

▶ TALENTO  
TECH  
BOYACÁ · CUNDINAMARCA



# Curso Ciberseguridad

## NIVEL EXPLORADOR 1 - BÁSICO

¡Bienvenido al nivel básico del programa de Ciberseguridad! Si te interesa proteger la información y entender cómo defender sistemas frente a amenazas digitales, este es el punto de partida ideal.

Al finalizar este nivel, estarás preparado para oportunidades laborales como analista de ciberseguridad junior, técnico en soporte de redes o asistente en proyectos de seguridad informática. Sectores como negocios, salud, tecnología y gobierno buscan constantemente profesionales con estas habilidades esenciales en el mundo actual.

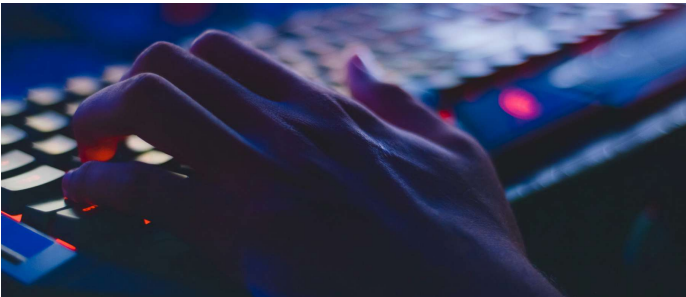
Aprenderás desde los fundamentos de la seguridad informática hasta la configuración de redes y la seguridad en la nube. Además, realizarás prácticas de laboratorio que te permitirán aplicar lo aprendido en situaciones reales.

Los Bootcamps de Talento Tech ofrecen una experiencia de aprendizaje integral, asegurando que no solo adquieras habilidades técnicas, sino también la confianza para enfrentar los desafíos del panorama tecnológico actual.



## Mínimo de ingreso:

Uso básico de un computador y navegación por internet  
 Deseable conocimiento básico en conceptos de redes de datos, seguridad informática y comunicaciones  
 Habilidades básicas de comprensión lectora, matemáticas y razonamiento abstracto.



## Objetivos

Comprender los fundamentos de ciberseguridad: Conocer los principios básicos y la importancia de proteger la información en entornos digitales.  
 Identificar amenazas y vulnerabilidades: Reconocer riesgos comunes y cómo afectan a sistemas y redes.

Configurar redes básicas: Aprender a configurar redes LAN y VLAN para asegurar una comunicación eficiente y segura.

Aplicar buenas prácticas de seguridad: Implementar acciones de higiene digital para proteger datos personales y corporativos.

Introducción a la seguridad en la nube: Entender cómo proteger datos y recursos en entornos cloud.

## Mínimo de Egreso:

Conocer los conceptos fundamentales de ciberseguridad.  
 Reconocer los modelos de seguridad en la red y sus principios básicos.  
 Aplicar acciones de higiene digital para proteger la confidencialidad, integridad y disponibilidad de la información.  
 Identificar vulnerabilidades, amenazas y riesgos en entornos digitales.  
 Entender los medios de transmisión y mecanismos de autenticación de redes.  
 Configurar redes LAN y VLAN básicas.  
 Reconocer el concepto de política de seguridad de la información para garantizar la protección de los recursos informáticos de una empresa

## Prerrequisitos

Conocimientos básicos de informática: Manejo de sistemas operativos y navegación web.  
 Interés en tecnología y seguridad: Curiosidad por entender cómo funcionan las redes y cómo se protegen.

Actitud proactiva: Disposición para aprender y resolver problemas de manera creativa.

## Duración Total: 159 HORAS

Técnico	105 Horas
Inglés	24 Horas
Habilidades de poder	15 Horas
Proyectos	15 Horas
<b>Total</b>	<b>159 Horas</b>

# Misión 1: Fundamentos de Seguridad Informática

## Entrenamiento

## Resultados de aprendizaje:

### 1 Mapa de ruta

**Objetivo:** Definir los objetivos y competencias a adquirir en la misión 1.

**Descripción:** Video educativo que introduce a la misión 1, presentando de forma clara y sencilla el proceso que el estudiante debe seguir para completar cada aspecto. Este video servirá como guía de orientación y estará diseñado para captar el interés del estudiante desde el inicio. Para lograrlo, se desarrollarán guiones basados en las 5W (Who, What, When, Where, Why - Quién, Qué, Cuándo, Dónde y Por qué), asegurando que cada aspecto importante del proceso sea cubierto y comprendido.

