GRUPO IT-TALENT®

DIPLOMADO CIBERSEGURIDAD

CAPACITACIÓN USACH - UNIVERSIDAD DE SANTIAGO DE CHILE

ALIGNMENT

SOLUCIONES ESTRATÉGICAS



REPORTE CIBERSEGURIDAD

Índice

02 Índice
03 IT-TALENT Headhunter Senior TI
04 Capacitación USACH
05 Introducción

06 **CONTEXTO**

06 Contexto
08 Metodología.
09 Análisis demográfico: Cargos.
10 Género.
12 ¿Cómo marcamos diferencia en lo profesional para el rubro de la ciberseguridad? por Julio Briones.
14 Análisis demográfico: Cantidad de empleados.
15 Análisis demográfico: Distribución etaria.
16 Distribución académica.
18 ¿Cómo operan los incentivos en la regulación de Ciberseguridad? por Paulina Silva.
20 Análisis demográfico: Tamaño de empresa.
21 Distribución académica.

22 **CONOCIMIENTOS ESTANDARIZADOS**

22 Conocimientos estandarizados.
25 Cambios y mejoras por Haridas Umpierrez

26 **RENTAS**

26 Rentas
29 Salarios según cargos
31 Salarios según empresas
32 Salarios y certificaciones
33 Opinión por Carlos Lobos de Medina
33 Formación académica.
35 Análisis de movilidad y estabilidad laboral.
37 Opinión por Lidia Herrera Mateluna

Final de estudio

38 Selección y retención
41 Conclusiones por Marco Muñoz

GRUPO IT-TALENT®

Con su oficina central en Santiago de Chile IT-Talent es una compañía multinacional, líder en la búsqueda de talentos en el ámbito de las tecnologías de la información. Esto abarca toda la vertical de la industria, desde soporte técnico hasta cargos gerenciales, incluyendo CIOs, CISO y CEOs de empresas tecnológicas.

El head hunter cuenta con una base de datos a nivel mundial de más de 1 millón de profesionales TI, segmentados y clasificados en 80 diferentes tecnologías y conocimientos. Esto ha permitido la contratación de más de mil talentos del área tanto en Latinoamérica como en Europa.

Asimismo, IT-Talent ha desarrollado una propuesta de valor única a nivel internacional, en la cual la tecnología y la automatización han transformado el proceso de selección de profesionales. Gracias a ello, el head hunter ha sido capaz de entregar siempre, tanto al candidato como a la empresa, un match único.

Actualmente IT-Talent tiene presencia en Chile, Argentina, Colombia, México y Perú. Dentro del corto plazo se sumarán Estados Unidos y España.

Nuestros resultados nos avalan y nuestros clientes hablan por nosotros. De hecho, ocho de las diez empresas más grandes de Chile trabajan con IT-Talent.



Capacitación USACH

Capacitación Usach, el organismo técnico de capacitación más importante de la Universidad de Santiago de Chile, tiene la misión de articular el conocimiento que genera el quehacer académico de la universidad con el mundo productivo, tanto a nivel nacional como regional.

Su rol ha sido especialmente relevante durante los últimos 15 años, mediante el diseño e impartición de más de 1.500 programas de formación continua. Entre ellos se incluyen cursos, diplomados y postítulos, los que son impartidos de manera presencial, online sincrónica, asincrónica, y en nuevas modalidades híbridas, para mejorar las competencias de las y los trabajadores del país.

Entre estos programas residen los Diplomados de Ciberseguridad, programa multidisciplinario que se origina en el año 2019, que a la fecha cuenta con 15 diplomados en distintas áreas de la ciberseguridad; además de 60 cursos especializados en distintas materias. Asimismo, se incluye una oferta de diversos cursos de fundamentos abiertos y gratuitos para el fácil ingreso al mundo de la seguridad de la información.

Tenemos el objetivo de impulsar el conocimiento y las prácticas de seguridad de la información a lo largo del país y en el resto de Latinoamérica. Entendiendo las diversas necesidades que enfrentan los actores en este contexto, ofrecemos un sistema de formación personalizado, en la forma de una malla flexible dentro de cada diplomado, lo que permite a los alumnos centrarse en aquellos tópicos que su contexto laboral requiere.

