Actividades formativas

CÓDIGO	**TÍTULO**
FFP-AV-2021-01	Inteligencia Artificial y Big Data
FFP-AV-2021-02	Instalación y mantenimiento de sistemas conectados a internet (IoT)
FFP-AV-2021-03	Ciberseguridad en Entornos de las Tecnologías de la Información

Características de los cursos

FFP-AV-2021-01.- Inteligencia Artificial y Big Data

Nivel: Intermedio

Número de horas: 100

Plazas: 20

Período de realización Del 22 de septiembre al 29 de octubre de 2021

Localidad de impartición: Curso online

Profesorado preferente: Encargado de impartición del curso de especialización Inteligencia Artificial y Big Data;

Objetivos:

- Aplicar sistemas de Inteligencia Artificial para identificar nuevas formas de interacción en los negocios que mejoren la productividad.
- Desarrollar e implementar sistemas de Inteligencia Artificial que faciliten la toma de decisiones ágiles dentro de un negocio gestionando y explotando datos masivos.
- Gestionar la transformación digital necesaria en las organizaciones para la consecución de la eficiencia empresarial mediante el tratamiento de datos.
- Aplicar Inteligencia Artificial en funcionalidades, procesos y sistemas de decisión empresariales.
- Gestionar los distintos tipos de Inteligencia Artificial para la consecución de transformación y cambio en las empresas.
- Administrar el desarrollo de procesos automatizados que permitan la mejora de la productividad de las empresas.
- Optimizar el desarrollo de procesos autónomos empleando herramientas de Inteligencia Artificial.
- Integrar sistemas de explotación de grandes volúmenes de datos aplicando soluciones de Big Data.
- Implantar las funcionalidades, procesos y sistemas de decisiones empresariales aplicando técnicas de Big Data en ellos.
- Ejecutar el sistema de explotación de datos según las necesidades de uso y las condiciones de seguridad establecidas asegurando el cumplimiento de los principios legales y éticos.
- Configurar las herramientas que se usan para construir soluciones Big Data y de Inteligencia Artificial.
- Gestionar de manera eficiente los datos, la información y su representación para transformarlos en conocimiento.

Competencias

Competencia científica	Competencia en innovación y mejora
Competencia didáctica	Competencia Digital (TIC)

Contenidos

1. Modelos de Inteligencia Artificial:
    - Caracterización de sistemas de Inteligencia Artificial.
    - Utilización de modelos de Inteligencia.
    - Caracterización de sistemas de Inteligencia Artificial.
    - Utilización de modelos de Inteligencia Artificial.
    - Procesamiento del Lenguaje Natural.
    - Análisis de sistemas robotizados.
    - Sistemas Expertos.
    - Aplicación de principios legales y éticos de la Inteligencia Artificial.
    - Procesamiento del Lenguaje Natural.
    - Análisis de sistemas robotizados.
    - Sistemas Expertos.
    - Aplicación de principios legales y éticos de la Inteligencia Artificial.

2. Sistema y aprendizaje automático:
    - Caracterización de la Inteligencia Artificial fuerte y débil.
    - Determinación de sistemas de aprendizaje automático (*Machine Learning*).
    - Algoritmos aplicados al aprendizaje supervisado y optimización del modelo.
    - Aplicación de técnicas de aprendizaje no supervisado.
    - Aplicación de modelos computacionales de redes neuronales y comparación con otros modelos.
    - Valoración de la calidad de los resultados obtenidos en la práctica con sistemas de aprendizaje automático.

3. Programación de Inteligencia Artificial:
    - Caracterización de lenguajes de programación. Principales lenguajes de programación para Inteligencia Artificial.
    - Desarrollo de aplicaciones de IA: Plataformas y entornos de modelado.

- Evaluación de la Convergencia tecnológica en diferentes sistemas.
- Evaluación de modelos de automatización industrial y de negocio.

4. Sistemas de Big Data:
    - Aplicación de técnicas de integración, procesamiento y análisis de información.
    - Configuración de cuadros de mando en entornos computacionales.
    - Gestión y almacenamiento de datos. Búsqueda de respuestas en grandes conjuntos de datos.
    - Aplicación de herramientas para la visualización de datos.
5. Big Data aplicado:
    - Gestión de soluciones con sistemas de almacenamiento y herramientas del centro de datos para la resolución de problemas.
    - Gestión de sistemas de almacenamiento y ecosistemas Big Data.
    - Generación de mecanismos de Integridad de los datos. Comprobación de mantenimiento de sistemas de ficheros.
    - Monitorización, optimización y solución de problemas.
    - Validación de técnicas *Big Data* en la toma de decisiones en Inteligencia de negocios BI.

