50 AÑOS formando los líderes que transforman el país

ACREDITACIÓN INSTITUCIONAL DE ALTA CALIDAD

VIGILADO **MINEDUCACIÓN**

Programa

CIBERSEGURIDAD PARA EJECUTIVOS

Con el **CESA** aprende a lo **largo de tu vida.**

PROGRAMA
CIBERSEGURIDAD PARA EJECUTIVOS

Modalidad

Blended
Online en vivo + 1 Clase presencial

Duración

45 horas

Metodología

¡Aprende con acción!

Este curso te sumerge en experiencias reales, guiadas por expertos que convierten la teoría en práctica de manera accesible y dinámica. Tu participación activa es clave para lograr tus objetivos de aprendizaje.

Certificaciones

Al completar el programa, recibirás un **Diploma CESA** que certifica tu **asistencia y participación**. Además, obtendrás una **credencial digital** emitida por el CESA que certifica el desarrollo de habilidades y competencias.

En un mundo cada vez más digitalizado, la seguridad de la información se ha convertido en una prioridad crítica para todas las organizaciones. Nuestro programa de ciberseguridad, ofrece una inmersión profunda en los conceptos esenciales y avanzados de la ciberseguridad.

El programa está estructurado en módulos que abarcan desde los conceptos básicos hasta las tecnologías emergentes y avanzadas en ciberseguridad así como la gobernanza de los datos. Los estudiantes aprenderán a aplicar inteligencia artificial y machine learning en estrategias de ciberseguridad, a diseñar y aplicar políticas de gobernanza de datos, y a implementar controles de seguridad efectivos. Además, se abordarán temas cruciales como la evaluación y gestión de riesgos, la seguridad en el Internet de las Cosas (IoT), y el análisis de riesgos y oportunidades en tecnologías emergentes como blockchain y criptoactivos.

Este programa no solo proporciona conocimientos teóricos, sino que también enfatiza el aprendizaje práctico y aplicado. Los estudiantes desarrollarán habilidades críticas para diseñar e implementar procedimientos de seguridad que aseguren la calidad e integridad de los datos en toda la organización. Con un enfoque en la resolución de problemas y la toma de decisiones estratégicas, los participantes estarán mejor preparados para enfrentar los desafíos modernos de la ciberseguridad y proteger los activos digitales en un mundo en constante evolución tecnológica.

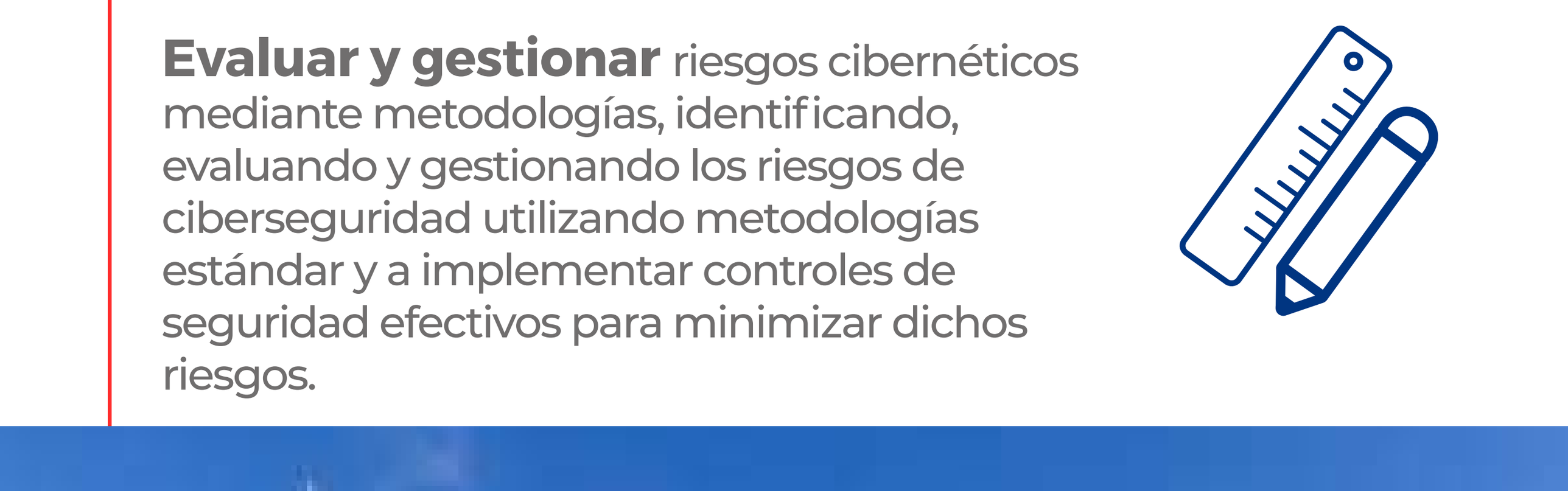
¿QUÉ LOGRARÁS CON EL PROGRAMA?

