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

IFCT0109 – Seguridad informática

MF0490_3 (90 horas)

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

- Introducción
- Determinación del nivel de registros necesario, 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 del sistema y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad
- Guía para la selección del sistema de almacenamiento y custodia de registros
- Resumen

Introducción

Hasta ahora, hemos estudiado la implantación de sistemas de información, la evaluación de objetivos y resultados mediante indicadores y métricas, y el uso de herramientas de monitorización para automatizar la obtención de datos.

Sin embargo, todo esto es inútil sin un sistema de almacenamiento que proteja y guarde adecuadamente los registros y datos.

En este capítulo, se definirá el nivel de registros necesarios según los objetivos de la organización, así como el período de retención y las necesidades de almacenamiento.

El manejo de datos está sujeto a normativas según su tipología. Es importante conocer los requisitos legales y establecer medidas de seguridad para evitar riesgos legales y de seguridad.

Estas medidas deben documentarse en un plan de seguridad que asigne responsabilidades claras en la gestión de registros para evitar fallos de seguridad.

Finalmente, se explorarán alternativas de almacenamiento y se ofrecerán recomendaciones para elegir un sistema adecuado de custodia de registros.

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

Hemos estudiado los procesos de información, su monitorización y evaluación mediante indicadores y métricas.

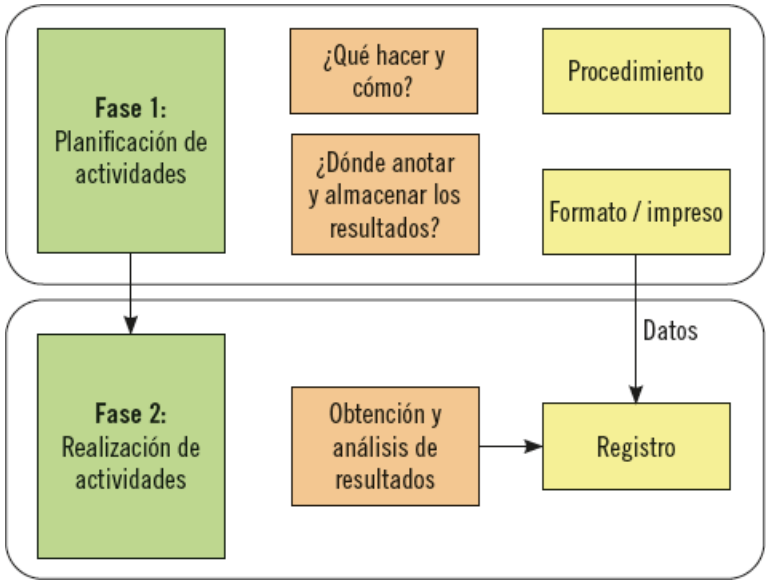
En todas estas fases, las organizaciones obtienen documentos que respaldan las decisiones de los responsables, asegurando una eficaz planificación, operación y control de los procesos.

Los registros y documentos son fundamentales para analizar el comportamiento y mejorar los procesos del sistema de gestión de una organización.

Conceptos Clave:

- **Registro:** Documento generado como resultado de una tarea del sistema.
- **Formato o Impreso:** Documento donde se anotan los datos relacionados con la realización de tareas.

Durante la planificación, se decide cómo se realizarán las actividades y dónde se anotarán los resultados. Los resultados se almacenan en registros y se analizan para tomar decisiones y mejorar el funcionamiento de la organización. Este ciclo de planificación y realización es importante para el éxito organizacional.



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

Control de Registros:

- **Identificación:** Los registros deben ser fácilmente identificables mediante un formato y un campo identificador (número de registro, fecha, etc.).
- **Almacenamiento:** Determinar dónde se almacenarán los registros para facilitar su localización.
- **Protección:** Establecer medidas de seguridad (contraseñas, copias de seguridad) para evitar accesos no autorizados y cambios indeseados.
- **Recuperación:** Implementar una metodología que permita acceder fácilmente a los datos históricos.
- **Retención:** Conservar los registros durante el tiempo necesario según las normativas (ISO 9001:2000 sugiere tres años) y los requerimientos legales.
- **Disposición:** Decidir el procedimiento para eliminar o archivar los registros una vez terminado el período de retención.

