Modulo 2 UD1466 - LAB-U1

Preguntas:

¿Cuál es la importancia de la gestión eficiente de la información en una organización?

garantizan la eficiencia operativa y también aseguran la integridad y disponibilidad de la información a lo largo del tiempo

¿Qué temas clave se abordan en el documento respecto a la organización y gestión de la información?

Sistemas de archivo, volúmenes lógicos y Seguridad

Describe las prácticas recomendadas para la nomenclatura y codificación de archivos.

Consistencia, descriptividad/legibilidad, no caracteres especiales, longitud adecuada. es recomendable fechar los documentos.

¿Qué beneficios ofrece el particionamiento de un disco duro físico?

El aislar los datos y poder agruparlo según su función o tipo. flexibilidad, seguridad y rendimiento.

Define el concepto de Punto Único de Fallo (SPOF) y menciona sus características.

es un componente o nodo dentro de un sistema que, si falla, puede causar la interrupción completa del sistema o servicio.

Las características son Dependencia crítica del sistema sobre esa pieza, falta de redundancia/copia/respaldo de ese componente en caso de fallo y que tenga un impacto significativo en el rendimiento del sistema.

¿Qué es el RPO (Recovery Point Objective) y cómo se aplica en la recuperación de datos?

La fracción máxima de tiempo donde la pérdida de datos es aceptable, por ejemplo, si es de 2 horas, hay que hacer una copia cada dos horas para que en caso de fallo sólo se pierdan dos horas de datos.

Explica el concepto de RTO (Recovery Time Objective) y su importancia en la continuidad del negocio.

Fracción máxima de tiempo durante la que es aceptable que el servicio esté caído. si es de 2 horas, el equipo de IT ha de restablecer el servicio dentro de esas dos horas como máximo.

una cuidada planificación ayuda minimizar el impacto de los fallos e incidentes en la organización.

¿Cuáles son las mejores prácticas para la custodia de ficheros de seguridad?

Tenerlos encriptado, almacenados en local y en remoto con mantenimiento constante, , con

sistemas de respaldo y en contenedores de seguridad como cajas fuertes o salas cerradas.

¿Qué es la LOPD y qué derechos otorga a los individuos respecto a sus datos personales?

La Ley de protección de datos, te da derecho a CRUD todos los datos que disponga una empresa de ti.

Menciona los pasos esenciales para crear un Plan de Continuidad de Negocio (BCP).

Análisis de impacto en el negocio, Evaluación de riesgos, Desarrollo de estrategias de continuidad, desarrollo de plan, implementación y capacitación del personal, revisión y actualización.

¿Cómo se relacionan los conceptos de RPO y RTO en un plan de continuidad de negocio?

Durante el proceso de análisis de impacto hay que tener en cuanta y calcular adecuadamente cuando y cuanto son los tiempos aceptables de caída de servicio y pérdida de datos. y tenerlas en cuenta en la fase de desarrollo de estrategias para implementar soluciones adecuadas.

Analiza las ventajas y desventajas del uso de controladoras RAID por software y hardware.

Por SW es más barato y flexible, con menos nivel de complejidad a la hora de configurarlo.

por HW es mas fiable y con mejor rendimiento pero necesitas HW específico y no es tan sencillo de configurar y mantener.

Discute la importancia de las auditorías de seguridad y su impacto en la protección de datos.

son importantísimas puesto que son uno de los mecanismos para identificar los riesgos potenciales que pueden hacer caer el sistema o servicio

Evalúa las medidas de prevención de infecciones por malware mencionadas en el documento.

Instalación de SW, actualización del mismo y del usuario, control de accesos.

¿Cuál es la diferencia entre una copia de seguridad completa, incremental y diferencial?

Completa es todos los datos, incremental es que guarda sólo el incremento de datos y diferencial guarda sólo la diferencia con lo anterior. las dos últimas ocupan menos espacio.

