GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO (MF0490_3)

SEGURIDAD INFORMÁTICA (IFCT0109)

Felipe de Abajo Aragón

Objetivos del módulo

Objetivo general

Gestionar servicios en el sistema informático.

Objetivos específicos

1. Analizar los procesos del sistema con objeto de asegurar un rendimiento adecuado a los parámetros especificados en el plan de explotación.
2. Aplicar procedimientos de administración a dispositivos de almacenamiento para ofrecer al usuario un sistema de registro de la información íntegro, seguro y disponible.
3. Administrar el acceso al sistema y a los recursos para verificar el uso adecuado y seguro de los mismos.
4. Evaluar el uso y rendimiento de los servicios de comunicaciones para mantenerlos dentro de los parámetros especificados.

Presentación personal

Mis estudios

- CFGS Desarrollo de Aplicaciones Web (DAW).
- Grado en Educación Social.
- Máster Universitario en Educación y TICs.
- Certificado de Profesionalidad de Habilitación para la Docencia en Grados A, B y C del Sistema de Formación Profesional.

Experiencias profesionales más relevantes

- LMS Administrator en The Core School (Grupo Planeta) y Le Cordon Bleu.
- Informático especializado en Microsoft 365 y Power Platform en Autismo Burgos.
- Desarrollador Power Plaform y Dynamics 365 en Meirovich Consulting.
- Formador de informática: SharePoint, Microsoft Forms y Microsoft 365.

Gestión de la seguridad y normativas

- Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información.
- Metodología ITIL. Librería de infraestructuras de las tecnologías de la información.
- Ley orgánica de protección de datos de carácter personal (LOPD).
- Normativas más frecuentemente utilizadas para la gestión de la seguridad física.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

- Directrices para la implementación.
- Complemento a la ISO 27001.
- Útil para organizaciones que buscan guía sobre mejores prácticas.

Metodología ITIL. Librería de infraestructuras de las tecnologías de la información

- Recomendaciones o mejores prácticas para gestionar servicios de informática y mejorar el nivel de los servicios y del soporte.
- Marco de referencia para la gestión de servicios tecnológicos a lo largo de todo su ciclo de vida.
- **Objetivo principal**: facilitar que los objetivos de la organización y los servicios vayan en la misma línea, incluso cuando cambian.
- **Fases y procesos**: estrategia del servicio, diseño del servicio, transición de servicios, ejecución de servicios y mejora continua de los servicios.

Estrategia del servicio | Metodología ITIL. Librería de infraestructuras de las tecnologías de la información

Descripción del ciclo de vida del servicio y describe como diseñar, desarrollar e implementar la gestión.

- **Estrategia de gestión de servicios de informática**: evaluación y métricas de la estrategia.
- **Gestión del portfolio de servicios de informática**: definición y documentación de servicios de informática.
- **Gestión financiera de servicios de informática**: determinación de los costes y elaboración de presupuestos.
- **Gestión de la demanda**: previsión de la demanda futura de los servicios de informática y presupuestos de recursos.
- **Gestión de la relación con la parte de negocio**: gestión de la retroalimentación y mejora de los servicios de informática.

Diseño del servicio | Metodología ITIL. Librería de infraestructuras de las tecnologías de la información

Descripción sobre cómo diseñar servicios y procesos.

- **Gestión del catálogo de servicios**: definir los servicios disponibles en un catálogo de servicios.
- **Gestión de la disponibilidad**: procesos en torno a la gestión y la monitorización de los servicios informáticos.
- **Gestión de la seguridad de la información**: creación, gestión y evaluación de servicios de seguridad de la información.
- **Gestión del nivel de servicios**: procesos de creación, gestión y retroalimentación para los acuerdos del nivel de servicios (SLA, en inglés).
- **Gestión de la capacidad**: monitorizar y optimizar las capacidades de los servicios.
- **Coordinación del diseño**: coordinación de diseños de procesos y políticas.
- **Gestión de proveedores**: selección y gestión de proveedores y monitorización del rendimiento.
- **Gestión de la continuidad de los servicios informáticos**: desarrollo, implementación y mantenimiento de servicios de continuidad y respuesta ante desastres.

Transición de servicios | Metodología ITIL. Librería de infraestructuras de las tecnologías de la información

Explica la gestión de la transición de nuevos servicios o cambios en los existentes.

- **Planificación y soporte en las transiciones**: responsabilidad de poner servicios en producción.
- **Gestión del cambio**: responsabilidad general de las solicitudes de cambio y gestión del riesgo en los cambios.
- **Evaluación de los cambios**: medir el impacto y la mejora o deterioro del rendimiento.
- **Gestión del lanzamiento y despliege**.
- **Gestión de la configuración de servicios**: monitoriza el ciclo de vida de los servicios informáticos y el hardware relacionado.
- **Validación y pruebas de los servicios**: pruebas del impacto y los beneficios de servicios informáticos previos al lanzamiento.
- **Gestión del conocimiento**: responsabilidad de la documentación y curación de de contenidos para la documentación de los servicios informáticos.

Ejecución de servicios | Metodología ITIL. Librería de infraestructuras de las tecnologías de la información

Guía para la entrega de servicios.

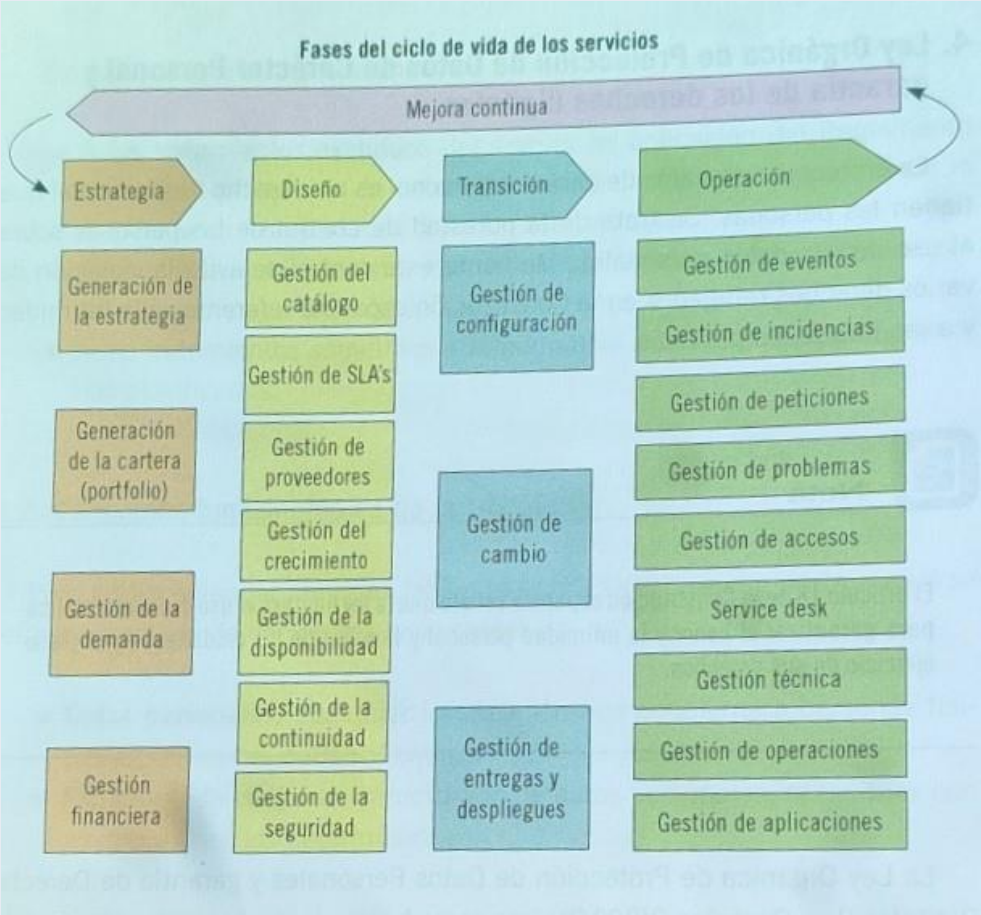
- **Gestión del acceso**: en relación con el acceso a los datos, controla que la asignación es correcta.
- **Gestión de eventos**: coordinada con la gestión de incidentes y problemas.
- **Entrega de solicitudes de servicio**: gestiona el ciclo de vida de una solicitud de servicio, desde la definición al cierre.
- **Gestión de incidentes**: triage y resolución de eventos disruptivos.
- **Gestión de problemas**: define la relación causal entre incidentes y encuentra o resuelve las causas que dan origen al problema.