Importancia del Control de Registros:

Para un control efectivo de los registros, es esencial garantizar su identificación, almacenamiento, protección, fácil recuperación, y adecuada disposición.

Beneficios de un Buen Control de Registros:

- **Acceso Rápido y Sencillo:** Mejora la eficiencia en el análisis de indicadores.
- **Auditorías Agilizadas:** Facilita el proceso de auditorías internas y externas.
- **Protección Mejorada:** Previene el uso indebido y la pérdida de datos.
- **Organización y Orden:** Ahorra tiempo y reduce costos al buscar documentos.

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

Con todos estos requerimientos de control las organizacionessuelen hacer una ficha de los registros que se van a almacenar.

LISTADO DE REGISTROS				
Nombre	**Identificación**	**Responsable**	**Ubicación del archivo**	**Período de retención**
Facturas proveedores	NIF proveedor	Departamento de compras	Carpeta proveedores	3 años
Facturas clientes	NIF cliente	Departamento de ventas	Carpeta clientes	3 años
Nóminas	DNI empleado	Departamento de RR. HH.	Carpeta empleados	3 años
Informes de resultados	Fecha de aprobación	Dirección	Carpeta de información financiera	3 años

Análisis de los requerimientos legales en referencia al registro

Los requerimientos legales establecen las condiciones necesarias que debe cumplir una actividad, proceso o servicio para alinearse con las normativas vigentes. En el caso de los registros, estos requerimientos cubren la obtención, tratamiento, almacenamiento y medidas de seguridad de los datos.

Para cumplir con estos requerimientos y evitar la ilegalidad, las organizaciones deben realizar una búsqueda exhaustiva de los textos legales pertinentes y mantenerse actualizadas sobre cualquier cambio.

Una legislación clave es la **Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de Derechos Digitales (LOPDGDD)**, que adapta la normativa europea del Reglamento General de Protección de Datos (RGPD) para proteger los datos personales y garantizar los derechos digitales y establece en su artículo 38 que los códigos de conducta serán vinculantes en cuanto a:

- Tratamiento leal y transparente.
- Intereses legítimos perseguidos por los responsables del tratamiento.
- Recogida y seudonimización de datos personales.
- Información proporcionada al público y a los interesados.
- Ejercicio de los derechos de los interesados.
- Información y protección de los menores, y consentimiento de los tutores.
- Medidas y procedimientos para garantizar la seguridad del tratamiento.
- Notificación de violaciones de seguridad a las autoridades y a los interesados.
- Transferencia de datos a terceros países u organizaciones internacionales.
- Procedimientos extrajudiciales para resolver conflictos relacionados con el tratamiento de datos.

Análisis de los requerimientos legales en referencia al registro

Principios de la LOPDGDD. La LOPDGDD destaca la importancia de:

- Exactitud y confidencialidad de los datos.
- Tratamiento basado en el consentimiento del afectado, especialmente para menores.
- Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.
- Manejo de categorías especiales de datos y datos de naturaleza penal.

Derechos de las Personas. La ley enfatiza la transparencia y la información al afectado, incluyendo los siguientes derechos:

- Derecho de acceso: Conocer qué datos personales se están tratando.
- Derecho de rectificación: Corregir datos inexactos.
- Derecho de supresión (derecho al olvido): Eliminar datos personales.
- Derecho a la limitación del tratamiento: Restringir cómo se utilizan los datos.
- Derecho a la portabilidad: Transferir datos a otro responsable.
- Derecho de oposición: Oponerse al tratamiento de datos.

