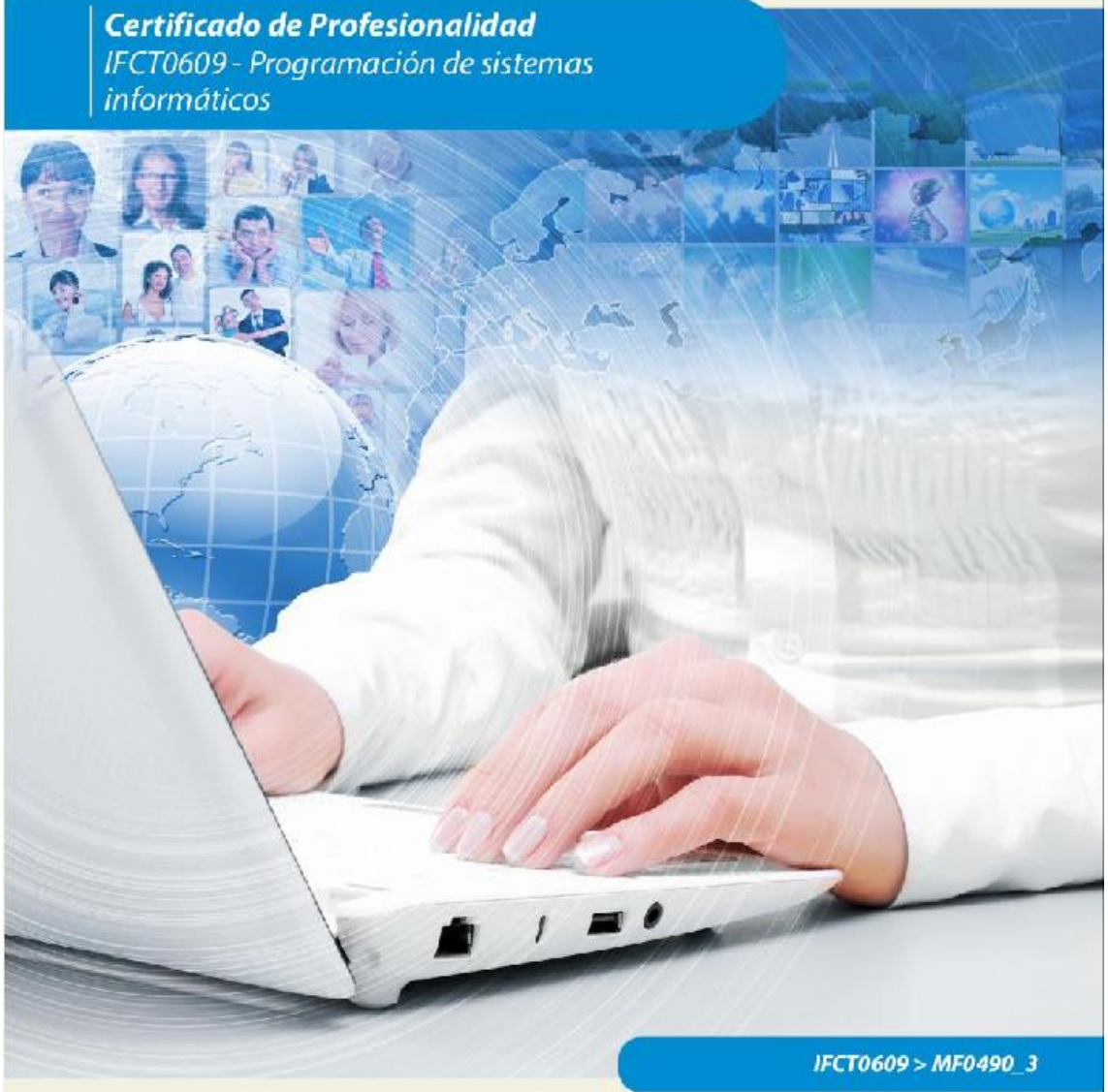
MF0490_3: Gestión de servicios en el sistema informático

Certificado de Profesionalidad
IFCT0609 - Programación de sistemas informáticos



IFCT0609 > MF0490_3

ic editorial

Ester Chicano Tejada

Gestión de servicios en el sistema informático IFCT0609

Ester Chicano Tejada

ic editorial

Gestión de servicios en el sistema informático. IFCT0609

1ª Edición

Editado por: IC Editorial
c/ Cueva de Viera, 2, Local 3
Centro Negocios CADI
29200 Antequera (Málaga)
Teléfono: 952 70 60 04
Fax: 952 84 55 03
Correo electrónico: iceditorial@iceditorial.com
Internet: www.iceditorial.com

ISBN: 978-84-1103-656-6

Presentación del manual

El **Certificado de Profesionalidad** es el instrumento de acreditación, en el ámbito de la Administración laboral, de las cualificaciones profesionales del Catálogo Nacional de Cualificaciones Profesionales adquiridas a través de procesos formativos o del proceso de reconocimiento de la experiencia laboral y de vías no formales de formación.

El elemento mínimo acreditable es la **Unidad de Competencia**. La suma de las acreditaciones de las unidades de competencia conforma la acreditación de la competencia general.

Una **Unidad de Competencia** se define como una agrupación de tareas productivas específica que realiza el profesional. Las diferentes unidades de competencia de un certificado de profesionalidad conforman la **Competencia General**, definiendo el conjunto de conocimientos y capacidades que permiten el ejercicio de una actividad profesional determinada.

Cada **Unidad de Competencia** lleva asociado un **Módulo Formativo**, donde se describe la formación necesaria para adquirir esa **Unidad de Competencia**, pudiendo dividirse en **Unidades Formativas**.

El presente manual desarrolla el Módulo Formatvo **MF0490_3: Gestión de servicios en el sistema informático**,

asociado a la unidad de competencia **UC0490_3: Gestionar servicios en el sistema informático**,

del Certificado de Profesionalidad **Programación de sistemas informáticos**.

Índice

Portada

Título

Copyright

Presentación del manual

Índice

Capítulo 1
Gestión de la seguridad y normativas

1. **Introducción**
2. **Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información**
3. **Metodología ITIL. Librería de infraestructuras de las tecnologías de la información**
4. **Ley Orgánica de protección de datos de carácter personal/Ley Orgánica de protección de Datos personales y garantía de los derechos digitales**
5. **Normativas más frecuentemente utilizadas para la gestión de la seguridad física**
6. **Resumen**
   Ejercicios de repaso y autoevaluación

Capítulo 2
Análisis de los procesos de sistemas

1. **Introducción**
2. **Identificación de procesos de negocio soportados por sistemas de información**
3. **Características fundamentales de los procesos electrónicos**
4. **Determinación de los sistemas de información que soportan los procesos de negocio y los activos y servicios utilizados por los mismos**
5. **Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios**
6. **Técnicas utilizadas para la gestión del consumo de recursos**
7. **Resumen**
   Ejercicios de repaso y autoevaluación

Capítulo 3
Demostración de sistemas de almacenamiento

1. **Introducción**
2. **Tipos de dispositivos de almacenamiento más frecuentes**

3. **Características de los sistemas de archivo disponibles**
4. **Organización y estructura general de almacenamiento**
5. **Herramientas del sistema para la gestión de dispositivos de almacenamiento**
6. **Resumen**

Ejercicios de repaso y autoevaluación

Capítulo 4

Utilización de métricas e indicadores de monitorización de rendimiento de sistemas

