1. Fiabilidad, Confidencialidad, Integridad y Disponibilidad

- **Fiabilidad**: Es la capacidad de un sistema para funcionar adecuadamente durante un periodo de tiempo específico bajo condiciones normales. Un sistema fiable debe:
    - Evitar fallos.
    - Tolerar defectos.
    - Recuperarse de ellos, tanto en términos de rendimiento como de los datos.
- **Confidencialidad**: Asegura que la información solo es accesible por personas o sistemas autorizados. Un mensaje o archivo es confidencial si solo puede ser comprendido por el destinatario autorizado, utilizando, por ejemplo, técnicas de cifrado.
- **Integridad**: Garantiza que los datos o archivos no han sido alterados de forma no autorizada. Asegura la correspondencia entre los datos y los hechos que reflejan.
- **Disponibilidad**: La información debe estar disponible cuando sea requerida por personas, aplicaciones o procesos autorizados. La alta disponibilidad garantiza que los sistemas sigan operativos sin interrupciones causadas por fallos de energía, problemas de hardware o actualizaciones.

---

2. Elementos Vulnerables en el Sistema Informático

- **Hardware**: Las vulnerabilidades del hardware pueden llevar a fallos en el sistema:
    - **Mal diseño**: Cuando los componentes no son adecuados para las especificaciones del sistema.
    - **Errores de fabricación**: Piezas defectuosas que pueden fallar al usarse.
    - **Suministro de energía**: Las fluctuaciones de voltaje pueden dañar los dispositivos si no se gestionan correctamente.
    - **Desgaste**: El uso constante y prolongado reduce la vida útil de los dispositivos.
    - **Descuido y mal uso**: Al no seguir los parámetros de uso y mantenimiento recomendados por los fabricantes, se acelera el desgaste de los componentes.
- **Software**: Los fallos en el software también representan vulnerabilidades que pueden ser aprovechadas para ataques:
    - **Errores de programación**: Bugs que dejan el sistema vulnerable.
    - **Software incorrecto o malicioso**: Programas que tienen intenciones maliciosas o que se utilizan de forma indebida para acceder o dañar sistemas.

---

3. Amenazas Físicas y Lógicas

- **Amenazas Lógicas**: Son las que afectan a los sistemas a través de software malicioso o fallos en el software:
    - **Software incorrecto**: Incluye errores de programación, instalación incorrecta de sistemas o componentes que permiten vulnerabilidades.
    - **Virus**: Programas maliciosos que se insertan en archivos ejecutables y se replican para infectar otros archivos.
    - **Gusanos**: Malware que se replica por sí solo y se propaga entre sistemas, a menudo sin intervención del usuario.
    - **Troyanos**: Programas que aparentan ser útiles, pero contienen funciones dañinas ocultas.
    - **Puertas traseras**: Accesos ocultos dejados por desarrolladores que pueden ser aprovechados por atacantes para eludir controles de seguridad.
    - **Bombas lógicas**: Software que se activa en un momento o condición específica para causar daño.
    - **Eavesdropping**: Técnica de interceptación de comunicaciones no autorizadas para obtener información.
- **Amenazas Físicas**: Son riesgos relacionados con el ambiente físico o accidentes que afectan el hardware y los sistemas:
    - **Incendios**: El fuego es una de las mayores amenazas físicas, capaz de destruir equipos y datos.
    - **Inundaciones**: El agua puede dañar severamente los equipos, ya sea por causas naturales o por sistemas de extinción de incendios.
    - **Condiciones climáticas**: Tormentas, terremotos y otros fenómenos naturales pueden afectar las instalaciones y equipos.
    - **Acciones hostiles**: Sabotajes, robos o actos de vandalismo que ponen en peligro la infraestructura física.

4. Seguridad Física y Ambiental

La **seguridad física** es esencial para proteger los equipos y la infraestructura informática. Se refiere a la implementación de barreras y controles de acceso para evitar que personas no autorizadas dañen, roben o accedan a los sistemas. Algunos ejemplos son:

- **Cámaras de seguridad**: Para monitorear áreas sensibles como centros de procesamiento de datos.
- **Cerraduras electrónicas**: Activadas mediante tarjetas de acceso o biometría.
- **Controles de acceso remoto**: Para gestionar quién puede entrar y salir del área donde se almacenan los equipos.

Principales amenazas en seguridad física:

1. **Desastres naturales**: Incendios, tormentas, terremotos e inundaciones.
2. **Amenazas humanas**: Sabotaje, robos, disturbios y vandalismo.
3. **Acciones hostiles deliberadas**: Sabotajes internos o externos.