Información a los Titulares de los Datos Personales Las organizaciones deben informar a los interesados sobre:

- La finalidad del uso de sus datos.
- La existencia de un fichero con sus datos.
- El responsable del fichero y su dirección.
- La posibilidad de ejercer los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) y otros derechos relacionados.
- El derecho a no prestar su consentimiento en el tratamiento de datos especialmente protegidos.

Análisis de los requerimientos legales en referencia al registro

Cumplimiento de los Requerimientos Legales en el Tratamiento de Datos
Teniendo en cuenta esta serie de requerimientos, es fundamental mantener la integridad de los dispositivos que tratan datos personales. No solo se debe vigilar quién accede a los datos, sino también asegurar que los dispositivos y equipos de información estén en condiciones adecuadas para almacenar correctamente los datos, evitando pérdidas de información y acceso no autorizado. Además de controlar los requerimientos legales, se recomienda establecer un control, actualización e inventario de los dispositivos como:

Equipos Informáticos:

- Inventario Actualizado: Mantener un inventario de todos los ordenadores y servidores.
- Registro de Configuraciones: Registrar las configuraciones de cada dispositivo para poder restaurarlos en caso de pérdida de datos.
- Dispositivos de Red (Módems, Routers, Switches, etc.):
- Inventario de Dispositivos de Red: Incluir todos los dispositivos de red y la seguridad establecida en cada uno.
- Licencias de Software:
- Licencias Legales y Actualizadas: Asegurar que todas las aplicaciones utilizadas en la organización tienen licencias legales y están actualizadas para evitar riesgos de pérdida de información.

Dispositivos de Hardware y Software de Seguridad:

- Medidas de Seguridad lógica: Configurar firewalls e instalar antivirus actualizados para evitar el acceso indebido de usuarios no autorizados.
- Medidas de Seguridad Física: Implementar medidas para proteger los dispositivos en caso de desastres naturales, robos, etc., y mantener condiciones ambientales adecuadas para minimizar el riesgo de averías y pérdida de información.

Análisis de los requerimientos legales en referencia al registro

Resumen de Requerimientos Legales y Recomendaciones

La siguiente tabla resume los aspectos básicos de los requerimientos legales y las recomendaciones de actuación para las organizaciones:

Aspecto	Requerimiento Legal	Recomendación
Acceso a Datos	Controlar quién accede a los datos	Establecer permisos y restricciones
Almacenamiento	Protección de la información	Uso de sistemas seguros y redundantes
Software	Licencias legales	Mantener software actualizado y con licencia
Seguridad de Dispositivos	Medidas contra acceso no autorizado	Uso de firewalls y antivirus actualizados
Seguridad Física	Protección en caso de incidentes	Medidas contra robos, incendios, y desastres

Recursos Adicionales

Desde la página de la Agencia Española de Protección de Datos (AEPD), en su apartado “Cumplimiento de las obligaciones”, se ofrecen guías y asistentes para que las empresas y organizaciones cumplan con sus obligaciones en relación a la protección de datos de los ciudadanos.

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

Introducción

Es fundamental, antes de implementar sistemas de información, identificar y acordar los requerimientos de seguridad que se incorporarán a estos sistemas. Estos requerimientos y controles deben alinearse con el valor de los datos involucrados y con el potencial daño que podría causar a la organización una pérdida o modificación no deseada. Por ello, las medidas de salvaguarda y los controles adicionales se determinarán según los requisitos de seguridad, la evaluación de los riesgos y el valor de la información protegida.

