. Medidas preventivas
17. Plan de Seguridad Informática
18. Conclusiones

fppt.com

Objetivo de la Unidad IV

ANALIZAR UN PLAN DE SEGURIDAD PARA UNA UNIDAD INFORMÁTICA



fppt.com

Seguridad

Conjunto de normas preventivas y operativas, con apoyo de procedimientos, programas, sistemas, y equipos de seguridad y protección, orientados a neutralizar, minimizar y controlar los efectos de actos ilícitos o situaciones de emergencia, que afecten y lesionen a las personas o los bienes de esta.

Seguridad en un departamento de TI

Incluye:

1. Seguridad de la información
2. Seguridad del personal
3. Seguridad de acceso físico
4. Seguridad de instalaciones
5. Seguridad de equipos
6. Seguridad física
7. Medidas preventivas

Medidas de Seguridad de una Departamento de TI

- Impartir instrucciones a los asociados o responsables de no suministrar información.
- Revisar los planes de seguridad de la organización.
- Establecer simples y efectivos sistemas de señales.
- Contar con resguardo de la información que se maneja.

Medidas de Seguridad de una Departamento de TI

- Establecer contraseñas para proteger información confidencial y privada.
- Evitar introducir alimentos, tales como refrescos, para impedir que puedan derramarse sobre los equipos.
- No fumar.

fppt.com

Medidas de Seguridad de una Departamento de TI

- Cada equipo de cómputo debe contar con un regulador de corriente para evitar problemas o daños en caso de falla eléctrica.
- Revisar un dispositivo de almacenamiento externo antes de introducirlo a la computadora para así evitar infectarlas con algún virus

fppt.com

Factores Inherentes al Departamento de TICS

La construcción del interior de la instalación de cómputo también tiene gran importancia. La división tradicional de las áreas casi nunca es la adecuada para la seguridad.

Es importante considerar las características físicas que deben tener las instalaciones para proporcionar seguridad.

Ejemplo:

a) Piso falso

b) Cableado

c) Paredes y techo

d) Puertas de acceso

e) Iluminación

f) Filtros

h) Ductos

fppt.com

Normas de Seguridad Informática

- Entre las normas más conocidas en seguridad informática están:

- - ISO/IEC 177991 (*Security Policy, Organizing Information Security, Asset Management, Human Resources Security, Physical and Environmental Security, Communications and Operations Management, Access Control, Information Systems Acquisition, Development and Maintenance, Information Security Incident Management, Business Continuity Management, Compliance*)

- - ISO 27000 (ISO 27000, vocabulario y definiciones -terminología para el resto de estándares de la serie-. ISO 27001, especificación del sistema de gestión de la seguridad de la información (SGSI). Esta norma es certificable bajo esquemas nacionales en cada país)

fppt.com

Políticas de Seguridad

- Políticas de uso aceptable
- Políticas de cuentas de usuario
- Políticas de listas de acceso
- Políticas de acceso remoto
- Políticas de contraseñas
- Políticas de respaldos.

fppt.com

Seguridad de Instalaciones

A. Factores inherentes a la localidad.

B. Factores inherentes al Departamento de TICS

fppt.com

Seguridad Física

1. Ubicación física y disposición del centro de cómputo.
2. Instalaciones físicas del centro de cómputo.
3. Control de acceso físico.
4. Aire acondicionado.
5. Instalación eléctrica.
6. Riesgo de inundación.
7. Protección, detección y extinción de incendios.
8. Mantenimiento

fppt.com

Seguridad Física

a) Piso falso

- Se debe tener en cuenta la resistencia para soportar el peso del equipo y el personal.
- Posibilidad de realizar cambios en la situación de unidades.
- Debe cubrir los cables de comunicación entre la unidad central de proceso y los dispositivos periféricos, cajas de conexiones y cables de alimentación eléctrica.
- Deberá proporcionar seguridad al personal.
- La altura recomendable será de 30 cm si el área de la sala de cómputo es de 100 metros cuadrados o menos, y de 40 a 60 cm si es mayor de 100 metros cuadrados. La altura mínima podrá ser de 18 cm si la sala es pequeña.
- con objeto de que el aire acondicionado pueda fluir adecuadamente en la cámara plena.
- Puede ser de acero, aluminio o madera resistente al fuego.