### Objetivos

**Comprender los Fundamentos de Ciberseguridad:** Conocer los principios básicos y la importancia de proteger la información en entornos digitales.

**Identificar Amenazas y Vulnerabilidades:** Reconocer riesgos comunes y cómo afectan a sistemas y redes.



Identificar los conceptos clave de seguridad informática, incluyendo la autenticación, la encriptación básica y los tipos de virus y ataques cibernéticos.

Explicar y ejemplificar los principios de confidencialidad, integridad y disponibilidad en entornos digitales. Realizar evaluaciones básicas de riesgos, amenazas y vulnerabilidades.

Reconocer métodos de ingeniería social y formular estrategias para protegerse de este tipo de ataques.

Reducir la superficie de ataque en sistemas personales mediante buenas prácticas de seguridad.

Detectar y analizar vulnerabilidades  
Desarrollar habilidades prácticas mediante la simulación y análisis de casos reales de ciberataques.

Implementar medidas básicas de seguridad en dispositivos y sistemas personales.

# Misión 1: Fundamentos de Seguridad Informática

## 2 Preparación

### Contenido del Módulo 1:

Introducción a la Seguridad Informática

Concepto de seguridad informática.  
Virus informáticos y tipos de ataques.  
Autenticación y mecanismos de seguridad.  
Conceptos básicos de encriptación.

Ciberseguridad

Pilares de la seguridad: confidencialidad, integridad y disponibilidad.  
Evaluación de riesgos, amenazas y vulnerabilidades.  
Ingeniería social y cómo protegerse.  
Superficie de ataque y su reducción.

Vulnerabilidades

Fundamentos y tipos de vulnerabilidades.  
Detección y análisis de vulnerabilidades.  
Metodologías y herramientas para el análisis.



## 3 English Code

Objetivo: Introducir vocabulario técnico en inglés relacionado con ciberseguridad.

Descripción:

Identificar y presentar un listado de términos esenciales al inicio de la formación de inglés con expresiones comunes en inglés técnico relacionados con ciberseguridad- glosario. Vocabulario específico de la documentación técnica.

Lectura de documentación guía de estudio.  
Comunicación básica en inglés técnico.  
Podcast completo en inglés especializado en ciberseguridad.

# Misión 1: Fundamentos de Seguridad Informática

## Experiencia

### 1 Simulación

Actividad:  
Análisis de casos reales de ataques cibernéticos.  
Implementación básica de medidas de seguridad en sistemas personales.

### 2 Laboratorios prácticos

Laboratorio 1: Análisis de vulnerabilidades utilizando herramientas básicas.  
Laboratorio 2: Configuración de medidas de seguridad en un entorno simulado.

### 3 Cápsulas

Propósito: Proporcionar herramientas y recursos de aprendizaje en diversos formatos multimedia para maximizar el aprendizaje y el desarrollo de los participantes sobre el módulo 1.

Los recursos incluyen:

Videos: Visualización de demostraciones y ejemplos prácticos.

Podcast: Información auditiva.

Infografías: Representaciones visuales que simplifican conceptos complejos.

Otros formatos: Tutoriales interactivos, foros y ejercicios prácticos.



### 4 Zona de Recarga - Power skills

Objetivo: Desarrollar y potenciar las habilidades de poder y socioemocionales necesarias para aprovechar oportunidades en el mercado laboral

Descripción: contenido módulo 1 y 2 de Power skills nivel básico

Comunicación y persuasión

Estrategias de comunicación persuasiva y su impacto en la influencia positiva.  
Manejo de conversaciones difíciles: cómo expresar críticas constructivas.  
Cómo adaptar el estilo de comunicación según la audiencia.

Resolución de conflictos

Identificación de los tipos y causas comunes de conflicto.  
Técnicas para abordar conflictos de manera constructiva.  
Estrategias de negociación y mediación en situaciones de tensión.

# Misión 1: Fundamentos de Seguridad Informática

## Conexión

### 1 Prosumidores

**Objetivo:** Enseñar metodologías para desarrollar proyectos y conceptos de educación financiera.

**Descripción:** contenido módulo 1 y 2 de Desarrollo de proyectos nivel básico

Exploración de proyectos enfocados en problemas regionales y sectoriales

**Objetivo:** Guiar a los estudiantes en la identificación de problemáticas locales y sectoriales de ciberseguridad mediante técnicas de observación y análisis.