1. **Introducción**
2. **Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información**
3. **Identificación de los objetos para los cuales es necesario obtener indicadores**
4. **Aspectos a definir para la selección y definición de indicadores**
5. **Establecimiento de los umbrales de rendimiento de los sistemas de información**
6. **Recolección y análisis de los datos aportados por los indicadores**
7. **Consolidación de indicadores bajo un cuadro de mando de rendimiento de sistemas de información unificado**
8. **Resumen**

Ejercicios de repaso y autoevaluación

Capítulo 5

Confección del proceso de monitorización de sistemas y comunicaciones

1. **Introducción**
2. **Identificación de los dispositivos de comunicaciones**
3. **Análisis de los protocolos y servicios de comunicaciones**
4. **Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones**
5. **Procesos de monitorización y respuesta**
6. **Herramientas de monitorización de uso de puertos y servicios tipo *sniffer***
7. **Herramientas de monitorización de sistemas y servicios tipo *Hobbit, Nagios* o *Cacti***
8. **Sistemas de gestión de información y eventos de seguridad (SIM/SEM)**
9. **Gestión de registros de elementos de red y filtrado *(router, switch, firewall*, IDS/IPS, etc.)**
10. **Resumen**

Ejercicios de repaso y autoevaluación

Capítulo 6

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

1. **Introducción**
2. **Determinación del nivel de registros necesario, los periodos de retención y las necesidades de almacenamiento**
3. **Análisis de los requerimientos legales en referencia al registro**

Capítulo 6

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

1. **Introducción**
2. **Determinación del nivel de registros necesario, los periodos de retención y las necesidades de almacenamiento**
3. **Análisis de los requerimientos legales en referencia al registro**
4. **Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros**
5. **Asignación de responsabilidades para la gestión del registro**
6. **Alternativas de almacenamiento para los registros del sistema y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad**
7. **Guía para la selección del sistema de almacenamiento y custodia de registros**
8. **Resumen**

Ejercicios de repaso y autoevaluación

Capítulo 7

Administración del control de accesos adecuados de los sistemas de información

1. **Introducción**
2. **Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos**
3. **Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos**
4. **Requerimientos legales en referencia al control de accesos y asignación de privilegios**
5. **Perfiles de acceso en relación con los roles funcionales del personal de la organización**
6. **Herramientas de directorio activo y servidores LDAP en general**
7. **Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)**
8. **Herramientas de sistemas de punto único de autenticación: *Single Sign On* (SSO)**
9. **Resumen**

Ejercicios de repaso y autoevaluación

Bibliografía

Capítulo 6

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

Contenido

1. Introducción
2. Determinación del nivel de registros necesario, los periodos de retención y las necesidades de almacenamiento
3. Análisis de los requerimientos legales en referencia al registro
4. Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros
5. Asignación de responsabilidades para la gestión del registro
6. Alternativas de almacenamiento para los registros del sistema y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad
7. Guía para la selección del sistema de almacenamiento y custodia de registros
8. Resumen

1. Introducción

Hasta ahora, se ha ido estudiando cómo implantar un sistema de información y cómo evaluar los objetivos y resultados a través de indicadores y métricas. Además, se ha aprendido a utilizar las distintas herramientas de monitorización de los sistemas de comunicaciones, para que los datos obtenidos para la obtención de los indicadores se consigan de la forma más automatizada posible.

Todo ello no serviría para nada sin un sistema de almacenamiento de la información que sea capaz de guardar los registros y datos y protegerlos debidamente.

En este capítulo, primeramente se determinará cómo definir el nivel de registros que una organización va a necesitar en función de sus objetivos y directrices, además de varias características a definir de los registros, como son: el período de retención y la necesidad de almacenamiento.

Además, la obtención, almacenamiento y tratamiento de datos son temas delicados porque pueden estar sometidos a varias normativas, atendiendo a la tipología de

datos a tratar. Por tanto, es importante conocer los principales requerimientos legales que hay que tener en cuenta, atendiendo al tipo de registros que manipulan las organizaciones, y también la selección y establecimiento de medidas de salvaguarda que eviten el riesgo de caer en ilegalidades o en problemas de seguridad de la información.

Todas estas medidas deben estar reflejadas en un documento de seguridad, en el que se designarán todas las responsabilidades relacionadas con la gestión de los registros para evitar un descontrol de las mismas que provoque fallos de seguridad.

También existen varias alternativas de almacenamiento de los registros del sistema, atendiendo a sus propiedades, y se proponen una serie de recomendaciones y factores a considerar para elegir un sistema de almacenamiento y custodia de registros adecuado.

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

Anteriormente, se han estudiado los diferentes procesos de información, su monitorización y su evaluación mediante la utilización de indicadores y métricas. En todas estas fases, las organizaciones obtienen una serie de documentos que sirven para apoyar y fundamentar las decisiones tomadas por los responsables.

Estos documentos sirven para que la organización se asegure una eficaz planificación, operación y control de los procesos. Los registros y documentos serán la base en la que se encuentren los datos para analizar el comportamiento y las mejoras de los distintos procesos del sistema de gestión de una organización.

En el tema de los documentos es importante tener claro una serie de conceptos:

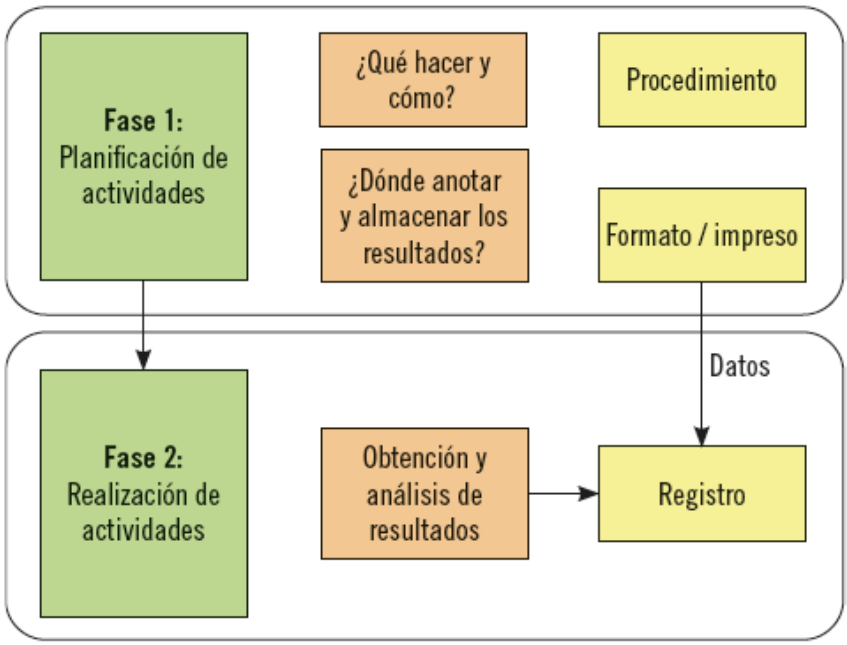
- **Registro:** formato o impreso cumplimentado como resultado de la realización de una tarea del sistema.
- **Formato o impreso:** tipo de documento en el que se anotan los datos relacionados con la realización de las tareas de un proceso.

En el momento en el que la organización planifica las diferentes actividades que llevará a cabo, se tomarán decisiones acerca de cómo se realizarán las actividades y dónde se deben anotar los resultados para su posterior análisis.