Comprender conceptos fundamentales de ciberseguridad en diversos entornos tecnológicos, utilizando marcos legales y regulaciones vigentes.

Implementar tecnologías emergentes en estrategias de ciberseguridad mediante la integración de inteligencia artificial y machine learning en la ciberseguridad.

Aplicar procedimientos de gobernanza de datos para desarrollar e implementar políticas que aseguren la calidad e integridad de los datos en toda la organización, utilizando herramientas tecnológicas avanzadas para facilitar la toma de decisiones estratégicas.

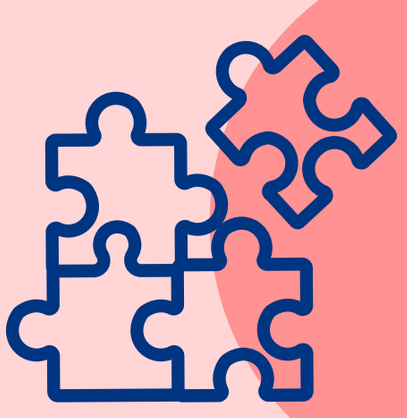
Evaluar y gestionar riesgos cibernéticos mediante metodologías, identificando, evaluando y gestionando los riesgos de ciberseguridad utilizando metodologías estándar y a implementar controles de seguridad efectivos para minimizar dichos riesgos.



¿QUÉ COMPETENCIAS Y HABILIDADES DESARROLLARÁS CON ESTE PROGRAMA?

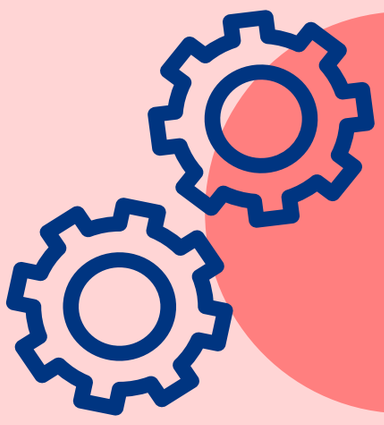
Liderazgo CESA

- Conectar a las personas.
- Multiplicar combinando talentos y recursos.
- Solucionar.



Data Driven

- Toma de decisiones basada en datos.
- Resolución de problemas.
- Comunicar con datos.
- Recopilación de datos • Interpretación.

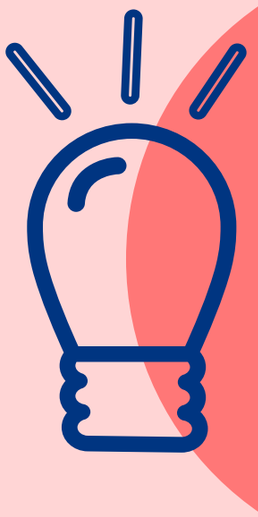


Aprendizaje continuo

- Autorregular el aprendizaje (autogestión).
- Establecer planes de acción objetivos.

Pensamiento crítico

- Analizar.
- Cuestionar y preguntar.
- Contrastar perspectivas.



Solución creativa de problemas

- Desarrollar diferentes tipos de pensamiento.
- Liderar equipos.
- Analizar información.
- Tomar decisiones.
- Generar soluciones creativas e innovadoras.

¿POR QUÉ DEBERÍA HACER ESTE PROGRAMA?*

Cada vez más se requiere a personas que cuenten con los conocimientos en temas relacionados con la Ciberseguirdad, entre las razones, podemos encontrar:

1. Incremento en la demanda de profesionales de ciberseguridad

La demanda de profesionales de ciberseguridad ha aumentado significativamente en los países del grupo Five Eyes (Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos), así como en países de América Latina y Europa.