Mejora continua de los servicios | Metodología ITIL. Librería de infraestructuras de las tecnologías de la información

Sobre la alineación de los servicios informáticos a medida que cambian las necesidades del negocio.

- **Gestión del acceso**: en relación con el acceso a los datos, controla que la asignación es correcta.
- **Gestión de eventos**: coordinada con la gestión de incidentes y problemas.
- **Entrega de solicitudes de servicio**: gestiona el ciclo de vida de una solicitud de servicio, desde la definición al cierre.
- **Gestión de incidentes**: triage y resolución de eventos disruptivos.
- **Gestión de problemas**: define la relación causal entre incidentes y encuentra o resuelve las causas que dan origen al problema.

Metodología ITIL. Librería de infraestructuras de las tecnologías de la información



Ley orgánica de protección de datos de carácter personal (LOPD)

- Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) es una ley de 1999.
- Reglamento General de Protección de Datos, es de 2016 y su ámbito de aplicación es toda la Unión Europea.
- La Ley Orgánica de Protección de Datos y de Garantía de los Derechos Digitales (LOPDGDD) adapta el Derecho al RGPD.

Normativas más frecuentemente utilizadas para la gestión de la seguridad física

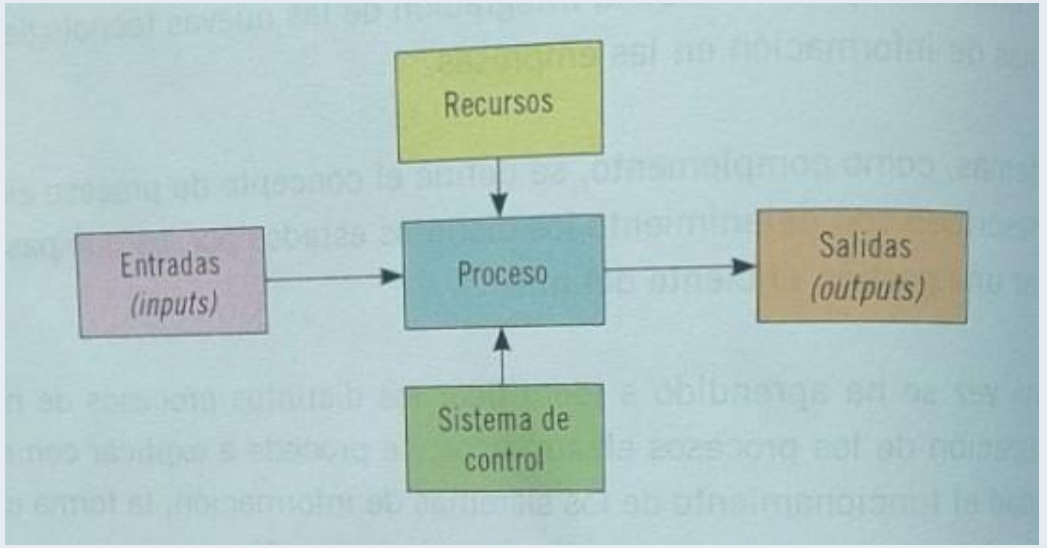
- 9ª sección de la norma 27002 (09-Seguridad Física y del Entorno). 2 partes según los tipos de medidas:
- **Áreas seguras**: perímetro de seguridad física; controles físicos de entrada; seguridad de oficinas, habitaciones y medios; protección contra amenazas internas y externas; trabajo en áreas seguras y áreas aisladas de carga y descarga.
- **Seguridad de los equipos**: ubicación y protección del equipo; servicios públicos de soporte; seguridad del cableado; mantenimiento de los equipos; seguridad de los equipos fuera de las instalaciones; seguridad de reutilización o retirada y retirada de propiedades de la organización.

Análisis de los procesos de sistemas

- Identificación de procesos de negocio soportados por sistemas de información.
- Características fundamentales de los procesos electrónicos.
- Estados de un proceso.
- Determinación de los sistemas de información que soportan los procesos de negocio y los activos y servicios utilizados por los mismos.
- Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios.
- Técnicas utilizadas para la gestión del consumo de recursos.

Identificación de procesos de negocio soportados por sistemas de información

- Definiciones de proceso de negocio:
  - Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.
  - Tareas conectadas de modo sistemático con el fin de obtener un producto o un servicio que tenga valor para el cliente.
- Cinco partes:
  - Proceso.
  - Entradas (input).
  - Salidas (outputs).
  - Recursos.
  - Sistemas de control.



Identificación de procesos de negocio soportados por sistemas de información

- Tipos de procesos de negocio:
  - Procesos para la gestión de una organización.
  - Procesos para la gestión de recursos.
  - Procesos operativos.
  - Procesos de apoyo.
  - Procesos de medición, análisis y mejora.
- Enfoque de gestión por procesos:
  - **Objetivos**: mejorar el rendimiento de la organización, elevar la satisfacción del cliente y fluidez entre áreas funcionales.
  - **Herramientas**: diseño, modelaje, documentación y optimización continua de los procesos de negocio.

Identificación de procesos de negocio soportados por sistemas de información

- Procesos de negocio y sistemas de información:
  - Los sistemas de información se crearon para apoyar procesos de negocio, para automatizar procesos de negocio o al menos parte de ellos (tareas).
  - Actualmente, los sistemas de información están mucho más integrados en los procesos de negocio, cualquier proceso que genera datos y supone un flujo de información puede ser informatizado.
  - La integración de los sistemas de información en los procesos de negocio supone un coste elevado pero a largo plazo se obtienen ventajas competitivas.

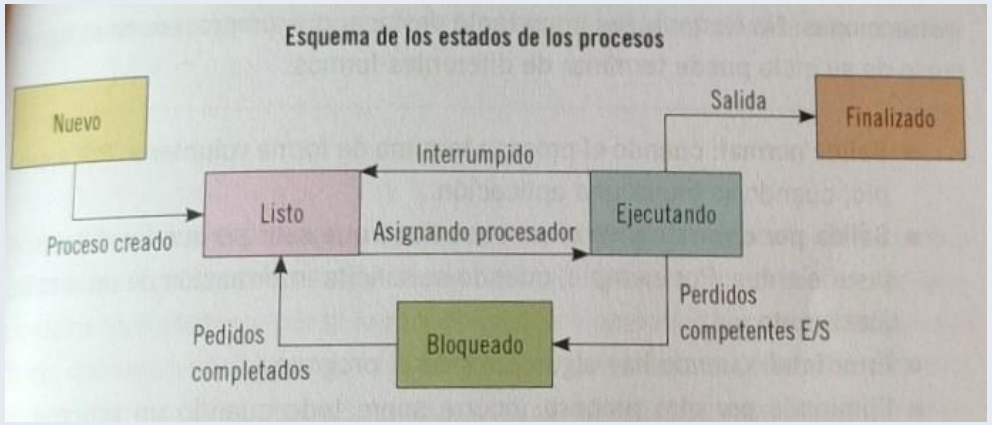
Características fundamentales de los procesos electrónicos

- Definición de proceso electrónico:
  - Consiste en cualquier programa en ejecución. Cuando lo que tiene un programa se carga en memoria y se ejecuta, pasa a ser un proceso.

- Recursos de los procesos electrónicos:
  - Necesarios para realizar la tarea con éxito: tiempo de CPU, memoria, archivos y dispositivos de entrada/salida.