Una vez tomadas estas decisiones de planificación, cuando se llevan a cabo las tareas, los resultados obtenidos se almacenan en forma de registros en la manera decidida en el proceso anterior. Mediante el análisis de resultados almacenados en

estos registros ya se puede realizar una correcta toma de decisiones en la organización y comprobar su correcto funcionamiento o, por el contrario, la puesta en marcha de medidas correctivas para obtener mejoras significativas.

Este proceso de planificación y realización de actividades de una organización se puede observar en la siguiente imagen:



Ya que los registros son la base para una correcta toma de decisiones, es fundamental ejercer un control exhaustivo de los mismos para evitar distorsiones de los resultados. Para un correcto control de los registros hay que tener en cuenta una serie de parámetros:

- **Identificación de los registros:** los registros deben poder identificarse con facilidad. Esta identificación hay que realizarla en dos niveles: en el primero se identifican los registros según el formato utilizado para su cumplimentación y en el segundo ya se diferencian por un campo identificador presente en el propio formato. Ejemplos de campos identificadores podrían ser el número de registro, la fecha de cumplimentación, etc.
- **Almacenamiento:** para un control correcto es fundamental establecer dónde se van almacenar los archivos de los registros para que sean de fácil localización en el momento de necesitarlos.
- **Protección:** hay que determinar una serie de controles y medidas de seguridad para evitar cambios indeseados en la información y el acceso de personas no

autorizadas. Ejemplos de medidas podrían ser el establecimiento de contraseñas de acceso o la realización de copias de seguridad.

- **Recuperación:** debido al alto volumen de registros almacenados, hay que establecer una metodología que permita encontrar y acceder a los datos históricos con facilidad.
- **Retención:** según el tipo de registro que se esté tratando, estos requieren ser conservados un determinado intervalo de tiempo u otro. Si se toman en consideración las recomendaciones de la norma ISO 9001:2000, se recomienda que los registros se conserven durante tres años. Aun así, dependiendo de las necesidades de la organización y de los requerimientos legales para algunos tipos de registros, habrá que establecer un período de retención u otro para estos registros especiales.
- **Disposición de los registros:** hay que establecer qué se va a hacer con los registros una vez terminado el período de retención, cómo va a ser el procedimiento para eliminarlos o dónde se van a almacenar o a archivar en caso de decidir conservarlos de modo indefinido.

Importante

Para un correcto control de los registros es importante su identificación, almacenamiento, protección, fácil recuperación y su conservación y disposición.

Con todos estos requerimientos de control las organizaciones suelen hacer una ficha de los registros que se van a almacenar. Un ejemplo de ficha podría ser la siguiente:

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

Si el establecimiento de estas medidas de control de los registros es correcto y adecuado se pueden obtener beneficios importantes para la organización:

- Mediante el control del almacenamiento de los datos se consigue que el acceso a los mismos sea más sencillo y rápido, lo que propiciará un análisis de los indicadores más ágil y resolutivo.
- Al ser el acceso a los registros más rápido, también se agiliza el proceso de realización de auditorías.
- Hay una mayor protección de los registros tras haber establecido previamente una serie de medidas de seguridad que evitan el uso indebido de los datos y las pérdidas imprevistas de los mismos.
- Hay una mayor organización y orden en el archivo de la organización, lo que puede ahorrar tiempo y gastos en el momento de necesitar algún documento determinado.

Actividades

1. Proponga un listado de registros para organizar los que pueda tener una autoescuela.
2. Ya se han ido mencionando los beneficios que tiene para una organización el establecimiento de medidas de control de los registros. Señale qué consecuencias puede haber si no se aplican estas medidas.

3. Análisis de los requerimientos legales en referencia al registro

Los requerimientos legales son aquellos que indican las condiciones necesarias específicas que debe reunir una actividad, proceso o servicio determinado para cumplir con los postulados que se establecen en los textos legales. En el caso de los registros, los requerimientos legales se referirán a los modos de obtención, tratamiento, sistemas de almacenamiento y medidas de seguridad de los registros.

Para cumplir con los requerimientos legales y no caer en la ilegalidad, la organización debe hacer una búsqueda exhaustiva de los textos legales que regulan los registros y actualizarse continuamente para estar al día de los cambios que hay que realizar en el sistema de registros de la misma.

Una de las legislaciones que hace mayor énfasis en la temática de los registros es la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de Derechos Digi-

tales (LOPDGDD) cuya finalidad es adaptar la normativa europea para proteger a las personas en lo que respecta al tratamiento de sus datos personales y garantizar los derechos digitales de la cuidadanía.

El artículo 38 de la LOPDGDD habla de que los códigos de conducta regulados por la sección 5ª del Capítulo IV del Reglamento (UE) 2016/679 serán vinculantes, y estos tendrán como objeto especificar la aplicación de la normativa en lo que respecta a:

a. el tratamiento leal y transparente;
b. los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;
c. la recogida de datos personales;
d. la seudonimización de datos personales;
e. la información proporcionada al público y a los interesados;
f. el ejercicio de los derechos de los interesados;
g. la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;
h. las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;
i. la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;
j. la transferencia de datos personales a terceros países u organizaciones internacionales, o
k. los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79.

Según la LOPDGDD se debe preservar la protección de datos a través de:

- Exactitud de los datos.
- Deber de confidencialidad.
- Tratamiento basado en el consentimiento del afectado.
- Consentimiento de los menores de edad.
- Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.
- Categorías especiales de datos.
- Tratamiento de datos de naturaleza penal.

Además trata sobre los derechos de las personas, dando especial importancia a la Transparencia e información al afectado a través de:

- Derecho de acceso
- Derecho de rectificación
- Derecho de supresión
- Derecho a la limitación del tratamiento
- Derecho a la portabilidad
- Derecho de oposición

En cuanto a los titulares de los datos personales, la organización, en términos generales, debe informar al interesado de:

- La finalidad para la que se van a utilizar sus datos.
- La existencia de un fichero con sus datos.
- El responsable del fichero y su dirección o la de su representante.
- La posibilidad de ejercer los derechos ARCO y POL en sus datos.
- En el caso de datos especialmente protegidos, los interesados deben estar informados de su derecho a no prestar su consentimiento en el tratamiento de estos datos.

Nota

Los datos especialmente protegidos son aquellos relativos a ideología, afiliación sindical, religión, origen racial, salud o vida sexual. Con este tipo de datos hay que tener un especial cuidado en su tratamiento.

Teniendo en cuenta toda esta serie de requerimientos, una buena manera de elevar su cumplimento es manteniendo una integridad en los dispositivos que tratan este tipo de datos. No solo hay que vigilar quién accede y hace uso de los datos, también hay que asegurar que los dispositivos y los equipos de información están en condiciones para que almacenen correctamente los datos y así evitar pérdidas de información y acceso de usuarios no autorizados. Por ello, además de controlar los requerimientos legales, se recomienda establecer un control, actualización e inventarización de dispositivos como:

- **Equipos informáticos:** se recomienda tener un inventario actualizado de todos los ordenadores y servidores que hay en la actualización. Además, es recomendable tener registradas las distintas configuraciones que hay en cada uno de ellos por si se produce alguna pérdida de datos y es necesario reestablecerlos.