**Temas:**

Introducción a la gestión de proyectos y su relevancia en la resolución de problemas.

Técnicas de observación y recolección de datos (observación directa, entrevistas, encuestas básicas).

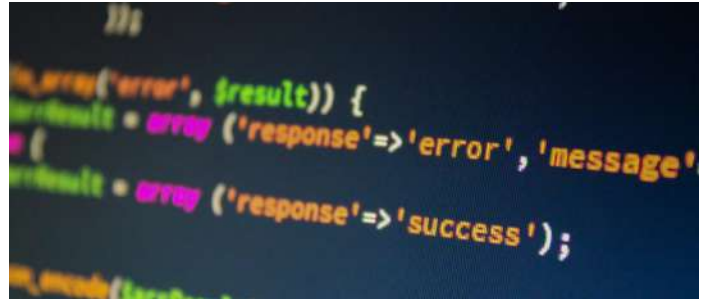
Diseño de ideas para la solución de problemas y conversión en proyectos

**Objetivo:** Enseñar a los estudiantes cómo convertir los problemas identificados en ideas de proyectos viables, considerando recursos limitados y un enfoque de sostenibilidad.

**Temas:**

Técnicas de generación de ideas (SCAMPER, mapas de empatía, etc.).

Priorización de ideas según su potencial impacto y viabilidad económica.



### 2 Co-creación

**propósito:** Aplicar de manera práctica los conocimientos de ciberseguridad en contextos específicos y dinámicos.

Los estudiantes trabajarán en proyectos que aborden sectores como el agro, educación, turismo, gobierno, finanzas, marketing, salud, entre otros, integrando sus conocimientos en un contexto en constante evolución.

### 3 Satélites

**Objetivo:** Facilitar la conexión con el sector laboral a través de interacción y networking.

**Actividades incluyen:**

Participación en conferencias, seminarios web, ferias de empleo y eventos de networking. Presentación de proyectos digitales o ideas emprendedoras, con la posibilidad de atraer inversores, colaboradores o clientes interesados en sus proyectos.

# Misión 2: Fundamentos de Redes y Sistemas Operativos GNU/Linux en Servidores

## Entrenamiento

### 1 Mapa de ruta

Definir los objetivos y competencias a adquirir en los Módulos 2 y 3.

Descripción: Video educativo que introduce a la misión 2, presentando de forma clara y sencilla el proceso que el estudiante debe seguir para completar cada aspecto. Este video servirá como guía de orientación y estará diseñado para captar el interés del estudiante desde el inicio. Para lograrlo, se desarrollarán guiones basados en las 5W (Who, What, When, Where, Why - Quién, Qué, Cuándo, Dónde y Por qué), asegurando que cada aspecto importante del proceso sea cubierto y comprendido.

## Objetivos

Configurar redes básicas: Aprender a configurar redes LAN y VLAN para asegurar una comunicación eficiente y segura.

Implementar medidas de gestión y seguridad en el entorno GNU/Linux: Desarrollar habilidades para crear y gestionar usuarios, configurar permisos y garantizar la seguridad de archivos, promoviendo buenas prácticas en entornos productivos.



## Resultados de aprendizaje:

Definir qué es una red y describir cómo funciona.

Identificar diferentes clasificaciones y topologías de redes.

Reconocer los dispositivos de interconexión como routers y switches, y su función en una red.

Explicar los modelos OSI y TCP/IP de manera clara y sencilla.

Aplicar conocimientos sobre direccionamiento IP.

Implementar y gestionar VLANs y redes inalámbricas.

Comprender la relevancia de GNU/Linux en servidores.

Gestionar usuarios y permisos de forma efectiva.

Realizar configuraciones básicas de servidores Linux.

# Misión 2: Fundamentos de Redes y Sistemas Operativos GNU/Linux en Servidores

## 2 Preparación

### Contenido del Módulo 2: Fundamentos de Redes:

Conceptos Básicos de Redes  
Definición y funcionamiento de las redes.  
Clasificación y topologías de redes.  
Dispositivos de interconexión: routers, switches, etc.  
Modelos OSI y TCP/IP.

Direccionamiento IP  
Comprensión de direcciones IP y su asignación.  
Subneteo básico y su importancia.

