FASE 3 CONSTRUCCION - SEGURIDAD INFORMATICA

HERNAN DE JESUS QUINTANA

JUAN IGNACIO BOLIVAR

OMAR YOVANY FORERO DIAZ

CARLOS ALBERTO SOSA

TUTOR

GRUPO: 301122_29

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

DISEÑO DE SITIOS WEB

MAYO 2019

SEGURIDAD INFORMATICA

Cuando hablamos de seguridad de la información estamos indicando que dicha información tiene una relevancia especial en un contexto determinado y que, por tanto, hay que proteger.

Hasta la aparición y difusión del uso de los sistemas informáticos, toda la información de interés para una organización (empresa) determinada se guardaba en papel y se almacenaba en grandes cantidades de abultados archivadores. Datos de los clientes o proveedores de la organización, o de los empleados quedaban registrados en papel, con todos los problemas que luego acarreaba su almacenaje, transporte, acceso y procesado.

Los sistemas informáticos permiten la digitalización de todo este volumen de información reduciendo el espacio ocupado, pero, sobre todo, facilitando su análisis y procesado. Se gana en 'espacio', acceso, rapidez en el procesado de dicha información y mejoras en la presentación de dicha información.

Pero aparecen otros problemas ligados a esas facilidades. Si es más fácil transportar la información también hay más posibilidades de que desaparezca 'por el camino'; si es más fácil acceder a ella también es más fácil modificar su contenido, etc.

Desde la aparición de los grandes sistemas (mainframes) aislados hasta nuestros días, en los que el trabajo en red (networking) es lo habitual, los problemas derivados de la seguridad de la información han ido también cambiando, evolucionando, pero están ahí y las soluciones han tenido que ir adaptándose a los nuevos requerimientos técnicos. Aumenta la sofisticación en el ataque y ello aumenta la complejidad de la solución, pero la esencia es la misma.

DEFINIMOS EL CONCEPTO DE SEGURIDAD INFORMÁTICA:

Medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican (Infosec Glossary-2000 tradicionalmente la seguridad informática se desglosa en dos grandes grupos la Seguridad Física y la Seguridad Lógica.

La seguridad lógica: De un sistema informático consiste en la aplicación de barreras y procedimientos que protejan el acceso a los datos y a la información contenida en él trata de conseguir los siguientes objetivos:

- Restringir el acceso a los programas y archivos.
- Asegurar que los usuarios puedan trabajar sin supervisión y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Verificar que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y que la información recibida sea la misma que la transmitida.
- Disponer de pasos alternativos de emergencia para la transmisión de información.

La seguridad física de un sistema informático consiste en la aplicación de barreras físicas y procedimientos de control frente a amenazas físicas al hardware. Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el sistema. Las principales amenazas que se prevén son:

- Desastres naturales, incendios accidentales y cualquier variación producida por las condiciones ambientales.
- Amenazas ocasionadas por el hombre como robos o sabotajes.
- Disturbios internos y externos deliberados.
- Evaluar y controlar permanentemente la seguridad física del sistema es la base para comenzar a integrar la seguridad como función primordial del mismo. Tener controlado el ambiente y acceso físico permite disminuir siniestros y tener los medios para luchar contra accidentes.

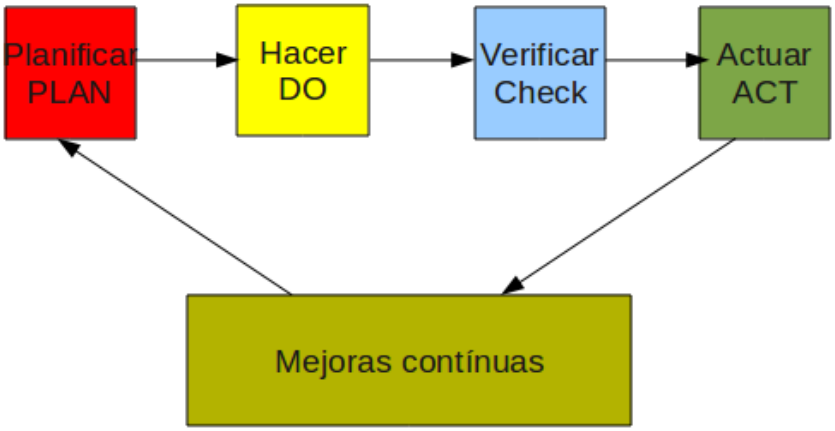
SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El objetivo de un Sistema de Gestión de la Seguridad de la Información (SGSI) es proteger la información y para ello lo primero que debe hacer es identificar los 'activos de información' que deben ser protegidos y en qué grado.