- **Dispositivos de red *(módems, routers, switches*, etc.):** en el inventario también deberían incluirse todos los dispositivos de red que forman parte de la organización y la seguridad que hay establecida en cada uno de ellos.
- **Licencias de *software:*** el uso de licencias de *software* ilegales son uno de los principales factores de riesgo para la pérdida de la información. Por ello, es imprescindible que las licencias de aplicaciones que se utilicen en la organización sean todas legales y estén actualizadas constantemente para evitar este tipo de riesgos.
- **Dispositivos *hardware* y *software* de seguridad:** para evitar el uso indebido de usuarios no autorizados de los datos personales es imprescindible establecer medidas de seguridad en cuanto a *software* y *hardware*, para minimizar los riesgos todo lo posible. Así, se recomienda configurar firewalls y tener instalado un buen antivirus que se actualice constantemente y así conseguir una reducción notable de este tipo de riesgos.
- **Medidas de seguridad física:** además de tener inventariados y protegidos los distintos dispositivos, también es recomendable tomar una serie de medidas físicas que los protejan en caso de catástrofes naturales, robos, etc., y los mantengan en condiciones ambientales propicias que minimicen los riesgos de avería y así conseguir evitar pérdidas de información.

A modo de resumen, en la tabla siguiente se recogen unos aspectos básicos referentes a los requerimientos legales y las recomendaciones de actuación para las organizaciones:

Obligación legal		Recomendación
Los datos deben recogerse solo con fines determinados explícitos y legítimos	→	No usar estos datos para otras finalidades
Los datos deben ser adecuados y pertinentes en relación a su finalidad	→	No recoger datos si no son absolutamente necesarios
Los datos deben ser exactos y veraces respecto a la situación del titular	→	Mantener actualizados los datos constantemente
Los datos deben ser conservados solamente durante el tiempo necesario para las finalidades para las que han sido recogidos	→	Cancelar y eliminar los datos cuando ya no son necesarios

Desde la página de la 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.

Actividades

3. Proponga más recomendaciones para una organización que quiera cumplir con los requerimientos legales sobre Protección de Datos.
4. Busque más información sobre la Agencia Española de Protección de Datos y sus funciones fundamentales.

Aplicación práctica

Usted, como responsable de tratamiento de datos de su empresa, está diseñando la metodología de recogida de unos datos personales de los responsables de ventas de los concesionarios de la provincia por temas estadísticos. En el momento de recoger los datos personales, ¿de qué tendrá que informar respecto a su derecho de acceso a los responsables de ventas que entreviste?

SOLUCIÓN

En el momento de recabar los datos personales de los responsables de ventas de los concesionarios, la LOPDGDD establece que los interesados tendrán derecho de acceso a los datos personales y a la siguiente información:

- los fines del tratamiento;
- las categorías de datos personales de que se trate;
- los destinatarios a los que se comunicarán;
- si es posible, el plazo previsto de conservación de los datos personales;
- la existencia del derecho a solicitar al responsable la rectificación o supresión de datos personales o la limitación, u oponerse a dicho tratamiento;
- el derecho a presentar una reclamación ante una autoridad de control;
- cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
- la existencia de decisiones automatizadas, incluida la elaboración de informes.

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

Como ya se ha mencionado anteriormente, antes de implementar los sistemas de información es fundamental identificar y acordar los requerimientos de seguridad que se van a incorporar a estos sistemas de información y de registros.

Estos requerimientos y controles deben ser acordes con el valor de los datos involucrados y con el daño que podrían causar en la organización una pérdida o modificación indeseada de los mismos. Por este motivo, las medidas de salvaguarda y los controles adicionales se determinarán en función de los requisitos de seguridad, de la evaluación de los riesgos y del valor de la información protegida.

Los controles de salvaguarda de los sistemas de registros se pueden dividir en tres partes diferenciadas:

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

4.1. Medidas de seguridad administrativa

Las medidas de seguridad administrativas son aquellas que se deben implementar para conseguir los objetivos definidos por la organización en los siguientes aspectos:

- **Cumplimiento de los requerimientos legales:** controles establecidos para evitar incumplimientos de la normativa vigente, de las obligaciones establecidas por contrato o de la política de seguridad establecida por la organización. Incluye controles respecto al cumplimiento de la normativa referente a la protección de datos personales, los derechos de propiedad intelectual y la privacidad y confidencialidad de la información, entre otros.
- **Política de seguridad:** la organización debe establecer e implementar una política de seguridad en la que se definan una serie de directrices y orientaciones estratégicas en materia de seguridad.
- **Organización de la seguridad de la información:** incluye el establecimiento de controles internos (compromiso de cumplimiento de los directivos, designación de responsables de seguridad, etc.) y de controles externos (identificación y medidas de control de riesgos relacionados con terceros, entre otros), mediante los cuales se gestione la seguridad de la información y del sistema de registros.
- **Clasificación y control de activos:** tal y como se ha comentado anteriormente, hay que elaborar y mantener actualizado un inventario con todos los dispositivos y equipos relacionados con los sistemas de información y registro de la organización.
- **Seguridad relacionada con los recursos humanos:** además de los controles internos, también hay que establecer una serie de controles y medidas que permitan que los empleados conozcan el alcance de sus responsabilidades respecto a la seguridad de la información (tanto antes, como durante, como una vez finalizada la relación laboral).
- **Administración de incidentes:** un sistema de registros debe tener implementados una serie de controles referentes a la gestión de los incidentes (tanto

presentes como potenciales) que puedan afectar a la integridad, confidencialidad y disponibilidad de la información. Estos controles pueden ser, entre otros, reportes de eventos o reportes de debilidades de seguridad de la información.

- **Continuidad de las operaciones:** aparte de implementar controles que eviten las posibles incidencias, también hay que establecer controles que permitan volver cuanto antes a la normalidad cuando se produce algún tipo de interrupción de operaciones o de falla en los sistemas de registros.

Recuerde

Es imprescindible saber diferenciar los conceptos de confidencialidad, integridad y disponibilidad de la información. La confidencialidad consiste en asegurar que no acceden a la información usuarios no autorizados; la integridad se basa en garantizar la exactitud y confiabilidad de la información; y la disponibilidad es la capacidad de que los usuarios autorizados puedan acceder a la información cuando lo requieran.

4.2. Medidas de seguridad física

Como ya se ha comentado, además de establecer medidas de protección en el sistema de información también es fundamental tener en cuenta que puede haber agentes físicos externos que afecten notablemente a la seguridad de la información.

Por ello, es necesario establecer una serie de controles para mantener un perímetro de seguridad física adecuado y que se ubiquen los dispositivos en un entorno ambiental apropiado (zonas libres de humedad, zonas donde la luz solar no dé directamente a los equipos, etc.).

Además, el establecimiento de un perímetro de seguridad puede ayudar a evitar y prevenir accesos no autorizados y otras amenazas como robos o daños malintencionados.

4.3. Medidas de seguridad técnica

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

- **Control de accesos:** medidas que controlen el acceso a la información y a las instalaciones por parte de los responsables autorizados y protegiendo los ar-

chivos y registros contra su divulgación no autorizada. Ejemplos de medidas pueden ser la gestión de acceso de los usuarios, el control de accesos a la red y el control de accesos a las aplicaciones, entre otras.

- **Gestión de comunicaciones:** las comunicaciones y las operaciones realizadas con los registros deben estar protegidas e incluir medidas que aseguren que estas se realizan de un modo correcto. Algunas de estas medidas pueden ser la realización de copias de seguridad, la protección contra código malicioso *(malware)*, la gestión de la seguridad de la red, etc.
- **Diseño, uso y mantenimiento de sistemas de información:** en el momento de diseñar un sistema de información ya deben tenerse en cuenta los controles de seguridad que habrá que incluir para que haya una adecuada integración sin caer en problemas de seguridad innecesarios. Estos controles del sistema de información deben mantenerse y actualizarse hasta que el sistema deje de utilizarse definitivamente.

