



INSTITUTO INTERNACIONAL DE  
**INTRAEMPRENDIMIENTO**  
*Emprendiendo dentro de las organizaciones*



# **ASESORAMIENTO ACELERACIÓN EXPRESS**

**PROTEGE TU NEGOCIO ANTE  
AMENAZAS DIGITALES Y FORTALECE  
LA SEGURIDAD DE TU EMPRESA**

[www.institutodeintraemprendimiento.es](http://www.institutodeintraemprendimiento.es)







# PRESENTACIÓN

**DOTA A TU PYME DE LAS HERRAMIENTAS NECESARIAS  
PARA ENFRENTAR LOS DESAFÍOS DIGITALES ACTUALES**

El programa de Aceleración Exprés para PYMES y MICROPYMES, es una iniciativa de **INCIBE** (*Instituto Nacional de Ciberseguridad*), dentro del programa **INCIBE EMPRENDE 2023-2026**. Actividad Gratuita, financiada con fondos europeos **NEXT GENERATION** y diseñada específicamente para empresas que buscan mejorar sus capacidades en ciberseguridad de forma rápida y efectiva.

Empresas y Negocios que quieran aprender sobre las mejores prácticas necesarias para fortalecer su infraestructura digital, mejorar la gestión de riesgos y garantizar la continuidad de su negocio en un entorno cada vez más digitalizado.

# ¿A QUIÉN VA DIRIGIDO?



**Pequeñas y medianas empresas, con un equipo de entre 3 y 50 empleados que quieran implementar soluciones de seguridad digital y protegerse frente a ciberamenazas emergentes.**



**Sectores que dependen de la seguridad de datos como comercio, educación, salud, entre otros.**

**No se requieren conocimientos previos avanzados, ya que el programa incluye formación introductoria en planificación de seguridad.**





El programa de aceleración tiene una duración de 20 horas, distribuidas en sesiones prácticas e intensivas, diseñadas para asegurar que los participantes obtengan los conocimientos y recursos necesarios en un tiempo reducido.

Acceso a mentores y expertos del sector que guían a los participantes en la creación de estrategias efectivas. Las sesiones se realizan en formato online y/o presencial adaptándose a las características de la empresa o negocio.

# DURACIÓN



**20 horas de duración**



**Online y/o presencial**



# COMPETENCIAS Y HABILIDADES

Al finalizar el programa, las empresas participantes podrán:

- Desarrollar un Plan Director de Seguridad adaptado a cualquier tipo de organización y adaptado a su sector.
- Diagnóstico personalizado de vulnerabilidades y riesgos de la empresa.
- Identificar y gestionar riesgos de seguridad informática con metodologías efectivas.
- Mejorar la protección de los datos sensibles de sus clientes y empleados.
- Cumplir con los estándares de seguridad y normativas legales aplicables a su sector.
- Implementación rápida de medidas de ciberseguridad adaptadas a las necesidades del negocio.
- Implementar estrategias de defensa proactiva para la mitigación de amenazas cibernéticas.
- Aprender a utilizar e Integrar la inteligencia artificial en sus procesos de ciberseguridad.
- Establecer controles y auditorías de seguridad para evaluar la madurez organizacional. Aplicar la ISO 27032 y otras normativas en la gestión de seguridad.



# CALENDARIO CONTENIDO

SE REALIZARAN SESIONES PREVIAS DE COORDINACIÓN Y EXPLICACIÓN DE LA ACTIVIDAD CON LOS SOCIOS Y SPONSORS DE LAS COMPAÑÍAS ASI COMO CON LOS RESPONSABLES O COORDINADORES NOMBRADOS O QUEINTERVENGAN EN LA ACTIVIDAD. SESIONES ONLINE Y/O PRESENCIALES



## BLOQUE 1: FUNDAMENTOS DE LA CIBERSEGURIDAD EMPRESARIAL

- Introducción a los conceptos claves para la protección de Sistemas y Datos
- ¿Qué es un Plan Director de Seguridad?
- Importancia en la gestión de riesgos.
- Relación con la estrategia corporativa.



