

TÉCNICO



TÉCNICO EXPERTO EN VIDEOVIGILANCIA, PROTECCIÓN
DE DATOS Y SEGURIDAD PRIVADA

T014

- DIPLOMA AUTENTIFICADO POR NOTARIO EUROPEO -



DESTINATARIOS

Este curso está dirigido a empresarios, directivos, emprendedores, trabajadores y cualquier persona que pretenda adquirir conocimientos relativos a videovigilancia, protección de datos y seguridad privada.

Permite conocer los sistemas de videovigilancia, el video y tratamiento de la imagen, el almacenamiento de la información obtenida, los sistemas de control de acceso y presencia y la protección y seguridad del sistema y de los datos e información aportada por el sistema, entre otros aspectos relacionados con el curso. Además, al final de cada unidad didáctica el alumno/a encontrará ejercicios de autoevaluación que le permitirá hacer un seguimiento de los conocimientos adquiridos a lo largo del curso de forma autónoma.

El alumno recibirá acceso a un curso inicial donde encontrará información sobre la metodología de aprendizaje, la titulación que recibirá, el funcionamiento del Campus Virtual, qué hacer una vez el alumno haya finalizado e información sobre Grupo Esneca Formación. Además, el alumno dispondrá de un servicio de **clases en directo**.

FICHA TÉCNICA

CARGA HORARIA
300H



MODALIDAD
A DISTANCIA



*Incluye módulos con clases en
directo

CURSO INICIAL
ONLINE



TUTORIAS
PERSONALIZADAS



IDIOMA
ESPAÑOL



DURACION
HASTA UN AÑO
*Prorrogable



IMPORTE

VALOR ORIGINAL: ~~1520 €~~

VALOR ACTUAL: 380 €

CERTIFICACIÓN OBTENIDA

Una vez finalizados los estudios y superadas las pruebas de evaluación, el alumno recibirá un diploma que certifica el “**TÉCNICO EXPERTO EN VIDEOVIGILANCIA, PROTECCIÓN DE DATOS Y SEGURIDAD PRIVADA**”, de ESNECA BUSINESS SCHOOL, avalada por nuestra condición de socios de la CECAP y AEEN, máximas instituciones españolas en formación y de calidad.

Los diplomas, además, llevan el sello de Notario Europeo, que da fe de la validez, contenidos y autenticidad del título a nivel nacional e internacional.

