

Ficha Técnica Estructurada: Summer Challenges CUGDL 2026

Este documento detalla la estructura formal del proyecto bajo el modelo de Células de Innovación, integrando los requerimientos corporativos y académicos para el ciclo 2026.

Descripción General del Proyecto (Project Overview)

Campo / Field	Detalles / Details
Nombre del proyecto	Lexfania 2
Nombre de la Entidad Receptora	Sublai
Sector al que pertenece la Entidad Receptora	Legatech
Breve descripción del giro de la Entidad Receptora	Lexfania es una plataforma de inteligencia artificial jurídica que ayuda a abogados, despachos y equipos legales a investigar, analizar y trabajar información legal con mayor rapidez y mejor fundamento.
Descripción detallada de la problemática que sea desea resolver	La problemática central que Lexfania busca resolver es que la información legal existe, pero no siempre es fácil de encontrar, comprender, relacionar y aplicar de forma eficiente. En la práctica, los usuarios suelen depender de buscadores tradicionales, bases jurídicas difíciles de navegar, documentos extensos o consultas manuales que requieren mucho tiempo y conocimiento especializado. Esto genera pérdida de productividad, altos costos operativos y mayor exposición a riesgos legales, especialmente cuando las normas cambian o cuando se necesita relacionar distintas disposiciones jurídicas en un mismo caso.

Campo / Field	Detalles / Details
	<p>Lexfania parte de una necesidad clara: reducir la fricción entre la persona que tiene una duda legal y la información normativa que necesita para tomar mejores decisiones. La plataforma fue diseñada para democratizar el acceso a la información legal, simplificando la interpretación y correlación de normativas mediante inteligencia artificial, de modo que profesionales del derecho, empresas y usuarios puedan tomar decisiones informadas con mayor rapidez y eficiencia.</p>
<p>Objetivos SMART que se desean alcanzar</p>	<p>SMART: <i>Specific</i> (Específico), <i>Measurable</i> (Medible), <i>Achievable</i> (Alcanzable), <i>Realistic</i> (Realista) y <i>Time-bound</i> (Tiempo limitado)</p> <p>Reducir en al menos 50% el tiempo promedio que los usuarios dedican a buscar legislación, jurisprudencia y fundamentos legales aplicables a un caso.</p> <p>Lograr que al menos 80% de las respuestas evaluadas por usuarios sean calificadas como útiles, correctas o suficientemente fundamentadas para apoyar una investigación legal inicial.</p> <p>Conseguir que al menos 1,000 usuarios registrados utilicen Lexfania para consultas legales, análisis de documentos o generación de contenido jurídico.</p>
<p>Alcance y limitaciones del proyecto</p>	<p>Grupo de Creatividad Digital y Crecimiento de Lexfania</p> <p>Propósito</p> <p>Diseñar, producir y ejecutar estrategias creativas digitales que aumenten la visibilidad, adopción y conversión de Lexfania entre abogados, despachos, empresas, estudiantes de derecho y áreas legales internas.</p> <p>Incrementar en un 40% la generación de leads calificados para Lexfania en un periodo de 6 meses, mediante campañas de contenido digital, materiales educativos, casos de uso y</p>

Campo / Field	Detalles / Details
	<p>estrategias creativas enfocadas en abogados, despachos y áreas legales internas.</p> <p>Grupo de Ciberseguridad, Cumplimiento e ISO 27001</p> <p>Propósito</p> <p>Diseñar, documentar e implementar las políticas, lineamientos, controles y procesos de ciberseguridad necesarios para fortalecer la protección de la información en Lexfania y preparar a la empresa para una futura certificación o alineación con SOC2 -ISO/IEC 27001.</p>
<p>Entregables que se desean lograr</p>	<p>Entregables principales</p> <ul style="list-style-type: none"> ● Diagnóstico inicial de ciberseguridad. ● Alcance del SGSI. ● Inventario de activos. ● Matriz de riesgos. ● Declaración de aplicabilidad. ● Políticas de seguridad. ● Procedimientos operativos. ● Plan de respuesta a incidentes. ● Plan de continuidad. ● Registro de proveedores críticos. ● Evidencias de cumplimiento. ● Programa de capacitación. ● Roadmap hacia ISO 27001. ● Evaluación de madurez.
<p>Cantidad de Integrantes por equipo</p>	<p>3</p>

