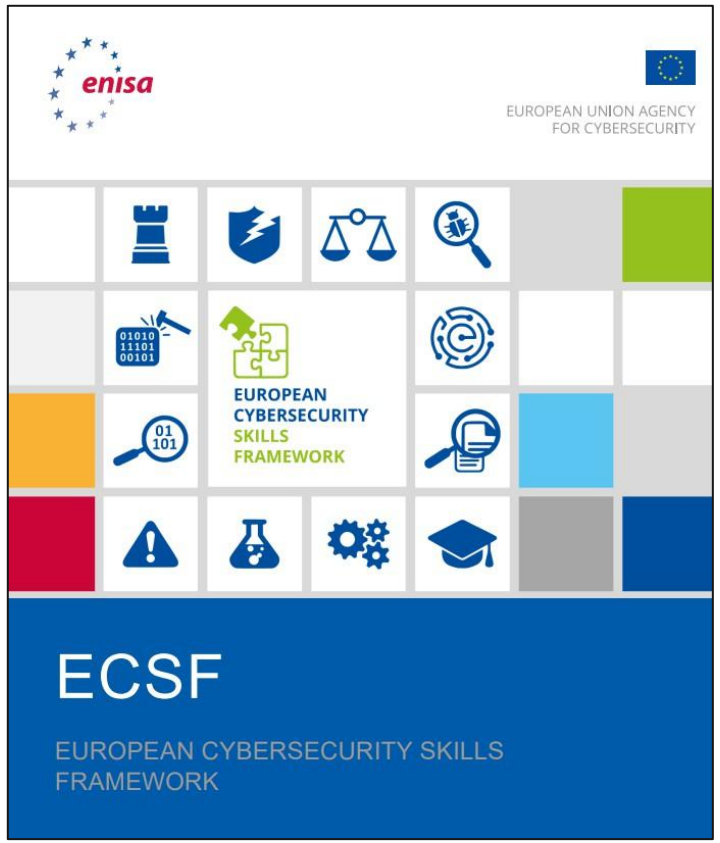
CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Workshop: Perfiles de Ciberseguridad

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

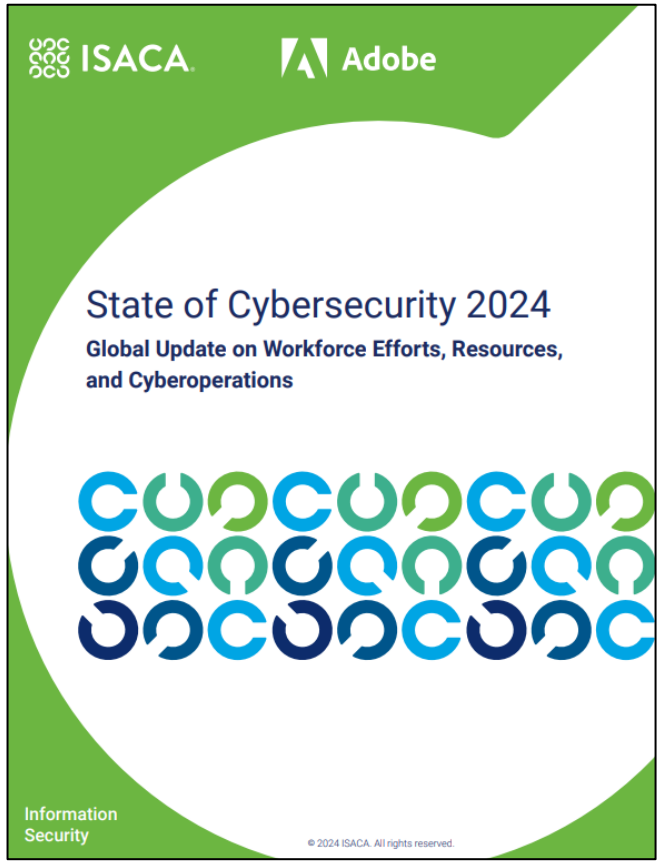
DIPLOMADO
CIBERSEGURIDAD

Documentos Claves

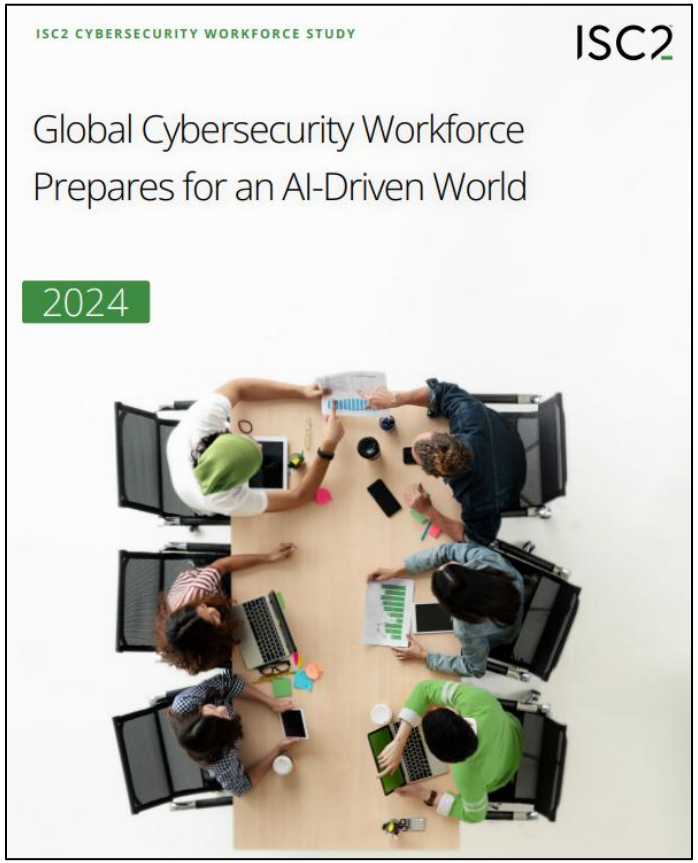


https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

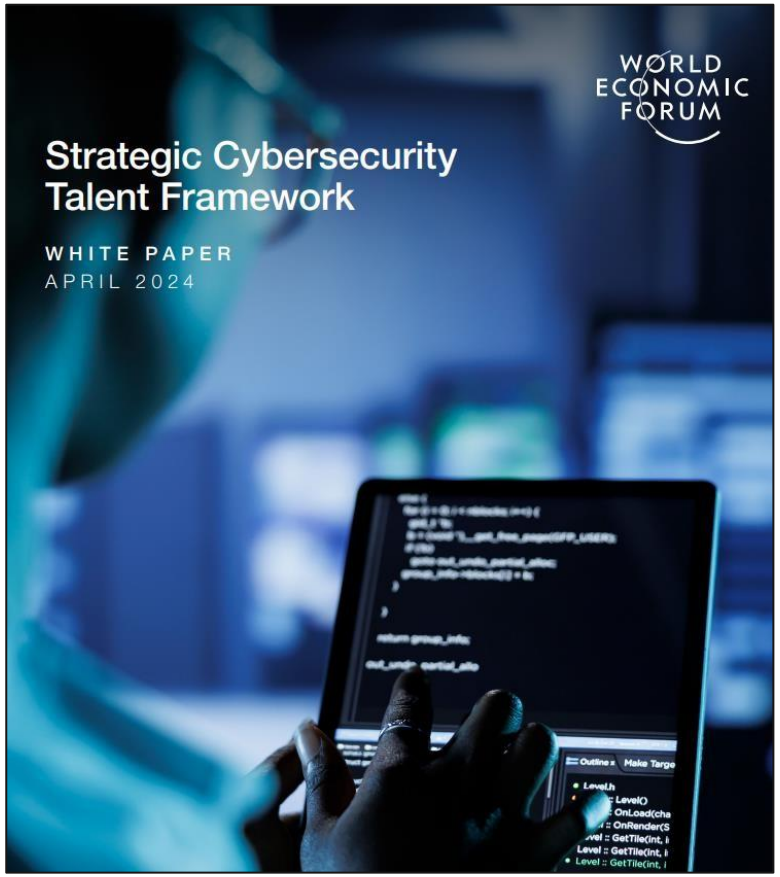
Documentos Claves



ISACA 2024



ISC2 2024



https://www.weforum.org/publications/strategic-cybersecurity-talent-framework/

Profesor

Carlos Lobos de Medina

Ingeniero Civil en Informática y Magister en Informática © de la Universidad de Santiago de Chile, Diplomado en Auditoría de Sistemas, Postitulado en Seguridad Computacional de la Universidad de Chile.

Especialista en gobernanza, gestión y control de tecnologías de información empleando modelos como COBIT, ITIL, ISO 27001 e ISO 22301. Posee certificaciones internacionales CISA, CISM, COBIT, ISO Lead Auditor 27001, ISO Lead Auditor BS 25599 e ITIL V3, entre otras.

carlos.lobos@usach.cl

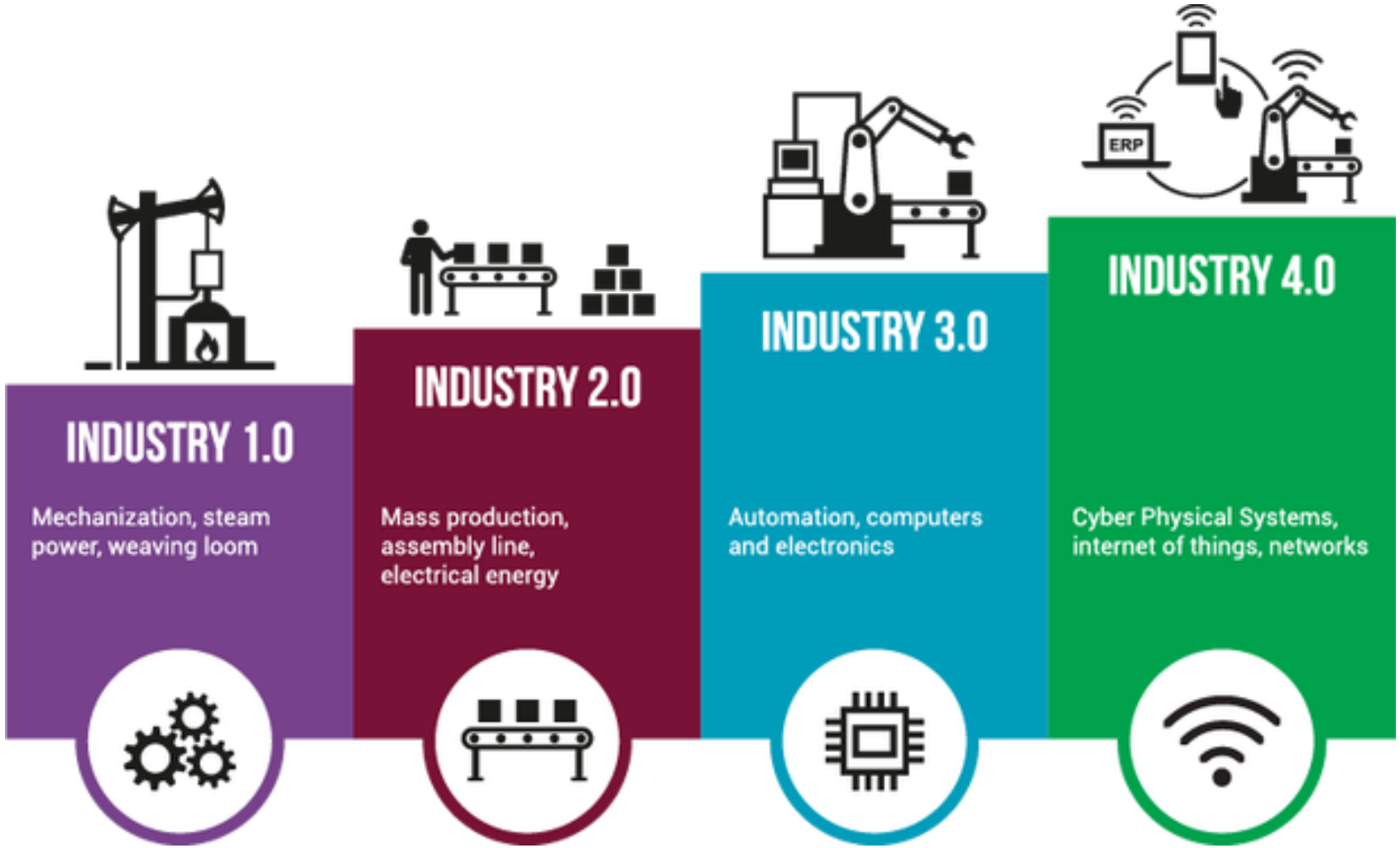
https://www.linkedin.com/in/clobos/

Agenda

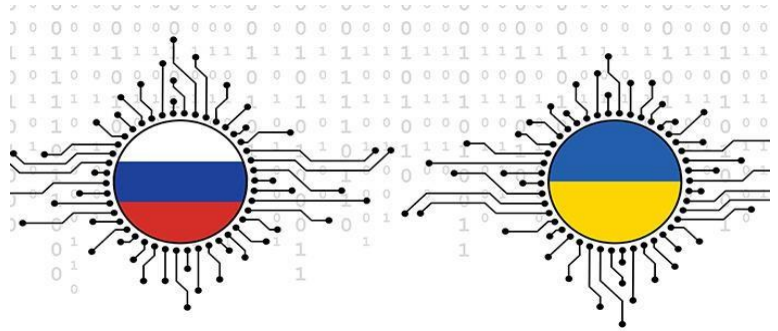
- Contexto general
- Tendencias en el Mercado Laboral
- Hacia donde especializarse
- Primeros pasos en la Ciberseguridad
- Perfiles Detallados

Contexto General

4ª Revolución Industrial



Contexto General de Riesgos



Contextos Normativos

POLÍTICA NACIONAL DE CIBERSEGURIDAD

¿Necesitamos profesionales en Ciberseguridad?