FFP-AV-2021-02.- Instalación y mantenimiento de sistemas conectados a internet (IoT)

Nivel: Intermedio

Número de horas: 100

Plazas: 20

Período de realización Del 22 de septiembre al 29 de octubre de 2021

Localidad de impartición: Curso online

Profesorado preferente: Encargado de impartición del curso de especialización Instalación y mantenimiento de sistemas conectados a internet (IoT);

Objetivos:

- Analizar la normativa y la documentación técnica de la infraestructura de dispositivos y sistemas conectados para obtener y procesar información Curso de especialización en Instalación y mantenimiento de sistemas conectados a internet (IoT)
- Identificar y seleccionar herramientas, equipos de instalación y montaje, materiales de seguridad de IoT, analizando las condiciones de la infraestructura para aplicar el plan de aprovisionamiento de los recursos y medios necesarios.
- Obtener y valorar el coste de materiales y recursos humanos, para elaborar presupuestos de instalación y mantenimiento de proyectos de IoT.
- Ubicar y fijar elementos IoT de la infraestructura, sensores, dispositivos elementos auxiliares, entre otros, para su instalación y mantenimiento.
- Identificar y evaluar el soporte lógico asociado a sistemas de comunicación de IoT para su instalación, configuración y mantenimiento.
- Identificar y analizar equipos, sensores, elementos auxiliares de dispositivos de acceso a redes para instalar, configurar y mantener la conectividad de sistemas de comunicación de IoT.
- Aplicar pruebas funcionales, test sobre dispositivos y de comprobación de la infraestructura de IoT, ya sea in situ o a distancia en remoto con software específico para verificar y validar su funcionamiento.
- Redactar, siguiendo los protocolos, informes técnicos de instalación, configuración y mantenimiento de instalaciones de IoT para cumplimentar la documentación técnica y administrativa asociada a los procesos de instalación, montaje y de mantenimiento.
- Aplicar el programa establecido para realizar el plan de mantenimiento (predictivo, preventivo y correctivo) de los sistemas y equipos conectados en condiciones de calidad y seguridad.
- Detectar las disfunciones y las anomalías o averías de los sistemas y equipos conectados para efectuar el mantenimiento correctivo de los mismos.
- Aplicar los protocolos y las medidas preventivas de riesgos laborales y protección ambiental durante el proceso productivo para evitar daños en las personas y en el entorno laboral y ambiental.

- Actuar con responsabilidad y autonomía en el ámbito de su competencia, organizando y desarrollando el trabajo asignado cooperando o trabajando en equipo con otros profesionales en el entorno de trabajo.
- Adaptarse a las nuevas situaciones laborales originadas por cambios tecnológicos y organizativos en los procesos productivos, actualizando sus conocimientos, utilizando los recursos existentes para el aprendizaje a lo largo de la vida y las tecnologías de la comunicación y de la información.
- Resolver de forma responsable las incidencias relativas a su actividad, identificando las causas que las provocan dentro del ámbito de su competencia y autonomía.
- Comunicarse eficazmente, respetando la autonomía y competencia de las distintas personas que intervienen en el ámbito de su trabajo.
- Aplicar procedimientos de calidad, de accesibilidad universal y de «diseño para todas las personas» en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

Competencias

Competencia científica	Competencia en innovación y mejora
Competencia didáctica	Competencia Digital (TIC)

Contenidos

1. Instalación de dispositivos y sistemas conectados, IoT.
    - Caracterización de sistemas conectados a internet.
    - Obtención de información y adecuación a proyectos IoT.
    - Determinación de recursos humanos y materiales en la implementación y puesta en servicio de proyectos IoT.
    - Configuración de dispositivos de sistemas de internet de las cosas.
    - Plan de seguridad y confidencialidad de datos en las instalaciones de IoT.
    - Instalación de dispositivos y sistemas conectados a internet, IoT.
    - Puesta en servicio y verificación de funcionamiento y prestaciones de sistemas IoT.
    - Aplicación de normas de prevención de riesgos laborales en sistemas IoT.