REDES SOCIALES



CONTENIDO FORMATIVO

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
 - Formación, tratamiento y transmisión de la imagen analógica
 - Características y formatos de vídeo analógico
 - Ventajas e inconvenientes del vídeo analógico
4. Análisis de la señal de vídeo e imagen Digital
 - Formación, tratamiento y transmisión de la imagen digital
 - Características y formatos de vídeo analógico
 - Ventajas e inconvenientes del vídeo digital
5. 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:
 - Protección mediante un sistema de alimentación ininterrumpida los dispositivos de toda la instalación de video vigilancia
 - Copias de seguridad y sistemas de prevención de pérdidas de datos
 - Redundancia
 - Acceso protegido y gestión de privilegios en los sistemas de videovigilancia
 - Autenticación de la información. Marca de Agua
 - 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
 - A demanda
 - Planificada
 - Continua
 - Por eventos
 - Detección de movimiento
2. Configuraciones de visualización
3. Búsqueda inteligente de eventos
4. Generación de eventos
5. Seguridad: Gestión de alertas y avisos; Interacción con otros sistemas y/o redes de comunicación o CRA (Centrales receptoras de alarmas)
6. Análisis, proceso y obtención de información relevante: Video Inteligente: Video procesado por herramientas de software informático:
 - Conteo de personas
 - Reconocimiento Facial
 - Seguimiento de objetos y personas
 - Lector de Matriculas
 - Avisos sobre objetos que desaparecen / aparecen
 - Análisis de trayectorias y recorridos
 - Obtención de informes y estadísticas
 - Detección de situaciones anómalas
 - Procesado de Imagen
 - 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
 - Restricciones de los sistemas y de funcionalidad
 - Limitaciones de los dispositivos de captación de vídeo, transmisión de vídeo, comunicación y almacenamiento.
 - Problemática del medio de comunicación (distancias, interferencias, atenuaciones, etc.)
 - Problemática debida al medio y la localización del sistema (entorno)
 - Protecciones de los aparatos (lps)
 - Factor Humano
2. Evaluación de los niveles de riesgo y tipos de amenazas
3. Evaluación de las necesidades de vigilancia y nivel de protección
4. Análisis de la situación: ¿Qué hay que vigilar?
5. Planteamiento: ¿Cómo y cuándo vigilar? ¿Desde dónde vigilar? ¿Quién ha de vigilar?
6. Estructuración del sistema y búsqueda de la ubicación óptima de los dispositivos
7. Planteamiento de las funcionalidades del sistema
8. Integración con otros sistemas y redes: reacciones y posibilidades ante una detección o evento
9. Criterios de selección del dispositivos
10. Interpretación y evaluación del proyecto y la infraestructura necesaria para acometerlo
11. Estimación de tiempos de ejecución, recursos y personal necesario
12. Interpretación de manuales así como de las características y funciones de los aparatos proporcionados por los fabricantes. (incluso en otros idiomas)
13. Comprobación del cumplimiento de la Normativa y reglamentación sobre Seguridad Privada y Ley Orgánica de Protección de Datos
14. Configuración del sistema y puesta en marcha tanto del software como del hardware, según las especificaciones y funcionalidades requeridas.
15. Documentación generada o utilizada en el proceso:
 - Usada:
 - Proyecto: memoria, planos, pliego de condiciones y requisitos necesarios
 - Proyecto de las instalaciones a Vigilar
 - Normativa técnica
 - Normativa legal aplicada
 - Generada
 - Informe de puesta en marcha
 - Libro de seguimiento e incidencias
 - Reflejo fiel del estado final de la instalación
 - Informe de configuración del sistema
 - 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
 - Electro cerraduras
 - Puertas y Barreras
 - Torniquetes y Tornos
 - Rampas y Elevadores
 - Sistemas diseñados para minusválidos
 - Otros tipos de activaciones o eventos
2. Dispositivos, Sistemas y tecnologías de identificación / autenticación
 - Relojes de control y / o tarificación
 - Teclados: Códigos y contraseñas de acceso
 - Lectores de tarjeta
 - Códigos de barra
 - Banda Magnética
 - Lectores de proximidad
 - Tarjetas o chips de proximidad. Tecnología RFID
 - Bluetooth
 - Otras
 - Sensores Biométricos e Identidad biométrica; Como identificar a través de rasgos y factores únicos en cada persona
 - Lector de Huella digital
 - Lector de Palma o estructura de la mano
 - Reconocimiento Facial
 - Reconocimiento del Iris
 - Reconocimiento de retina
 - Sistemas de reconocimiento de voz
3. Dispositivos, Software y datos de control del sistema
 - Hardware de control e integración de sistema
 - Conectividad y cableado. Infraestructura, funcionamiento y topología de los sistemas de control de acceso y presencia
 - Punto de gestión y monitorización del sistema:
 - Configuración y parametrización del sistema
 - Solución Hardware o Software.
 - Herramientas de extracción de informes
 - Software de tratamiento de datos.
 - 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:
 - Generación de estadísticas y datos de ocupación
 - Tarificación de servicios y tiempos
4. Sistemas de localización, control y detección de personas en un entorno cerrado; control de errantes no intrusivo
5. Sistemas de control médico, acceso a datos y posibilidad de actualización de información automatizado. (Aplicable a otros procesos similares)
6. Gestión de alarmas y eventos
 - Accesos no deseados
 - Alertas no permitidos o fuera de horario
 - Alarmas de averías o mal funcionamiento del sistema
 - Interacción con otros sistemas y/o redes de comunicación o CRA (Centrales receptoras de alarmas)
7. Soluciones de control logístico y de distribución
8. 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
 - 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
 - Restricciones de los sistemas y de su funcionalidad
 - Problemática del medio de comunicación (número máximo de dispositivos, distancias, interferencias, atenuaciones, etc.)
 - Problemática debida al medio y la localización del sistema (entorno)
 - Protecciones de los aparatos (lps)
 - Factor Humano
2. Evaluación de los niveles de riesgo y tipos de amenazas
3. Evaluación de las necesidades y definición del servicio y funcionalidades a implantar
4. Interpretación y evaluación del proyecto y la infraestructura necesaria para acometerlo
5. Estimación de tiempos de ejecución, recursos y personal necesario
6. Interpretación de manuales así como de las características y funciones de los aparatos proporcionados por los fabricantes. (incluso en otros idiomas)
7. Análisis de la situación: ¿Qué accesos hay que controlar?
8. Planteamiento y planificación: ¿Cómo y cuándo se controlan? ¿Desde dónde controlar y gestionar el sistema?
9. Estructuración del sistema y búsqueda de la ubicación optima de los dispositivos
10. Planteamiento de las funcionalidades del sistema
11. Integración con otros sistemas y redes: Reacciones y posibilidades ante una detección o evento
12. Comprobación el cumplimiento de la normativa y reglamentación sobre seguridad privada y Ley Orgánica de Protección de Datos
13. Configuración del sistema y puesta en marcha tanto del software como del hardware, según las especificaciones y funcionalidades requeridas.
14. Documentación generada o utilizada en el proceso:
 - Usada:
 - Proyecto: memoria, planos, pliego de condiciones y requisitos necesarios
 - Proyecto de las instalaciones a controlar
 - Normativa técnica
 - Normativa legal aplicada
 - Generada
 - Informe de puesta en marcha
 - Libro de Seguimiento e incidencias
 - Reflejo fiel del estado final de la instalación
 - Informe de Configuración del sistema
 - 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