2. Transformación digital y pandemia:

La transformación digital acelerada y el impulso hacia el trabajo remoto debido a la pandemia de COVID-19 han aumentado las vulnerabilidades a las amenazas cibernéticas, lo que ha llevado a una mayor demanda de expertos en ciberseguridad.

3. Crecimiento en comparación con otras ocupaciones:

Este aumento en la demanda de profesionales de ciberseguridad ha superado el crecimiento de otras ocupaciones en muchos países, destacándose especialmente en Chile, Nueva Zelanda y Polonia.

4. Variedad de roles en ciberseguridad:

La creciente demanda abarca una variedad de roles dentro de la profesión de ciberseguridad, clasificados por la OCDE en cuatro principales: Analistas, Arquitectos e ingenieros, Auditores y Asesores, y Gerentes.

5. Mayores demandas; arquitectos y analistas:

A nivel global, los arquitectos y analistas de ciberseguridad son los trabajos más demandados en el sector.

Fuente: OCDE

https://www.oecd.org/en/topics/cyber-security-skills.html

¿PARA QUIÉN ES EL PROGRAMA?

Este programa de ciberseguridad está diseñado para gerentes y directivos de nivel medio y alto que buscan adquirir conocimientos fundamentales en ciberseguridad. Está especialmente orientado a aquellos con responsabilidades en la toma de decisiones estratégicas y la protección de activos digitales dentro de sus organizaciones, pero que no poseen un trasfondo técnico en ciberseguridad.

¿CUÁL ES EL CONTENIDO DEL PROGRAMA?

Módulo I:
Fundamentación de la Ciberseguridad y Seguridad de la Información

- Identificar los principales riesgos, amenazas y vulnerabilidades en ciberseguridad en el entorno corporativo.
- Aplicar principios fundamentales de seguridad de la información en diferentes contextos organizacionales.
- Conocer sobre las regulaciones y normas de ciberseguridad relevantes para la empresa a nivel internacional y regional.
- Analizar casos prácticos de incidentes de ciberseguridad.

Módulo II:
Diseño de Estrategia de Ciberseguridad, protocolos de prevención y directrices en la organización

- Conocer sobre el diseño e implementación de políticas de ciberseguridad que mitiguen riesgos y protejan activos críticos, así como de protocolos de prevención de ciberseguridad.
- Desarrollar directrices efectivas para la respuesta a incidentes de seguridad.
- Evaluar la efectividad de estrategias preventivas y correctivas en la ciberseguridad corporativa.
- Aplicar herramientas de gestión de amenazas y respuesta a incidentes en entornos diversos.
- Analizar las mejores prácticas para la gestión de la ciberseguridad en diferentes contextos.

Módulo III:
Gobernanza de la Estrategia de Ciberseguridad y Gobernanza de Datos

- Desarrollar un marco de gobernanza de datos alineado con la estrategia global de ciberseguridad.
- Aproximarse a las herramientas para gestionar la estrategia de ciberseguridad corporativa.
- Implementar controles de calidad e integridad de datos en la organización.
- Aplicar modelos de gobernanza para garantizar el cumplimiento normativo y la seguridad en la gestión de datos.
- Evaluar herramientas tecnológicas que soporten la gobernanza y seguridad de la información en procesos corporativos.

Módulo IV:
Rol de la alta dirección dentro de la gestión de la estrategia

- Evaluar cómo el liderazgo de la alta dirección influye en la cultura organizacional de ciberseguridad y en la capacidad de respuesta ante crisis.
- Desarrollar planes de acción estratégicos en los que la alta dirección lidere la implementación de controles de ciberseguridad y la gestión de riesgos.
- Diseñar políticas y estrategias de ciberseguridad que alineen la cultura organizacional con los objetivos y riesgos corporativos.

Módulo V:
Inteligencia Artificial, Innovaciones y Tendencias en Ciberseguridad

- Conocer tecnologías emergentes y su impacto en la ciberseguridad.
- Aplicar IA en estrategias de ciberseguridad.
- Evaluar los riesgos y estrategias de seguridad en el IoT.

