

CUALIFICACIÓN PROFESIONAL:

Operaciones auxiliares con tecnologías digitales

<i>Familia Profesional:</i>	Informática y Comunicaciones
<i>Nivel:</i>	1
<i>Código:</i>	IFC821_1
<i>Estado:</i>	BOE
<i>Publicación:</i>	RD 546/2023

Competencia general

Realizar operaciones auxiliares con tecnologías digitales en cualquier entorno productivo que requiera el uso de herramientas digitales para la búsqueda, tratamiento y almacenaje de información, creación, edición, publicación y difusión de contenidos digitales, utilizando herramientas colaborativas como soporte de desarrollo para tareas propias del entorno laboral, garantizando la seguridad y la operatividad del 'hardware', cumpliendo la normativa aplicable en materia de propiedad intelectual e industrial, normativa de servicios de la sociedad de la información, protección de datos, accesibilidad y planificación de la actividad preventiva y estándares de calidad.

Unidades de competencia

UC2741_1: Operaciones auxiliares de manejo de información, creación de contenidos y comunicación usando medios digitales

UC2742_1: Operaciones auxiliares de seguridad y de resolución de problemas 'hardware'

Entorno Profesional

Ámbito Profesional

Desarrolla su actividad profesional en cualquier tipo de organización que requiera el uso de herramientas digitales y la aplicación de planes de economía circular, en entidades de naturaleza pública o privada, empresas de tamaño pequeño/mediano/grande o microempresas, tanto por cuenta propia como ajena, con independencia de su forma jurídica. Desarrolla su actividad dependiendo, en su caso, funcional y/o jerárquicamente de un superior. En el desarrollo de la actividad profesional se aplican los principios de accesibilidad universal de acuerdo con la normativa aplicable.

Sectores Productivos

Se ubica en los sectores productivos que requieran el uso de herramientas digitales y la aplicación de planes de economía circular.

Ocupaciones y puestos de trabajo relevantes

Los términos de la siguiente relación de ocupaciones y puestos de trabajo se utilizan con carácter genérico y omnicomprendivo de mujeres y hombres.

- Trabajadores vinculados a todos los sectores productivos

Formación Asociada (30 horas)

Módulos Formativos

MF2741_1: Manejo de información, creación de contenidos y comunicación usando medios digitales (15 horas)

MF2742_1: Seguridad y resolución de problemas 'hardware' (15 horas)

UNIDAD DE COMPETENCIA 1

Operaciones auxiliares de manejo de información, creación de contenidos y comunicación usando medios digitales

Nivel: 1

Código: UC2741_1

Estado: Tramitación BOE

Realizaciones profesionales y criterios de realización

RP1: Acceder a información y datos, buscando desde repositorios o fuentes digitales, Internet o intranet, usando herramientas de acceso y búsqueda y almacenando la información para su uso posterior, cumpliendo la normativa de protección de datos y propiedad intelectual.

CR1.1 Los datos, información y contenido en entornos o fuentes digitales tales como Internet, intranet, extranet o repositorios, se buscan, partiendo de las necesidades de información, usando navegadores y/u otras herramientas de acceso, ajustando las búsquedas según los resultados y navegando mediante hiperenlaces en su caso entre los resultados según estrategias de búsqueda de baja complejidad, seleccionando, en su caso, fuentes confiables.

CR1.2 Los datos e información obtenida de entornos o fuentes digitales o Internet se almacenan en su conjunto o por elementos aislados, seleccionando el medio y ubicación concreta de almacenamiento, de modo que se facilite su localización posterior.

CR1.3 Los datos e información almacenada bajo petición o ante una necesidad de acceso a los mismos, se recupera localizando su ubicación, para adaptarlos, agregarlos o editarlos en forma de contenidos en su caso y/o enviarlos a la persona que inicia dicha petición o bien para su difusión.

RP2: Crear contenidos digitales a partir de componentes elementales, usando herramientas de edición y publicación en su caso, cumpliendo la normativa de protección de datos y propiedad intelectual.

CR2.1 Las herramientas de edición y publicación de contenidos tales como editores de texto, audio, vídeo, gestores de contenido (CMS) o paquetes ofimáticos se instalan, descargándolos desde fuentes confiables o usando soportes obtenidos del distribuidor, configurándolos para su utilización.

CR2.2 Los textos, imágenes, elementos de audio o vídeo, se editan, localizando su ubicación en sistemas de almacenamiento local o repositorios 'online', alterando o adaptando sus características generales o globales tales como tamaño y las relacionadas con la apariencia o formato de almacenamiento, respetando el tipo de licencia de uso en su caso.

CR2.3 Las plantillas de contenido se elaboran, incluyendo los componentes comunes a los documentos finales y almacenándolas en una ubicación que permita su reutilización.

CR2.4 Los elementos de contenido tales como texto, imágenes, audio o vídeo se integran para formar contenidos, garantizando la coherencia del resultado, usando herramientas ofimáticas, gestores de contenido o funcionalidades de la herramienta de publicación o sitio 'web' en función del formato resultante solicitado o deseado.

