CONCLUSIÓN

Un plan de seguridad para un centro de computación puede garantizar el restablecimiento de los procesos en el menor tiempo posible ya que contempla de una forma organizada y centralizada los procedimientos a seguir al presentarse una eventualidad.

Al diseñar un plan de seguridad es necesario realizar un estudio detallado de todos los componentes que integran el centro de computación así como también su configuración, funcionamiento y comunicación.

Establecer medidas de control para la seguridad del centro de computación y sus componentes tomando en consideración la relación recurso / riesgo, minimiza en cierto modo las amenazas a las cuales esta expuesto dicho centro.

Para la elaboración de este proyecto fue indispensable recurrir a fuentes de información metodológicas inherentes al tema establecidas por diferentes autores, tales como Jerry Fitzgerald, Baskerville. Con la finalidad de establecer los procedimientos de la investigación. De ellos resultó la metodología apropiada, tomada básicamente de los esquemas planteados por Jerry Fitzgerald y Baskerville para el cumplimiento de los objetivos de la investigación.

Fue de gran utilidad al aplicar el procedimiento de análisis de vulnerabilidades propuesta por Jerry Fitzgerald, ya que permitió en forma eficaz la detección de amenazas que atenta al sistema de cómputo y el establecimiento de medidas de control para la seguridad de este.

Algunos de los resultados que podemos mencionar como parte de la conclusión:

El desarrollo del análisis de vulnerabilidades hizo notar como el ambiente cliente / servidor en general una gran cantidad de puntos vulnerables, este análisis consta de tres etapas donde en el primer paso se estudiaron los componentes del sistema de la empresa Procedamos, con el fin de identificar los aspectos que se requerían proteger o “puntos de control”, es decir, los elementos que requerían de algún nivel de seguridad.

Posteriormente la segunda etapa “Estudio de las Amenazas o Riesgos” se indagó en profundidad los principales problemas que atentan con la seguridad del sistema cliente / servidor de la empresa en estudio. La categoría de la clasificación de las amenazas fueron: pérdida de error, errores y omisiones, desastres y siniestros, sabotaje, acceso no autorizado, robo, pérdida de privacidad y fraude.

Y por último se procedió a la construcción de la matriz de estado con esta se logro establecer los puntos de control dentro del sistema o los puntos de relación entre los componentes y las amenazas que pueden tener cada uno de esos componentes. Se realizo tomando en cuenta todos los componentes especificos y las amenazas encontradas en la fase anterios de estudio.

La matriz de control ofrece una visión global de cómo afecta cada amenaza a la totalidad de los componentes como se observaron el la tabla 11 de el capitulo IV.

RECOMENDACIONES

Adicionalmente se observaron aspectos que podrían ser no muy recomendables, por ejemplo que el servidor de respaldo se encuentre dentro de las instalaciones de la organización, hecho este que originaria pérdida doble, al momento de un desastre o siniestro natural, y/o artificial por lo tanto, se recomienda almacenarlo fuera del edificio, lugar este que podría ser el CITIBANK (donde se encuentran ubicadas las cintas de respaldo).

Se recomienda usar Password para crear, junto con los mecanismos antes mencionados, una barrera que impida el acceso no autorizado al sistema. Conducir una análisis de riesgo para identificar problemas críticos y controlar fuertemente estos programas o sistemas.

Llevar datos estadísticos de la disponibilidad del sistema en base a tiempo de mantenimiento, tiempo promedio entre fallas, tiempo promedio para reparar y confiabilidad.

Llevar datos históricos de la fecha, duración y costo de las paradas del proceso debido a fallas de equipos, tiempo de mantenimiento, etc.

Establecer una política de seguridad que establezca quien tiene derecho de acceso a información especifica, que defina rutinas de adiestramiento y que rija el

comportamiento general tanto de los operadores y analistas como de cualquier ente externo que interactué con el sistema.

Realizar mantenimiento preventivo y predictivo regular al Hardware y todas las instalaciones, en especial al banco de baterías.

Tomar la información obtenida en este estudio como base para continuar con el estudio de los controles que pueden aplicarse sobre los puntos específicos del sistema y elaborar el plan de contingencia a seguir en caso de alguna eventualidad.

Se recomienda idear forma de tener más control con las entradas / salidas del personal (fijo, contartado, visitantes) pues se pueden extraviar cosas de pequeño tamaño pero alto valor).

Y por ultimo se recomienda actualizar este plan anualmente, crear el líder (gerente de seguridad informatica).

REFERENCIAS BIBLIOGRAFIA

- ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. 1° Edición. ISBN 987-9131-26-6. Uruguay. 1997.

- BAVARESCO, AURA (1992)

- Compumagazine. Piratería: informe especial. MP Ediciones. Argentina. Septiembre 2001.

- Compumagazine. Delito informático. MP Ediciones. Argentina. Diciembre 2001.

- CHAVEZ NILDA, (1994)

- E. Alcalde / j. Morera. Introducción a los Sistemas Operativos.1° edición. España 1992

- Estrategias de Seguridad. BENSON Christopher (Inobis Consulting Pty Ltd). Microsoft© Solutions. Noviembre 2000.

- MENDEZ (1993)

- FERNADEZ, Carlos M. Seguridad en sistemas informáticos. Ediciones Díaz de Santos S.A. ISBN 84-86251-95-8. España. 1988.

- FITZGERALD, JERRY. Comunicación de datos en los negocios. Conceptos básicos de seguridad. Mexico 1994.

- FITZGERALD, JERRY. Controles internos para sistemas de computación. Mexico1992.

- HERNÁNDEZ, Roberto. Firewalls: Seguridad en las redes e Internet. Boletín de Política Informática N° 2. España. 2000.

- LUCENA LÓPEZ, Manuel José. Criptografía y Seguridad en Computadores. Dpto. de Informática Universidad de Jaén. Edición virtual. España. 1999.

- RODRÍGUEZ, Claudio. HUNRICHSE, Rodrigo. Publicación Edición Virtual. Seguridad Informática. Mecanismo de control y auditoria orientados a garantizar la seguridad de los proceso y de datos en ambiente de producción. Universidad de Concepción DIICC-Facultad de Ingeniería. Chile. Mayo 1999.

- TANENBAUM, Andrew. Redes de computadoras. 1990.

ANEXOS

ENCUESTA

Gerencia a la cual pertenece: _____

1. Departamento: _____

2. ¿Qué aplicaciones del sistema de computación de la empresa usa usted para cumplir sus funciones laborales?

_____

_____

_____

_____

3. ¿Considera usted que el sistema de computación es vulnerable?
R= Si

¿A que?

_____

_____

_____

_____

R= No

¿Por qué?

_____

_____

_____

_____

4. En caso de ser el sistema de computo vulnerable explique en que forma se ven afectadas sus actividades

5. ¿Qué soluciones aportaría para minimizar o eliminar estas vulnerabilidades

6. En caso de que el sistema de computación no pueda prestar sus servicios en forma completa y se encuentre degradado por alguna emergencia ¿Qué aplicación de su uso considera prioritaria?

PLAN DE SEGURIDAD

Cuales son los objetivos que deseamos alcanzar con nuestro plan de seguridad

1. _____

_____

2. _____

_____

3. _____

_____

4. _____

_____

5. _____

_____

Que se desea proteger con el plan de seguridad

Que tipos de redes utilizan

Cuantos servidores hay

Cuantas estaciones de trabajo

Descripción del software

Descripción de Hardware

En Procedatos utilizan alguna metodología de seguridad. Cual utilizan