Tipos de controles de salvaguarda

- Medidas de seguridad administrativa
- Medidas de seguridad física
- Medidas de seguridad técnica

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

Medidas de seguridad administrativa

Las medidas de seguridad administrativas son esenciales para cumplir los objetivos de seguridad de la organización en los siguientes aspectos:

- **Cumplimiento de los requerimientos legales:**
  - Controles para evitar incumplimientos de la normativa vigente, obligaciones contractuales y la política de seguridad de la organización.
  - Incluye cumplimiento de la normativa sobre protección de datos personales, derechos de propiedad intelectual, privacidad y confidencialidad de la información.
- **Política de seguridad.** Establecimiento e implementación de una política de seguridad con directrices y orientaciones estratégicas en materia de seguridad.
- **Organización de la seguridad de la información:**
  - Establecimiento de controles internos (compromiso de cumplimiento de los directivos, designación de responsables de seguridad).
  - Controles externos (identificación y medidas de control de riesgos relacionados con terceros).
- **Clasificación y control de activos.** Elaboración y mantenimiento de un inventario actualizado de todos los dispositivos y equipos relacionados con los sistemas de información y registro de la organización.
- **Seguridad relacionada con los recursos humanos.** Establecimiento de controles y medidas para que los empleados conozcan sus responsabilidades respecto a la seguridad de la información antes, durante y después de la relación laboral.

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

Medidas de seguridad administrativa

Las medidas de seguridad administrativas son esenciales para cumplir los objetivos de seguridad de la organización en los siguientes aspectos (II):

- **Administración de incidentes:**
  - Implementación de controles para la gestión de incidentes que puedan afectar la integridad, confidencialidad y disponibilidad de la información.
  - Incluye reportes de eventos y debilidades de seguridad de la información.
- **Continuidad de las operaciones:**
  - Controles para evitar incidencias y medidas que permitan reestablecer la normalidad rápidamente tras interrupciones o fallas en los sistemas de registros.

Medidas de seguridad física

Además de las medidas de protección en los sistemas de información, es esencial considerar que agentes físicos externos pueden afectar significativamente la seguridad de la información. Por ello, se deben establecer controles para mantener un perímetro de seguridad física adecuado y ubicar los dispositivos en un entorno ambiental apropiado. Estas medidas incluyen:

- **Perímetro de seguridad física:** Establecimiento de barreras físicas que eviten y prevengan accesos no autorizados, robos o daños malintencionados.
- **Condiciones ambientales:** Ubicación de equipos en zonas libres de humedad y lejos de la luz solar directa para evitar daños.

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

Medidas de seguridad técnica

Las medidas de seguridad técnica se aplican a sistemas de datos personales en soportes electrónicos, servicios e infraestructuras de tecnologías de la información. Estas medidas incluyen:

- **Control de accesos:**
  - Gestión del acceso de los usuarios autorizados.
  - Control de accesos a la red y a las aplicaciones para proteger archivos y registros contra divulgación no autorizada.
- **Gestión de comunicaciones:**
  - Protección de las comunicaciones y operaciones realizadas con los registros.
  - Medidas como la realización de copias de seguridad, protección contra código malicioso (malware) y gestión de la seguridad de la red.
- **Diseño, uso y mantenimiento de sistemas de información:**
  - Integración de controles de seguridad desde la fase de diseño del sistema de información.
  - Mantenimiento y actualización de estos controles hasta que el sistema deje de utilizarse definitivamente.

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

TIPOS DE MEDIDAS	MEDIDA
ADMINISTRATIVAS	Definición de políticas de seguridad.
	Establecimiento de controles para cumplir con los requerimientos legales.
	Organización de la seguridad de la información mediante controles internos y externos.
	Clasificación y control de activos: elaboración y actualización de inventario de dispositivos.
	Definición de controles respecto a los recursos humanos.
	Administración de incidentes.
	Continuidad de las operaciones.
FÍSICAS	Establecimiento del perímetro de seguridad.
	Medidas de seguridad ambientales.
TÉCNICAS	Gestión de comunicaciones y operaciones
	Control de accesos.
	Diseño, uso y mantenimiento de sistemas de información.