VLANs y Redes Inalámbricas  
Concepto y configuración de VLANs.  
Fundamentos de redes inalámbricas.  
Seguridad en Wi-Fi.

### Contenido del Módulo 3: Sistemas Operativos GNU/Linux en Servidores:

Introducción a GNU/Linux  
Historia y uso en el ámbito empresarial.  
Ventajas del software libre.

Terminal y Comandos Básicos  
Navegación por el sistema de archivos.  
Comandos esenciales: `ls`, `cd`, `mkdir`, `rm`, etc.

Gestión de Usuarios y Permisos  
Creación y gestión de usuarios y grupos.  
Manejo de permisos y seguridad en archivos.

Comandos Avanzados y Scripting  
Uso de editores de texto: `nano`, `vi`.  
Automatización y scripting básico en Bash.

## 3 English Code

Objetivo: Ampliar el vocabulario técnico en inglés relacionado con redes y sistemas operativos.

Descripción:

Lectura de documentación técnica en inglés.  
Casos de estudio  
Terminología específica de redes y Linux.  
Comunicación de conceptos técnicos en inglés.





# Misión 2: Fundamentos de Redes y Sistemas Operativos GNU/Linux en Servidores

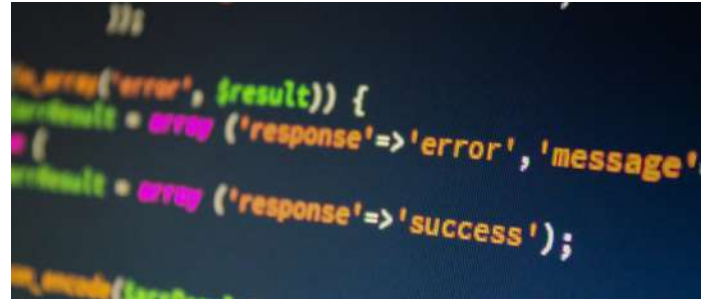
## Experiencia

### 1 Simulación

#### Actividad:

Configuración de redes LAN y VLANs en entornos simulados.

Prácticas con direccionamiento IP y subneteo.



### 2 Laboratorios prácticos

Laboratorio 1: Configuración de una red LAN básica en Packet Tracer.

Laboratorio 2: Creación y gestión de VLANs.

Laboratorio 3: Instalación y configuración básica de un servidor Linux.

Laboratorio 4: Implementación de servicios web y DHCP en Linux.

### 3 Cápsulas

Propósito: Proporcionar herramientas y recursos de aprendizaje en diversos formatos multimedia para maximizar el aprendizaje y el desarrollo de los participantes sobre el módulo 2 y 3.

Los recursos incluyen:

Videos: Visualización de demostraciones y ejemplos prácticos.

Podcast: Información auditiva.

Infografías: Representaciones visuales que simplifican conceptos complejos.

Otros formatos: Tutoriales interactivos, foros y ejercicios prácticos.

### 4 Zona de Recarga - Power skills

Objetivo: Desarrollar y potenciar las habilidades de poder y socioemocionales necesarias para aprovechar oportunidades en el mercado laboral.

Descripción: contenido módulo 3 y 4 de Power skills nivel básico

Atención al detalle y calidad en la ejecución

Cómo aplicar una mentalidad de calidad en la ejecución de tareas.

Técnicas de revisión y control de calidad para minimizar errores.

Atención al detalle en proyectos de alto impacto.

Resolución de conflictos

Técnicas para gestionar el estrés en situaciones de alta presión.

Adaptación al cambio: estrategias para mantener el enfoque y la calma en entornos de cambio constante.

Identificación de factores de estrés personal y técnicas para minimizarlos.

# Misión 2: Fundamentos de Redes y Sistemas Operativos GNU/Linux en Servidores

## Conexión

### 1 Prosumidores

**Objetivo:** Enseñar metodologías para desarrollar proyectos y conceptos de educación financiera.

**Descripción:** contenido módulo 3 y 4 de Desarrollo de proyectos nivel básico

Fundamentos de planificación y presupuesto en proyectos

**Objetivo:** Introducir a los equipos en los conceptos de planificación de proyectos y presupuesto básico, permitiendo que cada miembro contribuya con su especialidad a la estructuración del proyecto

**Temas:** Introducción al ciclo de vida del proyecto  
Fases de planificación

**Herramientas de planificación accesibles:** cronograma básico en hojas de cálculo y presupuesto inicial.

**Educación financiera:** Fundamentos de presupuesto y administración de recursos en proyectos colaborativos.

**Asignación de recursos y costos desde una perspectiva integral:** costos técnicos, recursos humanos, impacto social.

Trabajo en equipo y gestión financiera colaborativa

**Objetivo:** Capacitar a los estudiantes en técnicas de colaboración, roles de equipo y manejo financiero compartido para una administración trans-

parente y eficiente de los recursos del proyecto.