Es en este espíritu que nos interesa conocer el estado de la fuerza laboral, sobre todo en términos de educación y capacitación, para así implementar estrategias de mejora a nuestros diplomados, y seguir siendo uno de los principales impulsores de la formación en ciberseguridad.

INTRODUCCIÓN

Con el incremento constante de infraestructura digital y almacenamiento de datos, la ciberseguridad es una disciplina que se ha hecho más y más presente en las empresas a nivel mundial. Por lo mismo, el requerimiento de profesionales con especializaciones en el área ha ido en aumento. Este informe busca caracterizar el estado de la fuerza laboral que se ha formado hasta el momento en Latinoamérica.

Esta caracterización es general y transversal, se busca entender la distribución por género, nivel educacional y edad de la fuerza laboral, así como también en qué empresas se está impartiendo servicios de ciberseguridad y cómo estas diferencias se reflejan en la remuneración de los profesionales. En particular este estudio entrega un análisis a la relación que existe entre la certificación y la renta del profesional.

Finalmente, y a modo de profundizar en la caracterización de la fuerza laboral, se ofrece un breve análisis con respecto a las habilidades y conocimientos requeridos en los distintos cargos existentes, a modo de entender los requerimientos del mercado en materia de ciberseguridad.

Contexto

GRUPO IT-TALENT | ALIGNMENT | DIPLOMADO CIBERSEGURIDAD
CAPACITACION USACH - UNIVERSIDAD DE SANTIAGO DE CHILE

CONTEXTO

Las amenazas a la ciberseguridad se han hecho más y más presentes en los últimos tiempos. Sin ir más lejos, según cifras del Boletín de Seguridad 2021 de Kaspersky, los sistemas de detección de esa compañía detectaron 380 mil nuevos archivos maliciosos cada día. Esto representa un incremento de 5,7% en comparación con el año anterior. Es decir, 20.000 nuevos descubrimientos diarios más que en 2020.

Sin embargo no se trata solamente de un aumento de amenazas, sino del tipo de éstas: el informe señala que uno de los factores importantes de este aumento está directamente relacionado al incremento del número de dispositivos móviles utilizados en todo el mundo. Además, a esto se suman ciertos hábitos que se acentuaron con la Pandemia, como el uso de la huella digital, concepto que refiere a los datos que van dejando las personas a medida que navegan por diferentes sitios en Internet o usan las redes sociales.



Gracias a este dato, según señaló un informe de IBM y Monitor Consulting publicado durante el 2021, en Chile los consumidores elevaron este uso y el 84% rehusaron sus credenciales en línea en múltiples cuentas. El problema es que estos mismos hábitos son replicados por esos consumidores como trabajadores de una empresa. Es ahí donde el problema se vuelve más complejo.

Se hace evidente la necesidad de reforzar la fuerza laboral en materia de ciberseguridad. Para comprender la manera en la que debe realizarse ese refuerzo, es necesario entender el estado actual de esta. Es por eso que este informe busca analizar y ofrecer una visión comprensiva tanto para quienes desean actualizar sus conocimientos en el área, como para aquellos que desean ingresar al mercado laboral de ciberseguridad; así como entregar una mirada a los empleadores de los cambios que son necesarios en materia de ciberseguridad en sus empresas.

METODOLOGÍA

Los datos presentados en este informe se recolectaron mediante una encuesta realizada por el equipo de IT-Talent Research área especializada de IT-TALENT GROUP especializada en investigación y estudios asociados en conjunto con Alignment.

La data fue recolectada durante los últimos seis meses de 2021, en base a una encuesta realizada de forma online a diferentes profesionales ligados a las tecnologías de la información en Latinoamerica.

Universo de desarrollo: Latinoamérica.

Participantes: Residentes latinoamericanos.

Perfil de los encuestados: Profesionales de Tecnologías de la Información, con foco en profesionales que trabajan en los segmentos de la ciberseguridad.

Muestra: Por conveniencia, basada en las redes que cuenta IT-Talent, con link de acceso público y compartible, contestada por +500 profesionales y personas ligadas a la informática.

Herramienta de recolección de la muestra: Plataformas digitales entre los días agosto y diciembre de 2021.

Estos resultados son generalizables a profesionales TI.

Las rentas expuestas en este informe son líquidas, se encuentran en dólares americanos y no incluyen bonos.



