Curso online. Técnico Especialista TIC en Control de Acceso y Videovigilancia

Working
Formación Integral S.L.

www.workingformacion.com

OBJETIVOS

Este curso de Técnico Especialista TIC en Control de Acceso y Videovigilancia le ofrece una formación especializada en la materia. Debemos saber que en el ámbito de la informática y las comunicaciones, es necesario la implantación y gestión de elementos informáticos en sistemas domóticos/inmóticos, de control de accesos y presencia, y de videovigilancia dentro del área profesional de sistemas y telemática. Así, con el presente curso se pretende aportar los conocimientos necesarios para el mantenimiento y gestión de incidencias en proyectos de video vigilancia, control de accesos y presencia, la instalación y puesta en marcha de un sistema de control de acceso y presencia y la instalación y puesta en marcha de un sistema de video vigilancia y seguridad.

CONTENIDOS

UNIDAD FORMATIVA 1. INSTALACIÓN Y PUESTA EN MARCHA DE UN SISTEMA DE VIDEO VIGILANCIA Y SEGURIDAD.

UNIDAD DIDÁCTICA 1. SISTEMAS DE VIDEOVIGILANCIA

1. Definición de sistemas de CCTV y video vigilancia
2. Aplicación de los sistemas de video a la seguridad
3. Identificación de los principales campos de aplicación mediante el estudio de casos reales
4. Descripción de la evolución de los sistemas de video vigilancia

UNIDAD DIDÁCTICA 2. VIDEO Y TRATAMIENTO DE LA IMAGEN

1. Definición de los conceptos de luz, imagen y video
2. Descripción de los tipos de lentes y sus características principales
3. Análisis de la señal de vídeo e imagen analógica
4. Formación, tratamiento y transmisión de la imagen analógica
5. Características y formatos de vídeo analógico
6. Ventajas e inconvenientes del vídeo analógico
7. Análisis de la señal de vídeo e imagen Digital
8. Formación, tratamiento y transmisión de la imagen digital
9. Características y formatos de vídeo analógico
10. Ventajas e inconvenientes del vídeo digital
11. Parámetros de evaluación de las señales de video

UNIDAD DIDÁCTICA 3. SISTEMAS DE VIDEO VIGILANCIA Y SEGURIDAD ANALÓGICOS

1. Hardware: cámaras y dispositivos de sistema
2. Soporte, cableado y topología del sistema analógico de vídeo vigilancia
3. Configuración, métodos de gestión y visualización en sistemas analógicos
4. Topología, escalabilidad e Infraestructura de un sistema analógico
5. Características del sistema analógico

UNIDAD DIDÁCTICA 4. SISTEMAS DE VÍDEO VIGILANCIA Y SEGURIDAD DIGITALES

1. Hardware: cámaras y dispositivos de sistema
2. Soporte, cableado, tecnologías de transporte y topología del sistema digital de vídeo vigilancia
3. Configuración, métodos de gestión y visualización en sistemas digitales
4. Topología, escalabilidad e Infraestructura de un sistema digital
5. Características del sistema digital y conectividad con otras redes
6. Integración analógica en el mundo digital: Sistemas mixtos

UNIDAD DIDÁCTICA 5. ALMACENAMIENTO DE LA INFORMACIÓN OBTENIDA

1. Sistemas de almacenamiento en formato analógico
2. Sistemas de almacenamiento formato digital
3. Dimensionado del sistema de almacenamiento en función de los requerimientos del proyecto
4. Protección y seguridad de los datos e información aportada por el sistema:

5. Protección mediante un sistema de alimentación ininterrumpida los dispositivos de toda la instalación de video vigilancia
6. Copias de seguridad y sistemas de prevención de pérdidas de datos
7. Redundancia
8. Acceso protegido y gestión de privilegios en los sistemas de videovigilancia
9. Autentificación de la información. Marca de Agua
10. Copias seguridad actualizadas de la información de control del sistema. Accesos, zonas de vigilancia, Bases de datos, horarios, etc.