**Temas:** Roles y responsabilidades en equipos multidisciplinares.

Toma de decisiones en grupo y resolución de conflictos.

**Educación Financiera:** Registro y seguimiento de gastos en proyectos colaborativos.

Estrategias de optimización de recursos en equipo.

### 2 Co-creación

**Propósito:** Aplicar de manera práctica los conocimientos de redes y Linux en contextos específicos y dinámico.

Los estudiantes trabajarán en proyectos que aborden sectores como el agro, educación, turismo, gobierno, finanzas, marketing, salud, entre otros, integrando sus conocimientos en un contexto en constante evolución.

### 3 Satélites

**Objetivo:** Facilitar la conexión con el sector laboral a través de interacción y networking

**Actividades incluyen:** Participación en conferencias, seminarios web, ferias de empleo y eventos de networking.

Presentación de proyectos digitales o ideas emprendedoras, con la posibilidad de atraer inversores, colaboradores o clientes interesados en sus proyectos.

# Misión 3: Seguridad en la Nube con AWS y Gestión de la Seguridad de la Información

## Entrenamiento

### 1 Mapa de ruta

Definir los objetivos y competencias a adquirir en los Módulos 4 y 5

Descripción: Video educativo que introduce a la misión 3, presentando de forma clara y sencilla el proceso que el estudiante debe seguir para completar cada aspecto. Este video servirá como guía de orientación y estará diseñado para captar el interés del estudiante desde el inicio. Para lograrlo, se desarrollarán guiones basados en las 5W (Who, What, When, Where, Why - Quién, Qué, Cuándo, Dónde y Por qué), asegurando que cada aspecto importante del proceso sea cubierto y comprendido.

### Objetivos

Aplicar buenas prácticas de seguridad: Implementar acciones de higiene digital para proteger datos personales y corporativos.

Introducción a la seguridad en la nube: Entender cómo proteger datos y recursos en entornos cloud.

### Resultados de aprendizaje:

Identificar los beneficios y las responsabilidades del modelo de seguridad en la nube de AWS, diferenciando el alcance del modelo de responsabilidad compartida.

Identificar los beneficios y las responsabilidades del modelo de seguridad en la nube de AWS, diferenciando el alcance del modelo de responsabilidad compartida.

Gestionar de manera efectiva accesos y permisos mediante AWS IAM, configurando políticas, roles y autenticación multifactor para proteger recursos en la nube.

Implementar medidas de protección como grupos de seguridad, redes VPC y cifrado de datos, asegurando tanto la infraestructura como la información en reposo y en tránsito.

Emplear servicios como AWS CloudWatch y AWS Config para monitorear actividades, generar registros y responder proactivamente a posibles incidentes de seguridad.

Configurar una instancia segura, aplicando políticas básicas de seguridad y automatizando tareas con AWS Lambda para responder a amenazas.

# Misión 3: Seguridad en la Nube con AWS y Gestión de la Seguridad de la Información

## 2 Preparación

### Contenido del Módulo 4: Seguridad en la Nube con AWS

Introducción a la Seguridad en AWS

Beneficios y responsabilidades en la nube de AWS.

Modelo de responsabilidad compartida.

Protección del Acceso a Recursos

Uso de AWS IAM para gestión de accesos.

Políticas de seguridad y permisos.

Roles y autenticación multifactor.

Protección de Infraestructura y Datos

Configuración de grupos de seguridad y VPCs.

Cifrado de datos en reposo y en tránsito.

Uso de Amazon S3 para almacenamiento seguro.

Generación de Registros y Monitoreo

Importancia de la monitorización.

Servicios como AWS CloudWatch y AWS Config.

Gestión de Usuarios y Permisos

Creación y gestión de usuarios y grupos.

Manejo de permisos y seguridad en archivos.

Comandos Avanzados y Scripting

Uso de editores de texto: `nano`, `vi`.

Automatización y scripting básico en Bash.