En resumen, se pueden observar los distintos tipos de medidas respecto a los requisitos de seguridad de sistemas de registros en la siguiente tabla:

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.

Actividades

5. Señale en qué se diferencian las medidas de seguridad administrativas, físicas y técnicas.
6. Busque más información y ponga más ejemplos de agentes físicos externos que pueden afectar a la seguridad de la información.

Aplicación práctica

Usted, como responsable de seguridad de su empresa, está evaluando los riesgos de perder los registros que se van recogiendo, y se ha dado cuenta de que no hay establecido ningún control de acceso a la información y que cualquier usuario podría acceder a ellos. ¿Qué tipo de medida debería establecer para aumentar el nivel de seguridad en este aspecto?

SOLUCIÓN

Teniendo en cuenta que hay medidas de seguridad técnicas, administrativas y físicas, el establecimiento de permisos y de control de accesos a los registros de una empresa se corresponde con una medida de seguridad técnica, una medida que se puede aplicar a los soportes electrónicos para evitar el acceso no autorizado de usuarios.

5. Asignación de responsabilidades para la gestión del registro

La gestión de los registros es un tema muy delicado para las organizaciones. Es de vital importancia tener sumo cuidado en la recogida, tratamiento y análisis de la información, aparte de tomar medidas de seguridad para evitar que los registros se eliminen o modifiquen involuntariamente y que haya manipulaciones no autorizadas de los mismos.

Por estos motivos, las organizaciones deben asignar responsables encargados de que se cumplan todos los requerimientos legales y de seguridad, además de asegurar que se han recogido los datos adecuados para un correcto análisis y obtención de conclusiones útiles para su buen funcionamiento.

La LOPDGDD obliga a las organizaciones a designar en su documento de seguridad a un responsable de tratamiento de datos que se encargue de autorizar, coordinar, controlar y, en ocasiones, ejecutar las medidas definidas en ese mismo documento.

Atendiendo a la LOPDGDD, las principales obligaciones del responsable de tratamiento de datos son las siguientes:

- Someter los sistemas de información, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del reglamento, procedimientos e instrucciones.
- Analizar el informe de auditoría y elevar las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas.
- Implantar, revisar y modificar (en caso de ser necesario) controles periódicos para verificar el cumplimiento de lo establecido en el documento de seguridad.
- 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.
- Cuidar que los armarios y archivadores que contengan información con datos personales de nivel alto se encuentren en áreas con acceso protegido y que estas estén cerradas cuando no sea necesario el acceso a las mismas.
- Adoptar las medidas oportunas para que el acceso de los usuarios esté limitado a los recursos que precisen para el desarrollo de sus funciones.
- Confeccionar y mantener actualizada una relación de usuarios y perfiles de usuarios a ficheros no automatizados y los accesos autorizados para cada uno de ellos.
- Establecer mecanismos para evitar que un usuario pueda acceder a ficheros distintos de los autorizados.

- Adoptar las medidas oportunas para que el personal ajeno que tenga acceso a los ficheros no automatizados esté sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.
- Controlar que realicen copias de los documentos que contengan datos de nivel alto solo las personas autorizadas en el documento de seguridad.
- Redactar y revisar la existencia de un procedimiento que indique cómo proceder a la destrucción de las copias o reproducciones desechadas que contengan datos de nivel alto de forma que se evite el acceso a la información.
- Definir y documentar las funciones y obligaciones del personal en relación con los ficheros.
- Establecer un procedimiento de notificación y gestión de las incidencias relativas a los ficheros.
- Establecer un registro en el que se haga constar el tipo de incidencia, el momento en el que se ha producido o detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.
- Disponer lo oportuno para que se archiven los soportes o documentos de acuerdo con los criterios que garanticen la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos ARCO y POL al tratamiento de los datos.
- Identificar el tipo de información que contienen los soportes y documentos que contengan datos de carácter personal.
- Inventariar los soportes y documentos que contengan datos personales.

Recuerde

Los derechos ARCO reflejados en la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales se corresponden con los derechos de acceso, rectificación, cancelación y oposición que tienen los interesados respecto a sus datos. Estos derechos se ven complementados con los derechos POL que ofrece el Reglamento General de Protección de Datos; Portabilidad, olvido o supresión y limitación del tratamiento.

Actividades

7. En este capítulo se ha hablado del responsable de tratamiento de datos. Comente en qué se podría diferenciar de un responsable de seguridad. Justifique su respuesta.

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

El registro de un sistema es una base de datos jerárquica que almacena sus ajustes de configuración.

Contiene la configuración de los componentes de bajo nivel del sistema operativo, como las aplicaciones, los controladores de dispositivos, los servicios, la interfaz de usuario y las aplicaciones de terceros.

Además, también facilita información para comprobar el rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad del sistema.

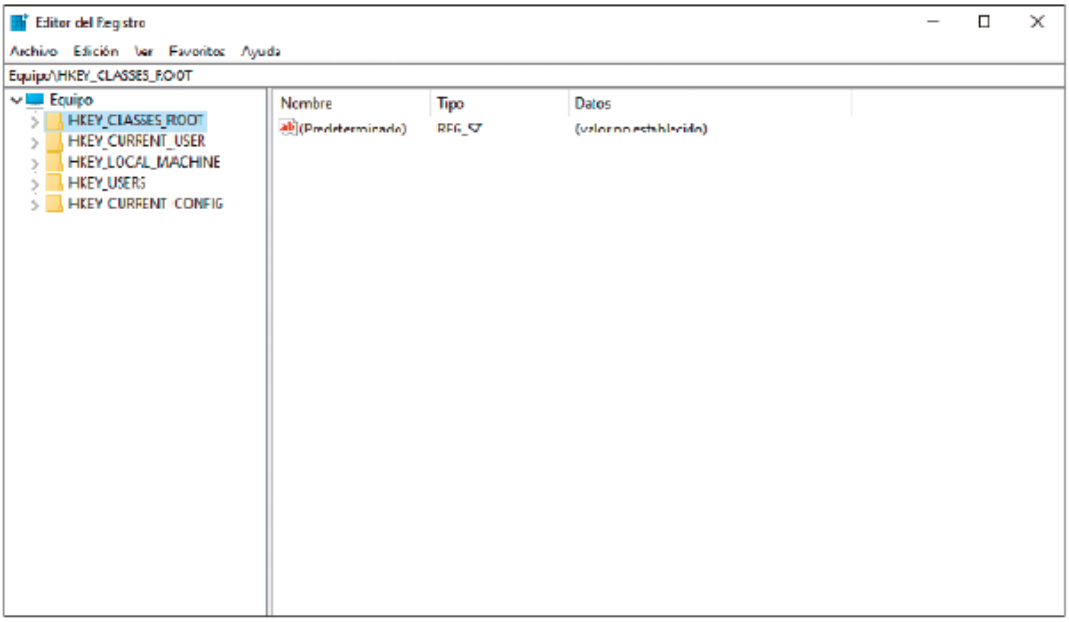
Nota

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

El registro de *Windows* contiene todo tipo de configuraciones del sistema operativo útiles para, por ejemplo:

- Saber qué aplicaciones están instaladas, los documentos que se pueden crear y con cuál de ellas se puede abrir cada tipo de archivos.
- Definir qué programas deben iniciarse al encender el equipo.
- Limpiar el arranque de *Windows* para que el inicio sea más rápido.
- Gestionar los distintos dispositivos de *hardware* del ordenador y los *drivers* y recursos que utilizan.
- Guardar las configuraciones de las cuentas de usuario que haya en el sistema.
- Determinar las características y el aspecto general de elementos como las carpetas, ventanas o el Escritorio de *Windows*.