UNIDAD DIDÁCTICA 6. FUNCIONALIDADES Y GESTIÓN DEL SISTEMA DE VIDEO VIGILANCIA

1. Métodos de Grabación
2. A demanda
3. Planificada
4. Continua
5. Por eventos
6. Detección de movimiento
7. Configuraciones de visualización
8. Búsqueda inteligente de eventos
9. Generación de eventos
10. Seguridad: Gestión de alertas y avisos; Interacción con otros sistemas y/o redes de comunicación o CRA (Centrales receptoras de alarmas)
11. Análisis, proceso y obtención de información relevante: Video Inteligente: Video procesado por herramientas de software informático:
12. Conteo de personas
13. Reconocimiento Facial
14. Seguimiento de objetos y personas
15. Lector de Matriculas
16. Avisos sobre objetos que desaparecen / aparecen
17. Análisis de trayectorias y recorridos

18. Obtención de informes y estadísticas
19. Detección de situaciones anómalas
20. Procesado de Imagen
21. Otras

UNIDAD DIDÁCTICA 7. PLANIFICACIÓN DEL PROCESO DE ACOMETIDA E IMPLANTACIÓN DE UN PROYECTO DE VIDEO VIGILANCIA

1. Evaluación de las recomendaciones y puntos clave previos a acometer un proyecto de vídeo vigilancia
2. Restricciones de los sistemas y de funcionalidad
3. Limitaciones de los dispositivos de captación de vídeo, transmisión de vídeo, comunicación y almacenamiento.
4. Problemática del medio de comunicación (distancias, interferencias, atenuaciones, etc.)
5. Problemática debida al medio y la localización del sistema (entorno)
6. Protecciones de los aparatos (Ips)
7. Factor Humano
8. Evaluación de los niveles de riesgo y tipos de amenazas
9. Evaluación de las necesidades de vigilancia y nivel de protección
10. Análisis de la situación: ¿Qué hay que vigilar?
11. Planteamiento: ¿Cómo y cuándo vigilar? ¿Desde dónde vigilar? ¿Quién ha de vigilar?
12. Estructuración del sistema y búsqueda de la ubicación optima de los dispositivos
13. Planteamiento de las funcionalidades del sistema
14. Integración con otros sistemas y redes: reacciones y posibilidades ante una detección o evento
15. Criterios de selección del dispositivos
16. Interpretación y evaluación del proyecto y la infraestructura necesaria para acometerlo
17. Estimación de tiempos de ejecución, recursos y personal necesario

18. Interpretación de manuales así como de las características y funciones de los aparatos proporcionados por los fabricantes. (incluso en otros idiomas)
19. Comprobación del cumplimiento de la Normativa y reglamentación sobre Seguridad Privada y Ley Orgánica de Protección de Datos
20. Configuración del sistema y puesta en marcha tanto del software como del hardware, según las especificaciones y funcionalidades requeridas.
21. Documentación generada o utilizada en el proceso:
22. Usada:
23. Proyecto: memoria, planos, pliego de condiciones y requisitos necesarios
24. Proyecto de las instalaciones a Vigilar
25. Normativa técnica
26. Normativa legal aplicada
27. Generada
28. Informe de puesta en marcha
29. Libro de seguimiento e incidencias
30. Reflejo fiel del estado final de la instalación
31. Informe de configuración del sistema
32. Informe de seguridad acorde con la LOPD

UNIDAD DIDÁCTICA 8. SIMULACIÓN DEL DESARROLLO DE UN PROYECTO DE VIDEOVIGILANCIA SIGUIENDO LAS PAUTAS QUE SE INDIQUEN

1. Observación del proyecto de forma global: sistemas que involucra, dispositivos a instalar, espacios reservados, infraestructura, canalizaciones y conectividad de los elementos para hacerse a la idea del alcance del mismo.
2. Realización de un estudio previo de las necesidades, características y funcionalidades del proyecto a implantar. Comprobación que el sistema nos aporta todo lo que necesitamos.

3. Análisis de la solución propuesta e instalación física de los dispositivos y la totalidad de sus conexiones, tanto con el sistema de videovigilancia como con el resto de sistemas involucrados
4. Parametrización y ajuste del sistema de videovigilancia
5. Comprobación de que el sistema funcione según exigencias del proyecto, y en caso contrario, aplicación de los métodos de detección y corrección de errores, para posteriormente volver a comprobar el sistema.
6. Realización del informe de la puesta en marcha y la documentación necesaria

UNIDAD FORMATIVA 2. INSTALACIÓN Y PUESTA EN MARCHA DE UN SISTEMA DE CONTROL DE ACCESOS Y PRESENCIA.

UNIDAD DIDÁCTICA 1. SISTEMAS DE CONTROL DE ACCESO Y PRESENCIA

1. Definición de los sistemas de control de acceso y presencia. Características más importantes.
2. Valoración de las necesidades y razones para la integración de un sistema de control de accesos y presencia
3. Identificación de los principales campos de aplicación mediante el estudio de casos reales

UNIDAD DIDÁCTICA 2. COMPONENTES Y CARACTERÍSTICAS DE LOS SISTEMAS Y DISPOSITIVOS QUE FORMAN EL CONTROL DE ACCESO Y PRESENCIA.