Asignación de responsabilidades para la gestión del registro

La gestión de los registros es un aspecto importante para las organizaciones. Es esencial cuidar meticulosamente la recogida, tratamiento y análisis de la información, así como implementar medidas de seguridad para evitar la eliminación o modificación involuntaria de los registros y prevenir manipulaciones no autorizadas. Por ello, las organizaciones deben asignar responsables que garanticen el cumplimiento de los requerimientos legales y de seguridad, asegurando además la adecuada recolección de datos para un análisis correcto y la obtención de conclusiones útiles.

La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) obliga a las organizaciones a designar un responsable de tratamiento de datos en su documento de seguridad. Este responsable se encarga de autorizar, coordinar, controlar y, en ocasiones, ejecutar las medidas definidas en dicho documento.

Principales obligaciones del responsable de tratamiento de datos según la LOPDGDD:

- Auditorías: Someter los sistemas de información a una auditoría interna o externa cada dos años para verificar el cumplimiento del reglamento, procedimientos e instrucciones.
- Análisis de auditorías: Analizar el informe de auditoría y elevar las conclusiones al responsable del fichero para adoptar las medidas correctoras adecuadas.
- Controles periódicos: Implantar, revisar y modificar (si es necesario) controles periódicos para verificar el cumplimiento del documento de seguridad.
- Acceso autorizado:
  - Controlar que solo el personal autorizado pueda acceder a la información en papel de nivel alto.
  - Actualizar el listado de personal autorizado a acceder a datos personales en soporte papel de nivel alto.
- Seguridad física: Asegurar que los armarios y archivadores con datos personales de nivel alto estén en áreas con acceso protegido y que se mantengan cerradas cuando no se necesite acceso.

Asignación de responsabilidades para la gestión del registro

Principales obligaciones del responsable de tratamiento de datos según la LOPDGDD (II):

- Limitación de acceso: Adoptar medidas para que el acceso de los usuarios esté limitado a los recursos necesarios para sus funciones.
- Gestión de usuarios y perfiles:
    - Confeccionar y mantener actualizada una relación de usuarios y perfiles de usuarios a ficheros no automatizados y los accesos autorizados para cada uno.
    - Establecer mecanismos para evitar que un usuario acceda a ficheros no autorizados.
- Seguridad para personal ajeno: Adoptar medidas para que el personal ajeno con acceso a los ficheros no automatizados cumpla las mismas condiciones y obligaciones de seguridad que el personal propio.
- Control de copias:
    - Controlar que solo las personas autorizadas realicen copias de documentos con datos de nivel alto.
    - Redactar y revisar un procedimiento para la destrucción de copias desechadas que contengan datos de nivel alto, evitando el acceso a la información.
- Definición de funciones y obligaciones: Definir y documentar las funciones y obligaciones del personal en relación con los ficheros.
- Gestión de incidencias:
    - Establecer un procedimiento de notificación y gestión de incidencias relativas a los ficheros.
    - Establecer un registro que consigne el tipo de incidencia, momento de detección, persona notificadora, destinatario de la comunicación, efectos derivados y medidas correctoras aplicadas.

Asignación de responsabilidades para la gestión del registro

Principales obligaciones del responsable de tratamiento de datos según la LOPDGDD (III):

- Conservación y consulta:
    - Asegurar el archivo de soportes o documentos de acuerdo con criterios que garanticen la correcta conservación, localización y consulta de la información.
    - Posibilitar el ejercicio de los derechos ARCO y POL al tratamiento de los datos.
- Identificación e inventario:
    - Identificar el tipo de información contenida en los soportes y documentos con datos personales.
    - Inventariar los soportes y documentos que contengan datos personales.

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

Introducción

El registro de un sistema es una base de datos jerárquica que almacena sus ajustes de configuración. Contiene configuraciones de componentes de bajo nivel del sistema operativo, como aplicaciones, controladores de dispositivos, servicios, interfaz de usuario y aplicaciones de terceros. Además, facilita información para comprobar el rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad del sistema.