Campo / Field	Detalles / Details						
<p>Licenciaturas de los integrantes del equipo (Mínimo 3, Máximo 5 por equipo)</p>	<table border="1"> <thead> <tr> <th data-bbox="584 483 1002 555">CARRERA</th> <th data-bbox="1002 483 1425 555">CANTIDAD DE ESTUDIANTES</th> </tr> </thead> <tbody> <tr> <td data-bbox="584 555 1002 663">Ciberseguridad</td> <td data-bbox="1002 555 1425 663">2</td> </tr> <tr> <td data-bbox="584 663 1002 813">Inteligencia Artificial y Ciencia de Datos</td> <td data-bbox="1002 663 1425 813">1</td> </tr> </tbody> </table>	CARRERA	CANTIDAD DE ESTUDIANTES	Ciberseguridad	2	Inteligencia Artificial y Ciencia de Datos	1
CARRERA	CANTIDAD DE ESTUDIANTES						
Ciberseguridad	2						
Inteligencia Artificial y Ciencia de Datos	1						
<p>Cantidad de equipos por reto</p>	<p>1</p>						
<p>Habilidades técnicas requeridas por los estudiantes</p>	<table border="1"> <thead> <tr> <th data-bbox="584 1171 1002 1243">CARRERA</th> <th data-bbox="1002 1171 1425 1243">HABILIDADES TÉCNICAS</th> </tr> </thead> <tbody> <tr> <td data-bbox="584 1243 1002 2009">Ciberseguridad</td> <td data-bbox="1002 1243 1425 2009"> <ul style="list-style-type: none"> 🎬 Conocimiento de redes, servidores, sistemas operativos y seguridad de la información. 🎬 Interés en ISO 27001, gestión de riesgos, políticas internas y protección de datos. 🎬 Capacidad para documentar lineamientos, procedimientos y controles de seguridad. 🎬 Atención al detalle para identificar riesgos, accesos, vulnerabilidades y buenas prácticas. 🎬 Conocimientos básicos de respaldos, control de accesos, monitoreo y respuesta a incidentes. </td> </tr> </tbody> </table>	CARRERA	HABILIDADES TÉCNICAS	Ciberseguridad	<ul style="list-style-type: none"> 🎬 Conocimiento de redes, servidores, sistemas operativos y seguridad de la información. 🎬 Interés en ISO 27001, gestión de riesgos, políticas internas y protección de datos. 🎬 Capacidad para documentar lineamientos, procedimientos y controles de seguridad. 🎬 Atención al detalle para identificar riesgos, accesos, vulnerabilidades y buenas prácticas. 🎬 Conocimientos básicos de respaldos, control de accesos, monitoreo y respuesta a incidentes. 		
CARRERA	HABILIDADES TÉCNICAS						
Ciberseguridad	<ul style="list-style-type: none"> 🎬 Conocimiento de redes, servidores, sistemas operativos y seguridad de la información. 🎬 Interés en ISO 27001, gestión de riesgos, políticas internas y protección de datos. 🎬 Capacidad para documentar lineamientos, procedimientos y controles de seguridad. 🎬 Atención al detalle para identificar riesgos, accesos, vulnerabilidades y buenas prácticas. 🎬 Conocimientos básicos de respaldos, control de accesos, monitoreo y respuesta a incidentes. 						