2. Mantenimiento y reparación de dispositivos y sistemas conectados, IoT:
    - Operaciones de mantenimiento predictivo de equipos y sistemas conectados, IoT.

- Realización del mantenimiento preventivo de sistemas de comunicaciones conectados, IoT.
- Realización del mantenimiento preventivo de equipos conectados, IoT.
- Realización del mantenimiento correctivo en instalaciones, sistemas y equipos.
- Aplicación de normas de prevención de riesgos laborales en dispositivos y sistemas conectados de IoT.

FFP-AV-2021-03.- Ciberseguridad en Entornos de las Tecnologías de la Información

Nivel: Intermedio

Número de horas: 100

Plazas: 15

Período de realización Del 22 de septiembre al 29 de octubre de 2021

Localidad de impartición: Curso online

Profesorado preferente: Encargado de impartición del curso de especialización Ciberseguridad en Entornos de las Tecnologías de la Información;

Objetivos:

- Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.
- Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.
- Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes.
- Configurar sistemas de control de acceso y autenticación en sistemas informáticos, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.
- Diseñar y administrar sistemas informáticos en red y aplicar las políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.
- Analizar el nivel de seguridad requerido por las aplicaciones y los vectores de ataque más habituales, evitando incidentes de ciberseguridad.
- Implantar sistemas seguros de desplegado de software con la adecuada coordinación entre los desarrolladores y los responsables de la operación del software.
- Realizar análisis forenses informáticos analizando y registrando la información relevante relacionada.
- Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados.
- Definir y aplicar procedimientos para el cumplimiento normativo en materia de ciberseguridad y de protección de datos personales, implementándolos tanto internamente como en relación con terceros.
- Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.

Competencias

Competencia científica	Competencia en innovación y mejora
Competencia didáctica	Competencia Digital (TIC)

Contenidos

1. Incidentes de ciberseguridad:
    - Desarrollo de planes de prevención y concienciación en ciberseguridad.
    - Auditoría de incidentes de ciberseguridad.
    - Investigación de los incidentes de ciberseguridad.
    - Implementación de medidas de ciberseguridad.
    - Detección y documentación de incidentes de ciberseguridad.

2. Bastionado de redes y sistemas.
    - Diseño de planes de securización.
    - Configuración de sistemas de control de acceso y autenticación de personas:
    - Administración de credenciales de acceso a sistemas informáticos.
    - Diseño de redes de computadores seguras.
    - Configuración de dispositivos y sistemas informáticos.
    - Configuración de dispositivos para la instalación de sistemas informáticos.
    - Configuración de los sistemas informáticos.
3. Puesta en producción segura.
    - Prueba de aplicaciones *web* y para dispositivos móviles.
    - Determinación del nivel de seguridad requerido por aplicaciones.
    - Detección y corrección de vulnerabilidades de aplicaciones *web*.
    - Detección de problemas de seguridad en aplicaciones para dispositivos móviles.
    - Implantación de sistemas seguros de desplegado de *software*.

4. Análisis forense informático.
    - Aplicación de metodologías de análisis forenses.
    - Realización de análisis forenses en dispositivos móviles.
    - Realización de análisis forenses en *Cloud*:
    - Realización de análisis forenses en *IoT*:
    - Documentación y elaboración de informes de análisis forenses. Apartados de los que se compone el informe.

5. *Hacking* ético.
    - Determinación de las herramientas de monitorización para detectar vulnerabilidades:
    - Ataque y defensa en entorno de pruebas, de las comunicaciones inalámbricas.
    - Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros.
    - Consolidación y utilización de sistemas comprometidos.
    - Ataque y defensa en entorno de pruebas, a aplicaciones *web*.
6. Normativa de ciberseguridad.
    - Puntos principales de aplicación para un correcto cumplimiento normativo.
    - Diseño de sistemas de cumplimiento normativo.
    - Legislación para el cumplimiento de la responsabilidad penal.
    - Legislación y jurisprudencia en materia de protección de datos.
    - Normativa vigente de ciberseguridad de ámbito nacional e internacional:
    - Esquema Nacional de Seguridad (ENS).
    - Ley PIC (Protección de infraestructuras críticas).