Microsoft estima que en 2025 habrá 3,5 millones de vacantes de ciberseguridad

La escasez de equipos de seguridad OT amenaza la protección en el 16% de las organizaciones industriales europeas

43% de las organizaciones experimentaron más ataques el año pasado y la escasez de habilidades en materia de ciberseguridad es un problema que necesita una respuesta rápida

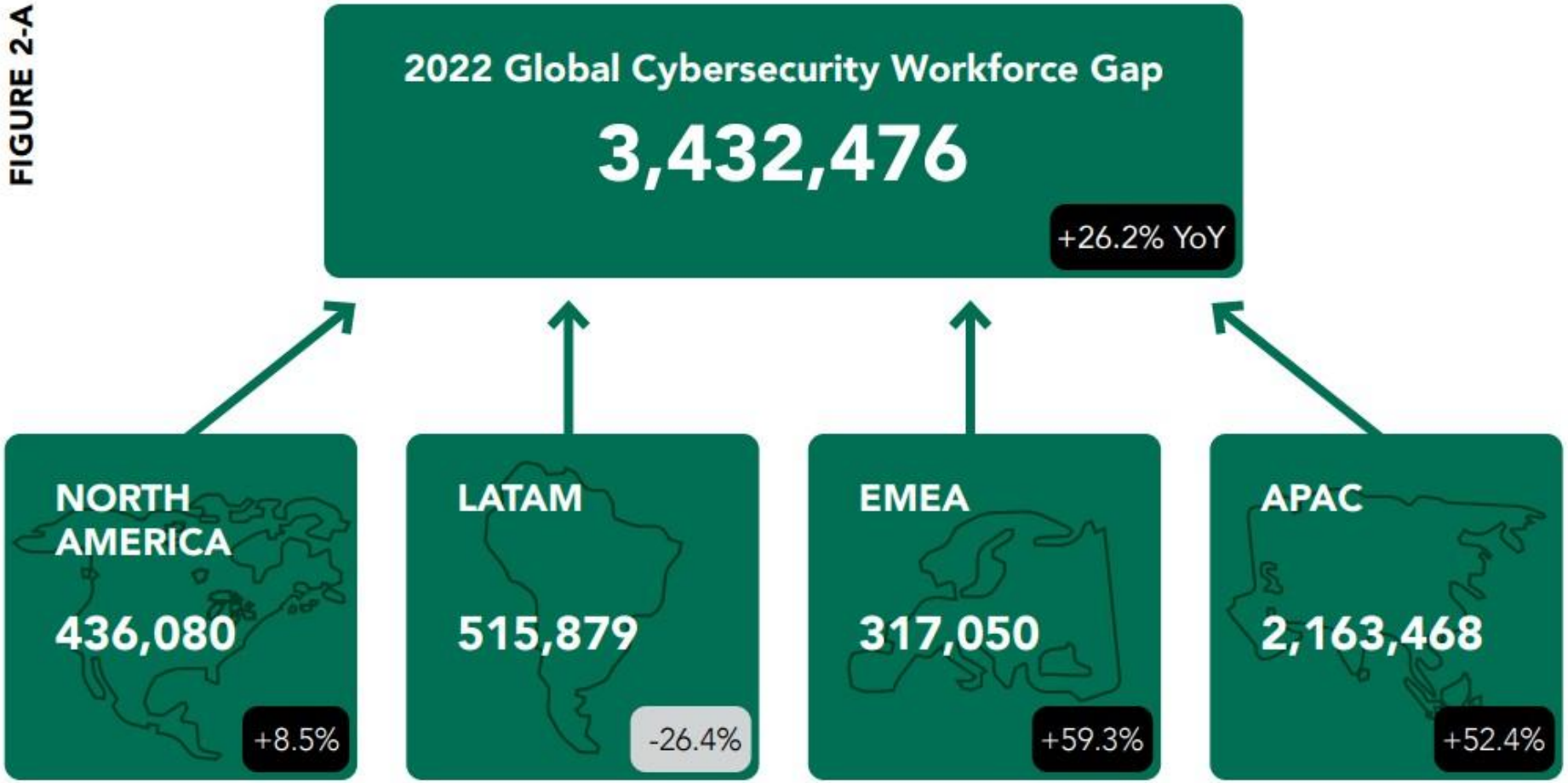
Empresas de LatAm necesitan 700.000 profesionales para combatir los ciberataques

Los arquitectos en la nube y los expertos en ciberseguridad son los más demandados

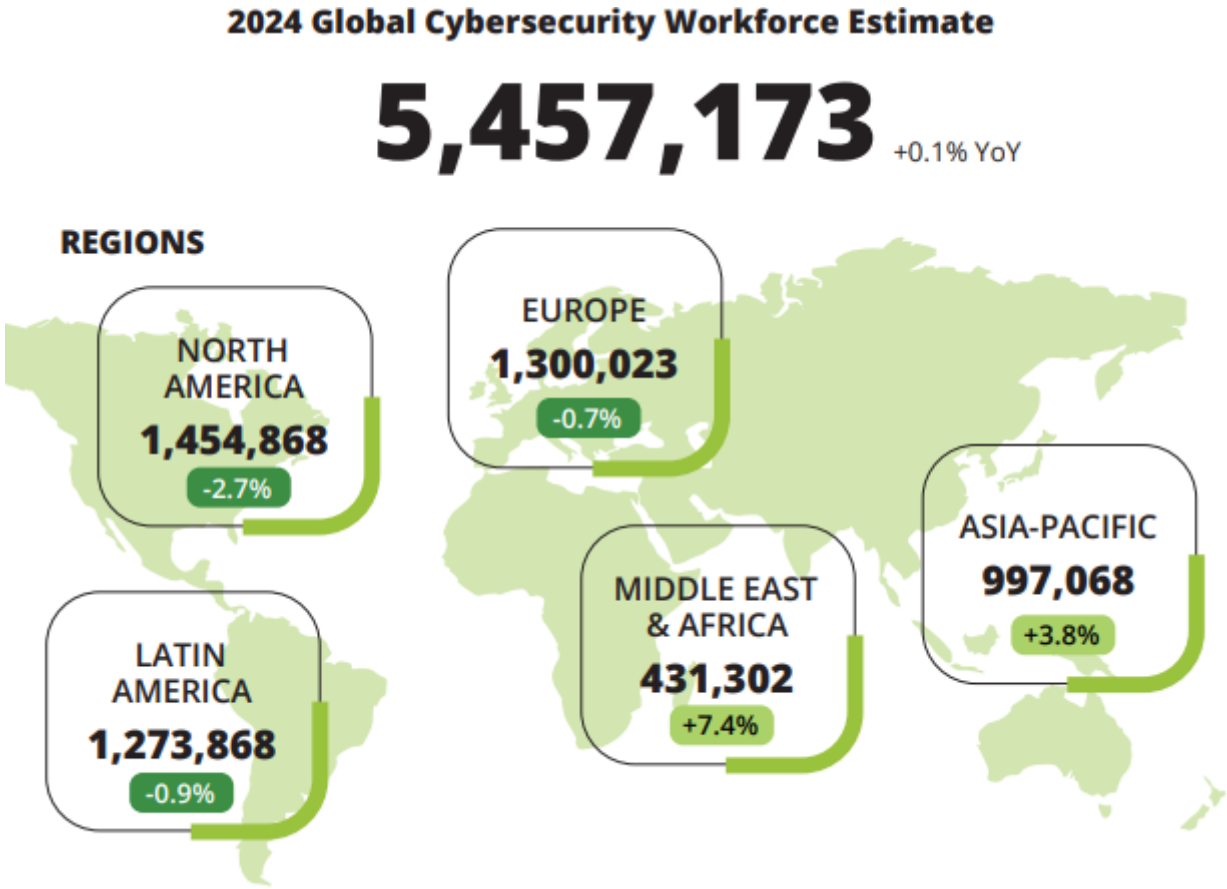
Headhunters acusan falta de profesionales especializados en ciberseguridad en Chile

¿Necesitamos profesionales en Ciberseguridad (2022)?

FIGURE 2-A

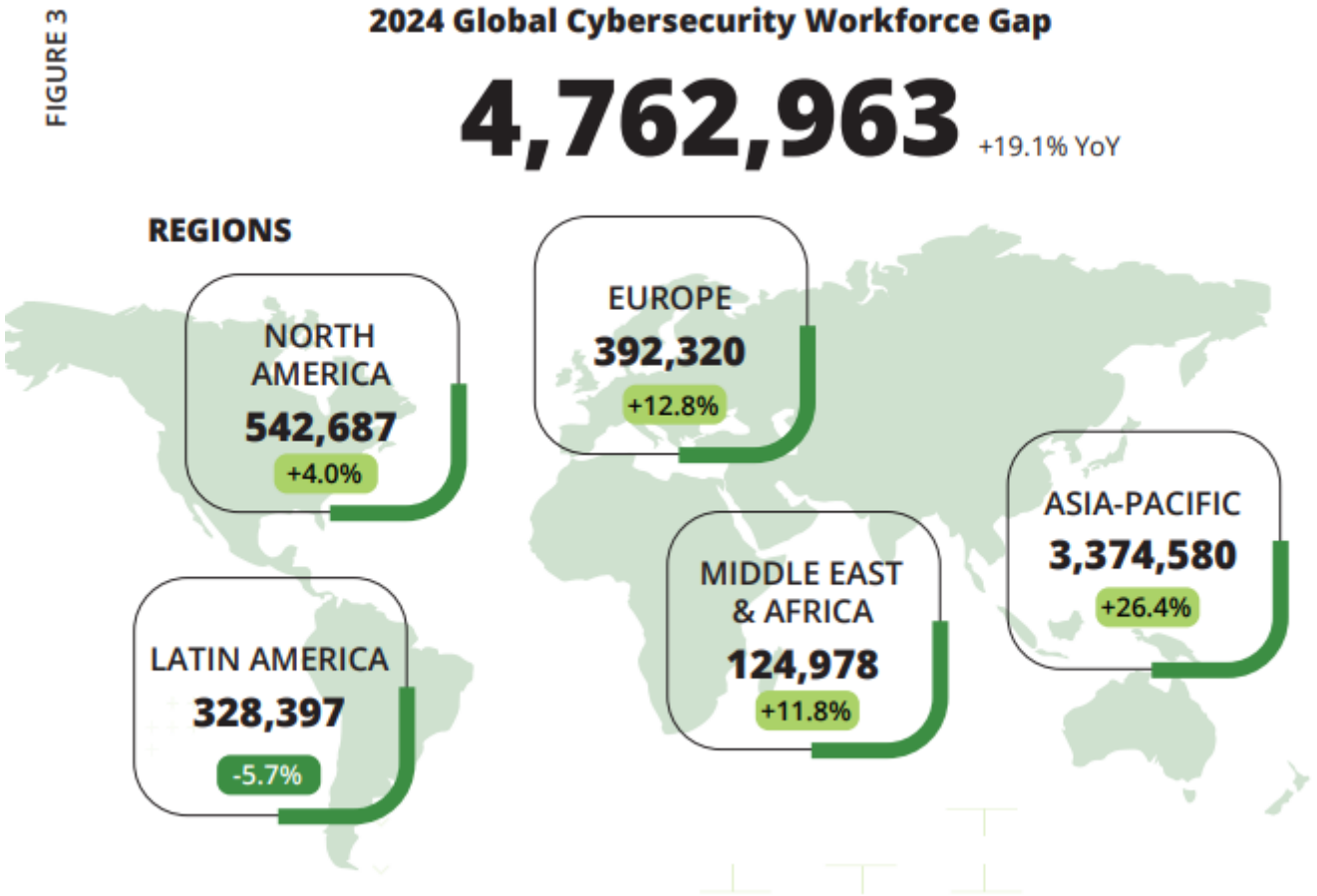


¿Necesitamos profesionales en Ciberseguridad (2024)?



¿Necesitamos profesionales en Ciberseguridad (2024)?