Para entrar en el registro de *Windows* vaya a **Inicio -> Ejecutar**… e introduzca el comando **regedit**. Pulse en **Aceptar** y aparecerá una consola del sistema, el **Editor del Registro**, con una serie de categorías agrupadas en forma de árbol como la que se puede ver en la siguiente imagen:



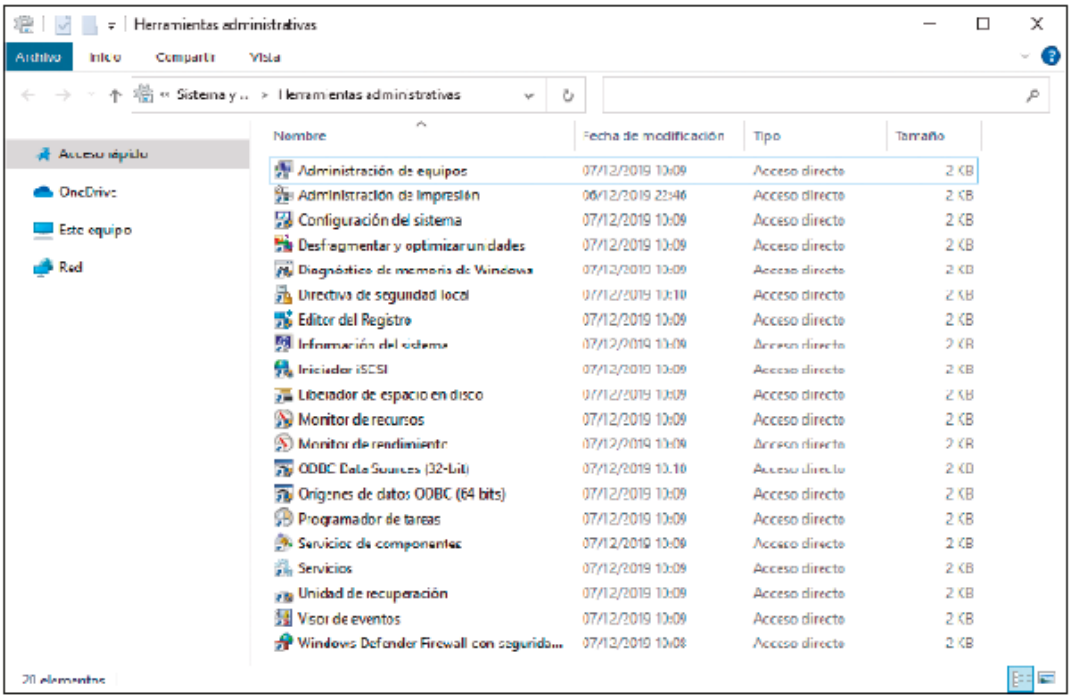
Editor del Registro de Windows

Para entrar en una carpeta o subcarpeta, haga doble clic sobre ellas. Las carpetas (o claves) principales son las siguientes:

- **HKEY_CLASSES_ROOT:** contiene información sobre las aplicaciones registradas y los sistemas de archivos. En esta carpeta se define qué programa debe abrir cada aplicación por defecto.
- **HKEY_CURRENT_USER:** contiene información sobre las configuraciones del usuario que está utilizando *Windows* en ese momento. Cualquier modificación de alguna configuración solo afectará a la sesión que inicie ese usuario. Se pueden encontrar datos como: componentes que se muestran en el Panel de control, las unidades del sistema, el idioma del teclado, la configuración de la red, etc.
- **HKEY_LOCAL_MACHINE:** es uno de los apartados más importantes del equipo porque contiene información sobre las configuraciones de *software, hardware* y las cuentas de usuario que puede haber en el ordenador. La información de este apartado se aplica a todos los usuarios del equipo.
- **HKEY_USERS:** contiene los datos sobre los distintos perfiles de usuario que haya en *Windows*.
- **HKEY_CURRENT_CONFIG:** contiene información acerca del *hardware* del equipo. Es una carpeta dinámica que se va creando y configurando a tiempo real según las necesidades del sistema operativo.

Aparte del Editor del registro, si hay sospechas de que existe algún usuario no autorizado que esté utilizando el equipo, es muy útil revisar los registros del sistema para ver qué ha ocurrido en él cuando lo ha utilizado otro usuario.

Para ello, se puede utilizar el Visor de eventos de *Windows* haciendo **Inicio -> Configuración -> Panel de control -> Herramientas administrativas -> Visor de eventos:**

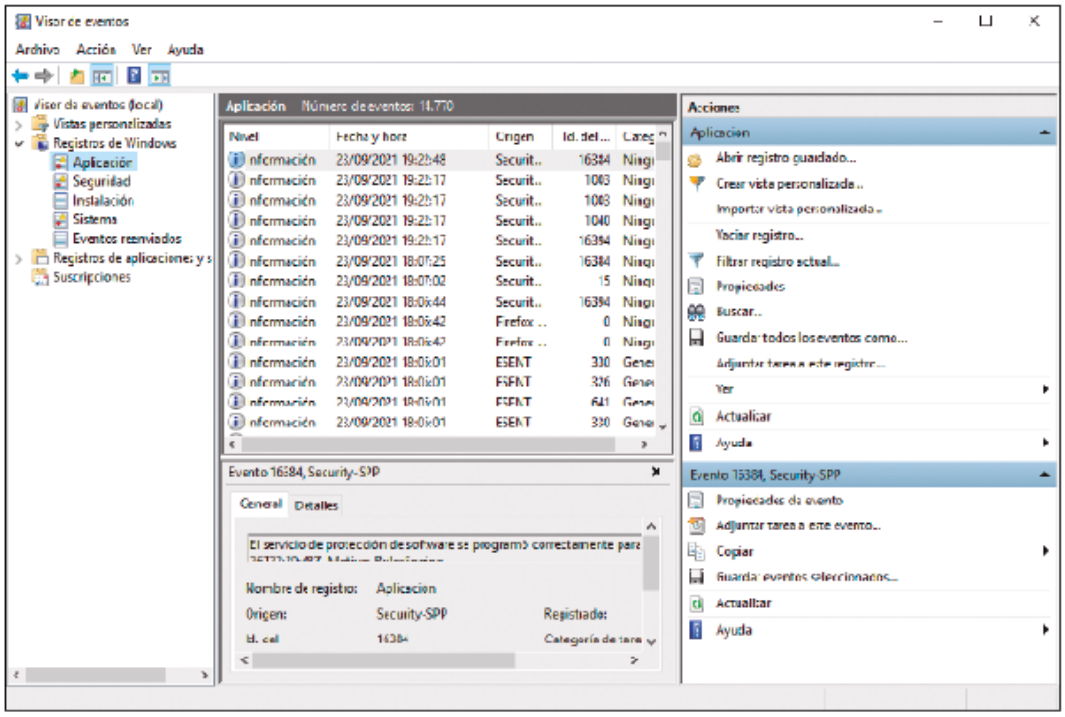


Panel de control, Herramientas administrativas

En el **Visor de eventos** se pueden observar distintos tipos de registros, en la carpeta Registro de *Windows:*

- **Registros de aplicación:** contiene los eventos registrados por aplicaciones o programas.
- **Registros de seguridad:** contiene los eventos ocurridos en los accesos del sistema. Por ejemplo, intentos de inicio de sesión, introducción de contraseñas erróneas, etc. También contiene eventos relativos a la utilización de los recursos.
- **Registros de instalación:** incluye los eventos relacionados con la instalación de aplicaciones en el equipo. Se utiliza frecuentemente para comprobar si hay algún *software* malicioso instalado.