Campo / Field	Detalles / Details				
	<table border="1" data-bbox="582 409 1425 1209"> <tr> <td data-bbox="582 409 1002 1209">Inteligencia Artificial y Ciencia de Datos</td> <td data-bbox="1002 409 1425 1209"> <ul style="list-style-type: none"> 📖 Programación básica en Python y manejo de bases de datos. 📖 Conocimiento o interés en inteligencia artificial, modelos de lenguaje, análisis de datos y procesamiento de lenguaje natural. 📖 Capacidad para limpiar, clasificar, analizar y visualizar información. 📖 Pensamiento lógico y analítico para detectar patrones, medir resultados y mejorar procesos. 📖 Curiosidad técnica para investigar nuevas herramientas, automatizaciones e integraciones con IA. </td> </tr> </table>	Inteligencia Artificial y Ciencia de Datos	<ul style="list-style-type: none"> 📖 Programación básica en Python y manejo de bases de datos. 📖 Conocimiento o interés en inteligencia artificial, modelos de lenguaje, análisis de datos y procesamiento de lenguaje natural. 📖 Capacidad para limpiar, clasificar, analizar y visualizar información. 📖 Pensamiento lógico y analítico para detectar patrones, medir resultados y mejorar procesos. 📖 Curiosidad técnica para investigar nuevas herramientas, automatizaciones e integraciones con IA. 		
Inteligencia Artificial y Ciencia de Datos	<ul style="list-style-type: none"> 📖 Programación básica en Python y manejo de bases de datos. 📖 Conocimiento o interés en inteligencia artificial, modelos de lenguaje, análisis de datos y procesamiento de lenguaje natural. 📖 Capacidad para limpiar, clasificar, analizar y visualizar información. 📖 Pensamiento lógico y analítico para detectar patrones, medir resultados y mejorar procesos. 📖 Curiosidad técnica para investigar nuevas herramientas, automatizaciones e integraciones con IA. 				
Habilidades blandas requeridas por los estudiantes	<p data-bbox="582 1417 1358 1487">[Listado de habilidades que considere como necesarias por parte de las y los estudiantes]</p> <table border="1" data-bbox="582 1568 1425 1960"> <thead> <tr> <th data-bbox="582 1568 1002 1637">CARRERA</th> <th data-bbox="1002 1568 1425 1637">HABILIDADES BLANDAS</th> </tr> </thead> <tbody> <tr> <td data-bbox="582 1637 1002 1960">Ciberseguridad</td> <td data-bbox="1002 1637 1425 1960"> <ul style="list-style-type: none"> • Pensamiento analítico y atención al detalle. • Discreción y responsabilidad en el manejo de información sensible. • Capacidad para documentar procesos </td> </tr> </tbody> </table>	CARRERA	HABILIDADES BLANDAS	Ciberseguridad	<ul style="list-style-type: none"> • Pensamiento analítico y atención al detalle. • Discreción y responsabilidad en el manejo de información sensible. • Capacidad para documentar procesos
CARRERA	HABILIDADES BLANDAS				
Ciberseguridad	<ul style="list-style-type: none"> • Pensamiento analítico y atención al detalle. • Discreción y responsabilidad en el manejo de información sensible. • Capacidad para documentar procesos 				

Campo / Field	Detalles / Details	
		<p>de forma clara y ordenada.</p> <ul style="list-style-type: none"> • Pensamiento preventivo para identificar riesgos antes de que ocurran. • Comunicación clara para explicar lineamientos técnicos a personas no técnicas. • Disciplina para seguir políticas, controles y procedimientos.
	<p>Inteligencia Artificial y Ciencia de Datos</p>	<ul style="list-style-type: none"> • Pensamiento lógico y resolución de problemas. • Curiosidad y aprendizaje continuo. • Paciencia para analizar datos, errores y resultados. • Capacidad de investigación y autoaprendizaje. • Comunicación clara para explicar hallazgos técnicos de forma sencilla. • Trabajo colaborativo con áreas legales, comerciales y de producto.
<p>Acceso a bases de datos o información</p>	<p>SI / NO</p>	

Summer Challenges CUGDL

Verano 2026

Campo / Field	Detalles / Details
confidencial	
Otra información adicional que se considere relevante	N/A