FIGURE 3



Tendencias del Mercado Laboral

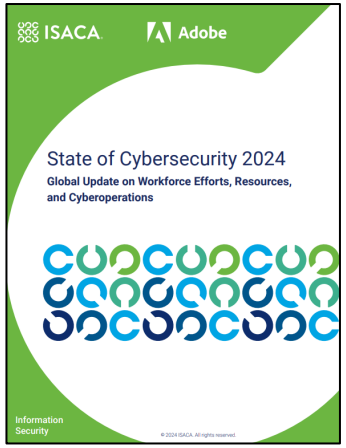
Fuentes de Referencia

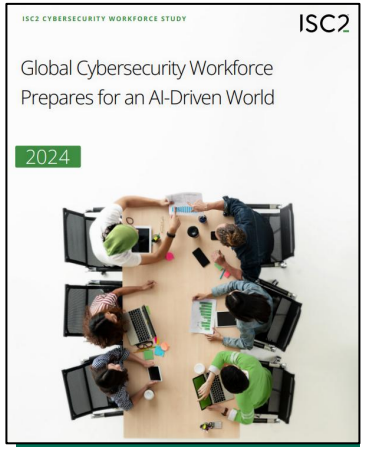
GRUPO IT-TALENT

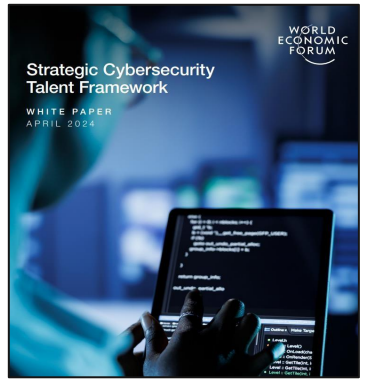
DIPLOMADO CIBERSEGURIDAD

ALIGNMENT SOLUCIONES ESTRATÉGICAS

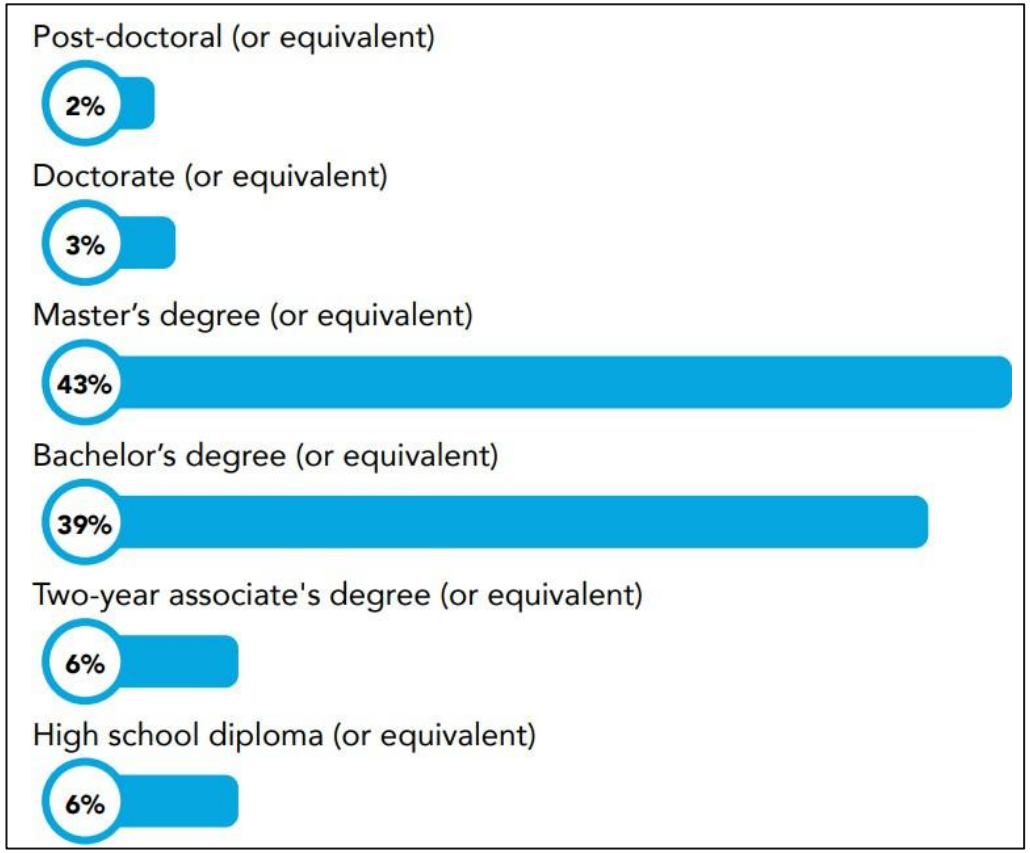
Análisis de empleos en Hispanoamérica (últimos seis meses)



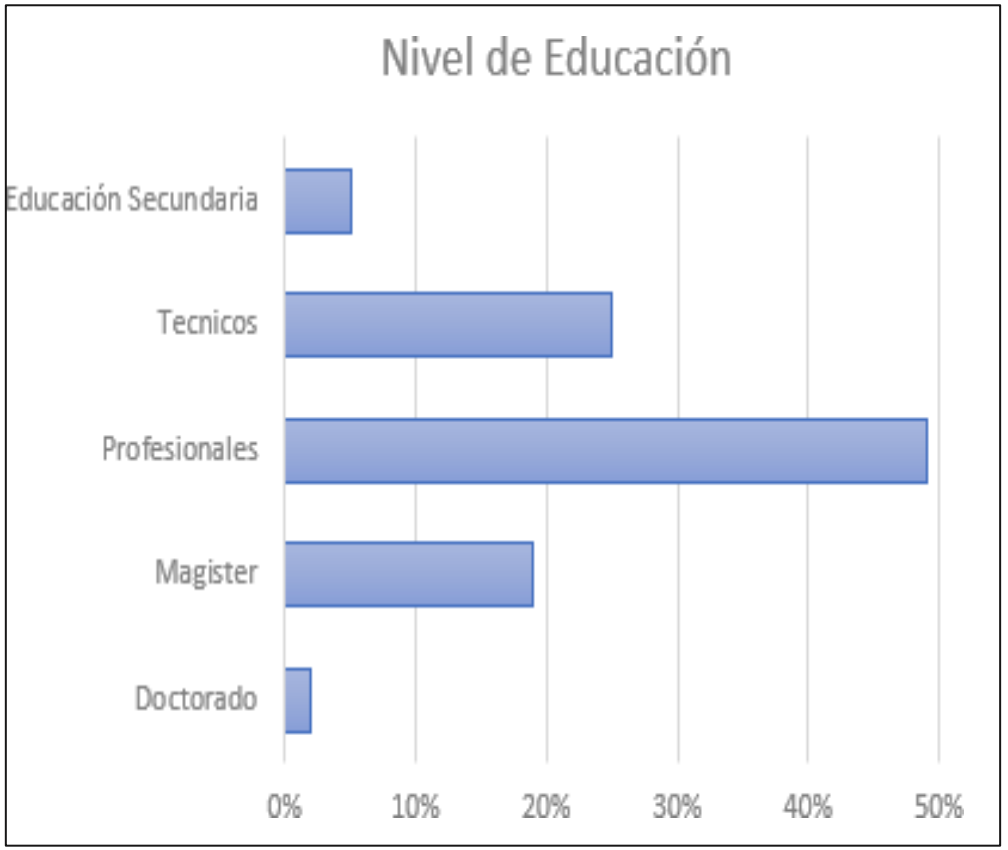




Contexto Educacional

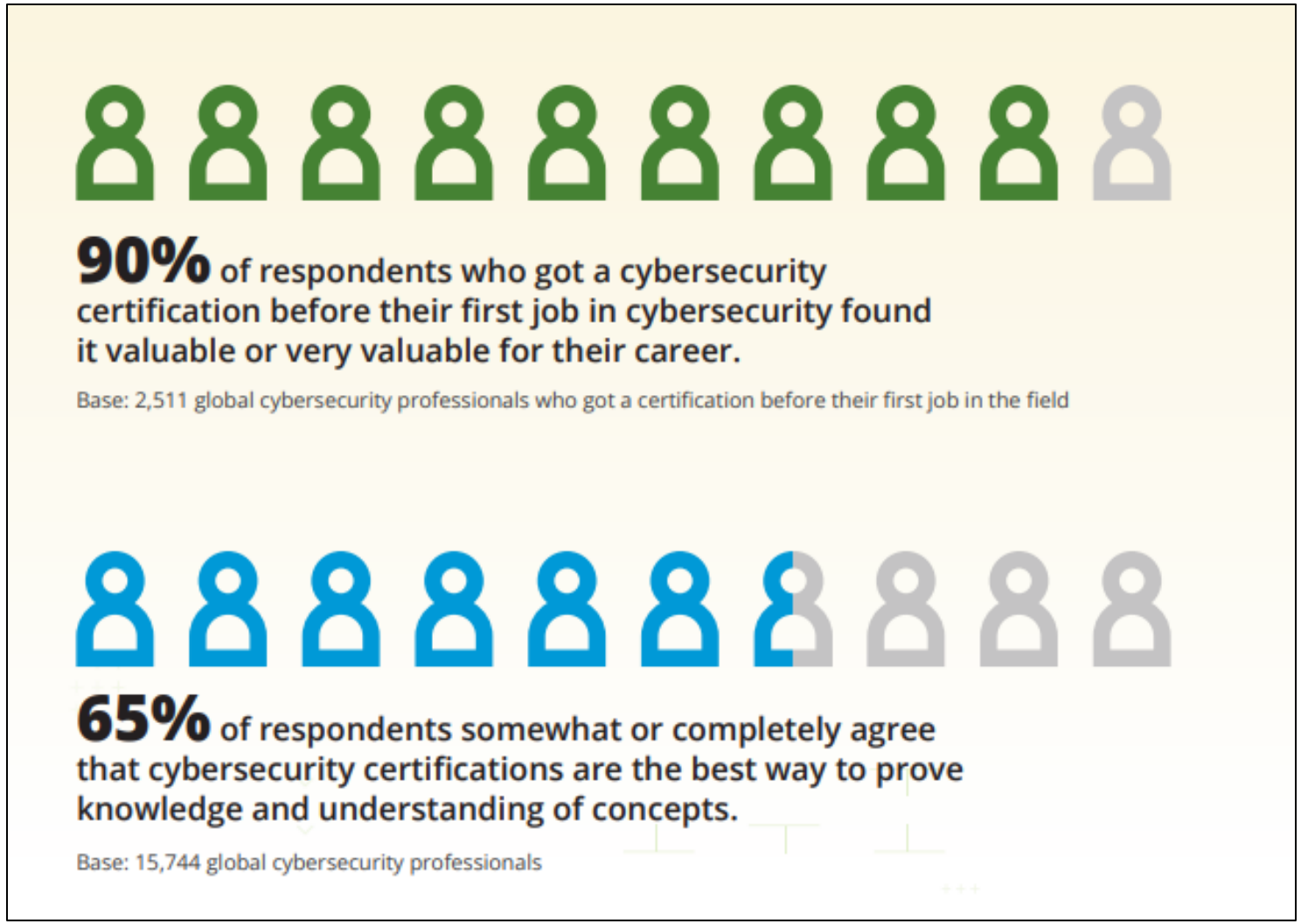


Cybersecurity Workforce Study 2022 – ISC2

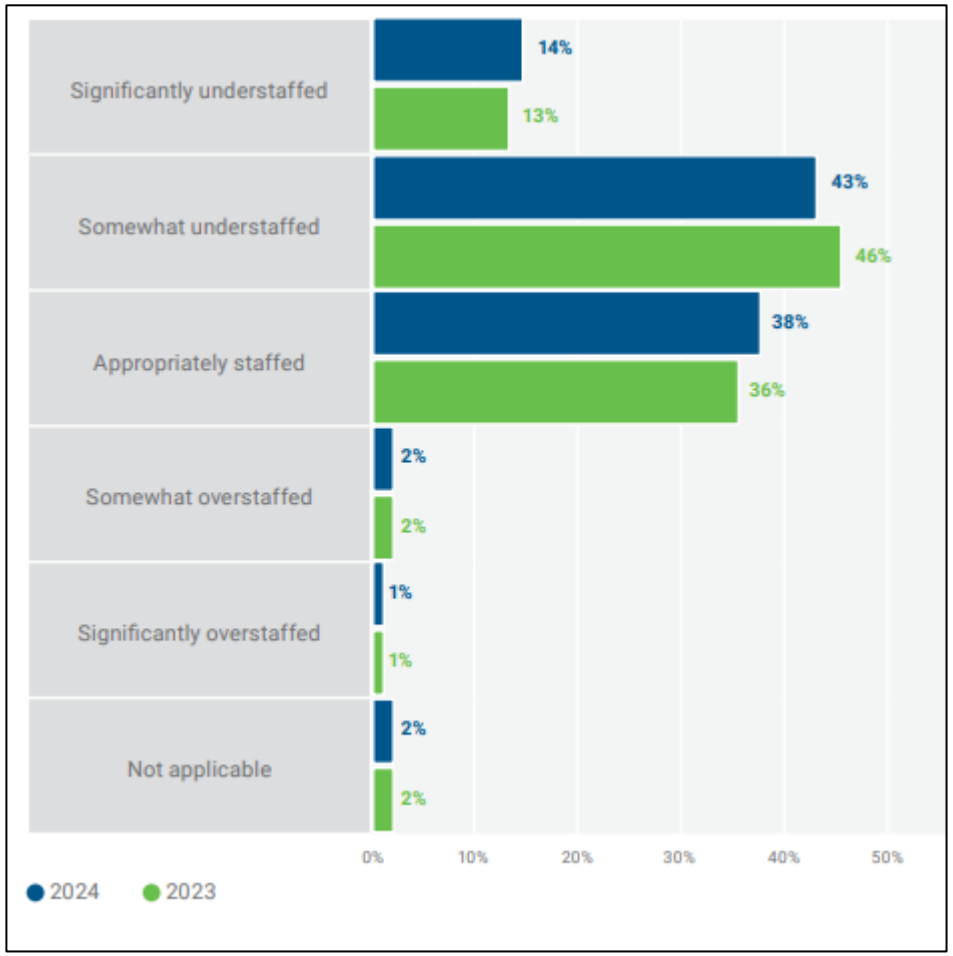


Reporte de Ciberseguridad
It Talent y Capacitación Usach

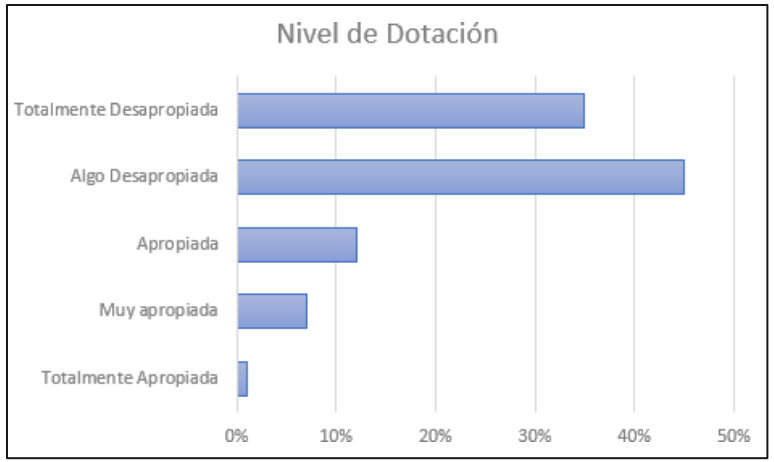
La importancia de una certificación – ISC2 2024