1. Sistemas mecánicos automatizados integrados en la gestión de accesos
2. Electro cerraduras
3. Puertas y Barreras
4. Torniquetes y Tornos

5. Rampas y Elevadores
6. Sistemas diseñados para minusválidos
7. Otros tipos de activaciones o eventos
8. Dispositivos, Sistemas y tecnologías de identificación / autentificación
9. Relojes de control y / o tarificación
10. Teclados: Códigos y contraseñas de acceso
11. Lectores de tarjeta
12. Códigos de barra
13. Banda Magnética
14. Lectores de proximidad
15. Tarjetas o chips de proximidad. Tecnología RFID
16. Bluetooth
17. Otras
18. Sensores Biométricos e Identidad biométrica; Como identificar a través de rasgos y factores únicos en cada persona
19. Lector de Huella digital
20. Lector de Palma o estructura de la mano
21. Reconocimiento Facial
22. Reconocimiento del Iris
23. Reconocimiento de retina
24. Sistemas de reconocimiento de voz
25. Dispositivos, Software y datos de control del sistema
26. Hardware de control e integración de sistema
27. Conectividad y cableado. Infraestructura, funcionamiento y topología de los sistemas de control de acceso y presencia
28. Punto de gestión y monitorización del sistema:
29. Configuración y parametrización del sistema
30. Solución Hardware o Software.
31. Herramientas de extracción de informes
32. Software de tratamiento de datos.
33. Bases de datos e información de control

UNIDAD DIDÁCTICA 3. FUNCIONALIDADES Y APLICACIONES DE LOS SISTEMAS DE CONTROL DE ACCESO Y PRESENCIA

1. Control, monitorización y gestión de prioridades de acceso en instalaciones, identificación de las personas y datos relevantes que acceden, conocer el estado de los accesos y tener la posibilidad de gestionarlos.
2. Control de horarios y eficiencia en empresas o procesos productivos.
3. Tratamiento de datos:
4. Generación de estadísticas y datos de ocupación
5. Tarificación de servicios y tiempos
6. Sistemas de localización, control y detección de personas en un entorno cerrado; control de errantes no intrusivo
7. Sistemas de control médico, acceso a datos y posibilidad de actualización de información automatizado. (Aplicable o otros procesos similares)
8. Gestión de alarmas y eventos
9. Accesos no deseados
10. Alertas no permitidos o fuera de horario
11. Alarmas de averías o mal funcionamiento del sistema
12. Interacción con otros sistemas y/o redes de comunicación o CRA (Centrales receptoras de alarmas)
13. Soluciones de control logístico y de distribución
14. Soluciones de Gestión de Asistencia a Eventos

UNIDAD DIDÁCTICA 4. PROTECCIÓN Y SEGURIDAD DEL SISTEMA Y DE LOS DATOS E INFORMACIÓN APORTADA POR EL SISTEMA:

1. Protección, mediante un sistema de alimentación ininterrumpida, de los dispositivos de toda la instalación de control de accesos y presencia
2. Copias de seguridad y sistemas de prevención de pérdidas de datos
3. Redundancia

4. Acceso protegido y gestión de privilegios en los sistemas de gestión y monitorización del sistema de control de accesos y presencia
5. Copias seguridad actualizadas de la información de control del sistema. Accesos, zonas de vigilancia, Bases de datos, horarios, etc.

UNIDAD DIDÁCTICA 5. PROCESO DE ACOMETIDA E IMPLANTACIÓN DE UN PROYECTO DE CONTROL DE ACCESOS Y PRESENCIA

1. Evaluación de las recomendaciones y puntos clave previos a acometer un proyecto de control de accesos y presencia
2. Restricciones de los sistemas y de su funcionalidad
3. Problemática del medio de comunicación (número máximo de dispositivos, distancias, interferencias, atenuaciones, etc.)
4. Problemática debida al medio y la localización del sistema (entorno)
5. Protecciones de los aparatos (Ips)
6. Factor Humano
7. Evaluación de los niveles de riesgo y tipos de amenazas
8. Evaluación de las necesidades y definición del servicio y funcionalidades a implantar
9. Interpretación y evaluación del proyecto y la infraestructura necesaria para acometerlo
10. Estimación de tiempos de ejecución, recursos y personal necesario
11. Interpretación de manuales así como de las características y funciones de los aparatos proporcionados por los fabricantes. (incluso en otros idiomas)
12. Análisis de la situación: ¿Qué accesos hay que controlar?