La escalabilidad de un sistema describe la facilidad con la que se pueden agregar o quitar componentes del sistema mientras se mantiene su confiabilidad.

Registro de Windows

El registro de Windows contiene configuraciones del sistema operativo útiles para:

- Identificar aplicaciones instaladas y determinar con qué programas abrir cada tipo de archivo.
- Definir programas que deben iniciarse al encender el equipo, optimizando el arranque.
- Gestionar dispositivos de hardware, drivers y recursos utilizados.
- Guardar configuraciones de cuentas de usuario.
- Personalizar características y apariencia de elementos como carpetas, ventanas y el Escritorio de Windows.

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

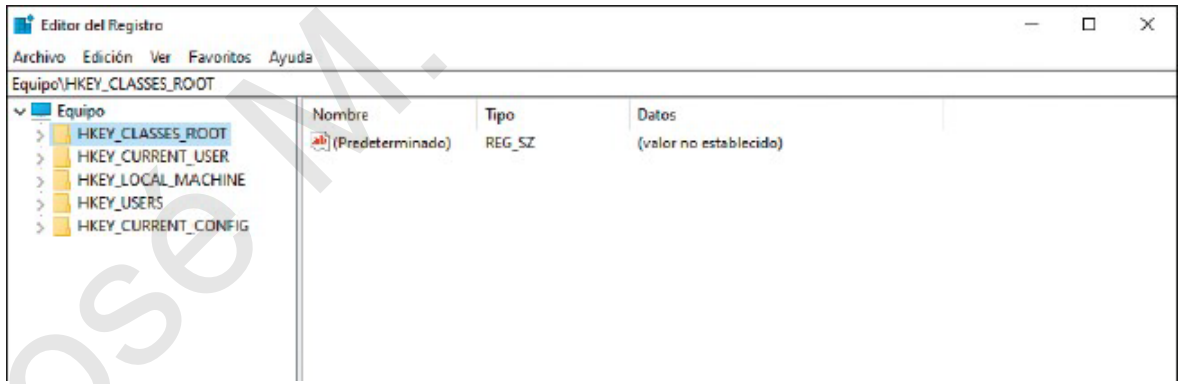
Registro de Windows

Para acceder al registro de Windows:

- Ir a Inicio -> Ejecutar, introducir el comando **regedit** y pulsar Aceptar para abrir el Editor del Registro.

Las claves principales del registro son:

- **HKEY_CLASSES_ROOT**: Información sobre aplicaciones registradas y sistemas de archivos.
- **HKEY_CURRENT_USER**: Configuraciones del usuario actual.
- **HKEY_LOCAL_MACHINE**: Configuraciones de software, hardware y cuentas de usuario aplicables a todos los usuarios del equipo.
- **HKEY_USERS**: Datos sobre perfiles de usuario.
- **HKEY_CURRENT_CONFIG**: Información del hardware del equipo, configurada en tiempo real.