### Contenido del Módulo 5: Gestión de la Seguridad de la Información

Políticas de Seguridad de la Información

Concepto e importancia.

Desarrollo e implementación en una organización.

Normativas y estándares de seguridad.

Planificación ante Desastres

Estrategias de planificación y recuperación.

Objetivos de Punto de Recuperación (RPO) y Tiempo de Recuperación (RTO).

Patrones de copias de seguridad y recuperación.

Uso de Amazon Storage Gateway para respaldos.

## 3 English Code

Objetivo: Consolidar el vocabulario técnico en inglés relacionado con seguridad en la nube y gestión de información.

Descripción:

Lectura de casos de estudio en inglés.

Terminología avanzada de AWS y seguridad.

Comunicación técnica avanzada en inglés.

# Misión 3: Seguridad en la Nube con AWS y Gestión de la Seguridad de la Información

## Experiencia

### 1 Simulación

#### Actividad:

Configuración de instancias seguras en AWS.  
Aplicación de políticas de seguridad y gestión de accesos.

### 2 Laboratorios prácticos

Laboratorio 1: Configuración de AWS IAM y políticas de acceso.

Laboratorio 2: Implementación de AWS Config y AWS Lambda para automatizar respuestas.

Laboratorio 3: Configuración de Amazon Storage Gateway y migración de datos.

Laboratorio 4: Simulación de recuperación ante desastres utilizando respaldos en AWS.

### 3 Cápsulas

Propósito: Proporcionar herramientas y recursos de aprendizaje en diversos formatos multimedia para maximizar el aprendizaje y el desarrollo de los participantes sobre el módulo 4 y 5.

Los recursos incluyen:

Videos: Visualización de demostraciones y ejemplos prácticos.

Podcast: Información auditiva.

Infografías: Representaciones visuales que simplifican conceptos complejos.

Otros formatos: Tutoriales interactivos, foros y ejercicios prácticos.



### 4 Zona de Recarga - Power skills

Objetivo: Desarrollar y potenciar las habilidades de poder y socioemocionales necesarias para aprovechar oportunidades en el mercado laboral.

Descripción: Contenido módulo 5 y 6 de Power skills.

Inteligencia emocional

Temas a tratar: Introducción a la inteligencia emocional: autoconocimiento y autocontrol. La empatía y su rol en la interacción interpersonal.

Estrategias para gestionar emociones en situaciones difíciles.

Trabajo en equipo.

Temas a tratar: Dinámicas y roles en el trabajo en equipo: cómo contribuir eficazmente.

Importancia de la colaboración y la comunicación en el logro de objetivos comunes.

Resolución de conflictos y toma de decisiones en equipo.

# Misión 3: Seguridad en la Nube con AWS y Gestión de la Seguridad de la Información

## Conexión

### 1 Prosumidores

**Objetivo:** Enseñar metodologías para desarrollar proyectos y conceptos de educación financiera.

**Descripción:** contenido módulo 5 de Desarrollo de proyectos nivel básico.

**Cierre del proyecto con análisis financiero**

**Objetivo:** Permitir que los equipos presenten su proyecto colaborativo y su análisis financiero, destacando la integración de múltiples áreas de conocimiento.

**Temas:** Técnicas de presentación y “pitch” colaborativo, con enfoque en la viabilidad y sostenibilidad de la propuesta.

**Integración de análisis financiero y técnico en la presentación.**

**Actividad práctica:** Los equipos presentan su proyecto final ante el grupo o un panel simulado. En la presentación, cada miembro explica la contribución de su área al proyecto y el equipo argumenta cómo su solución aborda el problema de manera integral, considerando el impacto financiero, social y técnico.

### 2 Co-creación

**Propósito:** Aplicar de manera práctica los conocimientos de redes y Linux en contextos específicos y dinámicos.

Los estudiantes trabajarán en proyectos que aborden sectores como el agro, educación, turismo, gobierno, finanzas, marketing, salud, entre otros, integrando sus conocimientos en un contexto en constante evolución.

### 3 Satélites

**Objetivo:** Facilitar la conexión con el sector laboral a través de interacción y networking.

**Actividades incluyen:** Participación en conferencias, seminarios web, ferias de empleo y eventos de networking.

**Presentación de proyectos digitales o ideas emprendedoras,** con la posibilidad de atraer inversores, colaboradores o clientes interesados en sus proyectos.

