DATOS IDENTIFICATIVOS DE LA UNIDAD FORMATIVA

UNIDAD FORMATIVA	MANTENIMIENTO Y GESTIÓN DE INCIDENCIAS EN PROYECTO DE VIDEOVIGILANCIA, CONTROL DE ACCESOS ,Y PRESENCIA	Duración Condicionada	40
Código	UF1139		
Familia profesional	INFORMÁTICA Y COMUNICACIONES		
Área Profesional	Sistemas y Telemática		
Certificado de profesionalidad	Implantación y gestión de elementos informáticos en sistemas domóticos/inmóticos, de control de accesos y presencia, y de videovigilancia	Nivel	3
Módulo formativo	Implantación y mantenimiento de sistemas de control de accesos y presencia, y de videovigilancia	Duración	220
Resto de unidades formativas que completan el módulo	Instalación y puesta en marcha de un sistema de videovigilancia y seguridad	Duración	90
	Instalación y puesta en marcha de un sistema de control de acceso y presencia		90

Apartado A: **REFERENTE DE COMPETENCIA**

Esta unidad formativa se corresponde con la RP4 de la UC1220_3 IMPLANTAR Y MANTENER SISTEMAS DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEOVIGILANCIA.

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

Capacidades y criterios de evaluación

C1: Describir los procedimientos de mantenimiento y resolver las incidencias de los sistemas de control de accesos y presencia, y de videovigilancia, para mantener operativo el sistema.

CE1.1 Describir los procesos de mantenimiento de los equipos y dispositivos que forman los sistemas de control de accesos y detección de presencia, y de videovigilancia identificando los parámetros de funcionalidad óptima.

CE1.2 Elaborar y actualizar los procedimientos de mantenimiento estableciendo el número de revisiones preventivas y las acciones a realizar en cada revisión del sistema.

CE1.3 Identificar nuevas funcionalidades y mejoras de los componentes hardware y software de los sistemas de control de accesos y detección de presencia, y de videovigilancia que existen en el mercado, para proponer actualizaciones compatibles.

CE1.4 Clasificar la tipología y características de las averías de naturaleza física y lógica que se presentan en los sistemas de control de accesos y detección de presencia, y de videovigilancia.

CE1.5 Describir las técnicas generales y los medios técnicos específicos necesarios para la localización de averías de naturaleza física y lógica en los sistemas de control de accesos y detección de presencia, y de videovigilancia.

CE1.6 En varios casos prácticos simulados, debidamente caracterizados, para el diagnóstico, localización y resolución de averías en los sistemas de control de accesos y presencia, y de videovigilancia:

- Interpretar la documentación del sistema, identificando los distintos bloques funcionales y componentes específicos que lo componen.
- Identificar los síntomas de la avería caracterizándola por los efectos que produce.
- Realizar un plan de intervención en el sistema para determinar la causa o causas que producen la avería.
- Localizar el elemento (físico o lógico) responsable de la avería y realizar la sustitución (mediante la utilización de componentes similares o equivalentes) o modificación del elemento, configuración y/o programa, aplicando los procedimientos requeridos y en un tiempo adecuado.
- Realizar las comprobaciones, modificaciones y ajustes de los parámetros del sistema, según las especificaciones de la documentación técnica del mismo, utilizando las herramientas apropiadas, que permitan su puesta a punto en cada caso.
- Elaborar un informe-memoria de las actividades desarrolladas y resultados obtenidos, estructurándolo en los apartados necesarios para una adecuada documentación de las mismas (descripción del proceso seguido, medios utilizados, medidas, explicación funcional y esquemas).

Contenidos

1. Procesos de mantenimiento en sistemas de videovigilancia.

- Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento de los dispositivos hardware del sistema.
  - Mantenimiento de cámaras y dispositivos hardware de tratamiento de video.

- Comprobación de dispositivos de interconexión, sujeción, cableado e infraestructura de monitorización y control.
- Mantenimiento de sistemas de almacenamiento.
- Mantenimiento de los Sistemas de protección y alimentación ininterrumpida o SAI.

o Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento del software del sistema. Verificación de que funciona según los requisitos especificados.
- Comprobación del funcionamiento del software de gestión, visualización, grabación y tratamiento de datos del sistema de videovigilancia.
- Comprobación de la correcta parametrización a nivel software de los dispositivos del sistema: cámaras, servidores, comunicación, etc.
- Actualización en caso necesario del software de gestión.
- Comprobación del sistema de copias de seguridad y el acceso a información del sistema.
- Comprobación del sistema de seguridad, nivel de privilegios y protección del sistema.
- Actualización del firmware de los dispositivos que lo requieran.

o Comprobación del correcto funcionamiento de integración con los sistemas y redes de comunicación conectados y certificación del cumplimiento de la Ley Orgánica de protección de datos y normativas técnicas.
- Mantenimiento del hardware y dispositivos físicos de comunicación o integración con otras redes:
  - Pasarelas de comunicación.
  - Módulos de entradas y salidas interconectadas entre sistemas.
- Pruebas y protocolos de evaluación y correcto funcionamiento de la comunicación a nivel software.
- Actualizar el sistema para seguir cumpliendo con la normativa técnica y legal en el momento de realizar el mantenimiento en caso de necesitarla .

o Generación de la nueva documentación o Actualización de la documentación ya existente tras las operaciones de mantenimiento.
o Comprobar que el personal al cargo hace un correcto uso del sistema, en caso negativo, aconsejar alternativas correctas, enseñar o referencias a los manuales de manejo.