13. Planteamiento y planificación: ¿Cómo y cuándo se controlan? ¿Desde dónde controlar y gestionar el sistema?
14. Estructuración del sistema y búsqueda de la ubicación optima de los dispositivos
15. Planteamiento de las funcionalidades del sistema
16. Integración con otros sistemas y redes: Reacciones y posibilidades ante una detección o evento
17. Comprobación el cumplimiento de la normativa y reglamentación sobre seguridad privada y Ley Orgánica de Protección de Datos
18. Configuración del sistema y puesta en marcha tanto del software como del hardware, según las especificaciones y funcionalidades requeridas.
19. Documentación generada o utilizada en el proceso:
20. Usada:
21. Proyecto: memoria, planos, pliego de condiciones y requisitos necesarios
22. Proyecto de las instalaciones a controlar
23. Normativa técnica
24. Normativa legal aplicada
25. Generada
26. Informe de puesta en marcha
27. Libro de Seguimiento e incidencias
28. Reflejo fiel del estado final de la instalación
29. Informe de Configuración del sistema
30. Informe de seguridad acorde con la LOPD

UNIDAD DIDÁCTICA 6. SIMULACIÓN DEL DESARROLLO DE UN PROYECTO DE CONTROL DE ACCESOS Y PRESENCIA SIGUIENDO LAS PAUTAS QUE SE INDIQUEN

1. Observación del proyecto de forma global: sistemas que involucra, dispositivos a instalar, espacios reservados, infraestructura, canalizaciones y conectividad de los elementos para hacerse a la idea del alcance del mismo.

2. Realización de un estudio previo de las necesidades, características y funcionalidades del proyecto a implantar. Comprobación que el sistema nos aporta todo lo que necesitamos.
3. Análisis de la solución propuesta e instalación física de los dispositivos y la totalidad de sus conexiones, tanto con el sistema de control de accesos como con el resto de sistemas involucrados
4. Parametrización y ajuste del sistema de control de accesos
5. Comprobación de que el sistema funcione según exigencias del proyecto, y en caso contrario, aplicación de los métodos de detección y corrección de errores, para posteriormente volver a comprobar el sistema.
6. Realización del informe de la puesta en marcha y la documentación necesaria

UNIDAD FORMATIVA 3. MANTENIMIENTO Y GESTIÓN DE INCIDENCIAS EN PROYECTOS DE VIDEO VIGILANCIA, CONTROL DE ACCESOS Y PRESENCIA.

UNIDAD DIDÁCTICA 1. PROCESOS DE MANTENIMIENTO EN SISTEMAS DE VIDEOVIGILANCIA

1. Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento de los dispositivos hardware del sistema.
2. Mantenimiento de cámaras y dispositivos hardware de tratamiento de vídeo
3. Comprobación de dispositivos de interconexión, sujeción, cableado e infraestructura de monitorización y control
4. Mantenimiento de sistemas de almacenamiento
5. Mantenimiento de los Sistemas de protección y alimentación ininterrumpida o SAI.
6. 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

7. Comprobación del funcionamiento del software de gestión, visualización, grabación y tratamiento de datos del sistema de videovigilancia
8. Comprobación de la correcta parametrización a nivel software de los dispositivos del sistema: cámaras, servidores, comunicación, etc.
9. Actualización en caso necesario del software de gestión
10. Comprobación del sistema de copias de seguridad y el acceso a información del sistema.
11. Comprobación del sistema de seguridad, nivel de privilegios y protección del sistema
12. Actualización del firmware de los dispositivos que lo requieran
13. 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.
14. Mantenimiento del hardware y dispositivos físicos de comunicación o integración con otras redes:
15. Pasarelas de comunicación
16. Módulos de entradas y salidas interconectadas entre sistemas
17. Pruebas y protocolos de evaluación y correcto funcionamiento de la comunicación a nivel software
18. Actualizar el sistema para seguir cumpliendo con la normativa técnica y legal en el momento de realizar el mantenimiento en caso de necesitarla
19. Generación de la nueva documentación o Actualización de la documentación ya existente tras las operaciones de mantenimiento
20. 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.