Luego debe aplicarse el plan PDCA ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo.

La organización debe entender la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad.

Un SGSI siempre cumple cuatro niveles repetitivos que comienzan por Planificar y terminan en Actuar, consiguiendo así mejorar la seguridad.



PLANIFICAR (Plan): consiste en establecer el contexto.

- En este nivel:
- Se crean las políticas de seguridad
- Se describe el alcance del SGSI
- Se hace el análisis de riesgos
- Se hace la selección de controles
- Estado de aplicabilidad

HACER (Do): consiste en implementar el sistema

- Implementar el sistema de gestión de seguridad de la información
- Implementar el plan de riesgos
- Implementar los controles

VERIFICAR (Check): consiste en monitorear y revisar

- Monitorea las actividades
- Revisa
- Hace auditorías internas

ACTUAR (Act): consiste en ejecutar tareas de mantenimiento y propuestas de mejora

- Implementa mejoras
- Acciones preventivas
- Acciones correctivas

¿POR QUÉ ES TAN IMPORTANTE LA SEGURIDAD INFORMÁTICA?

Prevenir el robo de datos tales como números de cuentas bancarias, información de tarjetas de crédito, contraseñas, documentos relacionados con el trabajo, hojas de cálculo, etc. es algo esencial durante las comunicaciones de hoy en día.

Muchas de las acciones de nuestro día a día dependen de la seguridad informática a lo largo de toda la ruta que siguen nuestros datos. Y como uno de los puntos iniciales de esa ruta, los datos presentes en un ordenador también pueden ser mal utilizados por intrusiones no autorizadas. Un intruso puede modificar y cambiar los códigos fuente de los programas y también puede utilizar tus imágenes o cuentas de correo electrónico para crear contenido perjudicial, como imágenes pornográficas o cuentas sociales falsas.

Hay también ciberdelincuentes que intentarán acceder a los ordenadores con intenciones maliciosas como pueden ser atacar a otros equipos o sitios web o redes simplemente para crear el caos. Los hackers pueden bloquear un sistema informático para propiciar la pérdida de datos. También son capaces de lanzar ataques DDoS para conseguir que no se pueda acceder a sitios web mediante consiguiendo que el servidor falle.

Todos los factores anteriores vuelven a hacer hincapié en la necesidad de que nuestros datos deben permanecer seguros y protegidos confidencialmente. Por lo tanto, es necesario proteger tu equipo y eso hace que sea necesaria y muy importante todo lo que es la seguridad informática.

CAPACITACIÓN EN SEGURIDAD INFORMÁTICA

Un plan de gestión de seguridad informática no puede existir sin capacitación especializada en las nuevas amenazas y en cómo contrarrestar las mismas.

La certificación en seguridad que más se busca hoy en día es la CISSP (Certified Information Systems Security Professional) es una certificación desarrollada y mantenida por (ISC)² (International Information Systems Security Certification Consortium). Es considerada la certificación de mayor reconocimiento a nivel mundial, en la industria de la seguridad informática. Las estadísticas dicen que tiene un 48% de preferencia.

En este enlace tienes un artículo relacionado con la capacitación CISSP.

Le siguen la GIAC, CISA, CISM, SSCP y otras que empiezan a ser requeridas por los profesionales de redes y seguridad informática.

Las cuatro áreas principales que cubre la seguridad informática son:

- **Confidencialidad:** Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.
- **Integridad:** Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.
- **Disponibilidad:** Los datos deben estar disponibles para los usuarios cuando sea necesario.
- **Autenticación:** Estás realmente comunicándote con los que piensas que te estás comunicando.

REFERENCIA BIBLIOGRAFICA

- Marzo de 2018, Equipo de expertos universidad internacional de valencia. ¿Que es la seguridad informática y como puede ayudarme? Recuperado de: https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/