Sobre la dotación actual en Ciberseguridad



ISACA - State of Cybersecurity 2024



Reporte de Ciberseguridad – IT Talent & Usach

Comprensión de la necesidades de contratación

Lo que se Quiere

VS

Lo que se Paga

Desde el Mercado Laboral - Facts

- Baja estandarización de cargos (<40%)
- Baja definición de competencias (<35%)
- Nula definición de rol organizacional (<95%)
- Baja publicación de sueldos(<10%)
- Baja definición de beneficios(<30%)
- Alta definición de modalidad (95%)

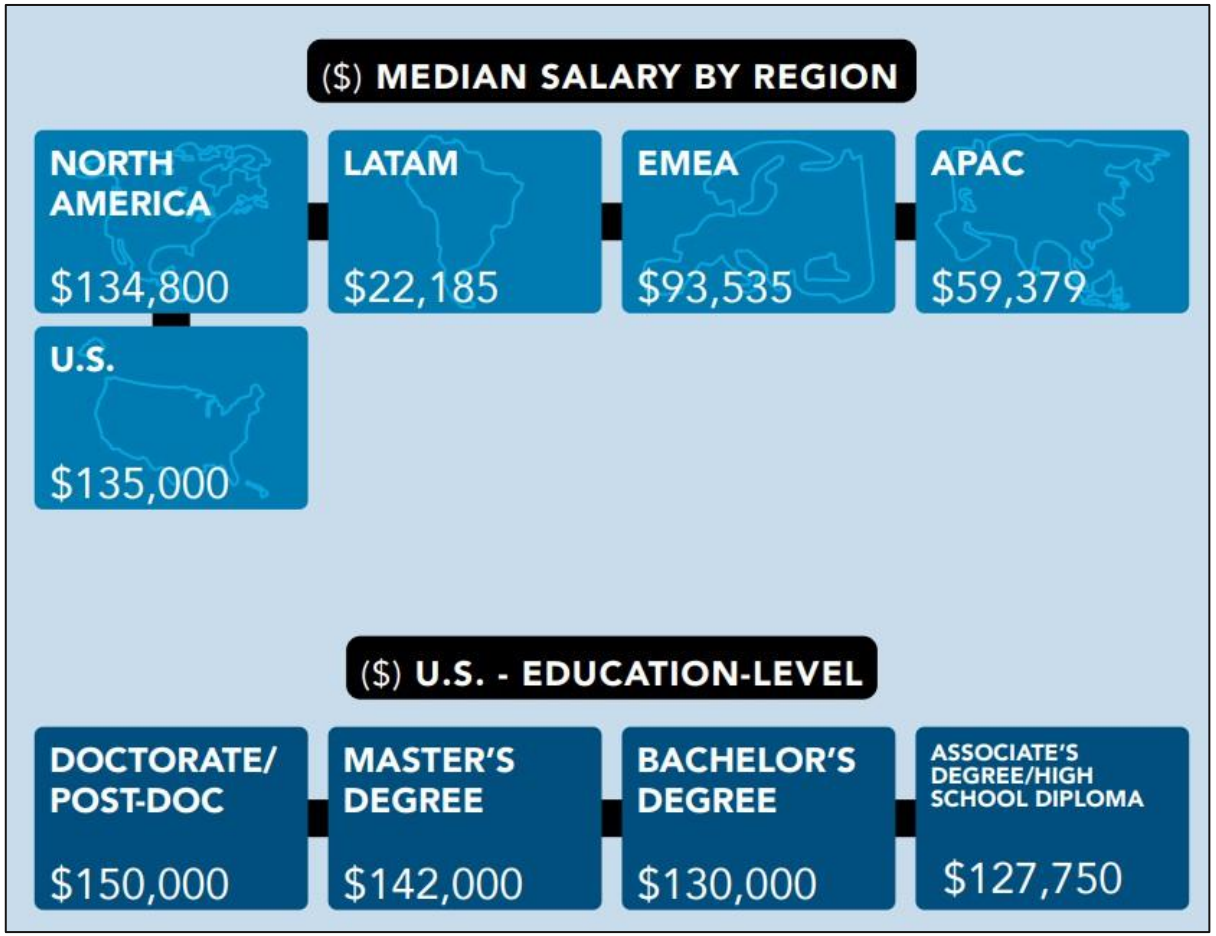
Estandarización de Cargos en PYMES– Realidad Latam

- Mucha concentración de funciones en la gestión y operación de la ciberseguridad.
- Funciones de riesgos, auditoria, protección de datos, entre otros muy ausentes en PYMES.
- CISOs con roles muy amplios o Jefes de TI con roles de Ciberseguridad
- PYMES que requieren super perfiles…… pero a veces son las que mejor pagan.

Estandarización de Cargos en Grandes Empresas– Realidad Latam

- Mayor desarrollo y definición en industrias financieras y de servicios tecnológicos.
- El líder en la materia de definición de cargos corresponden a empresas relacionadas a servicios de ciberseguridad.
- En general empresas de otros sectores industriales presentan perfiles con bajos niveles de estandarización.
- En general los sectores regulados presentan mejore definiciones.

Escalas de Sueldo Mercado Global



Cybersecurity Workforce Study 2022- ISC2

Escalas de Sueldo – Robert Half - Chile

Cargo	25° percentil	50° percentil	75° percentil
CISO	$5.150.000	$5.800.000	$6.970.000
Especialista de Seguridad	$2.750.000	$3.100.000	$3.720.000

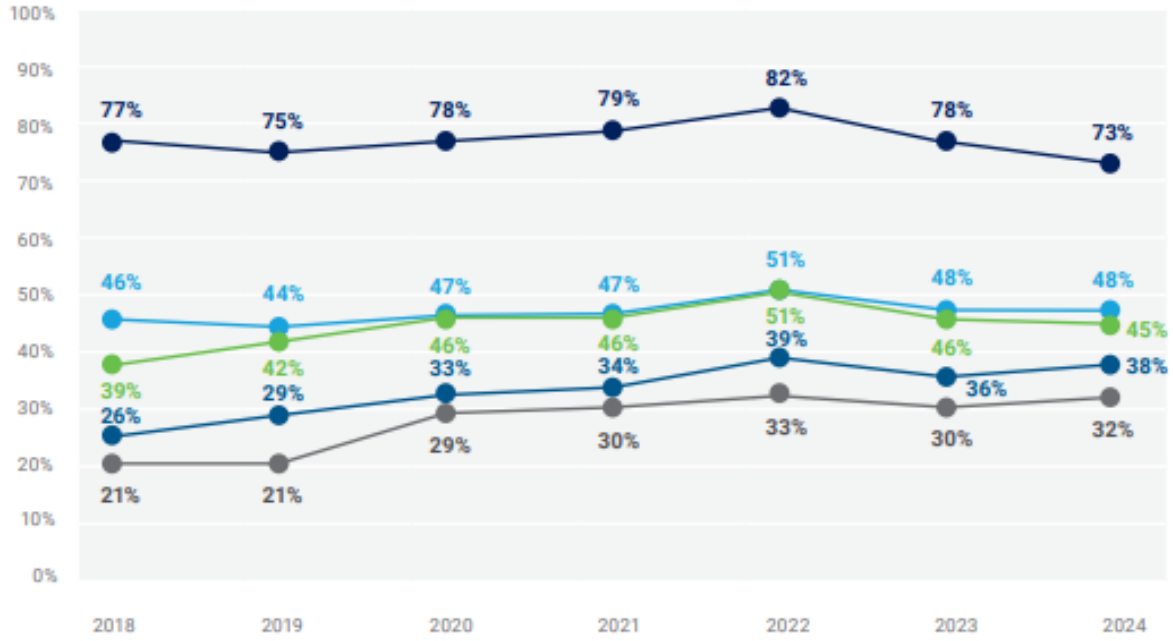
Cargo	25° percentil	50° percentil	75° percentil
Gerente de Proyectos TI	$4.350.000	$4.900.000	$5.880.000
Jefe de Proyectos TI	$2.750.000	$3.100.000	$3.720.000

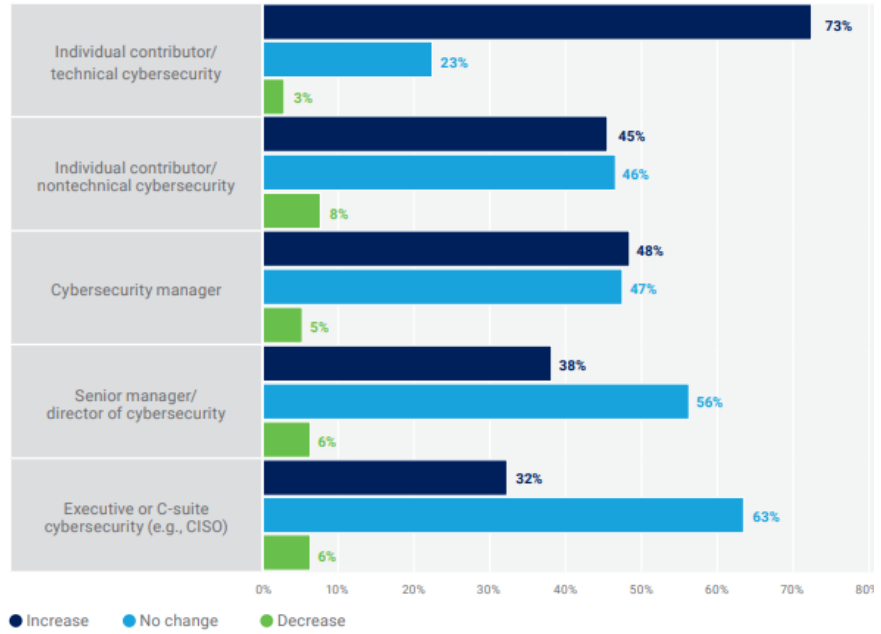
Escalas de Sueldo – Robert Half – Estados Unidos

Title	25th percentile	50th percentile	75th percentile
Information Systems Security Manager	$129,750	$157,250	$187,750
Security Architect	$126,250	$143,250	$162,500
Data Security Analyst	$115,000	$141,000	$166,750
Network Security Engineer	$109,750	$131,250	$153,500
Systems Security Administrator	$103,000	$124,250	$147,500
Network Security Administrator	$102,000	$122,250	$145,500

Tendencias de Contratación

FIGURE 14: Hiring Demand Trending (2018-2024)