Estados de los procesos electrónicos

- **Nuevo**: creado pero no adminitido como proceso ejecutable.
- **Listo**: esperando a ser ejecutado.
- **En ejecución**: instrucciones en ejecución en la CPU.
- **Bloqueado**: en espera a que se produzca un evento.
- **Terminado**: ejecución finalizada, deja de ser ejecutable y los recursos quedan liberados.



Manejo de señales, su administración y los cambios en las prioridades

- Definición de señal: mecanismo utilizado para notificar a los procesos los eventos del sistema y como mecanismo de comunicación y sincronización en los procesos.
- Se pueden generar por:
  - Excepciones.
  - Otros proceso.
  - Interrupciones del terminal.
  - Control de tareas.
  - Cuotas.
  - Notificaciones.
  - Alarmas.

Determinación de los sistemas de información que soportan los procesos de negocio y los activos y servicios usados

- Tipos de sistemas de información básicos que soportan procesos de negocio
  - Según el nivel de la organización:
    - Sistemas a nivel operativo.
    - Sistemas a nivel de conocimiento.
    - Sistemas a nivel administrativo.
    - Sistemas a nivel estratégico.
  - Según las funciones: ventas y marketing; manufactura y producción.
- Ejemplos de sistemas: procesamiento de transacciones, trabajo del conocimiento, de oficina, finanzas y contabilidad, RRHH, información gerencial, apoyo a la toma de decisiones, apoyo a ejecutivos.

Desarrollo de un sistema de información para una organización

- Fases:
  - Conocimiento de la organización.
  - Identificación de problemas y oportunidades.
  - Determinación de necesidades.
  - Diagnóstico.
  - Propuesta.
  - Diseño del SI.
  - Codificación.
  - Implementación.
  - Mantenimiento.

Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios

- Todos los sistemas operativos contienen funcionalidades para monitorizar procesos y servicios.
- Objetivo principal: reducir de la latencia y el aumento máximo del rendimiento.
- Definiciones de indicadores relevantes:
  - Latencia: mide tiempo entre petición y visualización de resultados.
  - Utilización: porcentaje de un componente o servicio que se usa.
  - Rendimiento: cantidad de trabajo que puede ser procesada por unidad de tiempo. Se mide en bits por segundo, Kbytes por hora, etc.
  - Eficiencia: cociente entre rendimiento y utilización.

Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios

- Herramientas para la monitorización de procesos y servicios en el sistema operativo
  - Windows:
    - Administrador de tareas.
    - Monitor del rendimiento.
    - Monitor de recursos.
    - Visor de eventos.
  - Linux: Monitor de sistema.

Demostración de sistemas de almacenamiento

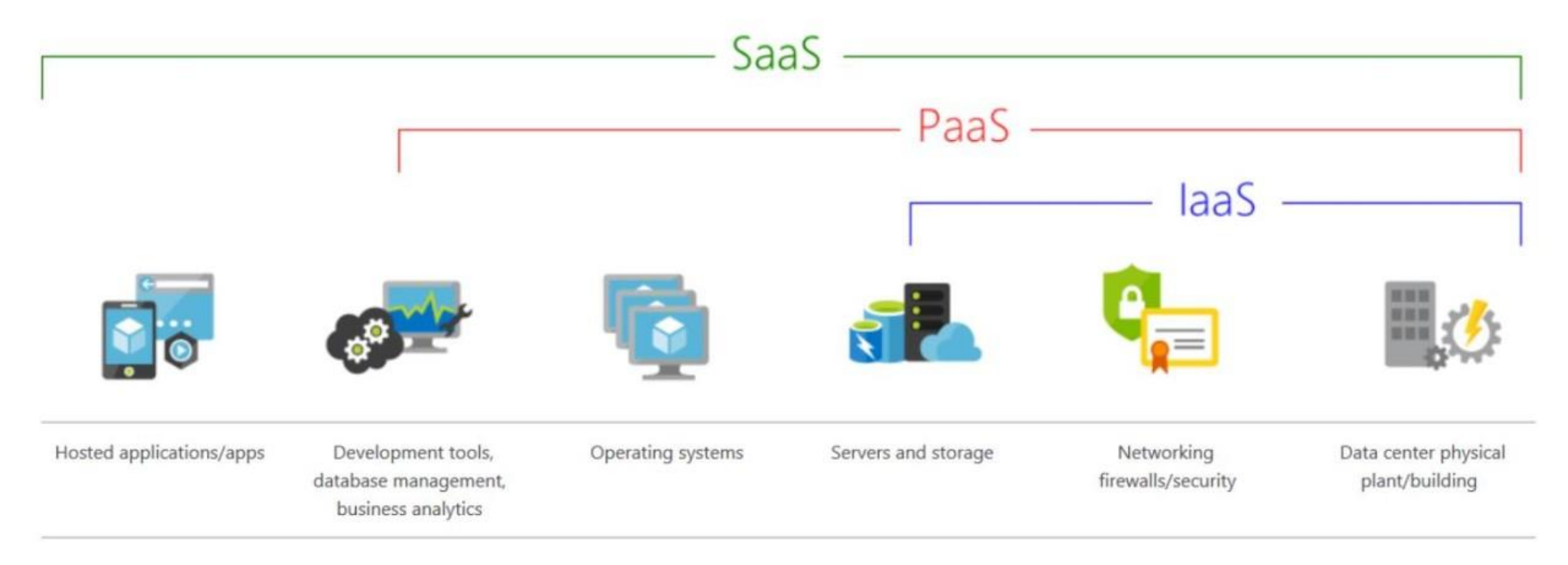
- Tipos de dispositivos de almacenamiento más frecuentes
- Características de los sistemas de archivo disponibles
- Organización y estructura general de almacenamiento
- Herramientas del sistema para gestión de dispositivos de almacenamiento.

Tipos de dispositivos de almacenamiento más frecuentes

- Por medios magnéticos:
  - Discos duros.
  - Discos duros externos.
  - Cabinas de discos.
  - Disquetes.
  - Cintas magnéticas.
- Por medio óptico:
  - CD-ROM.
  - DVD-ROM.
- Por medio electrónico:
  - Discos duros SSD (Solid State Disc).
  - PC-Cards.
  - Tarjetas de memoria flash.
  - Pen drives.

Tipos de dispositivos de almacenamiento más frecuentes

- Almancenamiento en red
- Almacenamiento en la nube



Características de los dispositivos de almacenamiento

- **Capacidad**: cantidad de datos almacenables.
- **Rendimiento**: eficiencia del sistema de almacenamiento.
- **Fiabilidad**: disponibilidad de datos ante solicitudes.
- **Recuperabilidad**: capacidad y facilidad de recuperación de datos.

Sistemas de archivos

- **Definición**: forma en que el sistema operativo organiza la información dentro de la memoria para la grabación y recuperación de datos.
- Tipos de sistemas de archivos:
  - De disco.
  - De red.
  - De propósito especial.

Sistemas de archivos

Sistema de archivo	Sistemas operativos soportados	Número máximo de archivos	Tamaño máximo de volumen	Capacidad de journaling
EXT2	LINUX, BSD, WINDOWS Y MAC OS X	10^18	16 Tb	No
EXT3	LINUX, BSD Y WINDOWS		32 Tb	Sí
EXT4	LINUX	2^32	1 Eb	Sí
REISERFS	LINUX	2^32	16 Tb	Sí
REISER3	LINUX	2^32	16 Tb	Sí
REISER4	LINUX			Sí
FAT12	WINDOWS (DOS)	4077	32 Mb	No
FAT16	WINDOWS (DOS)	65617	2 Gb	No
FAT32	DOSV7, WINDOWS 98, ME, 2000, XP, 2003 Y VISTA, 7	268435437	2 Tb	No
NTFS	WINDOWS 2000, XP, 2003, VISTA Y 7	4294967295	2^64	Sí
HPFS	OS/2, WINDOWS NT, LINUX Y FREEBSD	ILIMITADO	2 Tb	No
HFS	MAC OS Y MAC OS X	65535	2 Tb	No
HFS+	MAC OS 8, 9, X, DARWIN Y GNU/LINUX	2^32	8 Eb	Sí
ZFS	LINUX, MAC OS X, FREEBSD Y SOLARIS	2^48	16 Eb	No
XFS	IRIX, LINUX Y FREEBSD	64Tb	16 Eb	Sí

Organización y estructura general del almacenamiento

- Objetivos de las estructuras de datos:
  - Almacenamiento permanente de la información.
  - Capacidad de manipulación de un gran número de datos.
  - Independencia de los programas para la utilización de datos.
  - Capacidad de alojarse en soportes externos.
- Clasificación de los archivos
  - Según formato de los registros:
    - Homogéneos.
    - Heterogéneos.
  - Según el tamaño de los registros:
    - Longitud fija
    - Longitud variable.