## BLOQUE 2: EVALUACIÓN Y ANÁLISIS DE RIESGOS

- Identificación de amenazas y vulnerabilidades.
- Metodologías de evaluación de riesgos.
- Impacto financiero y operativo de los riesgos deciberseguridad.





### **BLOQUE 3: DISEÑO DEL PLAN DIRECTOR DE SEGURIDAD**

- Definición de objetivos y alcance.
- Desarrollo de políticas y procedimientos de seguridad.
- Roles y responsabilidades dentro de la organización.



### **BLOQUE 5: RESPUESTA A INCIDENTES Y CONTINUIDAD DEL NEGOCIO**

- Planes de contingencia y recuperación ante desastres.
- Gestión de crisis y comunicación en ciberseguridad.
- Evaluación y mejora continua de la respuesta a incidentes.



### **BLOQUE 4: IMPLEMENTACIÓN Y GESTIÓN DE LA SEGURIDAD**

- Estrategias de control y monitoreo.
- Integración con marcos normativos (ISO 27032, NIST, ENS).
- Seguridad en infraestructuras tecnológicas.



### **BLOQUE 6: AUDITORÍA Y CUMPLIMIENTO NORMATIVO**

- ISO 27032: Aplicación y cumplimiento.
- Marco legal y regulaciones en ciberseguridad.
- Implementación de auditorías de seguridad.





## BLOQUE 7: ESTRATEGIAS AVANZADAS DE SEGURIDAD

- Inteligencia artificial aplicada a la ciberseguridad.
- Ciberseguridad en entornos cloud y redes industriales.
- Análisis de tendencias y amenazas emergentes.



## BLOQUE 8: PROYECTO FINAL Y RESULTADOS ESPERADOS

- Desarrollo de un Plan Director de Seguridad para una organización.
- Presentación Final del Plan Director
- Retroalimentación y revisión del plan.



Financiado por  
la Unión Europea  
NextGenerationEU



GOBIERNO  
DE ESPAÑA

MINISTERIO  
PARA LA TRANSFORMACIÓN DIGITAL  
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO  
DE TELECOMUNICACIONES  
E INFRAESTRUCTURAS DIGITALES



Plan de  
Recuperación,  
Transformación  
y Resiliencia





EL 90% DE LOS  
ATAQUES  
CIBERNÉTICOS  
COMIENZAN CON UN  
SIMPLE ERROR  
HUMANO. NO ESPERES  
A SER VÍCTIMA DE UN  
FRAUDE O FILTRACIÓN  
DE DATOS.  
¡EMPIEZA HOY MISMO!



INFORMACIÓN DE  
INSCRIPCIÓN Y CONTACTO

> [agustin.ruiz@institutodeintraemprendimiento.es](mailto:agustin.ruiz@institutodeintraemprendimiento.es)

> [info@institutodeintraemprendimiento.es](mailto:info@institutodeintraemprendimiento.es)

> [institutodeintraemprendimiento.es](http://institutodeintraemprendimiento.es)

> [info@institutodeintraemprendimiento.es](mailto:info@institutodeintraemprendimiento.es)





# INSTITUTO INTERNACIONAL DE INTRAEMPREDIMIENTO

*Emprendiendo dentro de las organizaciones*



Financiado por  
la Unión Europea  
NextGenerationEU



GOBIERNO  
DE ESPAÑA

MINISTERIO  
PARA LA TRANSFORMACIÓN DIGITAL  
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO  
DE TELECOMUNICACIONES  
E INFRAESTRUCTURAS DIGITALES



Plan de  
Recuperación,  
Transformación  
y Resiliencia



incibe\_  
INSTITUTO NACIONAL DE CIBERSEGURIDAD