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

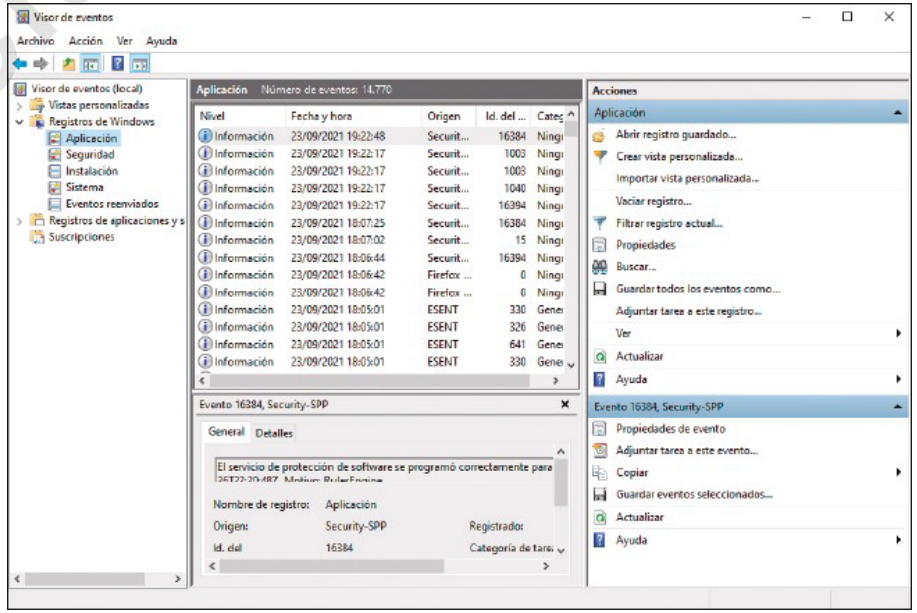
Registro de Windows

Para revisar los registros del sistema en caso de sospecha de uso no autorizado, se utiliza el **Visor de eventos de Windows**:

- Ir a Inicio -> Configuración -> Panel de control -> Herramientas administrativas -> Visor de eventos.

Tipos de registros en el Visor de eventos:

- **Registros de aplicación:** Eventos registrados por aplicaciones.
- **Registros de seguridad:** Eventos de acceso al sistema, como intentos de inicio de sesión y uso de recursos.
- **Registros de instalación:** Eventos relacionados con la instalación de aplicaciones.
- **Registros de sistema:** Eventos generados por componentes del sistema operativo.
- **Registros de eventos reenviados:** Eventos reenviados desde otros equipos



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

Registros en Linux

En el sistema operativo Linux, se utilizan archivos de registro para registrar eventos del sistema, como la conexión de dispositivos y nuevas sesiones. Estos archivos incluyen el programa generador, la prioridad, la fecha y la hora.

Para acceder a los archivos de registro en Linux, es necesario iniciar sesión como usuario "root". Para ver las últimas líneas de un archivo y sus actualizaciones, se utiliza el comando **tail –f**.

Para acceder al registro entero y ver actualizaciones en tiempo real, se utiliza el comando **less +F**.

Nombre de archivo	Funcionalidad
/var/log/auth.log	Información sobre eventos de autenticación de usuarios y permisos
/var/log/boot.log	Eventos y servicios iniciados al arrancar el sistema
/var/log/crond.log	Tareas de cron
/var/log/daemon.log	Mensajes sobre permisos o servicios en ejecución
/var/log/dmesg.log	Mensajes del núcleo Linux
/var/log/errors.log	Errores del sistema
/var/log/everything.log	Mensajes misceláneos no cubiertos por otros archivos
/var/log/httpd.log	Mensajes y errores de Apache
/var/log/mail.log	Mensajes del servidor de correo electrónico
/var/log/messages.log	Alertas generales del sistema
/var/log/mysqld.log	Archivo de MySQL
/var/log/secure	Registro de seguridad
/var/log/syslog.log	Registro del sistema de registro
/var/log/Xorg.0.log	Registros de Xorg
/var/log/user.log	Información sobre procesos utilizados por el usuario

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

La recolección, obtención de resultados y análisis de los registros es una tarea ardua y costosa. Por ello, es importante elegir el sistema de almacenamiento adecuado, garantizando una custodia correcta y evitando pérdidas inesperadas de información.

Para ello, deben considerarse varios factores.

Modelos de almacenamiento de datos:

- **Modelo tradicional de archivos:**
  - **Variables:** Conjunto de registros que pueden almacenar datos de diversos tipos.
  - **Archivos:** Lugar donde se almacenan los registros.
  - **Aplicaciones:** Gestionan y coordinan variables y archivos para facilitar el acceso a la información.

- **Modelo de bases de datos relacionales:**
  - Organiza los datos en tablas para una entrada de datos ágil y automatizada.
  - Utiliza aplicaciones como plataforma para introducir y tratar datos y registros.

