Introducción a la seguridad informática

Las naves salesianos | 2 GMªA

Aarón Cañamero mochales

2020

Actividades propuestas:

2. Realiza una tabla comparando ejemplo de seguridad pasiva y activa del campo de la informática y del campo de los vehículos.

Seguridad pasiva

|  |  |
| --- | --- |
| **Campo de la informática** | **Campo de los vehículos** |
| Copias de seguridad | Cinturón de seguridad |
| Crear particiones del disco | Pretensor y limpiador del cinturón |
| Comprobar el Antivirus | Airbags |
| Formatear el equipo | Corte de inyección |
|  | Sistemas de retención infantil |
|  | ecall |

Seguridad activa

|  |  |
| --- | --- |
| **Campo de la informática** | **Campo de los vehículos** |
| Utilización de contraseñas seguras | El sistema de frenado |
| Encriptar datos importantes | Sistema de dirección |
| Tener el Antivirus actualizado | Sistema de suspensión |
| Utilizar cortafuegos, etc | La iluminación |
| Tener otro usuario, auxiliar | Los neumáticos y su adherencia al suelo |
| Analizar el equipo periódicamente | Sistema de control de estabilidad |

3. ¿Cuál es el activo más valioso para una empresa?

La información es el activo mas importante de una empresa, tambien lo son los trabajadores.

1. ¿Qué vulnerabilidades podrían afectarle?

No tener un Antivirus, no tener un cortafuegos, no tener protección suficiente contra ataques informáticos, no tener ordenado correctamente los privilegios de cada usuario, etc.

1. ¿Qué amenazas son las que podrían afectarle? Clasifícalas.

**Amenazas naturales**: Son amenazas provocadas por condiciones medioambientales.

**Amenazas involuntarias**: Borrar, eliminar, estropear, algun tipo de fichero o sistemas, sin querer.

**Amenazas intencionadas**: Son aquellas en las que una persona interviene, para eliminar o crakear algo de la empresa, un software malicioso.

4. ¿Crees que la evaluación de riesgos será igual para todas las empresas? ¿Por qué?

No, cada empresa tiene que hacer un análisis de riesgo para evaluar adecuadamente, cada empresa tiene que saber cuanta seguridad vale sus activos y cuanta no.

5. Enumera posibles preguntas que podrían hacerse en la realización de una evaluación de riesgos.

¿Qué activos tiene que proteger?

¿Qué tipo de vulnerabilidades y amenazas pueden surgir?

¿Qué esfuerzo y dinero se está dispuesto a invertir?

¿Qué valor tienen los activos?

¿Cuál es el nivel de acceso a cada empleado?

¿Cómo se actuaria ante una amenaza o ataque?

Etc.

6. Busca en internet aplicaciones comerciales que permitan realizar una evaluación de riesgos.

Einforma, servicities, R-BOX.

7. A partir de los principios expresados en este epígrafe:

a) Plantea un posible ataque contra cada uno de estos principios.

b) Indica una posible solución para cada uno de los ataques planteados.

**Integridad**: Un ataque muy común seria alterar la información que se trasmite por una red o cambiar el funcionamiento de algunos datos.

Una solución muy común seria tener más protegida esta información, mediante un mejor cifrado.

**Confidencialidad**: Un ataque muy conocido seria robar los datos sensibles de los usuarios, por ejemplo, los usuarios de los empleados de la empresa.

Una posible solución sería usar mejores protocolos o cifrados.

**Disponibilidad**: Por ejemplo, quitar los permisos de un usuario sobre los servicios.

La solución más común seria utilizar un cortafuegos.

**Autenticación**: Ataques conocidos como robar la identidad a los usuarios, cambiar las contraseñas, los pines, etc.

Poner contraseñas mas seguras y cambiarlas periódicamente.

8. Busca más información sobre los sniffers en internet. ¿Qué son? ¿Qué utilidad tienen?

Programas capaces de capturar información que circula por la red a través de las tarjetas de red.

Tienen dos utilidades principales, legitimas e ilegitimas.

**Legitimas**: Ayudan a resolver problemas en la red, detectan los problemas y ayudan a analizar la red.

**Ilegítimas**: Ver y guardarse los datos sensibles de los usuarios, contraseña, tarjeta de crédito, numero de cuenta del banco. Etc.

9. ¿Crees que establecer normas a los usuarios de una organización para que tengan una contraseña de acceso segura es una buena política de seguridad?

Sí, ya que esta medida ayuda a que los datos e información de la empresa este mas segura, ya que una buena contraseña segura, puede ayudar muchisimo, contra ataques informáticos.

10. Indica qué políticas de seguridad establecerías para evitar la caída de los servidores de la organización.

Por ejemplo, tener servidores extras, para usarlo de respaldo, por si acaso se estropean los otros, tener sistemas RAID para tener la información mejor guardada y distribuida, tener los servidores de la organización en sitios seguros, restringiendo el acceso solo a las personas autorizadas, tener una política para las copias de seguridad y tener a disposición SAI para tener una alimentación interrumpida en caso de cortocircuitos.

11. ¿Quiénes crees que deben elaborar el plan de contingencia para una empresa?

Tiene que ser un grupo de personas, los responsables de cada área involucrada de la organización, estos deben analizar el impacto que pueda producirse ante un desastre y definir cuales deberán ser las soluciones alternativas a cada uno de los problemas. Y el personal del departamento de sistemas.

12. ¿Crees que un plan de contingencia, una vez creado es ya para toda la vida?

No, ningun plan de contingencia funcionaria, con esas medidas. Tiene que estar constantemente revisado, para que siempre pueda estar de acuerdo con las necesidades de la organización.