¿Cómo contribuyen las políticas de alta disponibilidad a la resiliencia de una organización?

asegurando que los datos estén disponibles en todos momento minimizando el tiempo de inactividad.

Describe el proceso de planificación de una auditoría de seguridad.

Involucra la definición del alcance, identificación de áreas críticas, desarrollo de un plan de auditoría detallado y asignación de responsabilidades. También incluye la programación de actividades y la comunicación con las partes interesadas

Explica los métodos de detección de malware y su efectividad.

Firmas digitales del propio malware, Heurística por comportamientos del SW, ejecutando Sandboxes para ejecución del malware sospechoso.

¿Qué estrategias se recomiendan para la destrucción segura de datos?

Formatear, desmagnetizar y romper físicamente.

Analiza los elementos clave para implementar un sistema de protección antivirus efectivo.

Mantener el SW actualizado así como los usuarios, Monitorizar el sistema de forma contínua y analizar el comportamiento para amenazas avanzadas.

¿Qué implica la implementación de sistemas de Single Sign On (SSO)?

Creación de llaves de encriptación mas seguras y poder acceder a múltiples servicios con esa misma clave encriptada

¿Cómo se asegura la integridad de los datos en una organización?

Se garantiza mediante controles de acceso, auditorías de seguridad, copias de seguridad regulares y el uso de tecnologías de verificación como hashes y sumas de verificación.

¿Qué es la migración de datos y por qué es importante?

Es el proceso de transferir datos de un sistema a otro. Es importante para actualizar tecnologías, mejorar la eficiencia y cumplir con nuevas regulaciones.

Explica la estructura jerárquica de almacenamiento de archivos.

Organiza archivos en una estructura de árbol con directorios y subdirectorios, facilitando la navegación y la administración de datos. debe ser nombrados de forma lógica y coherente que faciliten su comprensión.

Describe los diferentes niveles de protección RAID y sus aplicaciones.

RAID 0 ofrece el mejor rendimiento pero sin redundancia, mientras que RAID 1, RAID 5 y RAID 6 ofrecen varias formas de protección contra fallos de discos, con diferentes implicaciones en cuanto a capacidad y rendimiento.

Raid 0 edición y VJ, raid 1 BBDD, Raid 5 servidores de archivos y apps, raid 6 servidores de empresa.

¿Qué se entiende por análisis de vulnerabilidades en una auditoría de seguridad?

El análisis de vulnerabilidades identifica debilidades en sistemas, aplicaciones y redes que pueden ser explotadas. Involucra escaneos automáticos y evaluaciones manuales para descubrir problemas y proporcionar recomendaciones para mitigar riesgos.

¿Qué es un clúster de alta disponibilidad y cómo funciona?

Un clúster de alta disponibilidad es un grupo de servidores que trabajan juntos para minimizar el tiempo de inactividad y asegurar la continuidad del servicio. Utiliza técnicas como el failover automático para redirigir el tráfico a nodos activos en caso de fallo.

¿Cómo se lleva a cabo la verificación periódica de datos archivados?

Involucra revisar y comprobar regularmente los archivos almacenados para asegurar que no se hayan corrompido y que sigan siendo accesibles y legibles. Esto puede incluir restauraciones de prueba y verificaciones de integridad de datos.

Menciona los componentes de un sistema de protección antivirus.

Detección de Malware, prevención de infecciones y eliminación de infecciones.

¿Qué es una auditoría de cumplimiento y cuál es su propósito?

Ver si se cumplen las medidas de seguridad implementadas

Analiza las ventajas del uso de técnicas de protección en tiempo real contra el malware.

analizan todos los archivos que llegan por vias externas (discos externos o correo,) antes de abrirlos en el sistema.

Evalúa las implicaciones de la transferencia internacional de datos según la LOPD.

dependes de las legislaciones internacionales para la gestión y almacenamiento de datos y difieren bastantes según el país.

Describe cómo se implementa y configura una solución antivirus en una organización.

