

### DATOS IDENTIFICATIVOS DE LA UNIDAD FORMATIVA

UNIDAD FORMATIVA	AUDITORÍAS Y CONTINUIDAD DE NEGOCIO	DURACIÓN	50
		Condicionada	
Código	UF1895		
Familia profesional	INFORMÁTICA Y COMUNICACIONES		
Área Profesional	Sistemas y telemática		
Certificado de profesionalidad	GESTIÓN DE SISTEMAS INFORMÁTICOS	Nivel	3
Módulo formativo	Administración software de un sistema informático	Duración	120
Resto de unidades formativas que completan el módulo	Instalación y parametrización del software	Duración	90
	Mantenimiento del software	Duración	70

#### Apartado A: REFERENTE DE COMPETENCIA

Esta unidad formativa se corresponde con la RP6 y la RP7.

#### Apartado B: ESPECIFICACIÓN DE LAS CAPACIDADES Y CONTENIDOS

### Capacidades y criterios de evaluación

C1: Analizar y definir las políticas de realización de copias de respaldo y de recuperación de datos en función de las especificaciones de seguridad.

CE1.1 Clasificar los diferentes tipos de sistemas de copias de respaldo, basándose en el soporte empleado, en la topología o arquitectura y sistemas soportados (fichero, partición de disco y base de datos entre otros).

CE1.2 Describir los niveles de copias de respaldo explicando las diferencias entre ellos.

CE1.3 Asociar la política de realización de copias a los sistemas implicados, justificando las decisiones y cumpliendo la normativa vigente en materia de protección de datos de carácter personal.

CE1.4 A partir de un supuesto práctico en el que se da un escenario de sistemas de almacenamiento de información en el plan de explotación de una organización:

- Estimar el volumen de información a copiar por unidad de tiempo.
- Identificar áreas de almacenamiento de los soportes utilizados para las copias de respaldo.
- Planificar el acceso autorizado a los soportes.
- Mantener el registro de información respecto al contenido, versiones y ubicación de los archivos de datos.
- Organizar el inventario de medios de almacenamiento y archivos almacenados.
- Verificar que las copias de respaldo reciben el mismo nivel de seguridad que los archivos originales.

C2: Aplicar procedimientos de auditoría utilizando técnicas y herramientas adecuadas para garantizar los parámetros de funcionamiento del sistema informático.

CE2.1 Enumerar y explicar los objetivos a cumplir con la habilitación de auditorías del sistema.

CE2.2 Clasificar según prioridad, los eventos del sistema y de las aplicaciones susceptibles de ser auditados para el mantenimiento del óptimo funcionamiento del sistema.

CE2.3 Determinar, para cada evento detectado, la necesidad de llevar a cabo acciones correctivas, estableciendo las mismas en caso afirmativo.

CE2.4 En un supuesto práctico de aplicación de procedimientos de auditoría en un sistema debidamente caracterizado:

- Establecer las políticas de auditoría de forma adecuada para no sobrecargar el funcionamiento del sistema y afectar a su rendimiento.
- Seleccionar una lista de eventos a auditar que proporcionen información útil: inicio y detección de servicios, accesos a recursos, conexión y desconexión de usuarios, eventos de aplicaciones y eventos del sistema.
- Fijar las acciones correctivas necesarias asociadas a los eventos detectados.
- Aplicar e integrar las herramientas disponibles al sistema según el plan de auditoría establecido.
- Establecer alarmas para resaltar la detección de eventos prioritarios o críticos.
- Operar con las herramientas disponibles para la planificación, definición e implementación de auditorías.
- Analizar los registros de auditoría extrayendo información acerca del funcionamiento y estado del sistema para la realización del informe de auditoría.
- Interpretar documentación técnica del sistema y herramientas de auditoría.