- **Registros de sistema:** contiene los eventos que han sido generados por componentes del sistema operativo como, por ejemplo, errores al cargar alguno de sus componentes.
- **Registros de eventos reenviados:** contiene eventos que han sido reenviados a este registro desde otros equipos.



Visor de eventos

Además de los registros de *Windows*, en esta herramienta también se pueden ver los registros de aplicaciones y servicios, una nueva categoría de los registros de eventos.

Este tipo de registros almacenan eventos de una sola aplicación o componente en lugar de almacenar eventos que afectan a todo el sistema.

En el sistema operativo *Linux* se utilizan archivos de registro para registrar los eventos del sistema, entre ellos la conexión de dispositivos, sesiones nuevas y otros mensajes. En cada mensaje consta el programa que lo generó, la prioridad, la fecha y la hora.

Para acceder a los archivos de registro hay que iniciar la sesión como usuario *"root"*, ya que se trata de archivos protegidos.

Si se quieren ver las últimas líneas de un archivo y sus actualizaciones se utiliza el comando **tail –f**. Por ejemplo, si se quieren ver los eventos de autenticación como sesiones nuevas se utiliza: **tail –f/var/log/auth.log**.

Para finalizar la operación basta con pulsar la combinación de teclas [Ctrl] + [C].

Si en lugar de querer ver las últimas líneas de un archivo de registro se quiere acceder al registro entero, hay que utilizar el comando **less +F**. Con este comando se puede incluso ver cualquier actualización a tiempo real.

Para finalizarlo, se pulsa la combinación de teclas [Ctrl] + [C] y, a continuación, la tecla [Q].

Los archivos de registro varían según la versión de *Linux* que se utiliza. No obstante, la gran mayoría contienen al mínimo los archivos comunes que se reflejan en la tabla siguiente:

Nombre de archivo	**Funcionalidad**
/var/log/auth.log	Información sobre eventos de autenticación de usuarios y permisos.
/var/log/boot.log	Muestra eventos y servicios empezados cuando se inicia el sistema.
/var/log/crond.log	Tareas de cron.
/var/log/daemon.log	Muestra mensajes sobre permisos o servicios corriendo en el sistema.
/log/dmesg.log	Muestra mensajes del núcleo *Linux*.
/var/log/errors.log	Muestra errores del sistema.
/var/log/everything.log	Mensajes misceláneos no cubiertos por los otros archivos.
/var/log/httpd.log	Muestra 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	Muestra registros de *Xorg*.
/var/log/user.log	Muestra información acerca de los procesos usados por el usuario.

Actividades

8. Investigue sobre las distintas opciones y herramientas de gestión de registros que hay en su ordenador personal según el sistema operativo que tenga instalado y coméntelas.

Aplicación práctica

Se encuentra revisando las aplicaciones instaladas en uno de los equipos de la empresa en la que trabaja y se ha dado cuenta de que hay una aplicación que usted no ha instalado. Para saber quién la ha instalado y cuándo, quiere comprobar el historial del registro de la aplicación. Utilizando *Windows*, ¿qué herramienta usaría y cómo procedería para acceder al historial?

SOLUCIÓN

En caso de encontrar aplicaciones que no sabe quién las ha instalado y de querer visualizar el historial de la aplicación, utilice la herramienta **Visor de eventos**. Para acceder a ella vaya a **Inicio -> Configuración -> Panel de control -> Herramientas administrativas -> Visor de eventos**. El historial de registro de aplicación se encuentra dentro de la carpeta Registro de *Windows*, por lo que al cliquear sobre ella ya se puede visualizar sin problemas.

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

La tarea de recolección, obtención de resultados y análisis de los mismos con los registros es muy ardua y conlleva un coste bastante elevado. Por ello, es fundamental que la elección del sistema de almacenamiento de estos registros sea la apropiada (para que la custodia de los registros se realice correctamente y evitar pérdidas inesperadas de información), atendiendo a varios factores que se mencionarán en este apartado.

Pero antes de hablar de las distintas alternativas de sistemas de almacenamiento es importante mencionar los diferentes modelos de almacenamiento de datos en los sistemas de información:

- El modelo tradicional de archivos: este modelo está formado por varios elementos:
  - Variables: conjunto de registros que, al ser variables, pueden almacenar datos de tipos diversos.
  - Archivos: "Lugar" donde se almacenan los registros.
  - Aplicaciones: encargadas de gestionar y coordinar las variables y los archivos para que los usuarios puedan acceder a la información de un modo sencillo.
- Modelo de bases de datos relacionales: modelo utilizado para simplificar los sistemas de información, organizando los datos en tablas de bases de datos de modo que la entrada de datos sea más ágil y automatizada. Del mismo modo que en el modelo anterior, también son necesarias las aplicaciones que servirán como plataforma para introducir y tratar los datos y registros obtenidos.

Nota

En el mercado hay numerosas aplicaciones que gestionan las bases de datos relacionales. Son los llamados sistemas gestores de bases de datos o SGBD.

Atendiendo al modelo de almacenamiento de datos que se quiera utilizar para guardar y custodiar los registros, hay que elegir el sistema de almacenamiento de los registros. La mayoría de los registros se guardan en sistemas de almacenamiento

secundario por la elevada cantidad de información que conllevan. No obstante, la elección correcta del sistema de almacenamiento dependerá de una serie de factores y características:

- **Sistema operativo que se va a utilizar:** dependiendo del sistema operativo a utilizar, el formato de los archivos y registros será de un tipo u otro.
- **Requisitos legales/normativas:** según el tipo de registros que se vaya a tratar y almacenar, es posible que estos requieran un tipo de almacenamiento específico para que reciban una especial protección por el hecho de estar sujetos a una normativa estatal o internacional. Como recordatorio, las principales normativas a tener en cuenta en esta temática están relacionadas con:

    - Ley Orgánica de Protección de Datos de Datos Personales y garantía de los derechos digitales (LOPDGDD).
    - Normativas referentes a la propiedad intelectual.
    - Normativas que regulen temas relativos a la privacidad y confidencialidad de la información.
    - Normativas referentes al comercio electrónico.
      La globalización de los mercados requiere cada vez más tener un conocimiento concreto de las normativas internacionales, además de las nacionales, referentes al tratamiento de los datos y registros.

- **Capacidad de los recursos que se van a utilizar para almacenar y custodiar los registros:** el volumen de los datos y la capacidad que estos requieran para que se pueda trabajar con ellos con facilidad tendrán un papel importante en el momento de elegir un sistema de almacenamiento adecuado. Si el volumen de datos con el que se va a trabajar es grande o si se va a realizar un trabajo intenso con los mismos, será necesario un sistema de almacenamiento con capacidad suficiente que lo soporte.
- **Características de la red que se utilizará en la organización:** dependiendo del tipo de red (servidores remotos, redes locales, etc.) el sistema de almacenamiento a elegir tendrá características diferentes y requerirá unas medidas de seguridad distintas.
- **Complejidad del sistema de información:** el nivel de complejidad del sistema de información debe definir también el sistema de almacenamiento de los registros generados. Así, un sistema que tenga asignados numerosos perfiles de acceso y en el que intervengan varios equipos y dispositivos requerirá más capacidad y protección ante amenazas externas que un sistema de información que utilice un solo usuario en su equipo personal.