RP3: Utilizar herramientas colaborativas, de comunicaciones y redes sociales para trabajo en grupo y difusión de contenidos, configurando los permisos y roles de acceso, cumpliendo normativa de protección de datos y propiedad intelectual e industrial.

CR3.1 Los sistemas de correo electrónico, videoconferencia, mensajería y otros se utilizan para comunicarse con otras personas o grupos de ellas, configurando los datos propios mostrados tales como nombre, apellidos, apodo, avatar o imagen, seleccionando las personas que reciben o acceden a la información.

CR3.2 La identidad digital en redes sociales se configura, restringiendo o potenciando los contenidos publicados y los datos personales expuestos, según la imagen pública que se desee proyectar y comprendiendo los beneficios y los riesgos derivados de su exposición en estas redes.

CR3.3 Las redes sociales se utilizan para difundir mensajes o contenidos, previo registro, configurando los parámetros de visualización de la información mostrada a terceros, cumpliendo las normas de protocolo digital en las comunicaciones ('Netiquette').

Contexto profesional

Medios de producción

Dispositivos digitales: equipos informáticos, tableta, móvil. Dispositivos conectables asociados. 'Software' de base y aplicaciones de uso general. Herramientas de tratamiento de datos: editores y hojas de cálculo. Herramientas ofimáticas. Cliente de correo electrónico, mensajería, chat y videoconferencia. Conexión a Internet. Navegador. Buscadores. Redes sociales. Herramientas de gestión de contenidos (CMS). Editores de imagen, audio y vídeo.

Productos y resultados

Información y datos accedidos y almacenados. Contenidos digitales creados y publicados. Herramientas colaborativas utilizadas.

Información utilizada o generada

Normas externas de trabajo (normativa aplicable de propiedad intelectual e industrial, normativa de protección de datos, normativa sobre prevención de riesgos laborales -ergonomía-). Normas internas de trabajo (códigos de conducta para un uso seguro de la información, documentación de especificaciones de trabajo y procedimientos de operación, plan de calidad, plan de seguridad). Documentación técnica (manuales y ayudas del 'software' de uso general, manuales y ayudas de las herramientas ofimáticas, CMS, de comunicaciones y colaborativas).

UNIDAD DE COMPETENCIA 2

Operaciones auxiliares de seguridad y de resolución de problemas 'hardware'

Nivel: 1

Código: UC2742_1

Estado: Tramitación BOE

Realizaciones profesionales y criterios de realización

RP1: Resolver incidencias técnicas en el uso de dispositivos informáticos, identificando el origen del problema y aplicando una solución o escalándola en su caso, bajo supervisión de la persona responsable de los sistemas y siguiendo procedimientos estandarizados.

CR1.1 El subsistema físico de los equipos informáticos se mantiene, comprobando las condiciones ambientales de temperatura y humedad, ajustando dichas condiciones o reubicando el equipo en su caso, limpiando periódicamente las rejillas de ventilación y refrigeración, prestando atención a signos perceptibles de deterioro, tales como olor a quemado, desgastes evidentes, ruidos o sonidos no habituales y escalando el problema a la persona responsable de la entidad o al servicio técnico del propio fabricante si el problema persiste.

CR1.2 Los dispositivos conectados al sistema se mantienen, aplicando labores de limpieza, comprobación y sustitución de fungibles y partes sometidas a desgaste, sustituyendo los elementos deteriorados o gastados.

CR1.3 Los problemas de conexionado de cableado a la red de datos o con dispositivos asociados se solucionan, previa detección del problema, comprobando el ajuste mecánico de la conexión, sustituyendo el cable por otro en buen estado, escalando el problema a la persona responsable de la entidad o al servicio técnico del propio fabricante si el problema persiste.

CR1.4 Los problemas de conexionado inalámbrico a la red de datos o con dispositivos asociados se solucionan, previa detección del problema, comprobando y reconfigurando en su caso según indicaciones del fabricante, escalando el problema a la persona responsable de la entidad o al servicio técnico del propio fabricante si el problema persiste.

CR1.5 Las aplicaciones instaladas en los equipos informáticos se mantienen, configurando y aplicando actualizaciones de 'software', comprobando la capacidad de almacenamiento disponible y organizando y haciendo limpieza en su caso de datos y archivos en el sistema de ficheros físico o en la nube.

RP2: Configurar elementos de seguridad en equipos informáticos, siguiendo directrices de la entidad responsable de los sistemas, usando herramientas o aplicando buenas prácticas para proteger la confidencialidad e integridad y disponibilidad de la información.

CR2.1 Los programas antimalware se instalan, descargándolos de la página del fabricante, configurando las opciones de detección y acción ante amenazas detectadas y la actualización de patrones de virus.