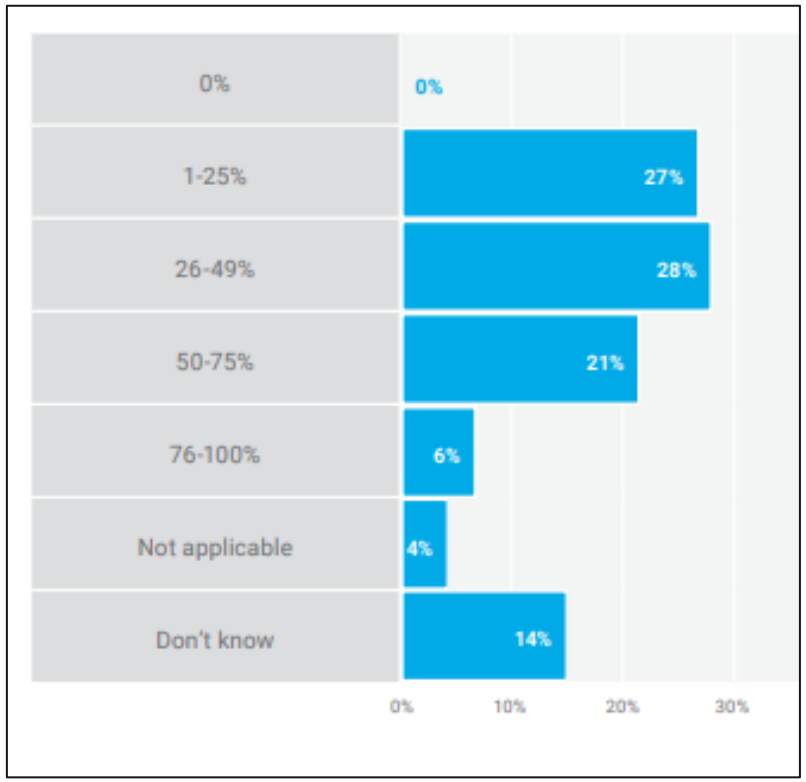




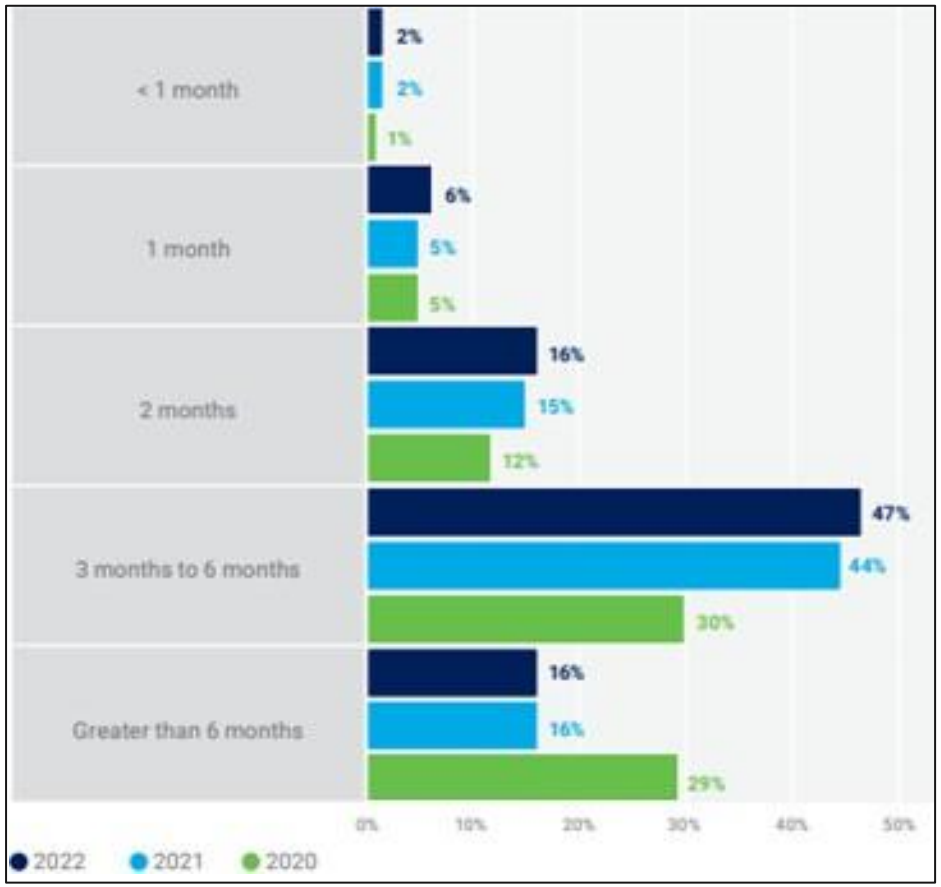
State of Cybersecurity 2024 - ISACA

Complejidad en completar las vacantes

Porcentaje de Quilificación requerida



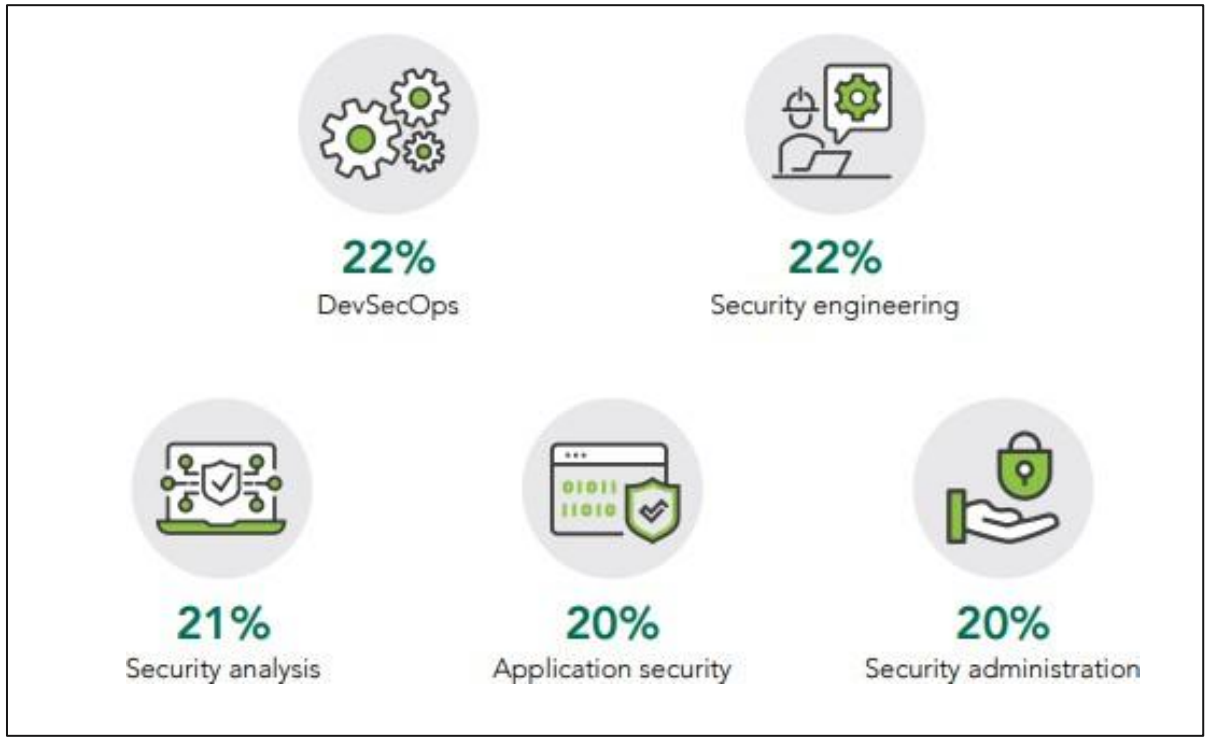
Tiempo medio en completar vacantes



State of Cybersecurity 2022 - ISACA

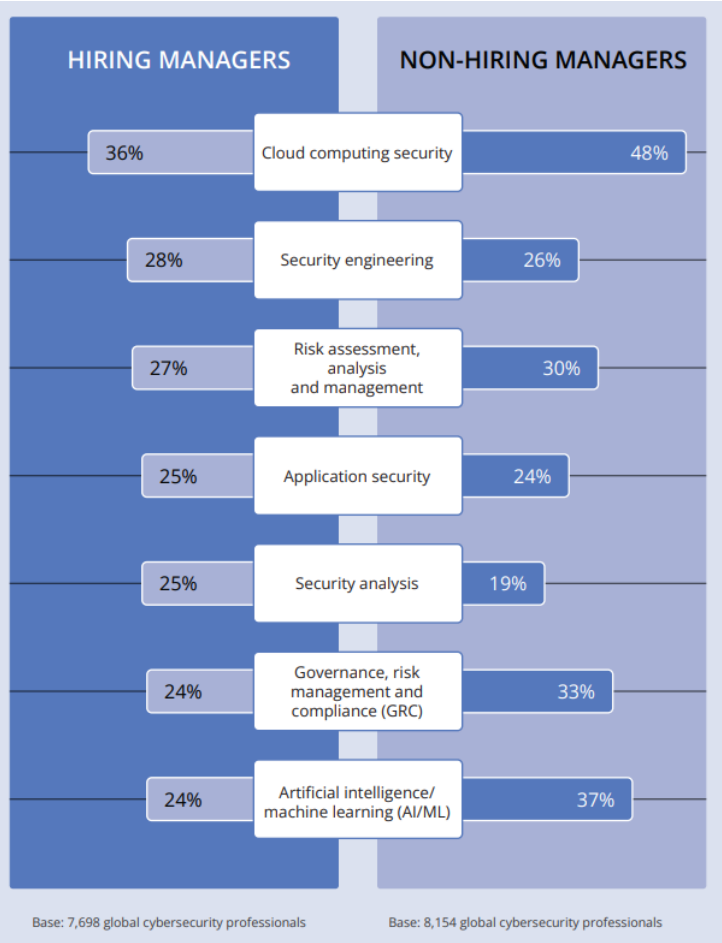
Tendencias del Mercado Laboral

Habilidades más Demandadas

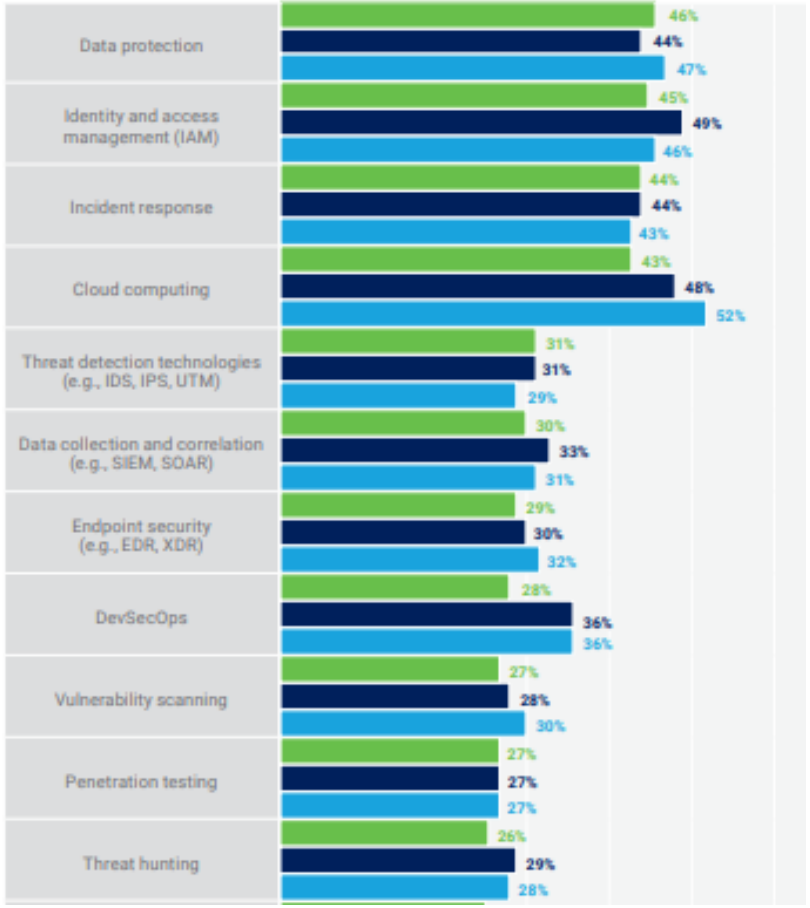


ISC2 - Cybersecurity Workforce Study 2021

Habilidades más Demandadas

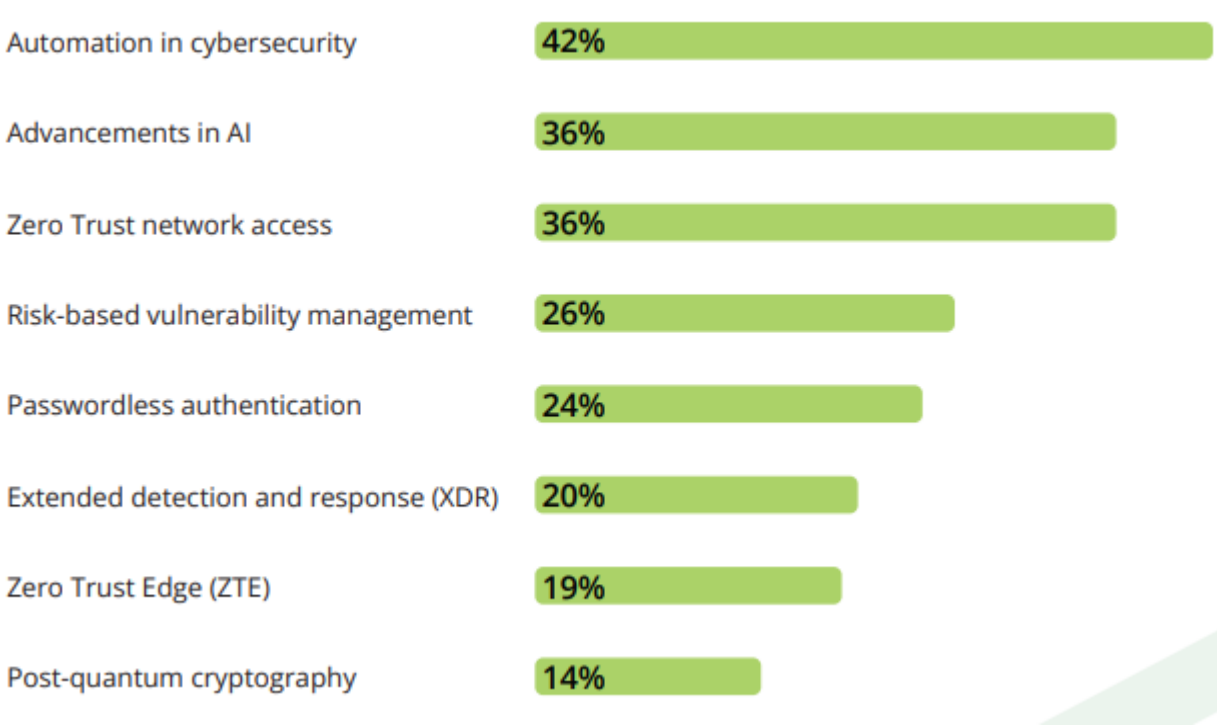


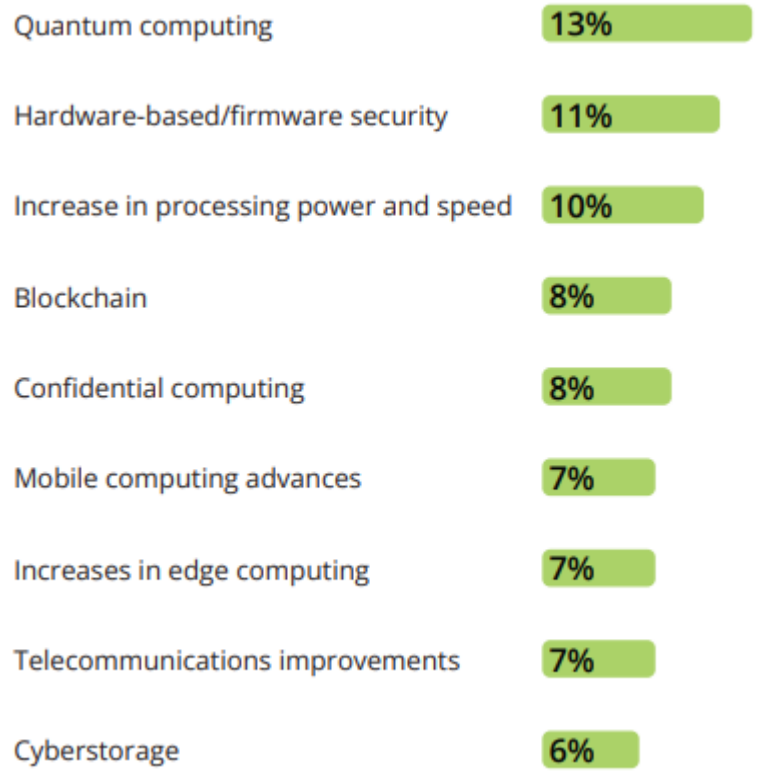
ISC2 - State of Cybersecurity 2024



Isaca- State of Cybersecurity 2024

Habilidades emergentes y tendencias – ISC2 2024





Perfiles Laborales en Ciberseguridad

Perfiles de la ANCI

1. **Jefe/a de Ciberseguridad:** Lidera la estrategia corporativa, define políticas y marcos de ciberseguridad, gestiona riesgos y asegura cumplimiento normativo (Ley Marco, ISO 27001, NIST, etc.).
2. **Operador(a) en Soporte de Ciberseguridad:** Ejecuta tareas de soporte técnico, gestión de incidentes y mantenimiento de controles operativos en infraestructura y redes.
3. **Controller de Ciberseguridad de Sistemas y Productos:** Supervisa la seguridad durante el ciclo de vida de productos y servicios tecnológicos, asegurando cumplimiento de políticas y estándares.
4. **Encargado(a) de Gestión de Riesgos Operativos y Continuidad Institucional:** Evalúa y mitiga riesgos tecnológicos y de continuidad del negocio, aplicando metodologías ISO 22301 e ISO 27005.
5. **Encargado(a) de Formación Técnica Profesional en Ciberseguridad:** Articula la formación técnica con las necesidades del sector, evaluando pertinencia curricular y empleabilidad.
6. **Encargado(a) de Hacking Ético:** Evalúa vulnerabilidades mediante pruebas de penetración y simulaciones controladas de ataque, conforme a principios éticos y estándares internacionales.
7. **Auditor(a) de Ciberseguridad:** Realiza auditorías técnicas y de cumplimiento, evalúa controles, conformidad y reporta hallazgos a la dirección.
8. **Analista de Ciberseguridad:** Monitorea eventos e incidentes en tiempo real, coordina la respuesta operativa y aplica protocolos de seguridad organizacional.
9. **Especialista en Seguridad en la Nube:** Implementa y gestiona controles de ciberseguridad en entornos cloud, protegiendo datos y asegurando continuidad operativa.
10. **Especialista en Operaciones de Ciberinteligencia:** Detecta, analiza y previene amenazas digitales mediante técnicas avanzadas de ciberinteligencia y análisis de comportamiento.

Sobre la Importancia

- La Ley Marco de Ciberseguridad exige que las instituciones públicas, operadores de servicios esenciales y proveedores críticos cuenten con personal calificado, con competencias verificables y formación continua.

- Hasta ahora, Chile no contaba con un marco de certificación laboral estandarizado en esta materia.

- La definición de estos perfiles permitirá:
- Establecer estándares nacionales de competencias en ciberseguridad.
- Certificar oficialmente a especialistas, auditores y técnicos.
- Alinear la formación técnico-profesional con las necesidades del mercado.
- Promover la empleabilidad y movilidad laboral del talento digital.
- Fortalecer la capacidad del país para responder a los desafíos de la Ley Marco de Ciberseguridad.

Fuente: https://confiden.cl/ley-ciberseguridad/nuevos-perfiles-laborales-ciberseguridad-chile-anci-chilevalora/

El proceso de Definición

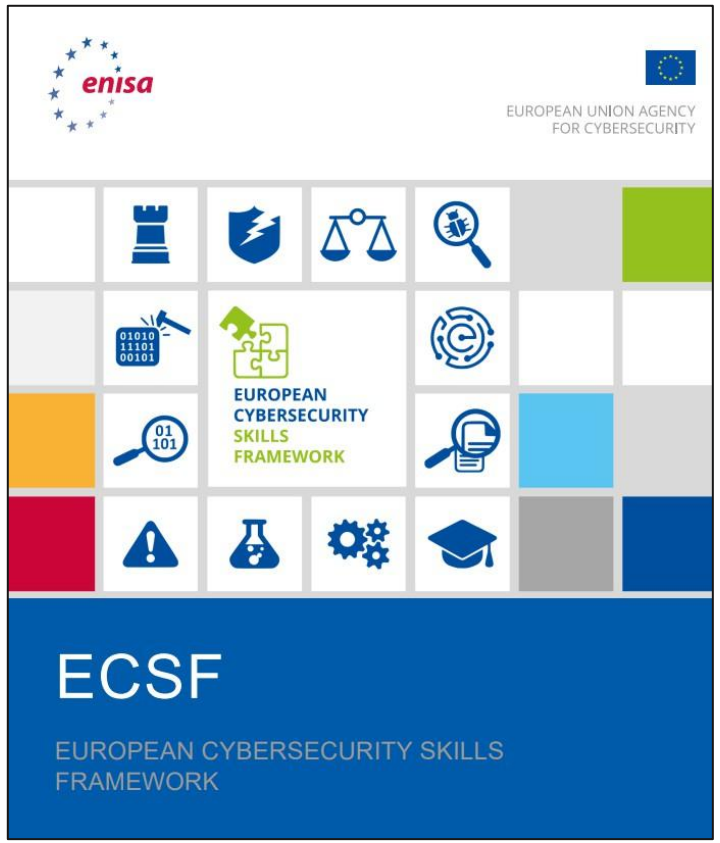
- El proceso fue liderado por el Organismo Sectorial de Competencias Laborales (OSCL) de Ciberseguridad, integrado por representantes de:

- Los empleadores: Alianza Chilena de Ciberseguridad, Chiletec y Equifax.
- Los trabajadores: Agrupación Nacional de Empleados Fiscales (ANEF).
- El Estado: Ministerio de Hacienda y Agencia Nacional de Ciberseguridad (ANCI).

- La metodología fue mixta, con encuestas, entrevistas, observaciones en terreno y paneles de expertos regionales, buscando identificar las funciones reales y competencias críticas del trabajo en ciberseguridad en Chile.

Fuente: https://confiden.cl/ley-ciberseguridad/nuevos-perfiles-laborales-ciberseguridad-chile-anci-chilevalora/

Documentos Claves



https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