## Contenidos:

### 1. Copias de respaldo

- Tipificar los datos según sus necesidades de copia.
- Diferenciar los distintos tipos de copias, distinguiendo las diferencias entre copias completas, incrementales, y diferenciales, así como las ventajas e inconvenientes de cada una de ellas, y las combinaciones más habituales de las mismas.
- Establecer correctamente los periodos de retención acordes con las normas de seguridad de la empresa, con las necesidades según el tipo de datos, y con la legislación vigente.
- Dimensionar las copias de seguridad:
  - Establecer el tamaño de copia completa acorde con los datos a copiar y la ocupación estimada en el dispositivo de copias.
  - Establecer el tamaño de las copias en función del tiempo, acorde con la política de copias a utilizar.
- Establecer la política de copias de la organización:
  - Definir el plan de copias indicando cada tipo de copia a realizar, la hora de programación, la ventana de copia, el periodo de retención.
  - Revisar la adecuación de la política de copias a las normas de la organización, así como a la legalidad vigente.
- Proponer los dispositivos de copia y soportes más adecuados en base a las necesidades de la organización:
  - Conocer las distintas alternativas posibles para los dispositivos de copia.
  - Razonar la mejor adecuación de cada alternativa a las necesidades de la organización.
- Realizar las copias de seguridad según los procedimientos y políticas vigentes en la organización:
  - Implementar y configurar las copias de seguridad.
  - Programar y ejecutar las copias de seguridad.
  - Verificar las copias de seguridad mediante restauraciones, documentando los tiempos de restauración y el resultado obtenido.
- Gestionar el ciclo de vida de los soportes:
  - Salvaguardar los soportes de copia, manteniéndolos en condiciones óptimas para su conservación.
  - Externalizar las copias.
  - Destruir los soportes tras su ciclo de vida útil de manera acorde con las normas de seguridad de la empresa, garantizando la imposibilidad de extracción de información de los mismos.
- Documentación de planes de recuperación:
  - Diseñar los pasos a seguir para la completa restauración de un sistema en producción.
  - Documentar las restauraciones a realizar para el restablecimiento de un sistema en producción, tras un problema mayor.

### 2. Legislación vigente

- Conocer las Leyes vigentes relacionadas con el tratamiento de datos:
  - Legislación vigente en materia de protección de datos de carácter personal.
  - Legislación vigente en materia de comercio electrónico.
  - Legislación vigente en materia de protección de la propiedad intelectual.
- Enumerar los puntos principales a tener en cuenta.

### 3. Alternativas a las copias

- Distinguir entre salvaguarda de datos, y disponibilidad del servicio.
- Enumerar las alternativas para garantizar la disponibilidad del servicio:
  - Diseñar alternativas en cluster.
  - Diseñar alternativas basadas en almacenamiento externo.
  - Diseñar alternativas basadas en copias de imágenes.
- Indicar ventajas e inconvenientes de las alternativas para garantizar la disponibilidad del servicio sobre las copias de seguridad.

### 4. Planes de auditoría

- Describir los objetivos de los planes de auditoría:
  - Distinguir entre las auditorías por su tipo y aplicación (de rendimiento, de seguridad, de mejora continua, de optimización de uso)
- Describir el perfil del auditor.
- Auditar el sistema:
  - Diseñar el plan de auditoría.
  - Utilizar herramientas de auditoría.
  - Documentar el resultado de la auditoría.

### Apartado C: **REQUISITOS Y CONDICIONES**

Deberá cumplir alguno de los requisitos siguientes:

- Estar en posesión del título de Bachiller.
- Estar en posesión de algún certificado de profesionalidad de nivel 3.
- Estar en posesión de un certificado de profesionalidad de nivel 2 de la misma familia y área profesional.
- Cumplir el requisito académico de acceso a los ciclos formativos de grado superior o haber superado las correspondientes pruebas de acceso a ciclos de grado superior.
- Tener superada la prueba de acceso a la universidad para mayores de 25 años y/o de 45 años.
- Tener, de acuerdo con la normativa que se establezca, los conocimientos formativos o profesionales suficientes que permitan cursar con aprovechamiento la formación.

En relación con las exigencias de los formadores o de las formadoras, instalaciones y equipamientos se atenderá las exigencias solicitadas para el propio certificado de profesionalidad.