CR2.2 El 'software' de base y las aplicaciones de los equipos informáticos se configuran para la instalación periódica de actualizaciones y parches de seguridad, indicando la periodicidad y el grado de automatización del proceso.

CR2.3 Las reglas de acción ante la recepción de correos sospechosos o no deseados se configuran o, en su caso, se aplican, indicando los parámetros de detección y las acciones asociadas, identificando y seleccionando orígenes no confiables, no abriendo o siguiendo hiperenlaces de ese tipo de fuentes.

CR2.4 La navegación por Internet se configura para la protección de la privacidad, seleccionando las acciones por defecto ante la petición de almacenaje de 'cookies' y el modo de navegación disponible, excluyendo visitar páginas 'web' no confiables y activando la protección antimalware para la navegación y el uso de protocolos de comunicaciones seguros (HTTPS).

CR2.5 Los datos en formularios online se introducen únicamente en páginas confiables, procurando que la información proporcionada sea la imprescindible para que se preste el servicio solicitado, no aceptando condiciones de servicio desproporcionadas o no comprensibles.

CR2.6 Las comunicaciones inalámbricas y los sitios web del usuario se protegen, activando el uso de cifrados seguros y estableciendo contraseñas fuertes, cambiándolas periódicamente y protegiendo el acceso a las mismas.

RP3: Mantener el inventariado de equipos y dispositivos asociados, etiquetando los elementos para facilitar su localización y referenciado en caso de avería, según instrucciones de la entidad responsable de los sistemas y cumpliendo la normativa medioambiental.

CR3.1 Los equipos y dispositivos asociados en uso o en almacenaje se etiquetan para facilitar su control, utilizando herramientas específicas al efecto y siguiendo normas de nomenclatura y catalogación.

CR3.2 Los equipos y dispositivos asociados que no están en uso, se embalan utilizando los recursos y materiales al efecto, almacenándolos en condiciones de seguridad.

CR3.3 Los equipos y dispositivos asociados que se requiera sustituir o añadir se localizan en el almacén o bien se reciben del proveedor, desembalándolos e instalándolos, configurándolos en su caso según indique el fabricante.

CR3.4 Los embalajes, residuos y elementos desechables se tratan para su gestión o reciclaje, depositándolos en contenedores según su naturaleza, eliminando contenidos o datos personales.

Contexto profesional

Medios de producción

Dispositivos digitales: equipos informáticos, tableta, móvil. Dispositivos conectables asociados. 'Software' de base y aplicaciones de uso general. Herramientas 'software'. Herramientas de etiquetado y aplicaciones de inventariado. Conexión WIFI, red de datos y conexión a Internet. Navegadores. Clientes de correo electrónico. Programas antimalware.

Productos y resultados

Incidencias técnicas en el uso de dispositivos informáticos resueltas. Elementos de seguridad en equipos informáticos configurados. Inventariado de equipos y dispositivos asociados mantenido.

Información utilizada o generada

Normas externas de trabajo (normativa aplicable de propiedad intelectual e industrial, normativa de protección de datos, normativa sobre prevención de riesgos laborales, normativa medioambiental).

Normas internas de trabajo (documentación de especificaciones de trabajo y procedimientos de operación, plan de calidad, plan de seguridad). Documentación técnica (manuales y ayudas del 'hardware', manuales y ayudas de las herramientas ofimáticas, CMS, de comunicaciones y colaborativas).

MÓDULO FORMATIVO 1

Manejo de información, creación de contenidos y comunicación usando medios digitales

Nivel:	1
Código:	MF2741_1
Asociado a la UC:	UC2741_1 - Operaciones auxiliares de manejo de información, creación de contenidos y comunicación usando medios digitales
Duración (horas):	15
Estado:	Tramitación BOE

Capacidades y criterios de evaluación

C1: Aplicar procedimientos auxiliares de acceso a información y datos, buscando desde repositorios o fuentes digitales, Internet o intranet, usando herramientas de acceso y búsqueda y almacenando la información para su uso posterior, cumpliendo la normativa de protección de datos y propiedad intelectual.

CE1.1 Reconocer la diferencia entre Internet, intranet y extranet, caracterizando cada una.

CE1.2 Enumerar herramientas de navegación y acceso a información y búsqueda, describiendo sus características y funcionalidades, explicando el uso del hipertexto, reconociendo las estructuras más habituales de presentación y los elementos que la componen.

CE1.3 Clasificar fuentes de información, discriminado según su grado de confiabilidad, el formato de datos que proporciona y la herramienta de acceso.

CE1.4 Enumerar medios físicos y lógicos para el almacenamiento de datos e información, describiendo la estructura organizativa y utilidades que permitan una eficaz recuperación de la misma.

CE1.5 Respetar los tipos de licencia que protegen la información o datos que se manejen, cumpliendo los reconocimientos y usos que permitan y aplicando la normativa de protección de datos personales respecto al acceso y almacenamiento, diferenciando las operaciones que garantizan su cumplimiento.