Los Perfiles

Perfil laboral	Función clave
Jefe/a de ciberseguridad	Dirigir la estrategia de ciberseguridad institucional, asegurar cumplimiento normativo y estándares técnicos.
Operador(a) en soporte de ciberseguridad	Brindar soporte técnico en tareas operativas, gestionar incidentes básicos y mantener registros de activos.
Controller de ciberseguridad de sistemas y productos	Verificar que sistemas y productos cumplan requisitos de seguridad en todas sus etapas (desarrollo, operación, mantenimiento).
Encargado(a) de gestión de riesgos operativos y continuidad institucional	Identificar y mitigar riesgos tecnológicos, asegurar continuidad de operaciones críticas.
Encargado(a) de formación técnica profesional en ciberseguridad	Relacionar la oferta formativa técnica con las necesidades reales del sector, favorecer prácticas y experiencias profesionales.

Perfil laboral	Función clave
Encargado(a) de hacking ético	Realizar pruebas de penetración controladas para detectar vulnerabilidades éticamente.
Auditor(a) de ciberseguridad	Auditar sistemas, procesos e infraestructuras para verificar conformidad y robustez en seguridad.
Analista de ciberseguridad	Monitorear eventos de seguridad, identificar incidentes y responder conforme a protocolos.
Especialista en seguridad en la nube	Proteger datos y operaciones que se desarrollan en entornos cloud, aplicando controles y metodologías específicas.
Especialista en operaciones de ciberinteligencia	Detectar amenazas, realizar análisis proactivo de riesgos y anticipar vectores de ataque.

Análisis de los Perfiles

https://anci.gob.cl/noticias/nuevos-perfiles-laborales-ciberseguridad/

Auditor de Ciberseguridad – Junior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Fundamentos de seguridad cibernética	Uso básico de herramientas de auditoría (Nessus, OpenVAS)	Conceptos básicos de redes y sistemas operativos	Realizar escaneos de seguridad básicos
Análisis básico de riesgos y vulnerabilidades	Realización de escaneos de seguridad y análisis de resultados	Normativas y estándares de seguridad cibernética (ISO 27001, NIST)	Asistir en la documentación de hallazgos de auditoría
Comunicación efectiva de hallazgos	Resolución básica de problemas de seguridad	Principios básicos de criptografía y autenticación	Colaborar en la revisión de políticas de seguridad
Colaboración en equipos de auditoría			Asistir en la preparación de informes de auditoría

US$1.700

Renta Media

Gestión de Riesgos
Auditor Líder ISO 27001
Hacking Ético

Auditor de Ciberseguridad – Intermedio

Competencias	Habilidades	Conocimientos	Tareas Específicas
Análisis avanzado de riesgos y vulnerabilidades	Uso avanzado de herramientas de auditoría (Metasploit, Burp Suite)	Arquitectura de sistemas de información y seguridad	Realizar pruebas de penetración en entornos controlados
Realización de pruebas de penetración	Interpretación avanzada de resultados de auditoría	Protocolos de seguridad y cifrado	Colaborar en la revisión de políticas y procedimientos de seguridad
Gestión de proyectos de auditoría	Análisis forense básico	Tendencias y amenazas actuales en ciberseguridad (MITRE)	Contribuir en el diseño e implementación de controles de seguridad
Documentación detallada de hallazgos y recomendaciones	Colaboración efectiva con equipos de TI y de gestión	Cumplimiento normativo y regulaciones de seguridad	Asistir en la preparación de planes de mitigación de riesgos

US$2.800

Renta Media

CISA – ISACA
CEH – Ec-Council
eJPT – INE Security

Auditor de Ciberseguridad – Senior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Liderazgo en proyectos de auditoría de ciberseguridad	Liderazgo en el uso de herramientas de auditoría avanzadas	Estrategias y políticas de seguridad cibernética a nivel empresarial	Coordinar y liderar auditorías de seguridad completas
Análisis forense avanzado	Desarrollo de estándares y procedimientos de auditoría	Marco regulatorio y de cumplimiento normativo específico	Supervisar y guiar equipos de auditoría junior e intermedios
Mentoría y desarrollo de talento en ciberseguridad	Comunicación estratégica de hallazgos y recomendaciones	Técnicas avanzadas de análisis de riesgos y amenazas	Contribuir en la planificación estratégica de seguridad de la organización
Gestión de incidentes de seguridad			Evaluar y recomendar soluciones de seguridad emergentes