Seguridad Física

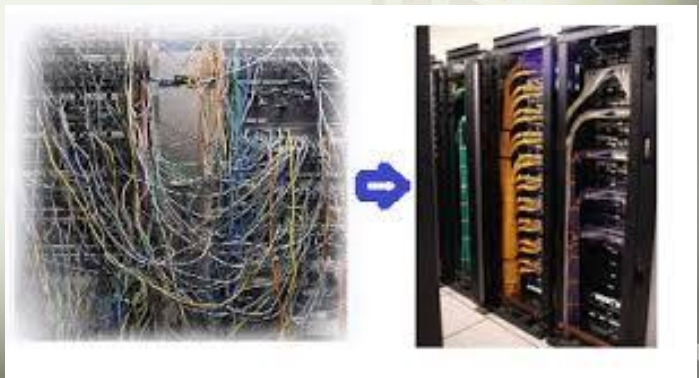
b) Cableado

El cableado en el cuarto de computadoras se debe procurar que quede por debajo del piso

falso, donde es importante ubicar los cables de forma que se aparten:

- Los cables de alto voltaje para la computadora.
- Los cables de bajo voltaje conectados a las unidades de las computadoras.
- Los cables de telecomunicación.
- Los cables de señales para dispositivos de monitoreo o detección (fuego, temperatura,

humedad, etc.).



Seguridad Física

c) Paredes y techo

- Las paredes irán con pintura plástica lavable para poder limpiarlas fácilmente y evitar la erosión.
- El techo real deberá pintarse, así como las placas del falso techo y los amarres, si éste se emplea como plenum para el retorno del aire condicionado.
- Es mejor usar placas metálicas o de madera prensada para el piso falso con soportes y amarres de aluminio.

fppt.com

Seguridad Física

d) Puertas de acceso

- Las puertas del local serán de doble hoja y con una anchura total de 1.40 a 1.60 cm.
- Es necesaria una salida de emergencia.
- Tener en cuenta las dimensiones máximas de los equipos si hay que atravesar puertas y ventanas de otras dependencias.

e) Iluminación

- La iluminación no debe alimentarse de la misma acometida que los equipos de cómputo.
- En el área de máquinas debe mantenerse un promedio mínimo de 450 luxes a 70 cm del suelo.
- Debe evitarse la luz directa para poder observar la consola y las señales.
- Del 100% de la iluminación, deberá distribuirse el 25% para la iluminación de emergencia y se conectará al sistema de fuerza interrumpible.

fppt.com

Seguridad Física

f) Filtros

- Se requieren filtros con una eficiencia del 99% sobre partículas de 3 micrones.
- Si hay contaminantes, elegir los filtros adecuados.
- El aire de renovación o ventilación será tratado tanto en temperatura y humedad como

en filtrado antes de entrar en la sala.

h) Ductos

- Serán de material que no desprenda partículas con el paso del aire.

Seguridad de Acceso Físico

SEGURIDAD DEL PERSONAL

- El control de acceso
- Estructura y disposición del área de recepción
- En áreas de alta seguridad admitir tanto a los empleados como a los visitantes de
- uno en uno.
- Acceso de terceras personas
- Identificación del personal

Seguridad de Personal

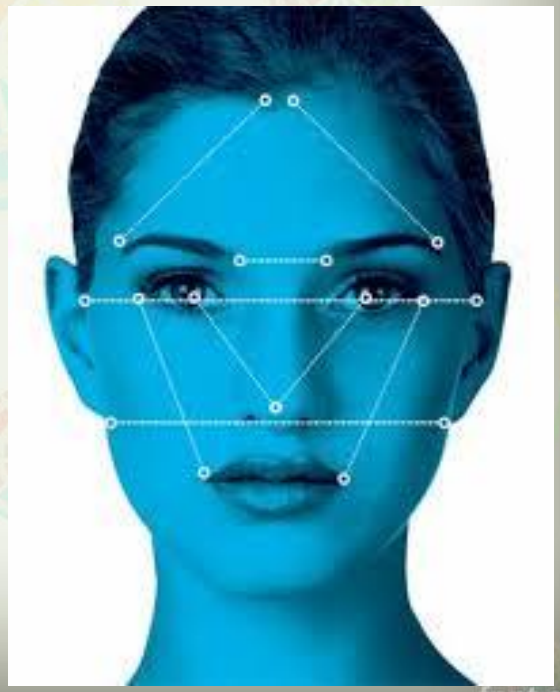
Se debe considerar:

- Aspectos ergonómicos en la oficina, se trata de posturas de trabajo con los diferentes dispositivos de cómputo de trabajo cotidiano como el teclado, el ratón, portadocumentos, posturas, la silla de trabajo, manejo de cargas y levantamiento de objetos.
- Aspectos ambientales como la iluminación y ventilación.
- Orden y limpieza en el puesto de trabajo y con las computadoras.
- Aspectos de seguridad en caso de emergencias.
- Aspectos Generales con archiveros y armarios, equipos e instalaciones eléctricas, utensilios de oficina, contra robos.
- Aspectos de bienestar

fppt.com

Algunos parámetros asociados a la identificación del personal

- 1. Guardias y escoltas especiales.
- 2. Registro de firma de entrada y salida.
- 3. Puertas con chapas de control electrónico.
- 4. Tarjetas de acceso y gafetes de identificación.
- 5. Entradas de dobles puertas
- 6. Identificación biométrica.
- 7. Equipos de monitoreo.
- 8. Alarmas contra robos.
- 9. Trituradores de papel.



fppt.com

Protección de los Equipos

- Servicios de mantenimiento (electricidad, agua, aire acondicionado, etc.)
- La limpieza de la instalación de cómputo
- El mal mantenimiento crea las condiciones para una fractura en la seguridad, como cuando las puertas y las ventanas no cierran correctamente, o bien, cuando se propicia incendios.
- Recordar que el agua y el detergente pueden dañar el equipo: es por eso que debe instruirse al personal de limpieza al respecto.

pt.com

Seguridad de la Información

La documentación de los sistemas, la programación y las operaciones también necesitan protección contra incendios.

Destrucción de esta documentación puede imposibilitar el uso de programas o archivos de respaldo.

Garantizar la actualización de toda la documentación como rutina y que las copias de seguridad se almacenen en un lugar lejano, así como las copias de seguridad de los programas y los archivos.

Seguridad de la Información

La proliferación de redes de datos aumenta las necesidades de tornar los datos seguros y auténticos, los mensajes y datos se deben proteger para que solo sean utilizados por las personas o procesos autorizados.

Se debe evitar:

- La alteración fraudulenta de los datos
- La creación de datos falsos
- La destrucción de datos correctos

Seguridad de la Información

Lugares para Almacenar la Información

Limitar los lugares en los cuales se almacena la información.

Es recomendable mantener toda la información, especialmente la sensible, en servidores centralizados y no en el disco duro de las computadoras personales.

Seguridad de la Información

- Acceso remoto a la Información

Muchas redes permiten el acceso remoto a la información. Esta forma de acceso facilita que personal no autorizado pueda llegar a la información. Se debe realizar una evaluación para determinar si vale la pena correr el riesgo de exponer una red a acceso público.

Se debe contratar un experto para minimizar el riesgo del uso de una red, este acceso es uno de los blancos de los hackers para quebrantar los códigos de seguridad.

Seguridad Shareware (BIOS Y Otros)

Algunas de sus vulnerabilidades son:

- Si se dispone de tiempo suficiente, acceder a la tarjeta donde se encuentre la BIOS y resetearla (se perderá la configuración BIOS y por tanto el password).
- Atacando la BIOS desde un dispositivo externo o programa.
- Probando posibles passwords, ya que no tiene límites de errores.

fppt.com

Medidas Preventivas

- Análisis de Riesgos
- Mantener las cosas simples
- El sistema que controla la "puerta" siempre puede fallar
- Encriptar tanto como sea posible
- La seguridad hacia el interior
- Educar a los usuarios ("Ingeniería Social“).
- Ejecutar solo los servicios imprescindibles
- Algunas personas tienen la manía de instalar los sistemas con la mayor cantidad posible de
- Mantenerse al día con las actualizaciones
- Digitalizaciones regulares
- Vigilancia
- Establecimiento de políticas