CE1.6 En un supuesto práctico de aplicación de procedimientos auxiliares de acceso a información y datos, buscando desde repositorios o fuentes digitales, Internet o intranet, usando herramientas de acceso y búsqueda y almacenando la información para su uso posterior, cumpliendo la normativa de protección de datos y propiedad intelectual:

- Buscar datos, información y contenido en entornos o fuentes digitales tales como Internet, extranet, intranet y repositorios, a partir de unas necesidades de información, usando navegadores y/u otras herramientas de acceso, ajustando las búsquedas según los resultados y navegando mediante hiperenlaces en su caso entre los resultados según estrategias de búsqueda de baja complejidad, seleccionando, en su caso, fuentes confiables.

- Almacenar los datos e información obtenida de entornos o fuentes digitales o Internet en su conjunto o por elementos aislados, seleccionando el medio y ubicación concreta de almacenamiento, de modo que se facilite su localización posterior.

- Recuperar unos datos o información almacenada bajo petición o ante una necesidad de acceso a los mismos, localizando su ubicación, para adaptarlos, agregarlos o editarlos en forma de

contenidos en su caso y/o enviarlos a la persona que inicia dicha petición o bien para su difusión.

C2: Aplicar procedimientos auxiliares para la creación de contenidos digitales a partir de componentes elementales, usando herramientas de edición y publicación en su caso, cumpliendo la normativa de protección de datos y propiedad intelectual.

CE2.1 Enumerar herramientas de edición y publicación de contenidos tales como editores de texto, audio, vídeo, gestores de contenido ('Content Management Systems' -CMS-) o paquetes ofimáticos, explicando los pasos para su instalación y configuración.

CE2.2 Describir procedimientos de edición de textos, imágenes, elementos de audio o vídeo, partiendo de su ubicación en almacenamiento local o repositorios 'online', explicando cómo alterar características generales o globales tales como tamaño y las relacionadas con la apariencia o formato de almacenamiento, respetando el tipo de licencia de uso en su caso.

CE2.3 Explicar el proceso de elaboración de plantillas de contenido, incluyendo los componentes comunes a los documentos finales, para almacenarlas en una ubicación que permita su reutilización.

CE2.4 Aplicar técnicas de inserción de elementos de contenido tales como texto, imágenes, audio o vídeo para formar contenidos, garantizando la coherencia del resultado, usando herramientas ofimáticas, gestores de contenido o funcionalidades de la herramienta de publicación o sitio 'web' en función del formato resultante solicitado o deseado.

CE2.5 Respetar los tipos de licencia que protegen la información o datos que se manejen, cumpliendo los reconocimientos y usos que permitan y aplicando la normativa de protección de datos personales respecto a su utilización, diferenciando las operaciones que garantizan su cumplimiento.

CE2.6 En un supuesto práctico de aplicación de procedimientos auxiliares para la creación de contenidos digitales a partir de componentes elementales, usando herramientas de edición y publicación en su caso, cumpliendo la normativa de protección de datos y propiedad intelectual:

- Instalar una herramienta de edición y publicación de contenidos tal como editor de texto, audio, vídeo, gestores de contenido (CMS) o paquete ofimático, descargándola desde una fuente confiable o usando soportes obtenidos del distribuidor, configurándola para su utilización.

- Editar los textos, imágenes, elementos de audio o vídeo, localizando su ubicación en sistemas de almacenamiento local o repositorios "online", alterando o adaptando sus características generales o globales tales como tamaño y las relacionadas con la apariencia o formato de almacenamiento, respetando el tipo de licencia de uso en su caso.

- Elaborar unas plantillas de contenido, incluyendo componentes comunes a los documentos finales y almacenándolas en una ubicación que permita su reutilización.

- Integrar elementos de contenido tales como texto, imágenes, audio o vídeo para formar contenidos, garantizando la coherencia del resultado, usando herramientas ofimáticas, gestores de contenido o funcionalidades de la herramienta de publicación o sitio "web" en función del formato resultante deseado.

C3: Aplicar procedimientos de difusión de contenidos y de trabajo en grupo utilizando herramientas colaborativas, de comunicaciones y redes sociales, considerando el alcance de compartición, cumpliendo normativa de protección de datos y propiedad intelectual e industrial.

CE3.1 Enumerar aplicaciones de correo electrónico, videoconferencia, mensajería y otros, describiendo el procedimiento para utilizarlas para comunicarse con otras personas o grupos de

ellas, configurando los datos propios mostrados tales como nombre, apellidos, apodo, avatar o imagen, seleccionando las personas que reciben o acceden a la información.

CE3.2 Explicar el proceso de configuración de la información personal y la publicación de contenidos en redes sociales, indicando cuál sería en cada caso la información mínima requerida y el contenido que se adapta al medio usado, de manera que se limite la exposición de los propios datos personales y se controle la imagen que de uno mismo se ofrece al exterior (identidad digital), entendiendo los beneficios y los riesgos derivados de su exposición en estas redes.