US$5.300

Renta Media

CGEIT & **CRISC** – ISACA
CIA – The IIA
OSCP – Offensive Security

Auditor de Ciberseguridad – Formación

Factor	Nivel
Empleabilidad A	Media
Empleabilidad B	Muy Baja
Consultoría	Muy Alta
Oportunidades	Alta
Proyección MP	Media
Proyección LP	Alta

Junior	Intermedio	Senior	
	Auditor Líder ISO 22301	Compliance ISO 373001	Gobierno y Gestión
	Peritaje Informático	Gestión Estratégica Ciber	
Auditor Líder ISO 27001	ISO 27002 COBIT	NIST CSF	
Gestión de Riesgos			
Auditoría a la Ciberseguridad	Pentesting Web	Pentesting Cloud	Técnico y Operativo
	Inteligencia de Amenazas	DevSecOps	
	Auditoría en Redes/Cloud	Respuesta a Incidentes	

Ciber Inteligencia – Junior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Fundamentos de ciberinteligencia	Uso básico de herramientas de inteligencia de amenazas (MISP)	Conceptos básicos de ciberseguridad y amenazas cibernéticas	Recopilar y analizar datos de fuentes abiertas
Análisis básico de amenazas	Interpretación básica de indicadores de compromiso (IOCs)	Principios básicos de análisis de datos	Colaborar en la creación de informes de inteligencia
Conocimiento de fuentes de inteligencia	Resolución básica de problemas de inteligencia de amenazas	Normativas y estándares de ciberinteligencia	Asistir en la identificación y documentación de tácticas, técnicas y procedimientos (TTP) de amenazas
Fundamentos de Ciberseguridad			Asistir en la identificación de posibles actores de amenazas

US$1.700

Renta Media

Inteligencia de Amenazas
MISP
MITRE

Ciber Inteligencia – Intermedio

Competencias	Habilidades	Conocimientos	Tareas Específicas
Análisis avanzado de amenazas	Uso avanzado de herramientas de inteligencia de amenazas (Maltego, Shodan)	Técnicas avanzadas de análisis de datos	Realizar análisis de correlación de amenazas
Análisis avanzado de indicadores de compromiso	Desarrollo de informes de inteligencia de amenazas	Protocolos de ciberinteligencia y compartición de información (STIX/TAXII)	Colaborar en la evaluación de impacto de amenazas
Colaboración efectiva con equipos de seguridad	Resolución de problemas avanzada de ciberinteligencia	Tendencias y desarrollos actuales en ciberamenazas	Contribuir en la identificación de campañas de amenazas
Documentación detallada de hallazgos de inteligencia	Modelado de amenazas, actores, TTP y APT	Cumplimiento normativo y regulaciones de ciberinteligencia	Participar en ejercicios de simulación de amenazas

US$2.500

Renta Media

MITRE – Attack IQ
CTIA – Ec – Council
CySA+ - CompTIA

Ciber Inteligencia– Senior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Liderazgo en proyectos de ciberinteligencia	Liderazgo en el desarrollo e implementación de estrategias de ciberinteligencia	Estrategias y políticas de ciberinteligencia a nivel empresarial	Coordinar y dirigir equipos de ciberinteligencia en proyectos complejos
Desarrollo de estándares y procedimientos de ciberinteligencia	Comunicación estratégica de hallazgos de inteligencia	Marco regulatorio y de cumplimiento normativo específico	Desarrollar y mejorar estándares y procedimientos de ciberinteligencia
Mentoría y desarrollo de talento en ciberinteligencia	Análisis forense avanzado de amenazas	Técnicas avanzadas de análisis de riesgos y amenazas	Mentorear y guiar a equipos junior e intermedios en ciberinteligencia
Gestión de incidentes de ciberinteligencia			Evaluar y recomendar soluciones de inteligencia de amenazas

US$3.500

Renta Media

CISSP – ISC2
CISM - ISACA
GCTI – GIAC

Ciber Inteligencia – Formación

Factor	Nivel
Empleabilidad A	Media
Empleabilidad B	Muy Baja
Consultoría	Alta
Oportunidades	Alta
Proyección MP	Media
Proyección LP	Alta

	Junior	Intermedio	Senior	
		Gestión de Incidentes	NIST CSF	Gobierno y Gestión
		Gestión de Riesgo	Gestión Estratégica Ciber	
	Técnica de Inteligencia			
	Análisis de Datos			
		Respuesta a Incidentes	Herramientas y técnicas OSINT para Red Team	Técnico y Operativo
		Pentesting	Preparación de Campañas para Red Team	
		Ciberdefensa Ransomware		

CSIRT Respuesta a Incidentes - Junior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Fundamentos de respuesta a incidentes cibernéticos	Uso básico de herramientas de analisis para respuesta a incidentes	Conceptos básicos de ciberseguridad y ataques cibernéticos	Asistir en la identificación y documentación de incidentes de seguridad
Análisis básico de incidentes	Interpretación básica de logs y alertas de seguridad	Principios básicos de análisis forense	Realizar análisis preliminares de incidentes
Conciencia de procedimientos de respuesta a incidentes	Resolución básica de problemas de respuesta a incidentes	Normativas y estándares de respuesta a incidentes (NIST SP 800-61)	Colaborar en la mitigación de incidentes menores
Colaboración en equipos de respuesta a incidentes			Asistir en la elaboración de informes de incidentes

US$1.500

Renta Media

Gestión de Incidentes
Respuesta a Incidentes

CSIRT Respuesta a Incidentes – Intermedio

Competencias	Habilidades	Conocimientos	Tareas Específicas
Análisis avanzado de incidentes	Uso avanzado de herramientas de respuesta a incidentes	Técnicas avanzadas de análisis forense	Realizar análisis profundos de incidentes complejos
Coordinación efectiva en la respuesta a incidentes	Desarrollo de planes de respuesta a incidentes	Protocolos y procedimientos de respuesta a incidentes	Coordinar y dirigir la respuesta a incidentes en tiempo real
Documentación detallada de incidentes	Resolución de problemas avanzada de respuesta a incidentes	Tendencias y desarrollos actuales en ciberamenazas	Contribuir en la mejora continua de los procedimientos de respuesta
Colaboración con equipos multidisciplinarios		Cumplimiento normativo y regulaciones de respuesta a incidentes	Participar en ejercicios de simulación de incidentes

US$2.700

Renta Media

MITRE – Attack IQ
GCIH– GIAC
CySA+ - CompTIA

CSIRT Respuesta a Incidentes – Senior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Liderazgo en proyectos de respuesta a incidentes	Liderazgo en la gestión de incidentes de alto perfil	Estrategias y políticas de respuesta a incidentes a nivel empresarial	Coordinar y dirigir equipos de respuesta en incidentes críticos
Desarrollo de estándares y procedimientos de respuesta a incidentes (ISO 27035)	Comunicación estratégica de hallazgos de incidentes	Marco regulatorio y de cumplimiento normativo específico	Desarrollar y mejorar estándares y procedimientos de respuesta a incidentes
Mentoría y desarrollo de talento en respuesta a incidentes	Análisis forense avanzado de incidentes	Técnicas avanzadas de análisis de riesgos y amenazas	Mentorear y guiar a equipos junior e intermedios en respuesta a incidentes
Gestión de incidentes críticos			Evaluar y recomendar soluciones para mejorar la capacidad de respuesta

US$4.500

Renta Media

CISSP – ISC2
CISM – ISACA
ECIH– Ec – Council

CSIRT Respuesta a Incidentes – Formación

Factor	Nivel
Empleabilidad A	Alta
Empleabilidad B	Muy Baja
Consultoría	Media
Oportunidades	Alta
Proyección MP	Media
Proyección LP	Muy Alta

	Junior	Intermedio	Senior	
		ISO 22301 Continuidad	ISO 27001 NIST CSF	Gobierno y Gestión
		Gestión de Riesgo	Gestión Estratégica	
	ISO 27035 Incidentes			
	Respuesta a Incidentes			
		Ciberdefensa Ransomware	Herramientas de Blue Team	Técnico y Operativo
		Inteligencia de Amenazas	SOC	
		Peritaje Informático	Ransomware Business Continuity Plan (RBCP)	

Especialista SOC - Junior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Fundamentos de seguridad operativa	Uso básico de herramientas de monitoreo de seguridad (SIEM, IDS/IPS, etc.)	Conceptos básicos de ciberseguridad y operaciones de seguridad	Monitorear y analizar alertas de seguridad
Análisis básico de eventos de seguridad	Interpretación básica de logs y alertas de seguridad	Principios básicos de incidentes de seguridad	Asistir en la identificación y documentación de incidentes
Conciencia de procedimientos de respuesta a incidentes	Resolución básica de problemas de seguridad operativa	Normativas y estándares de seguridad operativa (ISO 27002)	Colaborar en la gestión de incidentes menores
Colaboración en equipos de SOC			Asistir en la elaboración de informes de seguridad

US$2.100

Renta Media

Herramientas
Seguridad en Redes

Especialista SOC– Intermedio

Competencias	Habilidades	Conocimientos	Tareas Específicas
Análisis avanzado de eventos de seguridad	Uso avanzado de herramientas de monitoreo de seguridad (SIEM, IDS/IPS, etc.)	Técnicas avanzadas de análisis de eventos de seguridad	Realizar análisis profundos de alertas y eventos
Coordinación efectiva en el SOC	Desarrollo de planes de mejora de seguridad	Protocolos y procedimientos de seguridad operativa	Coordinar y dirigir actividades diarias del SOC
Documentación detallada de incidentes	Resolución de problemas avanzada de seguridad operativa	Tendencias y desarrollos actuales en ciberamenazas	Contribuir en la mejora continua de los procesos del SOC
Colaboración con equipos multidisciplinarios		Cumplimiento normativo y regulaciones de seguridad operativa	Participar en ejercicios de simulación de incidentes

US$3,000

Renta Media

CSA – Ec – Council
GSOC – GIAC
CySA+ - CompTIA

Especialista SOC – Senior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Liderazgo en proyectos de seguridad operativa	Liderazgo en la gestión de operaciones de seguridad	Estrategias y políticas de seguridad operativa a nivel empresarial	Coordinar y dirigir equipos de SOC en proyectos críticos
Desarrollo de estándares y procedimientos del SOC	Comunicación estratégica de hallazgos de seguridad	Marco regulatorio y de cumplimiento normativo específico	Desarrollar y mejorar estándares y procedimientos del SOC
Mentoría y desarrollo de talento en el SOC	Análisis forense avanzado de seguridad operativa	Técnicas avanzadas de análisis de riesgos y amenazas	Mentorear y guiar a equipos junior e intermedios en el SOC
Gestión de incidentes críticos			Evaluar y recomendar soluciones para mejorar la capacidad del SOC

US$5.800

Renta Media

CISSP – ISC2

CISM – ISACA

Especialista SOC – Formación

Factor	Nivel
Empleabilidad A	Alta
Empleabilidad B	Alta
Consultoría	Muy Alta
Oportunidades	Muy Alta
Proyección MP	Alta
Proyección LP	Muy Alta

Junior	Intermedio	Senior	
	Gestión de Incidentes	ISO 27001 NIST CSF	Gobierno y Gestión
	Gestión de Riesgo	Gestión Estratégica	
SOC			
Herramientas de Blue Team			
	Respuesta a Incidentes	Ciberdefensa Ransomware	Técnico y Operativo
	Inteligencia de Amenazas	Peritaje Informático	
	Seguridad en Redes	Ransomware Business Continuity Plan (RBCP)	

Implementación SGSI - Junior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Fundamentos de SGSI	Uso básico de herramientas de gestión de la seguridad de la información (GRC)	Conceptos básicos de seguridad de la información y gestión de riesgos	Asistir en la implementación de controles de seguridad
Asistencia en la documentación de SGSI	Interpretación básica de requisitos de normativas (ISO 27001)	Principios básicos de auditoría de seguridad	Colaborar en la realización de evaluaciones de riesgos
Conciencia de procedimientos de SGSI	Resolución básica de problemas de seguridad de la información	Normativas y estándares de seguridad de la información	Asistir en la elaboración de políticas y procedimientos de seguridad
Colaboración en equipos de implementación de SGSI			Asistir en la preparación de informes de implementación

US$1.700

Renta Media

ISO LI/LA 27001
Gestión de Riesgos

Implementación SGSI– Intermedio

Competencias	Habilidades	Conocimientos	Tareas Específicas
Implementación avanzada de SGSI	Uso avanzado de herramientas de gestión de la seguridad de la información (GRC)	Técnicas avanzadas de gestión de riesgos	Coordinar la implementación de controles de seguridad
Documentación detallada de SGSI	Desarrollo de planes de implementación de SGSI	Normativas y estándares de seguridad de la información (ISO 27001, ISO 22301)	Elaborar y mantener la documentación de SGSI
Coordinación efectiva en equipos de SGSI	Resolución de problemas avanzada de seguridad de la información	Procesos de auditoría interna y externa de seguridad	Coordinar actividades de concienciación en seguridad
Colaboración con equipos multidisciplinarios		Cumplimiento normativo y regulaciones de seguridad de la información	Participar en la preparación y respuesta a auditorías