Organización y estructura general del almacenamiento

- Clasificación de los archivos
    - Según su unidad básica de información:
        - Binarios.
        - Textuales.
        - Tipados.
    - Por la función del archivo:
        - Permanentes.
        - Temporales.
    - Por su vigencia:
        - Borradores.
        - Vigentes.
    - Por la función del contenido:
        - Maestro.
        - Constantes.
        - Históricos.

Organización y estructura general del almacenamiento

- Organización de almacenamiento de archivos.
  - Pila.
  - Organización secuencial.
  - Organización directa o aleatoria.
  - Organización indexada:
    - Área de índices.
    - Área primaria.
    - Área de excedentes.
  - Organización secuencial indexada.

Herramientas del sistema para gestión de dispositivos de almacenamiento

- Windows
  - Crear y formatear particiones del disco duro (Administrador de discos).
- Linux
  - Gparted.

Utilización de métricas e indicadores de monitorización de rendimiento de sistemas

- Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información.
- Identificación de los objetos para los cuales es necesario obtener indicadores.
- Aspectos a definir para la selección y definición de indicadores.
- Establecimiento de los umbrales de rendimiento de los sistemas de información.
- Recolección y análisis de los datos aportados por los indicadores.
- Consolidación de indicadores bajo un cuadro de mandos de rendimiento de sistemas de información unificado.

Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información

- Definiciones:
  - **Datos**: representación de la información de forma que se pueda comunicar, interpretar, almacenar y procesar automáticamente.
  - **Medición**: proceso de asignación de números a entidades o atributos del mundo real.
  - **Medida**: número o símbolo que proporciona indicación cuantiva de una cantidad. Sirven de herramientas para comparar atributos.
  - **Métrica**: se utilizan para interpretar lo que ocurre y de referencia para que los responsables tomen decisiones informadas.
  - **Indicador**: instrumento que proporciona evidencias cualitativas sobre si una determinada condición existe o si ciertos objetivos se han logrado.
  - **Indicador clave de rendimiento (KPI):** medida cuantificable o conjunto de datos usados para medir resultados con respecto a objetivos.

Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información

- Criterios de calidad de los indicadores:
  - **Específicos**: miden variables concretas y proporcionar información concreta y específica.
  - Pueden ser medidos y alcanzados.
  - **Realistas**: muestran una imagen fiel de la realidad.
  - **Temporales**: circunscritos a una unidad de tiempo, estableciendo cuándo hay que medir y cada cuánto se repite la medición.

Identificación de los objetos para los cuales es necesario obtener indicadores

- Indicadores relación de dependencia con objetivos.
- ¿Cómo definir buenos objetivos?
  - **Objetivos SMART**: específicos, medibles, alcanzables, relevantes y temporales.
  - Otros:
    - Visión a corto, medio y largo plazo.
    - Vista de pájaro / manos de hormiga.

Aspectos a definir para la selección y definición de indicadores

Además de definir el indicador en sí, conviene definir los elementos que aparece en la tabla y otros conceptos como el propósito del indicador, los grupos de interés, destinatarios y soporte.

Componente	Ejemplo
Definición	Incidentes ocurridos y solucionados en las siguientes veinticuatro horas en los equipos del departamento financiero.
Forma de calcularlo/ratio	Si se quiere medir en porcentaje la fórmula en este caso sería: (Incidentes solucionados/Incidentes totales)*100
Unidades	En este caso, las unidades son los porcentajes.
Periodicidad	Mensualmente, anualmente, trimestralmente, diariamente, etc. Si la importancia del indicador es clave, las mediciones y los controles deberán ser con más frecuencia que en indicadores secundarios.
Proceso	Los datos para conocer las incidencias ocurridas y las solucionadas en las veinticuatro horas siguientes a la incidencia se pueden obtener de informes de incidencias elaborados por el departamento de informática.
Fuente de los datos	De dónde se extraerán los datos para ejecutar el indicador.
Responsable	En esta ocasión, el responsable del indicador será el director financiero. De él dependerá el cumplimiento de los objetivos.

Aspectos a definir para la selección y definición de indicadores

- Pasos para construir un indicador:
  - Establecer objetivos y metas referentes a la medición.
  - Establecer áreas de desempeño relevantes que se van a medir.
  - Formular el indicador y establecer su fórmula de cálculo.
  - Validar los indicadores mediante criterios técnicos.
  - Recopilar los datos necesarios para ejecutar el indicador.
  - Establecer las metas o los valores deseados del indicador y la periodicidad de la medición.
  - Realizar observaciones de los resultados obtenidos y establecer supuestos con ellos.
  - Señalar la fuente de los datos obtenidos y los medios de verificación de los indicadores.
  - Evaluar los indicadores estableciendo referentes comparativos y formulando juicios.
  - Comunicar los resultados del desempeño logrado medido con el indicador.

Aspectos a definir para la selección y definición de indicadores

- Conviene responder a estas preguntas a la hora de definir un indicador:
  - ¿Qué se debe medir?
  - ¿Dónde es conveniente medir?
  - ¿Cuándo hay que medir? ¿Con qué frecuencia?
  - ¿Quién debe realizar la medición? ¿Automática o manual?
  - ¿Cómo se difundirán los resultados de la medición?
  - ¿Quién y con qué frecuencia revisa el sistema de revisión?
- En cuanto a los resultados, se definen valores contra los que contrastar el indicador:
  - Objetivo.
  - Expectativa.
  - Límite legal.
  - Límite de aceptabilidad.

Establecimiento de los umbrales de rendimiento de los sistemas de información

Definición de umbral: límites mínimo y máximo cuya superación desencadenaun evento de umbral (alarma).

Clasificaciones de umbrales:

- Según el tipo de datos y su medida resumen
  - Porcentajes: los más comunes, miden la proporción de cumplimiento de procesos. Ejemplo: Porcentaje de incidencias solucionados en menos de 24 horas.
  - Tasas: muestran frecuencia de un evento en el sistema de información.
- Según la forma de definir el valor umbral
  - Valores puntuales: cuando se define un punto de corte en términos absolutos.
  - Tendencias: se evalúa si el resultado de un indicador sigue una determinada tendencia.

Establecimiento de los umbrales de rendimiento de los sistemas de información

Clasificaciones de umbrales:

- Según las categorías de cumplimiento definidas
  - Valores óptimos.
  - Valores aceptables.
  - Valores críticos o insuficientes.

Criterios que conviene tener en cuenta para definir umbrales:

- Basados en evidencias y datos.
- Orientados a la práctica.
- Flexibles y dinámicos.
- Claramente definidos, medibles y alcanzables.

Recolección y análisis de los datos aportados por los indicadores

Una vez obtenidos los datos, conviene comprobar la validez del indicador analizando si cumple estos criterios:

- Pertinencia.
- Relevancia.
- Homogeneidad.
- Independencia.
- Coste.
- Simplicidad y comprensibilidad.
- No redundancia.
- Focalizado en áreas controladas.
- Participación.

Consolidación de indicadores en un cuadro de mandos de rendimiento

Definición de cuadro de mandos:

- Conjunto de indicadores que resumen el desempeño de un sistema.
- Una de las herramientas más valiosas para evaluar sistemas de información y tomar decisiones.
- Permite ver de forma global y unificada los indicadores, agrupándolos gráficamente, y así se puede saber si están cerca de sus límites mínimos o máximos.
- Los cuadros de mandos están muy relacionados con la mejora de los resultados de una organización.