CE3.3 Clasificar redes sociales, indicando el proceso de registro y configuración de parámetros de visualización de la información mostrada a terceros, explicando su utilización para difundir mensajes o contenidos cumpliendo las normas de protocolo digital en las comunicaciones ('Netiquette').

CE3.4 En un supuesto práctico de aplicación de procedimientos de trabajo en grupo utilizando herramientas colaborativas, de comunicaciones y redes sociales, considerando el alcance de la comunicación, cumpliendo normativa de protección de datos y propiedad intelectual e industrial:

- Instalar sistemas de correo electrónico, videoconferencia o mensajería, configurando los parámetros mínimos para su operatividad, añadiendo los datos propios mostrados tales como nombre, apellidos, apodo, avatar o imagen.
- Conectarse con otras personas o grupos de ellas usando las herramientas instaladas, seleccionando las personas que reciben o acceden a la información e interactuando cumpliendo unas normas de protocolo digital en las comunicaciones ('Netiquette').
- Cerrar en su caso la sesión de comunicaciones síncronas, pulsando la opción requerida según el tipo de herramienta, para impedir el acceso de personas no autorizados y la suplantación de identidad.

CE3.5 En un supuesto práctico de aplicación de procedimientos de difusión de contenidos utilizando redes sociales, considerando el alcance de compartición, cumpliendo normativa de protección de datos y propiedad intelectual e industrial:

- Registrarse en una red social, limitando la exposición de datos personales y configurando las opciones de privacidad.
- Crear una identidad digital en redes sociales, restringiendo o potenciando los contenidos publicados, según la imagen pública que se desee proyectar.
- Utilizar la red social para difundir mensajes o contenidos, cumpliendo las normas de protocolo digital en las comunicaciones ('Netiquette').

Capacidades cuya adquisición debe ser completada en un entorno real de trabajo

C1 respecto a CE1.6; C2 respecto a CE2.6; C3 respecto a CE3.4 y CE3.5.

Otras Capacidades:

Curiosidad acerca de los sistemas de información y su funcionamiento.

Proactividad en la comunicación y el intercambio de recursos, contenido y conocimiento.

Mantener una actitud asertiva, empática y conciliadora con los demás demostrando cordialidad y amabilidad en el trato.

Interpretar y ejecutar las instrucciones de trabajo.

Comunicarse eficazmente con las personas adecuadas en cada momento, respetando los canales establecidos en la organización.

Mostrar una actitud de respeto hacia los compañeros, procedimientos y normas de la empresa.

Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Acceso a información y datos

Herramientas de navegación y acceso a información y búsqueda. Características y funcionalidades. Hipertexto. Formatos de visualización y elementos de una página 'web'.

Fuentes de información. Clasificación. Internet, intranet y extranet. Recursos educativos abiertos (OER). Técnicas de valoración de la confiabilidad.

Medios físicos y lógicos para el almacenamiento de datos e información. Estructura organizativa y utilidades. Sistemas de archivos.

Propiedad intelectual y protección de datos en el acceso a la información.

Tipos de licencia. 'Software' privativo y 'software' libre. 'Creative Commons'.

2 Creación de contenidos digitales a partir de componentes elementales

Herramientas de edición y publicación de contenidos. Editores de texto, audio, vídeo. Gestores de contenido (CMS). Paquetes ofimáticos. Instalación y configuración.

Organización de elementos en repositorios locales. Repositorios 'online'.

Edición de textos, imágenes, elementos de audio o vídeo. Edición de características generales o globales. Formato de almacenamiento. Formatos comprimidos.

Plantillas de contenido.

Agregación de elementos de contenido tales como texto, imágenes, audio o vídeo. Coherencia visual de documentos. Agregación con herramientas ofimáticas, gestores de contenido y funcionalidades de la herramienta de publicación o sitio 'web'.

Propiedad intelectual y protección de datos en la reutilización de elementos de contenido.

3 Difusión de contenidos y trabajo colaborativo

Aplicaciones de comunicaciones interpersonales: correo electrónico, videoconferencia, mensajería entre otros. Procedimientos de uso. Comunicaciones en grupo. Configuración de la información personal. Configuración de la privacidad de la comunicación.

Redes sociales. Clasificación y objetivos. Registro y configuración de la información personal. Configuración de la privacidad y alcance. Identidad digital: estrategias, beneficios y riesgos.

Normas de protocolo digital en las comunicaciones ('Netiquette').

Parámetros de contexto de la formación

Espacios e instalaciones

Los talleres e instalaciones darán respuesta a las necesidades formativas de acuerdo con el contexto profesional establecido en la unidad de competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos laborales, accesibilidad universal, igualdad de género y protección medioambiental. Se considerará con carácter orientativo como espacios de uso:

- Instalación de 2 m² por alumno o alumna.

Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con el manejo de información, creación de contenidos y comunicación usando medios digitales, que se acreditará mediante una de las dos formas siguientes:

- Formación académica de nivel 1 (Marco Español de Cualificaciones para la Educación Superior) o de otras de superior nivel relacionadas con el campo profesional.
 - Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo.
2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.

MÓDULO FORMATIVO 2

Seguridad y resolución de problemas 'hardware'

Nivel:	1
Código:	MF2742_1
Asociado a la UC:	UC2742_1 - Operaciones auxiliares de seguridad y de resolución de problemas 'hardware'
Duración (horas):	15
Estado:	Tramitación BOE

Capacidades y criterios de evaluación

- C1:** Aplicar técnicas auxiliares de resolución de incidencias 'hardware' en el uso de un dispositivo informático, identificando el origen del problema y aplicando una solución inmediata siguiendo procedimientos estandarizados por el fabricante.
- CE1.1** Reconocer la arquitectura del subsistema físico de un equipo informático, diferenciando el objetivo y funciones de cada bloque.
- CE1.2** Identificar las condiciones ambientales de temperatura y humedad de un dispositivo a partir de las instrucciones del fabricante, aplicándolas a la hora de revisar la ubicación del mismo, reubicando el equipo en su caso, limpiando periódicamente las rejillas de ventilación y refrigeración.
- CE1.3** Identificar signos perceptibles de deterioro de un dispositivo informático, tales como olor a quemado, desgastes evidentes, ruidos o sonidos no habituales, aplicando una solución inmediata según la guía del fabricante del aparato ('resolución de problemas') o escalando el problema a la persona responsable de la entidad o al servicio técnico del propio fabricante si el problema persiste.
- CE1.4** Describir procedimientos de mantenimiento de dispositivos conectados a un sistema informático, tales como impresoras, escáneres, cámaras digitales, ratones o teclados, entre otros, explicando los pasos para su limpieza, comprobación y sustitución de fungibles y partes sometidas a desgaste.
- CE1.5** Enumerar tipos de cables y conectores o puertos, identificando el tipo de dispositivo asociado y sus características generales para solucionar problemas de conexionado, previa detección del problema, mediante comprobación del ajuste mecánico de la conexión, sustituyendo el cable por otro en buen estado o escalando el problema al servicio técnico del propio fabricante si el problema persiste.
- CE1.6** En un supuesto práctico de aplicación de técnicas de resolución de incidencias 'hardware' en el uso de un dispositivo informático, identificando el origen del problema y aplicando una solución inmediata siguiendo procedimientos estandarizados del fabricante:
- Mantener el subsistema físico de un equipo informático, comprobando las condiciones ambientales de temperatura y humedad, ajustando dichas condiciones o reubicando el equipo en su caso, limpiando periódicamente las rejillas de ventilación y refrigeración, prestando atención a signos perceptibles de deterioro, tales como olor a quemado, desgastes evidentes, ruidos o sonidos no habituales y escalando el problema al servicio técnico del propio fabricante si el problema persiste.

- Mantener unos dispositivos conectados al sistema, aplicando labores de limpieza, comprobación y sustitución de fungibles y partes sometidas a desgaste, sustituyendo los elementos deteriorados o gastados.
- Solucionar problemas de conexionado de cableado a la red de datos o con dispositivos asociados, previa detección del problema, comprobando el ajuste mecánico de la conexión, sustituyendo el cable por otro en buen estado, escalando el problema a la persona responsable de la entidad o al servicio técnico del propio fabricante si el problema persiste.

C2: Aplicar técnicas auxiliares de resolución de incidencias 'software' en el uso de un dispositivo informático, identificando el origen del problema y aplicando una solución inmediata siguiendo procedimientos estandarizados por el fabricante.

CE2.1 Describir el proceso de conexionado inalámbrico a la red de datos y con dispositivos asociados, explicando los pasos para su configuración y prueba, detectando problemas y reconfigurando en su caso según indique el fabricante, escalando el problema al servicio técnico del propio fabricante si el problema persiste.

CE2.2 Aplicar herramientas digitales 'software' a la solución de tareas propias de un hipotético entorno laboral, identificando el tipo de herramienta según el objetivo, tales como herramientas de difusión o comunicación de mensajes o contenidos, edición de texto, imágenes, audio, vídeo o tareas de cálculo, entre otras.

CE2.3 Explicar el procedimiento de actualización de las aplicaciones instaladas en los equipos informáticos detallando los pasos de configuración para aplicar los parches, enumerando las comprobaciones tales como capacidad de almacenamiento disponible.

CE2.4 Aplicar procedimientos de reorganización y limpieza de datos y archivos en el sistema de ficheros físico o en la nube.