UNIDAD DIDÁCTICA 2. INCIDENCIAS Y ALERTAS EN PROYECTOS DE VIDEO VIGILANCIA

1. Incidencias de fallos en hardware: Proceso de reinstalación de dispositivos averiados
2. Incidencias de fallos en Software: Proceso de reconfiguración / actualización / sustitución del software de gestión.
3. Tratamiento de errores o alertas de mal funcionamiento.
4. Sistemas y herramientas de detección de errores, tanto a nivel de hardware como software
5. Procesos de depuración y reconfiguración del sistema
6. Prueba y puesta en marcha de la nueva configuración del sistema
7. Incidencias de Modificación del entorno. Adaptación a las nuevas configuraciones.
8. Cambio de escenario a vigilar debido a muebles, árboles, arbustos u otros obstáculos físicos para el correcto funcionamiento del sistema.
9. Alteración de la estructura a vigilar. Procesos de reposicionamiento y nueva configuración del sistema
10. Gestión de cambios en la configuración requerida por la dirección del lugar
11. Avisos, Gestión y modificaciones en remoto del sistema de video vigilancia
12. Generación de la nueva documentación o actualización de la documentación ya existente tras las operaciones de gestión de incidencias
13. Actualización y mejora del estado del sistema de videovigilancia
14. Evaluación del estado del sistema
15. Propuestas de mejora del sistema
16. Aplicación de nuevas funcionalidades: Procesos para la actualización / ampliación / integración del sistema de video vigilancia

UNIDAD DIDÁCTICA 3. PROCESOS Y TAREAS DE MANTENIMIENTO EN SISTEMAS DE CONTROL DE ACCESOS Y PRESENCIA

1. Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento de los dispositivos hardware del sistema.
2. Mantenimiento mecánico de los dispositivos físicos de control de accesos: Barreras, puertas, tornos y resto de dispositivos mecánicos del sistema
3. Mantenimiento eléctrico y electrónico de las automatizaciones de control: Cerraduras, tarjetas y componentes electrónicos e informáticos del sistema
4. 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
5. Comprobación de Dispositivos de interconexión, sujeción, Cableado e infraestructura de monitorización, avisos y control
6. Mantenimiento de Soporte del sistema de Gestión y almacenamiento de datos
7. Mantenimiento de los Sistemas de protección y alimentación ininterrumpida o SAI.
8. 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
9. 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
10. Comprobación la correcta parametrización a nivel software de los dispositivos del sistema
11. Actualización en caso necesario del software de gestión

12. Comprobación del sistema de copias de seguridad y el acceso a información del sistema.
13. Comprobación del sistema de seguridad, nivel de privilegios y protección del sistema
14. Actualización del firmware de los dispositivos que lo requieran
15. 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.
16. Mantenimiento del hardware y dispositivos físicos de comunicación o integración con otras redes:
17. Pasarelas de comunicación
18. Módulos de entradas y salidas interconectadas entre sistemas
19. Pruebas y protocolos de evaluación y correcto funcionamiento de la comunicación a nivel software
20. Actualizar el sistema para seguir cumpliendo con la normativa técnica y legal en el momento de realizar el mantenimiento en caso de necesitarla
21. Generación de la nueva documentación o Actualización de la documentación ya existente tras las operaciones de mantenimiento
22. 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.

UNIDAD DIDÁCTICA 4. GESTIÓN DE INCIDENCIAS Y ALERTAS

1. Incidencias de fallos en hardware: Proceso de Re instalación de dispositivos averiados
2. Incidencias de fallos en Software: Proceso de reconfiguración / actualización / sustitución del software de gestión.
3. Tratamiento de errores o alertas de mal funcionamiento.

4. Sistemas y herramientas de Detección de errores, tanto a nivel de hardware como software
5. Procesos de Depuración y reconfiguración del sistema
6. Prueba y puesta en marcha de la nueva configuración del sistema
7. Incidencias de Modificación del entorno. Adaptación a las nuevas configuraciones.
8. Alteración de la estructura a controlar. Procesos de reposicionamiento y nueva configuración del sistema
9. Gestión de cambios en la configuración requerida por la dirección del lugar
10. Avisos, Gestión y modificaciones en remoto del sistema de control de accesos y presencia
11. Generación de la nueva documentación o Actualización de la documentación ya existente tras las operaciones de gestión de incidencias
12. Actualización y mejora del estado del sistema de control de accesos
13. Evaluación del estado del sistema
14. Propuestas de mejora del sistema
15. Aplicación de nuevas funcionalidades: Procesos para la actualización / ampliación / integración del sistema de control de accesos

MODALIDAD

METODOLOGÍA

Online. Se entrega el material a través de nuestra plataforma virtual homologada. Contará con acceso a la misma las 24 horas al día los 365 días a la semana.

http://cursosonline.workingformacion.com

DURACIÓN

200 horas

IMPARTIDO POR

Tutor experto en la materia. Contará con apoyo a través de nuestra plataforma en todo momento.

Al finalizar el curso se hará entrega de un
DIPLOMA HOMOLOGADO

Working

Formación Integral S.L.

Paseo Rosales 32, local 9 50008 Zaragoza
976 242 109 - info@workingformacion.com

www.workingformacion.com