Consolidación de indicadores en un cuadro de mandos de rendimiento

Elaboración e implantación de un cuadro de mandos:

- Como mínimo, contiene:
  - Datos.
  - Propósito y responsables.
  - Periodicidad.
  - Formato.
- Aspectos que conviene tener en cuenta:
  - Señalar solo la información necesaria de forma clara y sencilla.
  - Usar códigos de colores para indicar los cambios de estado.
  - indicar los objetivos asociados a los indicadores junto a ellos, para facilitar la comprensión de las medidas.
  - Facilitar la comparación de resultados entre distintas áreas de la organización.
  - Remarcar lo más importante para la organización, señalando los que no obtienen resultados previstos ni evolucionan según el plan.
  - Contar con el apoyo de la dirección y obtener consenso entre los participantes.

Confección del proceso de monitorización de sistemas y comunicaciones

- Identificación de los dispositivos de comunicaciones.
- Análisis de los protocolos y servicios de comunicaciones.
- Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones.
- Procesos de monitorización y respuesta.
- Herramientas de monitorización de uso de puertos y servicios tipo Sniffer.
- Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti.
- Sistemas de gestión de información y eventos de seguridad (SIM/SEM).
- Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.).

Identificación de los dispositivos de comunicaciones

Definición de dispositivos de comunicación: periféricos y medios necesarios para lograr que los elementos de la red se comuniquen entre ellos.

Definición de red: conjunto de dispositivos físicos y programas mediante los cuales se comunican los ordenadores, que son nodos de la red.

Definición de la gestión de redes: actividades que controlan, planifican, coordinan, asignan y monitorizan recursos de una red para conseguir los requerimientos a tiempo real.

Identificación de los dispositivos de comunicaciones

Tres grupos de dispositivos de comunicación:

- Equipos de red
  - Servidores.
  - Ordenadores.
- Medios de comunicación
  - Módems.
  - Tarjetas de interfaz de red..
  - Concentradores o hubs.
  - Repetidores.
  - Puentes.
  - Conmutadores o switches.
  - Enrutadores o routers.
  - Pasarelas, puertas de enlace o gateways.

Identificación de los dispositivos de comunicaciones

Tres grupos de dispositivos de comunicación:

- Conectores
  - Sistema de cableado.
  - Cableado de fibra óptica.
  - Enlaces inalámbricos.

Análisis de los protocolos y servicios de comunicaciones

Definición de servicio de comunicación: actividad final a la que se destina la información recibida en un dispositivo de destino.

Definición de protocolo de red: conjunto de normas y reglas que definen la forma en la que la información circula en una red.

Modelo OSI:

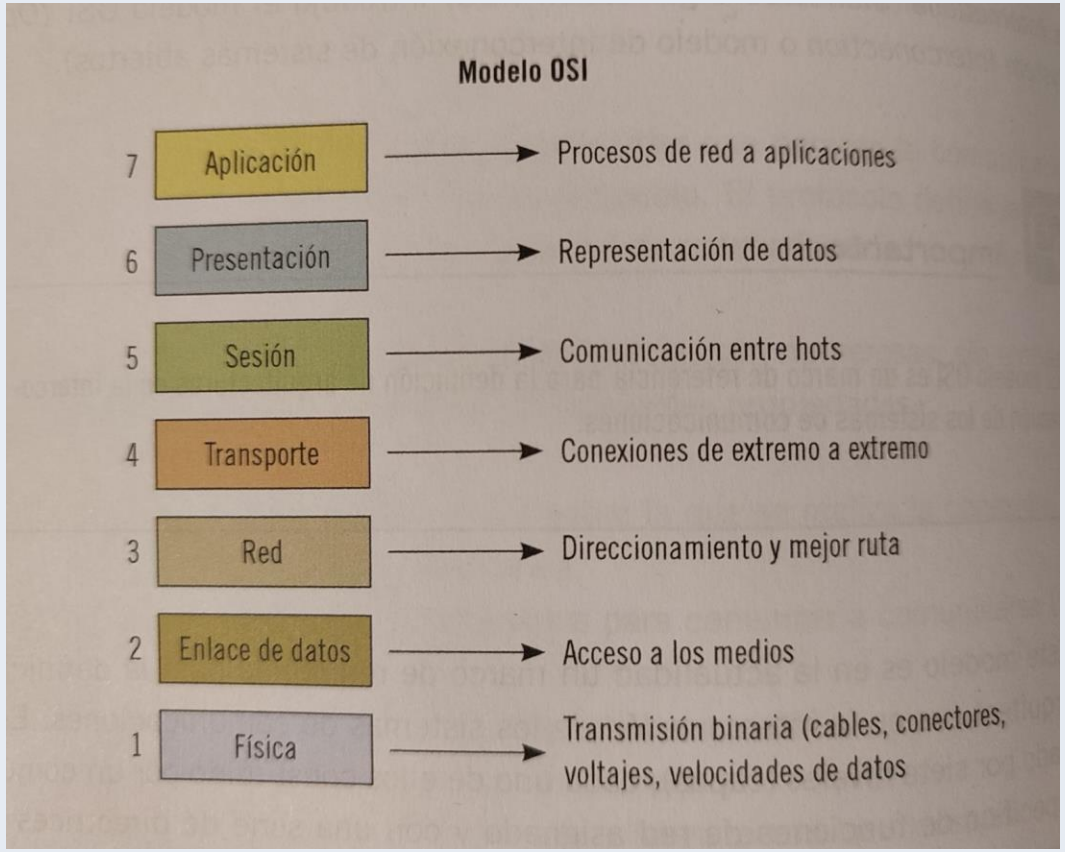
- **Definición**: marco de referencia para la definición de arquitecturas en la interconexión de sistemas de comunicación.

Análisis de los protocolos y servicios de comunicaciones

- Capas:
  - Física: se refiere a la transmisión binaria, es decir, cables, conectores, voltajes, etc.
  - Enlace a datos: que se refiere al acceso a los datos.
  - Red: direccionamiento y mejor ruta.
  - Transporte: donexiones de extremo a extremo.
  - Sesión: comunicación entre hots.
  - Presentación: representación de datos.
  - Aplicación: procesos de red y aplicaciones.

Análisis de los protocolos y servicios de comunicaciones

- Capas:

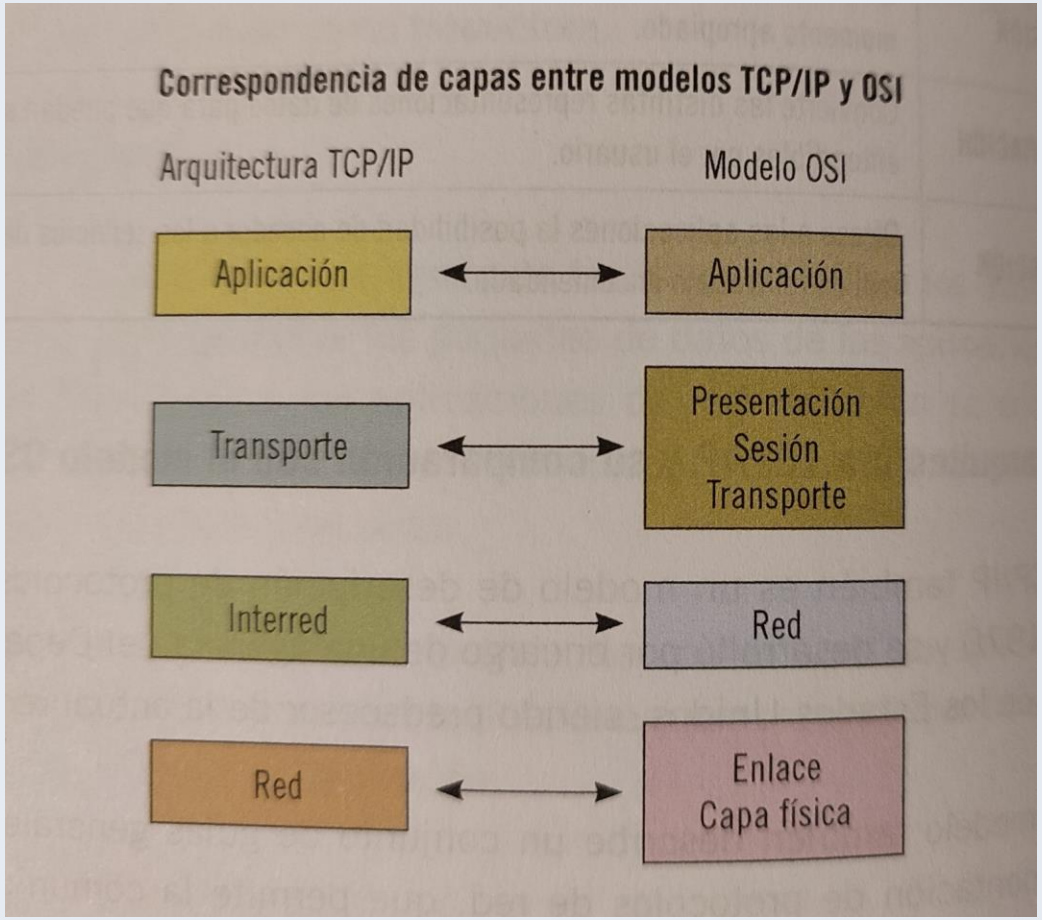


Análisis de los protocolos y servicios de comunicaciones

Modelo TCP/IP:

- **Definición**: marco de referencia para la definición de arquitecturas en la interconexión de sistemas de comunicación.
- Capas:
  - Capa 1 o de acceso al medio: define las rutinas para acceder al medio físico y se correspnde con las capas 1 y 2 del modelo OSI.
  - Capa 2 o de Internet: define el datagrama (routers) y gestiona el enrutamiento de la información y es similar a la capa 3 del modelo OSI.
  - Capa 3 o de transporte: se ocupa de servicios de entrega de datos entre nodos de red y es similar a la capa 3 del modelo OSI.
  - Capa 4 o de aplicación: define y gestiona las aplicaciones y procesos que utilizan la red y es similar a las capas 5, 6, y 7 del modelo OSI.

Análisis de los protocolos y servicios de comunicaciones



Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones

El protocolo IP permite la distinción única de todos los ordenadores conectados a Internet y generalmente tienen una IP fija.

Tiene dos versiones la IPv4 y la IPv6, que se ha creado por agotamiento de las IPs y está tiene más combinaciones.

Procesos de monitorización y respuesta

Fases de la administración del rendimiento de la red:

- Monitorización:
  - Utilización de enlaces: cantidad ancho de banda por cada enlace de área local.
  - Caracterización de tráfico: tipos de tráfico en la red, sirve para recolectar datos sobre los servicios más usadod y establecer patrones del uso.
  - Porcentaje de transmisión y recepción de información: información sobre elementos de la red que más solicitudes hacen y atienden como servidores, puertos, servicios, etc.
  - Utilización de de procesamiento: cantidad de procesador que un servidor consume para atender una aplicación.

Procesos de monitorización y respuesta

Fases de la administración del rendimiento de la red:

- **Análisis**: cuando ya se ha recogido la información, hay que interpretarla para analizar el estado y definir patrones y facilitan la toma de decisiones.

  Algunos de los comportamientos que se pueden observar son:
  - Tráfico inusual.
  - Elementos principales de la red.
  - Utilización elevada.
  - Control de tráfico.
  - Calidad del servicio.

Herramientas de monitorización de uso de puertos y servicios tipo Sniffer

Definición de sniffer: programa para capturar todos los datos que circulan a través del medio físico, los dispositivos y los equipos de una red.

Entre sus funcionalidades están:

- Análisis de fallos.
- Medición de tráfico de datos.
- Captura de nombres de usuarios.
- Analizar la información del uso de aplicaciones cliente-servidor transmitida por la red.

Herramientas de monitorización de uso de puertos y servicios tipo Sniffer

Ejemplos de sniffers:

- Kismet.
- Wireshark.
- Ettercap.
- TCPDump.

La tarjeta de red funciona en modo promiscuo. La información capturada puede utilizarse malintencionadamente.

Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti

Herramientas de software libre:

- Cacti.
- Naggios.
- Hobbit monitor.

Sistemas de gestión de información y eventos de seguridad (SIM/SEM)

Definición de SIEM: administración de eventos e información de seguridad.

Herramientas SIEM:

- Para qué sirven:
  - Gestionar y correlacionar la información de eventos de seguridad durante todas las fases en las que se produce un incidente.
  - Recoger, cotejar y hacer informes con los datos de los registros de actividad llamados logs de los dispositivos y recursos de la red.
  - Responder, prevenir, detectar y mitigar incidencias.

Sistemas de gestión de información y eventos de seguridad (SIM/SEM)

- Ejemplos:
  - Tivoli Security Information and Event Manager de IBM.
  - OSSIM: es gratuita.
  - Sentinel. de pago por uso.

Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

Definición de gestión de redes: actividades para controlar, planificar, coordinar, asignar y monitorizar recursos de redes.

Gestión de filtrado de red:

- Cortafuegos (Firewall):
  - Puede ser solo software o estar compuesto por elementos hardware y software.
  - Controla el acceso separando la red interna de equipos externos y denegando intentos de conexión no autorizada analizando servicios, direcciones, usuarios y comportamiento.

Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

Los sistemas de protección de ataques IPS/IDS (Intrusion Prevention-Detection Systems) se clasifican en los siguientes tipos:

- Sistemas de prevención de intrusiones (IPS):
  - Previenen e identifican actividad maliciosa, bloquean amenazas e informan sobre los ataques.
  - Siguen este proceso:
    - Clasificación de los paquetes por la cabecera y la información de flujo asociada.
    - Según la clasificación, se aplican filtros de estado de flujo.
    - Todos los filtros importantes se aplican en paralelo y cuando se identifican paquetes sospechosos se etiquetan.
    - Una vez identificado y etiquetado, el paquete sospechoso se descarta y actualiza su información de estado de flujo para descartar el resto del flujo.

Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

- Clasificación según la forma de detectar el tráfico malicioso:
  - Detección basada en firmas (antivirus).
  - **Detección basada en políticas**: requieren establecer políticas de seguridad.
  - **Detección basada en anomalías**: actúan en función del patrón de comportamiento normal de tráfico.
  - **Detección honey pot**: se usa un equipo configurado para llamar la atención de los hackers.

Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

- Sistemas de detección de intrusos (IDS):
  - Funcionalidades:
    - Detectar ataques y vulnerabilidades, accesos no autorizados a un computador o una red.
    - Monitorizar el tráfico de red y enviar alertas sobre actividades sospechosas.
    - Bloquear ataques examinando los riesgos en todos los paquetes entrantes y decidiendo si permitir o denegar el acceso.

Selección del sistema de registro en función de los requerimientos de la organización

- Determinación del nivel de registros necesarios, los periodos de retención y las necesidades de almacenamiento.
- Análisis de los requerimientos legales en referencia al registro.
- Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros.
- Asignación de responsabilidades para la gestión del registro.
- Alternativas de almacenamiento para los registros de sistemas y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad.
- Guía para la selección del sistema de almacenamiento y custodia de registros.

Determinación del nivel de registros necesarios, los periodos de retención y las necesidades de almacenamiento

En el control de registros conviene tener en cuenta lo siguiente:

- Identificación.
- Almacenamiento.
- Protección.
- Recuperación.
- Retención.
- Disposición de los registros.

Análisis de los requerimientos legales en referencia al registro

Definición de requerimientos legales: condiciones recogidas en textos legales que tiene que cumplir una actividad, proceso o servicio.

En el caso de los registros, existen condiciones en relación a la obtención, el tratamiento, los sistemas de almacenamiento y las medidas de seguridad.

Para cumplir la normativa, conviene hacer una búsqueda exhaustiva y estar actualizado para asegurarse de que el sistema está al día con las leyes aplicables como la LOPDGDD.

Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros

Antes de implementar sistemas de información, conviene identificar y acordar los requerimientos de seguridad que conviene incorporar a los sistemas y registros.

Además, conviene que los requerimientos y controles vayan acorde con los requisitos, la evaluación de los riesgos y el valor de la información protegida.

Existen tres tipos de medidas de seguridad: administrativa, física y técnica.

Asignación de responsabilidades para la gestión del registro

Para facilitar la gestión de los registros, conviene que las organizaciones asignen responsables encargados de lo siguiente:

- Cumplimiento de los requerimientos legales y de seguridad.
- La recopilación de los datos adecuados para poder analizar y obtener conclusiones sobre el funcionamiento.

Alternativas de almacenamiento para los registros de sistemas y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad

Definición de registro en el sistema operativo: base de datos jerárquica que almacena los ajustes de configuración y facilita información para comprobar el rendimiento, escalabilidad, confiabilidad, integridad y disponibilidad del sistema.

En Windows, contiene información sobre lo siguiente:

- Aplicaciones instaladas.
- Sistema de arranque.
- Dispositivos hardware y drivers que utilizan
- Aspecto de elementos como carpetas o ventanas.

Alternativas de almacenamiento para los registros de sistemas y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad

- Se accede mediante la aplicación Editor del registro o el comando regedit.
- Las principales carpetas son las siguientes:
  - HKEY_CLASSES_ROOT.
  - HKEY_CURRENT_USER.
  - HKEY_LOCAL_MACHINE.
  - HKEY_USERS.
  - HKEY_CURRENT_CONFIG.

Guía para la selección del sistema de almacenamiento y custodia de registros

Modelos de almacenamiento de datos en sistemas informáticos:

- Modelo tradicional de archivos.
- Modelo de bases de datos relacionales.

Para elegir el sistema de almacenamiento, conviene modelo de almacenamiento de datos evaluando los siguientes aspectos:

- Sistema operativo que se va a utilizar.
- Requerimientos legales.
- Capacidad de los recursos dedicados al almacenamiento y custodia.
- Características de la red que se utilizará en la organización.
- Complejidad del sistema de información.
- Tipo de alojamiento de los registros: tradicional, web, en la nube, etc.

Administración del control de accesos adecuados de los sistemas de información

- Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos.
- Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos.
- Requerimientos legales en referencia al control de accesos y asignación de privilegios.
- Perfiles de acceso en relación con los roles funcionales del personal de la organización.
- Herramientas de directorio activo y servidores LDAP en general.
- Herramientas de sistemas de gestión de identidades y autorizaciones (IAM).
- Herramientas de Sistemas de punto único de autenticación Single Sign On (SSO).

Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos

Principalmente, se encuentran en la normativa 27002:2005.

Se recomienda establecer una política de control de accesos:

- Reglas del control de acceso y los derechos para cada usuario o grupo de usuarios.
- Documentada y sometida a revisión periódica.

Para definirla, conviene tener en cuenta lo siguiente:

- Requerimientos de seguridad de las aplicaciones.
- Identificar la información relacionada con las aplicaciones comerciales.
- Políticas de divulgación y autorización de la información.

Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos

- Consistencia entre control de acceso y la clasificación de la información de los sistemas y redes.
- Legislación vigente y obligaciones contractuales.
- Perfiles de acceso estándar para puestos de trabajo comunes.
- Segregación de los roles de control de acceso.
- Requerimientos para autorización de solicitudes de acceso.
- Requerimientos para revisión periódica de controles de acceso.
- Revocación de los derechos de acceso.

Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos

También es necesario establecer los siguientes parámetros:

- Diferenciación entre reglas de obligatorio cumplimiento y las recomendaciones de cumplimiento opcional (*Must / Nice to have*).
- Basarse en la premisa de que está todo prohibido a no ser que esté expresamente permitido (*Just enough access*, JEA).
- Diferenciar entre los cambios en procesos según se inicien de forma automática o manual (Desencadenadores o *triggers*).
- Cambios en los permisos de usuarios que se inician automáticamente por el sistema o de forma manual por el administrador.
- Reglas que requieren aprobación específica y que no requieren.

Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos

Principios y buenas prácticas del control de accesos:

- **Registros del usuario**: procedimiento formal en relación a la creación y eliminación de registros de usuarios, así como para otorgamiento y revocación de acceso a sistemas de información y que esté basado en los siguientes principios:
  - Identificadores de usuario únicos, no redundantes o innecesarios.
  - Comprobación de la autorización para el acceso.
  - Comprobación de la adecuación del nivel de acceso otorgado con el propósito y de la consistencia con la política de seguridad.
  - Facilitar a usuarios un documento escrito donde se reflejen los derechos de acceso y requerir la firma en el documento para acreditar entendimiento y conformidad.

Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos

- Asegurarse de que los proveedores no faciliten el acceso hasta que se haya completado el proceso de autorización.
- Mantener registro formal de las personas autorizadas.
- Eliminar o bloquear los derechos de acceso a usuarios que han cambiado puesto o han dejado de trabajar para la organización.
- Realizar comprobaciones periódicas para eliminar o bloquear diferencias.

Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos

- **Gestión de privilegios**: procedimiento de autorización que controle la asignación y el uso de privilegios, teniendo en cuenta lo siguiente:
  - Privilegios de acceso asociados con cada elemento distinto del sistema de información.
  - Asignar privilegios para lo estrictamente necesario siguiendo el principio JEA.
  - Mantener actualizado el procedimiento.
  - No asignar privilegios hasta completar el proceso de autorización.
  - Promover el uso de automatizaciones para reducir la necesidad de asignar privilegios y el desarrollo y uso de aplicaciones que eviten la necesidad de usar privilegios.

Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos

- **Gestión de contraseñas de usuario**: procedimiento formal para la asignación de contraseñas a las cuentas de usuario que incluya lo siguiente:
  - Requerimiento de que usuarios firmen un documento para mantener confidencialidad de contraseñas y conservar claves grupales.
  - Asignación de una clave temporal segura que después deben cambiar a una clave propia.
  - Verificación de la identidad de los usuarios antes de facilitar contraseñas nuevas.
  - Facilitar contraseñas de modo seguro.
  - Cuando se recibe una contraseña, los usuarios deben reconocer la recepción.
  - Nunca deben almacenarse en lugares sin protección adecuada.

Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos

- **Revisión de los derechos de acceso del usuario**: procedimiento de revisión de derechos de acceso que incluya:
  - Revisión de derechos de accesos de usuarios periódicamente y después de cambios en la situación del usuario.
  - Revisión y reasignación cuando el usuario cambia de puesto de trabajo.
  - Revisión de autorizaciones para privilegios especiales más frecuente que para autorizaciones estándar.
  - Mantener registro de los cambios realizados en cuentas para llevar control en las revisiones periódicas.

Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos

Herramientas de Windows para administrar el control de acceso:

- La herramienta Cuentas de usuario del Panel de control permite crear, eliminar y gestionar cuentas de usuario y otorgar privilegios a cada cuenta (Cambiar tipo de cuenta).

Requerimientos legales en referencia al control de accesos y asignación de privilegios

En las leyes de protección de datos y las de ciberseguridad, se establecen los siguientes principios fundamentales de la información: integridad, confidencialidad y disponibilidad.

Medidas de seguridad de la LOPD

Los responsables del fichero están encargados de implantar medidas:

- **Organizativas**: enfocadas a establecer procedimientos, normas, reglas y estándares de seguridad para proteger los datos personales durante su tratamiento.

Requerimientos legales en referencia al control de accesos y asignación de privilegios

- **Técnicas**: orientadas a mantener la integridad, confidencialidad y disponibilidad y se distinguen en tres niveles condicionados por los datos que almacenan los distintos tipos de ficheros.