CE2.5 En un supuesto práctico de aplicación de técnicas de resolución de incidencias 'software' en el uso de un dispositivo informático, identificando el origen del problema y aplicando una solución inmediata siguiendo procedimientos estandarizados del fabricante:

- Solucionar problemas de conexionado inalámbrico de un equipo informático a una red de datos o con dispositivos asociados, previa detección del problema, comprobando y reconfigurando en su caso según indicaciones del fabricante, escalando el problema al servicio técnico del propio fabricante si el problema persiste.
- Resolver tareas propias de un hipotético entorno laboral tales como difusión o comunicación de mensajes o contenidos, edición de texto, imágenes, audio, vídeo o tareas de cálculo, entre otras, aplicando soluciones o herramientas digitales, previa identificación de las aplicaciones disponibles cuya funcionalidad se ajusta a la tarea a realizar.
- Mantener las aplicaciones instaladas en un equipo informático, configurando y aplicando actualizaciones de 'software', comprobando la capacidad de almacenamiento disponible y organizando y haciendo limpieza en su caso de datos y archivos en el sistema de ficheros físico o en la nube.

C3: Aplicar procedimientos de configuración de elementos de seguridad en equipos informáticos, usando herramientas o aplicando buenas prácticas para proteger la confidencialidad, integridad y disponibilidad de la información.

CE3.1 Enumerar programas antimalware, identificando sus funcionalidades.

CE3.2 Aplicar procedimientos de instalación de programas antimalware, previa descarga de la página del fabricante, configurando las opciones de detección y acción ante amenazas detectadas y la actualización de patrones de virus.

CE3.3 Describir el proceso de configuración de las actualizaciones y parches del 'software' de base de un equipo informático, detallando los pasos para el establecimiento de la periodicidad y el grado de automatización del proceso.

CE3.4 Identificar posibilidades de detección de correos potencialmente peligrosos o no deseados, explicando el establecimiento de reglas ante la recepción de los mismos, indicando los parámetros de detección y las acciones asociadas, identificando y seleccionando orígenes no confiables, no abriendo y no siguiendo hiperenlaces de ese tipo de fuentes.

CE3.5 Reconocer acciones para la protección de la navegación por Internet, explicando los parámetros de configuración de la privacidad y las acciones por defecto ante la petición de almacenaje de 'cookies' y el modo de navegación disponible, excluyendo visitar páginas 'web' no confiables y activando la protección antimalware para la navegación y el uso de protocolos de comunicaciones seguros (HTTPS).

CE3.6 Comprender los riesgos de introducir datos en formularios online, seleccionando únicamente en páginas confiables, procurando que la información proporcionada sea la imprescindible para que se preste el servicio solicitado, no aceptando condiciones de servicio desproporcionadas o no comprensibles.

CE3.7 Explicar el proceso de configuración de la protección de las comunicaciones inalámbricas y los sitios web del usuario, describiendo cómo se activa y/o comprueba el uso de cifrados seguros y estableciendo contraseñas fuertes, cambiándolas periódicamente y protegiendo el acceso a las mismas.

CE3.8 En un supuesto práctico de aplicación de procedimientos de configuración de elementos de seguridad en equipos informáticos, usando herramientas o aplicando buenas prácticas para proteger la confidencialidad, integridad y disponibilidad de la información:

- Instalar unos programas antimalware, descargándolos de la página del fabricante, configurando las opciones de detección y acción ante amenazas detectadas y la actualización de patrones de virus.

- Configurar el 'software' de base y las aplicaciones de un equipo informático para la instalación periódica de actualizaciones y parches de seguridad, indicando la periodicidad y el grado de automatización del proceso.

- Configurar reglas de acción ante la recepción de correos sospechosos o no deseados o, en su caso, aplicarlas, indicando los parámetros de detección y las acciones asociadas, identificando y seleccionando orígenes no confiables, no abriendo o siguiendo hiperenlaces de ese tipo de fuentes.

- Configurar la navegación por Internet para la protección de la privacidad, seleccionando las acciones por defecto ante la petición de almacenaje de 'cookies' y el modo de navegación disponible, excluyendo visitar páginas 'web' no confiables y activando la protección antimalware para la navegación y el uso de protocolos de comunicaciones seguros (HTTPS).

- Introducir datos en formularios online únicamente en páginas confiables, procurando que la información proporcionada sea la imprescindible para que se preste el servicio solicitado, no aceptando condiciones de servicio desproporcionadas o no comprensibles.

- Proteger las comunicaciones inalámbricas y los sitios web del usuario se protegen, activando el uso de cifrados seguros y estableciendo contraseñas fuertes, cambiándolas periódicamente y protegiendo el acceso a las mismas.

C4: Aplicar operaciones auxiliares de mantenimiento del inventariado de equipos y dispositivos asociados, etiquetando los elementos para facilitar su localización y referenciado en caso de avería, según estándares y cumpliendo la normativa medioambiental.

CE4.1 Identificar nomenclaturas de etiquetado, describiendo la información que debe contener y detallando el uso de herramientas al efecto.

CE4.2 Detallar el procedimiento de almacenaje de equipos y dispositivos asociados que no están en uso, previo embalaje protector, explicando las condiciones que mejoran su seguridad.