2. Incidencias y alertas en proyectos de video vigilancia .

o Incidencias de fallos en hardware: Proceso de reinstalación de dispositivos averiados .
o Incidencias de fallos en Software: Proceso de reconfiguración / actualización / sustitución del software de gestión.
o Tratamiento de errores o alertas de mal funcionamiento.
- Sistemas y herramientas de detección de errores, tanto a nivel de hardware como software.
- Procesos de depuración y reconfiguración del sistema.
- Prueba y puesta en marcha de la nueva configuración del sistema.

o Incidencias de Modificación del entorno. Adaptación a las nuevas configuraciones.
- Cambio de escenario a vigilar debido a muebles, árboles, arbustos u otros obstáculos físicos para el correcto funcionamiento del sistema.
- Alteración de la estructura a vigilar. Procesos de reposicionamiento y nueva configuración del sistema.
- Gestión de cambios en la configuración requerida por la dirección del lugar.

o Avisos, Gestión y modificaciones en remoto del sistema de videovigilancia.
o Generación de la nueva documentación o actualización de la documentación ya existente tras las operaciones de gestión de incidencias.
o Actualización y mejora del estado del sistema de videovigilancia.
o Evaluación del estado del sistema.
o Propuestas de mejora del sistema.
o Aplicación de nuevas funcionalidades: Procesos para la actualización / ampliación / integración del sistema de videovigilancia.

3. Procesos y tareas de mantenimiento en sistemas de control de accesos y presencia.

o Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento de los dispositivos hardware del sistema.
- Mantenimiento mecánico de los dispositivos físicos de control de accesos: Barreras, puertas, tornos y resto de dispositivos mecánicos del sistema.
- Mantenimiento eléctrico y electrónico de las automatizaciones de control: Cerraduras, tarjetas y componentes electrónicos e informáticos del sistema.
- Comprobación de los sistemas de identificación y autentificación: Verificar funcionamiento y funcionalidad de teclados, lectores de tarjetas, proximidad, biométricos y resto de dispositivos identificación y autentificación.
- Comprobación de Dispositivos de interconexión, sujeción, Cableado e infraestructura de monitorización, avisos y control
- Mantenimiento de Soporte del sistema de Gestión y almacenamiento de datos.
- Mantenimiento de los Sistemas de protección y alimentación ininterrumpida o SAI.

o Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento del software del sistema. Verificación de que funciona según los requisitos especificados.

- Comprobación del funcionamiento del software de gestión, monitorización y herramientas de tratamiento de datos, creación de informes y estadísticas, etc. Para que funcionen según las especificaciones de proyecto.
- Comprobación la correcta parametrización a nivel software de los dispositivos del sistema.
- Actualización en caso necesario del software de gestión.
- Comprobación del sistema de copias de seguridad y el acceso a información del sistema.
- Comprobación del sistema de seguridad, nivel de privilegios y protección del sistema.
- Actualización del firmware de los dispositivos que lo requieran.

o Comprobación del correcto funcionamiento de integración con los sistemas y redes de comunicación conectados y certificación del cumplimiento de la Ley Orgánica de protección de datos y normativas técnicas.
- Mantenimiento del hardware y dispositivos físicos de comunicación o integración con otras redes:
  - Pasarelas de comunicación.
  - Módulos de entradas y salidas interconectadas entre sistemas.
- Pruebas y protocolos de evaluación y correcto funcionamiento de la comunicación a nivel software.
- Actualizar el sistema para seguir cumpliendo con la normativa técnica y legal en el momento de realizar el mantenimiento en caso de necesitarla.

o Generación de la nueva documentación o Actualización de la documentación ya existente tras las operaciones de mantenimiento.
o Comprobación que el personal al cargo hace un correcto uso del sistema, en caso negativo, aconsejar alternativas correctas, enseñar o referencias a los manuales de manejo.

4. Gestión de incidencias y alertas.

o Incidencias de fallos en hardware: Proceso de Re instalación de dispositivos averiados.
o Incidencias de fallos en Software: Proceso de reconfiguración / actualización / sustitución del software de gestión.
o Tratamiento de errores o alertas de mal funcionamiento.
- Sistemas y herramientas de Detección de errores, tanto a nivel de hardware como software.
- Procesos de Depuración y reconfiguración del sistema.
- Prueba y puesta en marcha de la nueva configuración del sistema.

o Incidencias de Modificación del entorno. Adaptación a las nuevas configuraciones.
- Alteración de la estructura a controlar. Procesos de reposicionamiento y nueva configuración del sistema.
- Gestión de cambios en la configuración requerida por la dirección del lugar.

o Avisos, Gestión y modificaciones en remoto del sistema de control de accesos y presencia.
o Generación de la nueva documentación o Actualización de la documentación ya existente tras las operaciones de gestión de incidencias.
o Actualización y mejora del estado del sistema de control de accesos.
o Evaluación del estado del sistema.
o Propuestas de mejora del sistema.
o Aplicación de nuevas funcionalidades: Procesos para la actualización / ampliación / integración del sistema de control de accesos.

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.

Para cursar esta unidad formativa se debe haber superado la UF1137: Instalación y puesta en marcha de un sistema de video vigilancia y seguridad y la UF1138: Instalación y puesta en marcha de un sistema de control de acceso y presencia.

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: Implantación y gestión de elementos informáticos en sistemas domóticos/inmóticos, de control de accesos y presencia, y de videovigilancia.

.