Implementar estas medidas físicas reduce riesgos, mejora la eficiencia operativa y permite tener control sobre los posibles incidentes.

---

5. Protección del Hardware y los Datos

- **Protección física**: Incluye medidas como el control de acceso físico a los equipos, el uso de cerraduras y cámaras, y el aislamiento de zonas críticas.
- **Condiciones ambientales**: Es crucial mantener las condiciones adecuadas de temperatura, humedad y ventilación en los centros de datos para evitar fallos de hardware. Esto incluye:
    - **Sistemas de control de temperatura**: Para evitar sobrecalentamientos.
    - **Prevención de polvo y electricidad estática**: Factores que pueden dañar componentes electrónicos sensibles.
- **Prevención de desastres naturales**: Instalación de sistemas contra incendios, control de acceso en caso de emergencias y medidas de contención de agua para prevenir inundaciones.

---

6. Copias de Seguridad (Backup)

Las **copias de seguridad** son esenciales para proteger los datos y garantizar su recuperación en caso de pérdida. Existen varios tipos de copias de seguridad:

- **Copias totales**: Respaldan todos los archivos seleccionados, independientemente de si han sido modificados o no.
- **Copias incrementales**: Solo respaldan los archivos que han cambiado desde la última copia total o incremental.
- **Copias diferenciales**: Respaldan todos los archivos que han sido modificados desde la última copia total, pero no eliminan el bit de modificado.

La elección del tipo de copia de seguridad dependerá de la cantidad de datos, la frecuencia de las modificaciones y el espacio de almacenamiento disponible. Se recomienda realizar copias periódicas para asegurar que los datos siempre puedan recuperarse.

Un centro de respaldo es un CPD preparado para asumir las operaciones de un CPD principal en caso de emergencia (ej. incendios o desastres). Es utilizado por instituciones críticas como bancos y gobiernos para evitar interrupciones.

Elementos Clave:

- Ubicación: Entre 20 y 40 km del CPD principal para evitar que ambos se vean afectados por el mismo incidente.
- Equipamiento: Puede ser idéntico (sala blanca) o similar (sala de back-up).
- Software: Debe ser idéntico al del CPD principal para garantizar la continuidad.

Réplica de datos:

- **Copia síncrona:** Sin desfase entre ambos CPDs.
- **Copia asíncrona:** Puede haber retrasos en la actualización, aceptable para negocios no críticos.

Conectividad y Tecnología:

- Uso de fibra óptica para baja latencia.
- Tecnologías: iSCSI y Fibre Channel.

Plan de Contingencia:

- **Plan de respaldo:** Contempla las actuaciones necesarias antes de que se produzca un incidente. Esencialmente, mantenimiento y prueba de las medidas preventivas.
- **Plan de emergencia**: Contempla las actuaciones necesarias durante un incidente.
- **Plan de recuperación:** Contempla las actuaciones necesarias después de un incidente. Básicamente, indica cómo volver a la operación normal.

7. Centros de Respaldo

Un **centro de respaldo** es un centro de procesamiento de datos alternativo, diseñado para tomar el control en caso de que el centro principal se vea afectado por una contingencia grave. Los centros de respaldo están ubicados en diferentes localizaciones para evitar que un desastre afecte ambos centros al mismo tiempo.

Existen dos enfoques para el respaldo de datos:

- **Copia síncrona**: Los datos se copian en ambos centros simultáneamente.
- **Copia asíncrona**: Los datos se copian en el centro de respaldo con un desfase temporal, lo que puede provocar la pérdida de algunos datos en caso de fallo.

Los centros de respaldo son fundamentales para mantener la **alta disponibilidad** en organizaciones críticas como bancos o administraciones públicas.

---

8. Sistemas de Almacenamiento

- **SAN (Storage Area Network)**: Es una red dedicada que conecta servidores y sistemas de almacenamiento. Utiliza tecnologías como **Fibre Channel** o **iSCSI** para proporcionar acceso rápido y seguro a los datos. Las SAN se utilizan principalmente en grandes empresas donde se requiere un acceso rápido y fiable a grandes volúmenes de información.
- **NAS (Network Attached Storage)**: Es un dispositivo de almacenamiento conectado a la red que permite a varios usuarios acceder a los datos a través de protocolos como CIFS, NFS o FTP. Los sistemas NAS son ideales para compartir datos de manera centralizada en redes de usuarios múltiples.