CE4.3 Reconocer la importancia de la economía circular y el papel del reciclaje, identificando el tratamiento según su naturaleza, eliminados previamente sus contenidos o datos personales.

CE4.4 Describir procedimientos de destrucción segura de datos y sanitización de soportes de información obsoletos o reutilizables, identificando herramientas y opciones de utilización.

CE4.5 En un supuesto práctico de aplicación de operaciones auxiliares de mantenimiento del inventariado de equipos y dispositivos asociados, etiquetando los elementos para facilitar su localización y referenciado en caso de avería, según estándares y cumpliendo la normativa medioambiental:

- Etiquetar unos equipos y dispositivos asociados en uso o en almacenaje para facilitar su control, utilizando herramientas específicas al efecto y siguiendo normas de nomenclatura y catalogación.
- Embalar equipos y dispositivos asociados que no están en uso, utilizando los recursos y materiales al efecto, almacenándolos en condiciones de seguridad.
- Localizar en el almacén o bien recibir del proveedor equipos y dispositivos asociados que se requiera sustituir o añadir, desembalándolos e instalándolos, configurándolos en su caso según indique el fabricante.
- Tratar los embalajes, residuos y elementos desechables para su gestión o reciclaje, depositándolos en contenedores según su naturaleza, previo borrado de contenidos o datos personales.

Capacidades cuya adquisición debe ser completada en un entorno real de trabajo

C1 respecto a CE1.6; C2 respecto a CE2.5; C3 respecto a CE3.8 y C4 respecto a CE4.5.

Otras Capacidades:

Curiosidad acerca de las nuevas tecnologías y su funcionamiento.

Proactividad en la comunicación y el intercambio de recursos, contenido y conocimiento.

Mantener una actitud asertiva, empática y conciliadora con los demás demostrando cordialidad y amabilidad en el trato.

Interpretar y ejecutar las instrucciones de trabajo.

Comunicarse eficazmente con las personas adecuadas en cada momento, respetando los canales establecidos en la organización.

Mostrar una actitud de respeto hacia los compañeros, procedimientos y normas de la empresa.

Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Resolución de incidencias 'hardware' en el uso de un dispositivo informático

Arquitectura del subsistema físico de un equipo informático. Bloques, objetivo y funciones.

Mantenimiento de condiciones ambientales de temperatura y humedad de dispositivos.

Detección de averías y deterioro. Signos externos de desgaste. Resolución de problemas.

Mantenimiento de dispositivos conectados a un sistema informático. Impresoras, escáneres, cámaras digitales, ratones o teclados, entre otros.

Buses y conexionado. Tipos de cable, conectores y puertos. Características.

2 Resolución de incidencias 'software' en el uso de un dispositivo informático

Conexión inalámbrica a la red de datos y con dispositivos asociados. Estándares NFC. Bluetooth. Configuración y prueba. Resolución de problemas.

Herramientas digitales 'software' aplicables a tareas del entorno laboral. Aplicaciones de uso general y específico.

Actualización del aplicativo. Comprobaciones, automatización y periodicidad.

Reorganización y limpieza de datos y archivos en el sistema de ficheros físico o en la nube.

3 Configuración de elementos de seguridad y buenas prácticas en equipos informáticos

'Software' antimalware. Instalación, actualización, configuración y funcionalidades.

Actualizaciones y parches del 'software' de base. Periodicidad y automatización del proceso.

Detección de correos potencialmente peligrosos o no deseados. Reglas de acción. Buenas prácticas.

Protocolos seguros en clientes de correo. Autenticación.

Protección de la navegación por Internet. Privacidad. Cookies. Criterios de selección de páginas confiables. Protocolos de comunicaciones seguros (HTTPS).

Riesgos de la introducción de datos online. Condiciones de servicios 'online'.

Protección de las comunicaciones inalámbricas.

Protección en el acceso a sitios 'web'. Protocolos seguros. HTTPS.

Políticas de control de acceso seguro. Gestión de Contraseñas.

4 Mantenimiento del inventariado de equipos y dispositivos asociados

Nomenclaturas de etiquetado. Herramientas.

Almacenaje seguro de equipos y dispositivos asociados.

Economía circular y reciclaje.

Eliminación y borrado seguro de contenidos o datos personales. Herramientas.

Parámetros de contexto de la formación

Espacios e instalaciones

Los talleres e instalaciones darán respuesta a las necesidades formativas de acuerdo con el contexto profesional establecido en la unidad de competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos laborales, accesibilidad universal, igualdad de género y protección medioambiental. Se considerará con carácter orientativo como espacios de uso:

- Taller de 4 m² por alumno o alumna.

- Instalación de 2 m² por alumno o alumna.

Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con la con la seguridad y resolución de problemas 'hardware', que se acreditará mediante una de las dos formas siguientes:

- Formación académica de nivel 1 (Marco Español de Cualificaciones para la Educación Superior) o de otras de superior nivel relacionadas con el campo profesional.

- Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo.

2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.