Módulo VI:
Proyecto Integrador: Simulación de Estrategia de Ciberseguridad

- En el módulo final, los participantes aplicarán todos los conocimientos adquiridos en una simulación práctica donde deberán diseñar, implementar y defender una estrategia integral de ciberseguridad para un caso de estudio.

¿QUIERES REFORZAR TUS CONOCIMIENTOS?

Por tomar este programa tienes la posibilidad de complementar tus conocimientos con otros contenidos seleccionados para ti.

Crehana

Virtual CESA

¿QUIÉNES SON LOS EXPERTOS DOCENTES?

Luis Mariano Papagni

Ingeniero en Sistemas con posgrado en Derecho Informático y maestría en Regulación Digital, cuenta con 25 años de experiencia en tecnología en el sector público y privado. Ha ocupado cargos estratégicos en Argentina, impulsando la Transformación Pública Digital y contribuyendo a la innovación en administración gubernamental.

Jorge Bejarano

Ingeniero de Sistemas con más de 25 años de experiencia en tecnología y seguridad digital, ha liderado iniciativas clave en Colombia y representado al país en la ONU. Actualmente, es consultor del BID en Transformación Digital y Director Ejecutivo de Tech and Law Abogados Ingenieros Consultores SAS.

Carolina González Tabares

Directora de Lifelong Learning en el CESA, Carolina es experta en transformación digital y educación, liderando iniciativas innovadoras como el primer sistema de formación basado en Inteligencia Artificial en Colombia. Con un fondo en mercadeo y psicología del consumidor, impulsa el cambio en el ámbito educativo y empodera a las mujeres en tecnología.

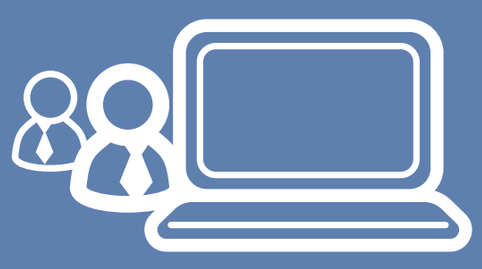
Orlando Garcés

Oficial de Políticas de Ciberseguridad en el CICTE de la OEA, con 23 años de experiencia en desarrollo e implementación de estrategias nacionales en América Latina y el Caribe. Ha trabajado en proyectos de ciberseguridad con la OEA, el BID y la Unión Europea, y posee múltiples maestrías y certificados en el campo.

¿POR QUÉ EL CESA?

Certificación de calidad:

Obtén un certificado con el Sello CESA de calidad y una credencial digital que validan tus habilidades y competencias adquiridas.

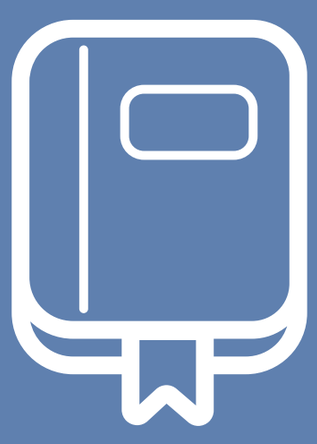


Oportunidades de networking:

Conecta con otros profesionales y aprovecha las oportunidades de networking, ya sea en entornos virtuales o presenciales, según la modalidad de tu programa.

Docentes expertos de la industria:

Aprende de profesionales con experiencia real en la industria, asegurando la relevancia y aplicabilidad de tus conocimientos.



Experiencia de aprendizaje personalizada:

Adapta tu proceso de aprendizaje a tus necesidades individuales, garantizando una experiencia educativa única.

Acceso a cursos complementarios:

Disfruta de cursos adicionales de CREHANA, enfocados en el área de conocimiento de tu programa.

Ruta de aprendizaje personalizada:

Accede a Luna del CESA para obtener una ruta de aprendizaje personalizada diseñada por IA (Inteligencia Artificial).

50 AÑOS formando los líderes que transforman el país

ACREDITACIÓN INSTITUCIONAL DE ALTA CALIDAD

VIGILADO **MINEDUCACIÓN**

Para mayor información escríbenos a
nuestra línea de **WhatsApp**

315 419 1199

cesa.edu.co

CESA

CESA_edu

cesa_edu