Sistema de Seguridad Informática

- Conjunto de medios administrativos, medios técnicos y personal que de manera interrelacionada garantizan niveles de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados.

fppt.com

Plan de Seguridad Informática

Expresión gráfica del Sistema de Seguridad Informática diseñado y constituye el documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad Informática en una Entidad y recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.

fppt.com

Plan de Seguridad Informática

Se distinguen tres etapas:

1) Determinar las necesidades de protección del sistema informático objeto de análisis, que

incluye: Caracterización del sistema informático. Identificación de las amenazas y estimación de los riesgos. Evaluación del estado actual de la seguridad.

2) Definir e implementar el sistema de seguridad que garantice minimizar los riesgos identificados en la primera etapa. Definir las políticas de seguridad. Definir las medidas y procedimientos a implementar.

3) Evaluar el sistema de seguridad diseñado

fppt.com

Partes del Plan de Seguridad Informática

- Caracterización del Sistema Informático.
- Resultados del Análisis de Riesgos.
- Políticas de Seguridad Informática.
- Sistema de Seguridad Informática.
- Medios humanos.
- Medios técnicos.
- Medidas y Procedimientos de Seguridad Informática.
- De protección física.
- A las áreas con tecnologías instaladas.
- A las tecnologías de información.

fppt.com

Partes del Plan de Seguridad Informática

- Soportes de información.
- Técnicas o lógicas.
- Identificación de usuarios.
- Autenticación de usuarios.
- Control de acceso a los activos y recursos.
- Integridad de los archivos y datos.
- Auditoria y alarmas.
- Seguridad de operaciones.
- Recuperación ante contingencias.
- Anexos.
- Programa de Seguridad Informática
- Listado de usuarios con acceso a redes de alcance global.
- Registros

fppt.com

Conclusiones

1. Los planes de seguridad informática contiene información referente a todos los aspectos informáticos existentes en una organización como el hardware, el software, comunicaciones, instalaciones, información y personal.
2. Los planes de seguridad informática son documentos que deben considerar planes de contingencia.
3. El contenido de los planes de seguridad informática varía de acuerdo ala organización que lo plantea pero debe abarcar todo los aspectos mencionados en el punto 1.

fppt.com

Bibliografía

- Aguirre, J. R. (2006). Libro electrónico de seguridad Informática y Criptografía.*Manual docente de libre distribución, Universidad Politécnica de Madrid*.
- Aneiro Rodríguez, L. O. (2000). Elementos de arquitectura y seguridad informática. *La Habana: Instituto Superior Politécnico" Eduardo García Delgado*.
- Arlin Cooper James, 1989, **“Computer and Comunication Security”**. Mc. Graw Hill
- Cerini, M., & Prá, P. (2002). Plan de Seguridad Informática. *Trabajo de Grado, Córdoba, Argentina: Universidad Católica de Córdoba, Facultad de Ingeniería*.
- Cano, J. J. (2004). Inseguridad informática: un concepto dual en seguridad informática. *Revista de Ingeniería*, (19), 40-44.
- Disterer, G. (2013). Iso/iec 27000, 27001 and 27002 for information security management.

fppt.com

Bibliografía

- de Marcelo Rodao, J. (2001). *Piratas cibernéticos: cyberwars, seguridad informática e Internet*. Ra-ma
- Gómez, J., & Baños, R. (2006). Seguridad en sistemas operativos Windows y Linux. *Ra-Ma*.
- Guagalango Vega, R. N., & Moscoso Montalvo, P. E. (2011). Evaluación técnica de la seguridad informática del Data Center de la Escuela Politécnica del Ejército.
- López, P. A. (2010). *Seguridad informática*. Editex.
- Morant, J. L., Ribagorda, A., Sancho, J., Pastor, J., & Sarasa, M. A. (1994). Seguridad y protección de la información. *Editorial Centro de Estudios Ramón Areces, Madrid*.
- Wang, C. H., & Tsai, D. R. (2009, October). Integrated installing ISO 9000 and ISO 27000 management systems on an organization. In *Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on* (pp. 265-267). IEEE.

fppt.com