9. Control de Acceso Lógico

Los **controles de acceso lógico** son medidas para proteger los datos y sistemas mediante el control de quién tiene acceso a qué recursos. Los pasos para el control de acceso incluyen:

1. **Identificación**: El usuario se identifica mediante nombres de usuario o tarjetas.
2. **Autenticación**: Verificación de la identidad mediante contraseñas, reconocimiento de voz o biometría.
3. **Autorización**: Asignar permisos específicos a los usuarios según su rol en la organización.

La combinación de estos tres pasos asegura que solo las personas autorizadas puedan acceder a los recursos del sistema.

---

10. Auditorías de Seguridad Informática

Las auditorías de seguridad son revisiones exhaustivas de los sistemas informáticos para identificar vulnerabilidades y proponer mejoras. Los tipos de auditorías incluyen:

. Tipos de auditorías.

Los servicios de auditoría pueden ser de distinta índole:

- **Auditoría de seguridad interna.** En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno
- **Auditoría de seguridad perimetral**. En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores
- **Test de intrusión**. El test de intrusión es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.
- **Análisis forense**. El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se denomina análisis postmortem.
- **Auditoría de páginas web**. Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código sql, Verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS), etc.
- **Auditoría de código de aplicaciones.** Análisis del código tanto de aplicaciones páginas Web como de cualquier tipo de aplicación, independientemente del lenguaje empleado

---

11. Criptografía

La **criptografía** es el arte de cifrar y descifrar información para protegerla durante su transmisión o almacenamiento. Sus principales objetivos son:

- **Confidencialidad**: Asegurar que solo el destinatario autorizado pueda leer el mensaje.
- **Autenticidad**: Verificar que el remitente es quien dice ser y que el mensaje no ha sido alterado.
- **Integridad**: Asegurar que el contenido del mensaje no ha sido modificado durante su transmisión.

La criptografía se basa en la aritmética: En el caso de un texto, consiste en transformar las letras que conforman el mensaje en una serie de números (en forma de bits ya que los equipos informáticos usan el sistema binario) y luego realizar cálculos con estos números para:

- **Modificarlos y hacerlos incomprensibles.** El resultado de esta modificación (el mensaje cifrado) se llama texto cifrado, en contraste con el mensaje inicial, llamado texto simple.
- **Asegurarse de que el receptor pueda descifrarlos**. El hecho de codificar un mensaje para que sea secreto se llama cifrado. El método inverso, que consiste en recuperar el mensaje original, se llama descifrado.

La criptografía utiliza dos tipos de claves:

- **Clave simétrica**: La misma clave se utiliza tanto para cifrar como para descifrar los mensajes.
- **Clave asimétrica**: Se usan dos claves diferentes, una para cifrar y otra para descifrar.

Seguridad Activa y Seguridad Pasiva.

Seguridad activa: Tiene como objetivo proteger y evitar posibles daños en los sistemas informáticos. Podemos encontrar diferentes recursos para evitarlos como:

- Una de esas técnicas que podemos utilizar es el uso adecuado de contraseñas, que podemos añadirles números, mayúsculas, etc.
- También el uso de software de seguridad informática: como por ejemplo ModSecurity, que es una herramienta para la detección y prevención de intrusiones para aplicaciones web, lo que podríamos denominar como “firewall web”.
- Y la encriptación de los datos.

seguridad pasiva: Su fin es minimizar los efectos causados por un accidente, un usuario o malware.

- Las prácticas de seguridad pasiva más frecuentes y más utilizadas hoy en día son: El uso de hardware adecuado contra accidentes y averías.
- También podemos utilizar copias de seguridad de los datos y del sistema operativo

Resumen: Cifrado y Descifrado

- Texto plano: Información original que se desea proteger.

Cifrado: Convierte el texto plano en texto cifrado o criptograma usando un algoritmo y una clave secreta.

- Sustitución: Cambia los elementos del mensaje (letras o símbolos).
- Transposición: Reordena los elementos del mensaje.

Descifrado: Proceso inverso que recupera el texto plano a partir del criptograma y la clave.

- Criptosistema: Conjunto de protocolos, algoritmos, gestión de claves y procesos que permiten el cifrado y descifrado.

Tipos de Cifrado:

1. **Cifrado simétrico:** Usa una misma clave para cifrar y descifrar.
2. **Cifrado asimétrico**: Usa una clave para cifrar y otra diferente para descifrar.

El cifrado simétrico es más antiguo, mientras que el asimétrico es la base de las técnicas modernas.

Continuar generando