Tipo de fichero (Y) / Nivel de seguridad (X)	Nivel básico	Nivel medio	Nivel alto
De carácter personal	☑		
Que contengan datos relativos a la comisión de infracciones administrativas o penales		☑	

Requerimientos legales en referencia al control de accesos y asignación de privilegios

Tipo de fichero (Y) / Nivel de seguridad (X)	Nivel básico	Nivel medio	Nivel alto
Que contengan datos sobre Hacienda Pública		☑	
Que contengan datos sobre servicios financieros		☑	
Que contengan datos sobre solvencia patrimonial y crédito		☑	
Que contengan datos suficientes que permitan elaborar un perfil del afectado		☑	

Requerimientos legales en referencia al control de accesos y asignación de privilegios

Tipo de fichero (Y) / Nivel de seguridad (X)	Nivel básico	Nivel medio	Nivel alto
Que contengan datos referentes a la ideología, religión, creencias, origen racial, salud o vida sexual del interesado			☑

Requerimientos legales en referencia al control de accesos y asignación de privilegios

Medidas obligatorias según el nivel de seguridad:

- Nivel básico:
  - Acceso únicamente a los datos necesarios para desarrollar sus funciones (principio de privilegios mínimos).
  - El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos a los autorizados.
  - La relación de usuarios con acceso autorizado al sistema de información contendrá específicamente el acceso autorizado para cada uno de ellos.
  - Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

Requerimientos legales en referencia al control de accesos y asignación de privilegios

- Nivel medio:
  - El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y verificación de que está autorizado.
  - Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.
  - En cuanto al control de acceso físico, exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentran ubicados los sistemas de información con datos de carácter personal.

Requerimientos legales en referencia al control de accesos y asignación de privilegios

- Nivel alto:
  - De cada acceso se guardará como mínimo la identificación del usuario, la fecha, la hora, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
  - Si se autoriza, la información que permita identificar el registro accedido.
  - Los mecanismos que permiten el registro de los datos, estarán control directo del responsable de seguridad sin que se deba permitir, la desactivación de los mismos.
  - El período mínimo de conservación de los datos registrados será de dos años.
  - El responsable de seguridad competente deberá revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y problemas detectados, al menos, una vez al mes.

Perfiles de acceso en relación con los roles funcionales del personal de la organización

Conviene tener en cuenta los roles funcionales de las personas, empezando por el organigrama.

Definición de organigrama: representación gráfica de la estructura de una organización, representando los departamentos y las relaciones jerárquicas entre los distintos puestos y departamentos.

También conviene saber las descripciones, funcionalidades y responsabilidades de cada puesto para decidir con más detalle sobre los permisos.

Después de asignar permisos a cada puesto de trabajo conviene concretar los usuarios que pertenecen a cada puesto y otorgar los permisos, identificaciones y contraseñas.

Herramientas de directorio activo y servidores LDAP en general

Definición de directorio activo: servicio de directorio que gestiona los elementos de una red, desde equipos hasta grupos, usuarios, políticas de seguridad y cualquier otro objeto.

Almacenan información de usuarios e información de seguridad, como contraseñas y permiten compartir la información con otros dispositivos de la red.

Funciones:

- **Gestión de identidad**: facilita la identificación inequívoca de personas.

Herramientas de directorio activo y servidores LDAP en general

- **Seguridad**:
  - Permite organizar y simplificar la localización y el acceso a distintos recursos de la red.
  - Aplica políticas de seguridad mediante la automatización de bloqueo de sistemas operativos.
  - Refuerza la utilización de contraseñas y credenciales.
  - Posibilita delegar tareas administrativas.
- **Gestión de la configuración**: facilita la gestión de la configuración de los elementos de red para aumentar la productividad y reducir costes de administración, soporte y formación.

Herramientas de directorio activo y servidores LDAP en general

El directorio activo está construido con protocolos compatibles con sistemas operativos Windows, Linux o Macintosh, como los siguientes:

- LDAP.
- DNS.
- DHCP.
- Kerberos.

Herramientas de directorio activo y servidores LDAP en general

Herramientas de directorio activo y servidores LDAP:

- Microsoft:
  - Active Directory (Sistemas operativos como Windows Server 2008).
  - Microsoft Entra ID (Microsoft 365).
- OpenLDAP.
- Apache:
  - Apache Directory Server.
  - Apache Directory Studio.

Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)

Definiciones de identidad digital:

- Representación de un individuo o entidad dentro de un sistema de información.
- Colección de identificadores o atributos únicos que representan a una persona, componente de software, máquina o recurso en un sistema informático.

Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)

Tipos de identidades digitales:

- **Identidades humanas**: personal interno o usuarios externos.
- **Identidades de carga de trabajo**: aplicaciones, servicios, scripts o contenedores.
- **Identidades de dispositivo**: equipos de escritorio, teléfonos móviles, etc.

Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)

Definiciones de la gestión de identidades y autorizaciones:

- Conjunto de sistemas y procesos encargados de gestionar y controlas la identidad de las personas que acceden a los recursos del sistema y todo aquello que puede hacer cada usuario con estos recursos.
- Puente entre personas físicas y servicios de identificación, autenticación, identidad, cumplimiento y autorización.

Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)

Funcionalidades de la gestión de identidades y autorizaciones:

- Creación y mantenimiento de perfiles de usuario.
- Administración de derechos y restricciones de acceso.

Facilitan soluciones para las siguientes situaciones:

- Aumento de usuarios internos y externos.
- Aumento de oportunidades de negocio por el desarrollo de la tecnología y la globalización.
- Integración de mecanismos de autorización que usan los usuarios.

Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)

Desventajas de la gestión de identidades y autorizaciones:

- Riesgos relacionados con la sincronización de contraseñas.
- Fallos en la autenticación y autorización, afectan al acceso a las aplicaciones.
- Implementarlas suele requerir reestructurar procesos de negocio.

Herramientas IAM:

- Oracle Identitiy Manager.
- Microsoft Entra ID.

Herramientas de Sistemas de punto único de autenticación Single Sign On (SSO)

Definición de SSO: sistema que permite acceder a distintos servicios sin necesidad de realizar la identificación y autenticación varias veces, con solo una autenticación.

Tipos de herramientas SSO:

- Enterprise Single Sign-On.
- Web Single Sign-On.
- Kerberos.
- OpenID.
- Identidad federada.

Referencias

MF0490_3: Gestión de servicios en el sistema informático (Ester Chicano Tejada).

ISO 27001 vs. ISO 27002: Understanding the difference (nemko.com)

¿Qué es la norma ISO 27002 y para qué sirve? - GlobalSuite Solutions

Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales - Wikipedia, la enciclopedia libre

BOE-A-2008-979 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

¿Sigue vigente el modelo de medidas de seguridad del Reglamento de desarrollo de la LOPD? | AEPD

Referencias

2.9.- MEDIDAS DE SEGURIDAD. ANÁLISIS DE RIESGOS | AEPD

Seguridad de los tratamientos | AEPD

Gestión del riesgo y evaluación de impacto en tratamientos de datos personales (aepd.es)

BOE.es - DOUE-L-2016-80807 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Referencias

¿Qué obligaciones específicas contiene el RGPD para los encargados de tratamiento? | AEPD

Principios | AEPD

Medidas de cumplimiento | AEPD

What Is IT Infrastructure Library (ITIL)? | IBM

Las 5 etapas del ciclo de vida del servicio ITIL (invgate.com)

¿Conoces todos los sistemas de almacenamiento de datos? (ambit-bst.com)

Referencias

¿Qué es XDR (Detección y respuesta ampliadas)? | IBM

EDR vs MDR vs XDR: Todo lo que debe saber - Acronis

Autenticación LDAP con Microsoft Entra ID - Microsoft Entra | Microsoft Learn

¿Qué es la administración de identidad y acceso (IAM)? | Seguridad de Microsoft

Microsoft Entra ID - Wikipedia

Autenticación frente a autorización - Microsoft identity platform | Microsoft Learn

Referencias

Seguridad y privacidad - Moodle - Sistema de gestión de aprendizaje

Security procedures | Moodle Developer Resources

Why Crowdsourcing is Better | Bugcrowd

What is the different between files and registers? - Quora

Registers in Computer Architecture (prepbytes.com)

Areas Claves De Desempeño - 2543 Palabras | Monografías Plus (monografias.com)

Introducción al concepto de identidad - Microsoft Entra | Microsoft Learn