US$2.800

Renta Media

CISM – ISACA
ISO LI/LA 22301
ISO LI 27005

Implementación SGSI – Senior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Liderazgo en proyectos de SGSI	Liderazgo en la implementación de SGSI a nivel empresarial	Estrategias y políticas de seguridad de la información	Dirigir y gestionar proyectos de implementación de SGSI
Desarrollo de estándares y procedimientos de SGSI	Comunicación estratégica de hallazgos de SGSI	Marco regulatorio y de cumplimiento normativo específico	Desarrollar y mejorar estándares y procedimientos de SGSI
Mentoría y desarrollo de talento en SGSI	Análisis forense avanzado de seguridad de la información	Técnicas avanzadas de análisis de riesgos y amenazas	Mentorear y guiar a equipos junior e intermedios en SGSI
Gestión de auditorías de SGSI		Normativa de Privacidad y protección de datos	Evaluar y recomendar mejoras en el SGSI

US$5.300

Renta Media

CISSP – ISC2
CISA – ISACA
CDPSE - ISACA

Implementación SGSI – Formación

Factor	Nivel
Empleabilidad A	Alta
Empleabilidad B	Muy Alta
Consultoría	Muy Alta
Oportunidades	Muy Alta
Proyección MP	Muy Alta
Proyección LP	Muy Alta

Junior	Intermedio	Senior	
	ISO 27002 CIS Control	NIST CSF	Gobierno y Gestión
	Auditor ISO 27001	Gestión Estratégica	
Implementador ISO 27001	Gestión Incidentes ISO 27035	Compliance ISO 37301	
Gestión de Riesgos	Gestión Continuidad ISO 22301	Privacidad ISO 27701	
	Inteligencia de Amenazas	Seguridad Cloud	Técnico y Operativo
	Seguridad en Redes	DevSecOps	

Especialista Seguridad Redes - Junior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Fundamentos de seguridad de redes	Configuración básica de firewalls y sistemas de detección de intrusiones (IDS/IPS)	Conceptos básicos de redes y protocolos de seguridad	Asistir en la monitorización y análisis de eventos de seguridad de red
Asistencia en la implementación de políticas de seguridad de red	Interpretación básica de registros y alertas de seguridad	Principios básicos de criptografía y autenticación	Colaborar en la identificación y documentación de incidentes de seguridad de red
Conciencia de procedimientos de respuesta a incidentes de red	Resolución básica de problemas de seguridad de red	Normativas y estándares de seguridad de red (NIST, ISO 27002)	Asistir en la gestión de parches y actualizaciones de seguridad
Colaboración en equipos de seguridad de red			Asistir en la preparación de informes de seguridad de red

US$2.100

Renta Media

Networking & Seguridad Fundamental (CCENT)

Especialista Seguridad Redes – Intermedio

Competencias	Habilidades	Conocimientos	Tareas Específicas
Implementación avanzada de controles de seguridad de red	Configuración avanzada de firewalls, IDS/IPS y sistemas de prevención de intrusiones	Técnicas avanzadas de seguridad de redes y mitigación de ataques	Coordinar la implementación y gestión de controles de seguridad de red
Análisis avanzado de eventos de seguridad de red	Uso avanzado de herramientas de análisis de tráfico de red (Wireshark, tcpdump)	Protocolos de seguridad y cifrado (TLS/SSL, IPsec)	Realizar análisis detallados de tráfico de red en busca de anomalías y amenazas
Coordinación efectiva en equipos de seguridad de red	Resolución de problemas avanzada de seguridad de red	Tendencias y desarrollos actuales en ciberamenazas	Coordinar actividades de respuesta a incidentes de seguridad de red
Colaboración con equipos multidisciplinarios	Diseño y segmentación de red	Cumplimiento normativo y regulaciones de seguridad de red	Participar en ejercicios de simulación de incidentes de seguridad de red

Renta Media

US$3.000

Certificaciones Especializantes (CCNA, CCNP)

Especialista Seguridad Redes – Senior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Liderazgo en proyectos de seguridad de red	Liderazgo en la planificación y ejecución de proyectos de seguridad de red	Estrategias y políticas de seguridad de red a nivel empresarial	Dirigir y gestionar proyectos críticos de seguridad de red
Desarrollo de estándares y procedimientos de seguridad de red	Comunicación estratégica de hallazgos de seguridad de red	Marco regulatorio y de cumplimiento normativo específico	Desarrollar y mejorar estándares y procedimientos de seguridad de red
Mentoría y desarrollo de talento en seguridad de red	Análisis forense avanzado y ofensivo seguridad de red	Técnicas avanzadas de análisis de riesgos y amenazas	Mentorear y guiar a equipos junior e intermedios en seguridad de red
Gestión de incidentes críticos de seguridad de red	Automatización de operaciones de red		Evaluar y recomendar soluciones para mejorar la seguridad de red

US$5.800

Renta Media

CISSP – ISC2
CISA – ISACA
Certificaciones Avanzadas (CCIE)

Especialista Seguridad Redes – Formación

Factor	Nivel
Empleabilidad A	Alta
Empleabilidad B	Baja
Consultoría	Alta
Oportunidades	Alta
Proyección MP	Media
Proyección LP	Alta

	Junior	Intermedio	Senior	
Gobierno y Gestión		CIS Control ISO 27002	ISO 27001 NIST CSF	
		Gestión de Riesgo	Gestión Estratégica	
Técnico y Operativo	Networking			
	Seguridad en Redes			
		Seguridad Perimetral	Seguridad Ofensiva	
		Diseño y Arquitectura Red	Peritaje Informático	
		Auditoría y Hardening	Programabilidad y Automatización	

Pentester - Junior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Fundamentos de seguridad cibernética	Uso básico de herramientas de pentesting (Nmap, Metasploit)	Conceptos básicos de redes y sistemas operativos	Asistir en la realización de pruebas de penetración
Asistencia en la identificación de vulnerabilidades	Interpretación básica de resultados de pruebas de penetración	Principios básicos de seguridad web	Colaborar en la elaboración de informes de pentesting
Conciencia de metodologías de pentesting	Resolución básica de problemas de seguridad	Normativas y estándares de pentesting	Asistir en la recomendación de medidas correctivas
Colaboración en equipos de pentesting			Asistir en la investigación de nuevas técnicas de pentesting

US$1.700

Renta Media

EHE – Ec-Council
eJPT – INE Security

Pentester – Intermedio

Competencias	Habilidades	Conocimientos	Tareas Específicas
Realización avanzada de pruebas de penetración	Uso avanzado de herramientas de pentesting (Burp Suite, SQLMap, etc.)	Técnicas avanzadas de explotación	Realizar pruebas de penetración en entornos controlados
Análisis avanzado de vulnerabilidades	Interpretación avanzada de resultados de pruebas de penetración	Principios avanzados de seguridad web	Colaborar en la elaboración de estrategias de mitigación
Coordinación efectiva en equipos de pentesting	Resolución de problemas avanzada de seguridad	Tendencias y desarrollos actuales en ciberamenazas	Coordinar y dirigir pruebas de penetración
Colaboración con equipos multidisciplinarios		Cumplimiento normativo y regulaciones de pentesting	Participar en la elaboración de políticas y procedimientos de pentesting

US$2.600

Renta Media

CEH – Ec-Council
eCPPT – INE Security
OSCP – Ofensive Security

Especialista Seguridad Redes – Senior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Liderazgo en proyectos de pentesting	Liderazgo en la planificación y ejecución de proyectos de pentesting	Estrategias y políticas de pentesting a nivel empresarial	Dirigir y gestionar proyectos críticos de pentesting
Desarrollo de estándares y procedimientos de pentesting	Comunicación estratégica de hallazgos de pentesting	Marco regulatorio y de cumplimiento normativo específico	Desarrollar y mejorar estándares y procedimientos de pentesting
Mentoría y desarrollo de talento en pentesting	Análisis forense avanzado de incidentes de seguridad	Técnicas avanzadas de análisis de riesgos y amenazas	Mentorear y guiar a equipos junior e intermedios en pentesting
Gestión de incidentes críticos de pentesting			Evaluar y recomendar soluciones para mejorar la seguridad basadas en los hallazgos de pentesting

US$5.100

Renta Media

OSCP – Ofensive Security
Certificaciones avanzadas
Ofensive Security + INE Security

Pentester – Formación

Factor	Nivel
Empleabilidad A	Alta
Empleabilidad B	Muy Baja
Consultoría	Alta
Oportunidades	Alta
Proyección MP	Media
Proyección LP	Muy Alta

Junior	Intermedio	Senior	
	Gestión de Riesgo	ISO 27001 NIST CSF	Gobierno y Gestión
Hacking Ético			
Seguridad en Redes			
	Pentesting Cloud	Herramientas y técnicas OSINT para Red Team	Técnico y Operativo
	Pentesting Web	Técnicas de Evasión de Sistemas de Seguridad y Creación de Malware	
	Desarrollo de Herramientas Python		
	Campañas para Red Team	Pentesting Web Avanzado	

Arquitecto Seguridad Cloud - Junior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Fundamentos de seguridad en la nube	Configuración básica de servicios de seguridad en la nube (Firewalls, WAF)	Conocimientos básicos de criptografía y protocolos de seguridad	Evaluación de la postura de seguridad en la nube en entornos básicos
Diseño básico de arquitecturas seguras en la nube	Uso básico de herramientas de monitorización y auditoría en la nube	Principios básicos de redes definidas por software (SDN)	Colaboración en la implementación de políticas de seguridad en la nube
Conciencia de amenazas específicas en la nube	Resolución básica de problemas de seguridad en la nube	Normativas y estándares de seguridad en la nube (CSA, ISO 27017)	Revisión y actualización de políticas y procedimientos de seguridad en la nube
Colaboración en equipos de seguridad en la nube			Participación en la elaboración de informes técnicos de seguridad en la nube

US$2.800

Renta Media

Certificaciones de Entrada
(Cloud Practicioner + Associate)

Arquitecto Seguridad Cloud – Intermedio

Competencias	Habilidades	Conocimientos	Tareas Específicas
Diseño avanzado de arquitecturas seguras en la nube	Configuración avanzada de servicios de seguridad en la nube	Profundo entendimiento de la infraestructura de nube (IaaS, PaaS, SaaS)	Diseño y despliegue de arquitecturas seguras y escalables en la nube
Análisis avanzado de amenazas y vulnerabilidades en la nube	Interpretación avanzada de logs y eventos de seguridad en la nube	Conocimientos avanzados de técnicas de ataque en la nube	Realización de análisis de riesgos y evaluaciones de seguridad en la nube
Coordinación efectiva en equipos de seguridad en la nube	Resolución de problemas complejos de seguridad en la nube	Tendencias y desarrollos actuales en seguridad en la nube	Coordinación y liderazgo en proyectos de seguridad en la nube
Colaboración con equipos multidisciplinarios		Cumplimiento normativo y regulaciones específicas en la nube	Participación en ejercicios de red teaming y simulaciones de incidentes en la nube

US$3.900

Renta Media

Certificaciones Especializantes
Associate + Profesional

Arquitecto Seguridad Cloud – Senior

Competencias	Habilidades	Conocimientos	Tareas Específicas
Liderazgo en proyectos de pentesting	Liderazgo en la planificación y ejecución de proyectos de pentesting	Estrategias y políticas de pentesting a nivel empresarial	Dirigir y gestionar proyectos críticos de pentesting
Desarrollo de estándares y procedimientos de pentesting	Comunicación estratégica de hallazgos de pentesting	Marco regulatorio y de cumplimiento normativo específico	Desarrollar y mejorar estándares y procedimientos de pentesting
Mentoría y desarrollo de talento en pentesting	Análisis forense avanzado de incidentes de seguridad	Técnicas avanzadas de análisis de riesgos y amenazas	Mentorear y guiar a equipos junior e intermedios en pentesting
Gestión de incidentes críticos de pentesting			Evaluar y recomendar soluciones para mejorar la seguridad basadas en los hallazgos de pentesting

US$5.500

Renta Media

Certificaciones avanzadas
Professional + Seguridad + Redes + Devops

Arquitecto Seguridad Cloud – Formación

Factor	Nivel
Empleabilidad A	Muy Alta
Empleabilidad B	Muy Alta
Consultoría	Muy Alta
Oportunidades	Muy Alta
Proyección MP	Muy Alta
Proyección LP	Muy Alta

	Junior	Intermedio	Senior
Gobierno y Gestión		CIS Control ISO 27002	Especialista Cloud CSA
		ISO 27017	Gestión Estratégica
	Arquitectura Cloud		
	Seguridad Cloud		
Técnico y Operativo		Arq. Cloud Avanzado	DevSecOps
		Networking Cloud	Pentesting Cloud
		DevOps	Gestión de Incidentes

Profesor

Carlos Lobos de Medina

Ingeniero Civil en Informática y Magister en Informática © de la Universidad de Santiago de Chile, Diplomado en Auditoría de Sistemas, Postitulado en Seguridad Computacional de la Universidad de Chile.

Especialista en gobernanza, gestión y control de tecnologías de información empleando modelos como COBIT, ITIL, ISO 27001 e ISO 22301. Posee certificaciones internacionales CISA, CISM, COBIT, ISO Lead Auditor 27001, ISO Lead Auditor BS 25599 e ITIL V3, entre otras.

carlos.lobos@usach.cl

https://www.linkedin.com/in/clobos/

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Empleabilidad en Ciberseguridad