- **Tipo de alojamiento de los registros:** hay varios tipos distintos de alojamiento de los registros que también hay que tener en cuenta y son importantes cuando se quiere seleccionar un sistema de almacenamiento:

    - **Alojamiento tradicional:** el alojamiento tradicional de datos se utiliza cuando la organización dispone en sus instalaciones de equipos destinados al almacenamiento. La organización autogestiona el almacenamiento de sus registros.
    - **Alojamiento web o *"web hosting":*** el alojamiento web es un tipo de almacenamiento en el que los datos y registros se encuentran almacenados en Internet (páginas web, servidores, etc.) y se puede acceder a ellos de modo virtual desde cualquier equipo o dispositivo. Este tipo de alojamiento puede ser gratuito aunque no es lo habitual y los servicios ofrecidos están bastante limitados. Suelen ser alojamientos de pago en los que se alquila espacio de almacenamiento en un disco virtual o en un sitio web.
    - **Alojamiento en la nube o *"cloud hosting":*** el servicio de *cloud hosting* ofrece el almacenamiento de datos y registros y la utilización de aplicaciones a través de Internet sin necesidad de que estén almacenados en el equipo. Son un tipo de alojamiento web y también hay de varias clases:

        - **Nubes públicas:** los sistemas de almacenamiento y las aplicaciones en las nubes públicas se encuentran en servidores externos al usuario, que pueden ser de acceso gratuito o de pago. Su principal ventaja es la gran capacidad de almacenamiento y procesamiento que ofrecen sin que haya necesidad de equipos adicionales.
        - **Nubes privadas:** en este caso los servicios que ofrecen las nubes privadas están dentro de las instalaciones de la organización y no es frecuente que oferten servicios a terceros. Al tener los datos localizados dentro de la organización, hay un mayor nivel de protección y seguridad.
        - **Nubes híbridas:** son una combinación de las nubes públicas y privadas. La organización gestiona su infraestructura de modo exclusivo pero también tiene acceso a algunos recursos de la nube pública.

Nota

Al ser una combinación de tecnologías, el sistema de nubes híbridas ofrece las ventajas de las nubes públicas y privadas.

Aunque todos estos factores son decisivos en el momento de hacer la selección del sistema de almacenamiento, los más importantes son los requisitos legales y las necesidades de los recursos que se van a utilizar. No obstante, cada vez cobra más importancia la utilización del *cloud hosting* como sistema de almacenamiento de los registros en una organización.

Este tipo de alojamiento permite a los usuarios acceder a una serie de aplicaciones estandarizadas con un coste relativamente bajo y ofreciendo a las organizaciones una gran flexibilidad y adaptabilidad a sus datos y registros.

En resumen, esta tecnología ofrece a las organizaciones una serie de ventajas:

- **Reducción de costes:** al ser necesarias menos infraestructuras hay una reducción de costes importante. Habitualmente el coste irá relacionado con la cantidad de recursos requeridos por la organización.
- **Accesibilidad:** los archivos y registros almacenados en la nube ofrecen una mayor accesibilidad que los almacenados en discos locales, ya que el usuario podrá acceder a ellos desde cualquier punto con acceso a Internet.
- **Escalabilidad:** esta tecnología está implementada de modo que se puede ir adaptando a las necesidades de los recursos de la organización, ofreciéndoles la posibilidad de adquirir más o menos recursos de un modo sencillo.
- **Seguridad:** aunque no lo parezca, el nivel de seguridad de esta tecnología es muy elevado y de ello se encarga el proveedor del servicio que, al estar especializado en almacenamiento de datos, tendrá acceso a mejores medidas de seguridad que cualquier organización.
- **Autoservicio:** las organizaciones pueden acceder a los recursos de la nube sobre la marcha y de modo prácticamente automático, sin necesidad de contactar con el proveedor del servicio para ello.

Para sintetizar los distintos conceptos y factores que formarán parte de la elección de un sistema de almacenamiento, se pueden visualizar en la siguiente tabla:

Factores para la elección del sistema de almacenamiento:	Características
Sistema operativo	*Linux, Windows* y otros.
Requisitos legales	LOPDGDD, derechos de propiedad intelectual, comercio electrónico, confidencialidad y privacidad de la información.
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, alojamiento red y alojamiento en la nube (público, privado o híbrido).

Como conclusión general, una vez vistos todos los factores relevantes para elegir el sistema de almacenamiento que va a utilizar una organización, solo cabe remarcar de nuevo la importancia de realizar un análisis exhaustivo del tipo de datos y registros que se van a almacenar y de que estos estén validados correctamente. La elección de los registros y su validez son la base de todo sistema de información, que puede llevar a decisiones equívocas y a errores de grandes magnitudes si no se recogen, almacenan y analizan con rigor y teniendo en cuenta las directrices establecidas por la organización.

Actividades

9. Señale qué más factores pueden tenerse en cuenta cuando se quiere establecer un sistema de almacenamiento de registros. Busque más información y ponga varios ejemplos.

Aplicación práctica

Pablo, Marta y usted están valorando las distintas opciones de alojamiento de los registros que se van originando en su empresa. No quieren tener costes demasiado elevados y, por ello, prefieren no tener infraestructura de almacenamiento en la organización. Además, quieren tener la posibilidad de acceder a una serie de aplicaciones desde cualquier ubicación ya que como directivos están viajando continuamente. ¿Qué tipo de alojamiento de datos sería el adecuado en este caso?

SOLUCIÓN

El tipo de alojamiento de datos más adecuado en esta ocasión es el servicio en la nube, ya que es la única tipología que permite la ejecución de aplicaciones, además del almacenamiento de archivos, de modo remoto, sin necesidad de tener una infraestructura instalada dentro de la organización y con un coste relativamente reducido.

8. Resumen

Los procesos de monitorización de sistemas de información ofrecen una serie de documentos que son de utilidad para los directivos en el momento de la toma de decisiones. Los registros son formatos o impresos cumplimentados como resultado de la realización de una tarea de un sistema de la organización. Todas las tareas que realice una organización quedarán documentadas en un registro, que debe cumplir con una serie de propiedades: identificación, almacenamiento, protección, recuperación, retención y disposición.

El almacenamiento de registros especiales puede suponer a la organización la obligación del cumplimiento de unas condiciones legales reflejadas en las distintas normativas vigentes, la más importante la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.

El cumplimiento de estos requerimientos legales será una de las medidas de un plan de seguridad de la organización, pero no la única: en el documento de seguridad también es necesario el establecimiento de una serie de medidas que aumenten la seguridad del sistema de registros, acordes con su valor y con el daño que se puede ocasionar en caso de su pérdida. Estas medidas de seguridad pueden ser administrativas, físicas o técnicas.

Debido al cuidado que hay que tener con el tratamiento y almacenamiento de los registros, las organizaciones deben asignar responsables que se encarguen de garantizar los requerimientos legales y de seguridad establecidos, evitando así problemas de descontrol.

Los registros hay que almacenarlos de modo que se garantice el rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad del sistema y, dependiendo del sistema operativo utilizado, las alternativas de almacenamiento del registro pueden ser distintas: mientras que en *Windows 10* se puede utilizar una aplicación para gestionar los registros, en *Linux* es necesaria la utilización de comandos.

Además, y a modo de conclusión, la elección del sistema de almacenamiento y custodia de estos registros debe realizarse teniendo en cuenta las características de la organización y de los registros.