Clasificación de la información en el ámbito de la seguridad informatica

1 Confidencial: cuando el nivel de confidencialidad de la información se incremente. Ejemplo solo información accesible para alta dirección.

2 Restringido: para niveles medios de confidencialidad. Información para directores de área y personal de alto rango.

3 Uso interno: información con un nivel bajo de confidencialidad. Cualquier miembro de la organización.

4 Público: cuando todas las personas pueden ver la información. Puede ser compartida sin restricciones.

¿Que es la seguridad física?

*DEF: medidas que se toman para proteger los equipos, el software y la información. Para que estos no puedan ser dañados o destruidos.

1 Controles de ingreso y salida para evitar el acceso de personas no autorizadas.

2 Control de la seguridad del software mediante el uso de licencias legítimas y actualizaciones periódicas.

3 Bloqueo de los ordenadores desatendidos y control de las contraseñas de BIOS y de los dispositivos de arranque.

4 Seguridad del hardware (para la preservación de su integridad) mediante la instalación de cerraduras, fijaciones, plataformas de goma y otros elementos que eviten los golpes, las caídas, las vibraciones y el robo.

5 Desconfianza y protección frente ataques de los soportes de información externos y de las conexiones a internet no seguras.

*Posible pregunta: Explica que es la seguridad física y pon algún ejemplo

¿Que es la seguridad lógica?

*DEF: Protección de datos procesos y programas.

Acceso ordenado y autorizado de los usuarios a la información.

Claves, cifrados, firmas digitales, certificados digitales.

Complemente a la seguridad física.

MECANISMOS: Copias de Seguridad y Control de Acceso

Sistema fiable

*Fiablidad: probabilidad de que un sistema se comporte tal y como se espera de él.

Tres aspectos para la fiabilidad de un sistema informático:

-Hay que tener un **balance** de estos factores

Confidencialidad: Prevenir la divulgación no autorizada de la información.

Un ejemplo de técnica de confidencialidad es la criptografía.

Integridad: Prevenir modificaciones no autorizadas de la información.

Debemos distinguir entre **integridad de los datos e integridad del origen**

Disponiblidad: Prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

Autenticación y no repudio IMPORTANTE

La autenticación: permite **verificar la identidad** de quien accede a un recurso y se le **permite o no el acceso** según dicha identidad. (3 métodos: saber, tener, o ser)

El no repudio permite probar la participación de las partes en una comunicación. Es decir dejar registrada la comunicación

No repudio en el origen: Que el emisor no diga que envió el mensaje.

No repudio en el destino: Que el destinatario no diga que no recibió el mensaje.

CIDAN – DCIAN *washington DC IAN desde dentro*

Amenazas | Clasificación por Origen | Clasificación por Causa IMPORTANTE

Amenaza: las amenazas son todas aquellas cosas que le pueden suceder a los activos que se salen de la normalidad”

Tipos de amenazas:

Interrupción: Un sistema deja de estar disponible o es destruido. No es DOS sino fallo teleco

Interceptación: Alguien esta viendo los datos (**sniffing**)

Modificación: Alguien esta viendo y modificando los datos (**MITM**)

Fabricación: Alguien se está haciendo pasar por una persona autorizada y genera datos falsos (**spoofing**)

Destrucción: Alguien no autorizado interviene una comunicación para inutilizarla.

Tipos de según el origen:

Externas: Atacantes no conocen la red por lo que tienen que hacer un reconocimiento

Internas: Los usuarios conocen la red y su funcionamiento

Suelen ser amenazas más serias.

Tipos de según la causa:

Accidentes:

Accidente físico (indendio, explosión inundación)

Avería

Interrupción de servicios esenciales (agua, energia o teleco)

Accidente mecánico (choque, caída o radiación)

Errores:

diseño (bugs), utilización, compatibilidad, inesperados (virus), librerías

Amenazas Intencionales Presenciales:

- Acceso físico no autorizado
- Destrucción
- Interceptación pasiva no autorizada
- Humanos: huelgas, abandono, enfermedad, baja temporal

Amenazas Intencionales Remotas:

- Acceso lógico no autorizado
- gusanos
- Denegación de servicio (De ancho de banda y de recursos del sistema)
- suplantación de origen
- MITM

*Posible pregunta examen

7- Tipos de amenaza según su origen y procedencia

8- Tipos de amenazas según la causa.

10 - tipos de amenazas humanas

Varias preguntas y respuestas IMPORTANTE

Pregunta: “DDOS”

Respuesta: Implementar un firewall y pedir ayuda al ISP

Pregunta: “Troyano”

Respuesta: Antivirus actualizado con detección de troyanos

Pregunta: “Hack para conseguir información”

Respuesta: Tener el sistema actualizado.

Pregunta: “Virus”

Respuesta: Antivirus actualizado con detección de troyanos

Pregunta: “Ingeniería social”

Respuesta: user procedimiento de seguridad actualizando las claves del sistema periódicamente.

Tipos de amenazas:

Factor humano:

Curiosos:

- Personas que entran en sistemas de manera no autorizada por curiosidad, desafío personal o por el deseo de aprender.

Intrusos Remunerados:

Encargados de penetrar sistemas a cambio de pagos. Normalmente tienen amplios conocimientos de la materia

Personal enterado: son personas internas o antiguos empleados. Motivación: revanchas o ofertas.

Terroristas:

Robo: robo de hardware de almacenamiento

Sabotaje: Reducir la funcionalidad del sistema de manera intencionada.

Fraude: Aprovechar los recursos de la organización para obtener beneficios propios.

Ingeniería social:

Hardware:

Mal Diseño: componentes no cumplen con los requerimientos.

Errores de Fabricación:

Suministro de energía: se debe proporcionar voltajes dentro de los parámetros requeridos.

Desgaste

Descuido:

Red de datos

Topología seleccionada: Disposición inadecuada de los nodos de una red.

Sistema operativos: Diferencias de sistemas operativos que pueden hacer mas vulnerables algunos de ellos.

Incumplimiento de normas de instalación: Errores de instalación de cableado de red.

Copias de seguridad

Copias Total

Copia incremental: slo los cambios realizados **desde la ultima copia incremental**.

> Se puede realizar una copia total el dia 1 de cada mes y luego copias incrementales el resto de días.

Copia diferencial: Guardan los cambios desde la **última copia total**

Consejos de implementacion:

si el volumen de datos es pequeño haremos copias totales.

Si el volumen de datos es mediano 4GB<*tamaño copia*<50GB

Haremos copias diferenciales. (Solo recuperaremos la total y la **ultima diferencial**)

Si el volumen de datos es grande 50GB<*tamaño copia*

Haremos copias incrementales que son las que menos ocupan.

Recuperaremos la ultima copia total y todas las incrementales.

- Todos los días 1 de cada mes, a las 23:00 horas: copia de seguridad total
- Todos los viernes a las 23:00 horas: copia de seguridad diferencial desde la copia de día 1
- Todos los días (excepto los viernes y el día 1) a las 23:00 horas: copia de seguridad incremental desde la copia del día anterior.

¿Que es un SAI

Sistema de alimentación ininterrumpida.

Off-line: Alimentación de red electrica. Si se corta la luz se activa la bateria.

> Puede haber un periodo de conmutación

In-line: Dispone de filtros activos que filtran la tension de entrada.

> Puede haber un periodo de conmutación
>
> Si se corta la luz se activa la batería.

On line: Genera alimentación eléctrica con una onda sinusoidal perfecta.

> En todo caso su electricidad proviene de la bateria por lo que no hay corte de suministro.