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

Para ello, deben considerarse varios factores (II)

Factores para la elección del sistema de almacenamiento

- **Sistema operativo:** Dependiendo del sistema operativo utilizado, el formato de los archivos y registros será diferente (e.g., Linux, Windows).
- **Requisitos legales/normativas:**
  - Normativas relevantes incluyen:
    - Ley Orgánica de Protección de Datos de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).
    - Normativas sobre propiedad intelectual, privacidad y confidencialidad de la información.
    - Normativas sobre comercio electrónico.
  - Conocimiento de normativas nacionales e internacionales si operamos en el exterior.
- **Capacidad de los recursos:** Volumen de datos y capacidad de procesamiento necesarios para manejar los datos de forma eficiente.
- **Características de la red:** Dependiendo del tipo de red (local, servidores remotos), el sistema de almacenamiento tendrá diferentes características y medidas de seguridad.
- **Complejidad del sistema de información:** Nivel de complejidad influye en los requerimientos de almacenamiento (e.g., múltiples perfiles de acceso, varios equipos).

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

Para ello, deben considerarse varios factores (III)

Factores para la elección del sistema de almacenamiento

- **Tipo de alojamiento de los registros:**
  - **Alojamiento tradicional:** Equipos de almacenamiento en las instalaciones de la organización, autogestionado.
  - **Alojamiento web (web hosting):** Almacenamiento en Internet accesible desde cualquier dispositivo.
  - **Alojamiento en la nube (cloud hosting):**
    - **Nubes públicas:** Servidores externos, acceso gratuito o de pago, gran capacidad.
    - **Nubes privadas:** Servicios dentro de la organización, mayor seguridad.
    - **Nubes híbridas:** Combinación de nubes públicas y privadas, aprovechando ventajas de ambos modelos.

Ventajas del cloud hosting

- **Reducción de costes:** Menos infraestructuras necesarias.
- **Accesibilidad:** Archivos accesibles desde cualquier punto con Internet.
- **Escalabilidad:** Adaptación a las necesidades de la organización.
- **Seguridad:** Alto nivel de seguridad gestionado por el proveedor del servicio.
- **Autoservicio:** Acceso a recursos de la nube de forma automática.

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

Factores para la elección del sistema de almacenamiento	Características
Sistema operativo	Linux, Windows y otros.
Requisitos legales	LOPDGDD, propiedad intelectual, comercio electrónico, confidencialidad y privacidad.
Capacidad de los recursos	Volumen de datos, intensidad de procesamiento.
Características de la red	Red local, utilización de servidores remotos.
Complejidad del sistema	Equipos y dispositivos del sistema, número de perfiles de usuario.
Tipo de alojamiento de datos	Tradicional, web hosting, cloud hosting (público, privado, híbrido).

Resumen

Los procesos de monitorización de sistemas de información generan documentos útiles para la toma de decisiones directivas. Los registros, que documentan las tareas realizadas por la organización, deben cumplir con propiedades esenciales: identificación, almacenamiento, protección, recuperación, retención y disposición.

El almacenamiento de registros puede implicar el cumplimiento de condiciones legales, especialmente bajo la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD). Este cumplimiento es una parte fundamental del plan de seguridad de la organización, que también debe incluir medidas de seguridad administrativas, físicas y técnicas, acordes con el valor de los registros y el potencial daño en caso de pérdida.

Las organizaciones deben asignar responsables para garantizar que se cumplan los requerimientos legales y de seguridad, evitando problemas de descontrol. Es importante almacenar los registros de manera que se aseguren el rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad del sistema.

Las alternativas de almacenamiento pueden variar según el sistema operativo: en Windows 10, la gestión de registros puede realizarse mediante aplicaciones, mientras que en Linux se requieren comandos específicos.

Finalmente, la elección del sistema de almacenamiento y custodia de registros debe basarse en las características de la organización y de los propios registros, asegurando así una gestión eficaz y segura.