Instalación de SW específico en todos los dispositivos y configuración de escaneos regulares y escaneos en tiempo real. Actualización de la librería de Virus y capacitación de los usuarios.

Discute las medidas técnicas y organizativas para la seguridad de los datos personales.

las mismas que para mantener una correcta seguridad. protección por cifrado, almacenamiento el lugares seguros y protegidos por llaves o claves, restringir el acceso a personal no imprescindible para su desempeño

¿Cuál es el papel de la capacitación continua del personal en la seguridad de la información?

Mantener a todo el personal al día de las nuevas tecnologías, legislaciones y métodos de seguridad para mejorar el factor humano de la seguridad corporativa.

Analiza los métodos de control de acceso basados en roles (RBAC) y atributos (ABAC).

RBAC define el perfil del usuario en base a un rol y a ello da permisos (contable, CEO, señora de la limpieza).

ABAC define unas atribuciones u en base a ello capacita a las personas (necesitan entrar en la puerta b, acceso a contabilidad, acceso a BBDD)

Evalúa la importancia de los sistemas de monitoreo de redes en la seguridad de la información.

Es interesante para tener claro que no hay tráfico que se desvía o que hay escuchadores insertados en la red o que no hay un consumo excesivo de tráfico que podría indexar una vulnerabilidad o un proceso actuando en remoto y por detrás del sistema.

¿Cómo afectan los costos y la complejidad a la elección del nivel de RAID en una organización?

cuanto mas complejo y críticos son los datos mas caro es mantener la redundancia y paridad necesaria para hacer el sistema seguro y estable.

Describe el proceso de evaluación y análisis durante una auditoría de seguridad.

revisión de políticas de seguridad, test de ataque, análisis de vulnerabilidades y controles de acceso y protección de datos. El objetivo es identificar las brechas y poner medidas correctivas.

¿Qué estrategias de redundancia y recuperación se recomiendan en un plan de continuidad de negocio?

sistemas de respaldo, centros de datos alternativos ,

¿Qué pasos incluye el desarrollo de un plan de respuesta a incidentes?

Implementar soluciones de redundancia y recuperación y crear planes detallados de respuesta a incidentes.

documentar los procedimientos de recuperación, asignar roles y responsabilidades y estableces procedimientos de comunicación para informar a Stakeholders.

¿Qué es el sandboxing y cómo se utiliza en la detección de malware?

abrir el archivo sospechoso en un entorno de prueba donde el resultado no afecta a la maquina en si.

¿Cuáles son las directrices de retención de datos según las políticas de salvaguarda?

definen durante cuanto tiempo se deben conservar los datos basándose en el cumplimiento de la LOPD o. basadas en necesidades del negocio.

¿Qué implica la recolección de información en una auditoría de seguridad?

seguir rigurosamente la LOPD y revisar los logs de acceso y eventos para detectar comportamientos anómalos.

Describe las prácticas comunes para el almacenamiento seguro de ficheros de seguridad.

Mantener copias de seguridad

¿Qué métodos de autenticación se mencionan para el acceso restringido por cuentas de usuario?

Contraseñas fuertes (128), doble factor, biometría y certificados digitales

¿Cómo se realiza la evaluación de impacto en un análisis de impacto en el negocio (BIA)?

determina el efecto de las caídas de servicio en las funciones críticas de negocio identificando los riesgos y los impactos financieros y ayuda a priorizar recursos de recuperación

Menciona las aplicaciones del balanceo de carga y sus ventajas.

Distribución del tráfico y cargas de trabajo entre varios servidores para optimizar el rendimiento y evitar sobrecargas.

¿Qué se entiende por la protección antivirus basada en firmas y análisis heurístico?

Basada en firmas del malware fáciles de detectar y el análisis heurístico identifica comportamientos sospechosos.

Describe las actividades de monitoreo y mantenimiento de una solución antivirus.

actualización de SW, escaneos del sistema y revisión de logs de forma periódica y respuesta rápida ante las alertas de ITSO