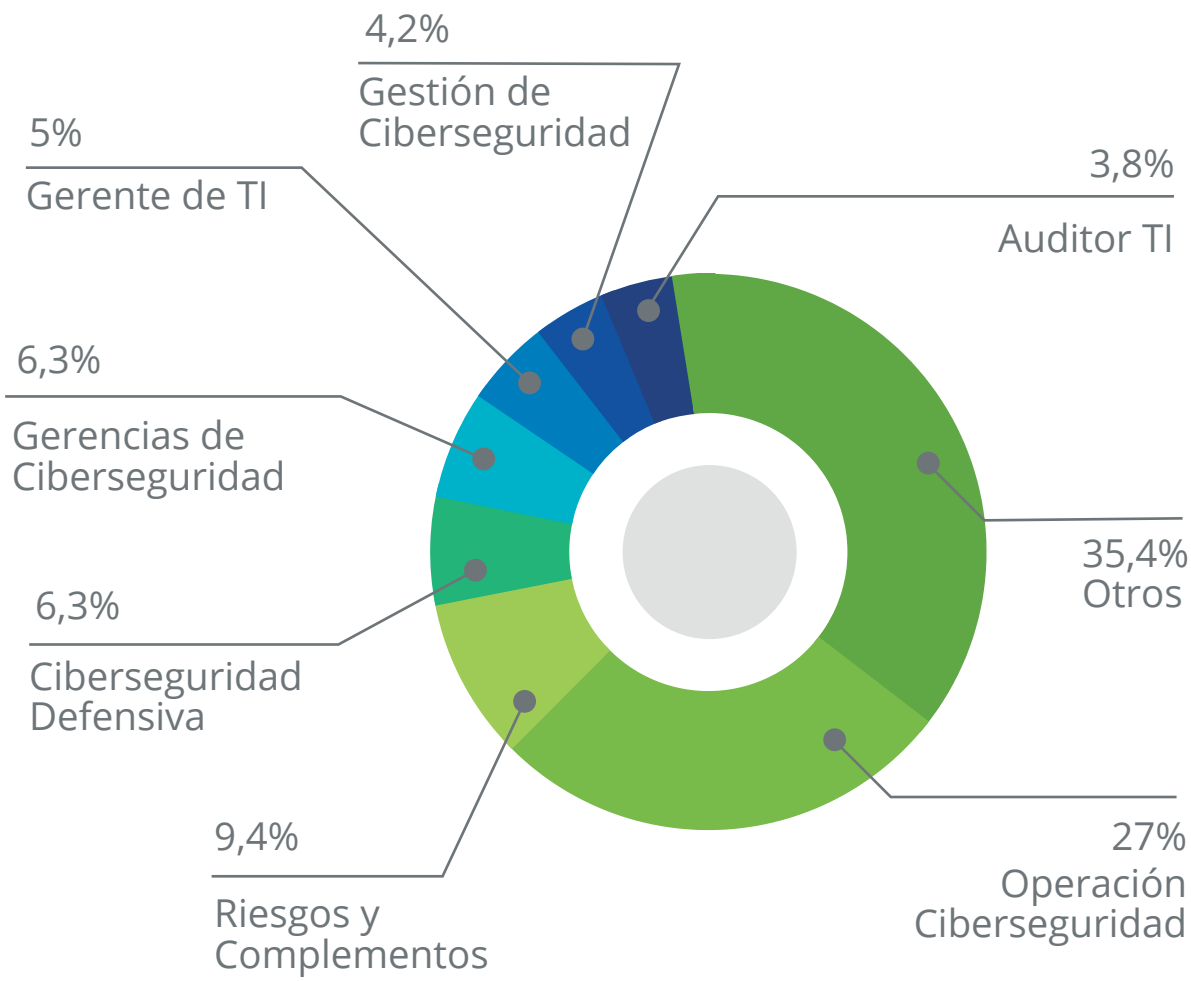
ANÁLISIS DEMOGRÁFICO

Cargos

En esta primera instancia, se entrega un un vistazo a la distribución general de la muestra tomada, con el fin de tener claro la distribución por género, edad y la proporción de tipos de cargos que se observa. Cabe destacar que se determinaron nueve cargos más la opción Otros. Esta última representa todos los que no están en la clasificación hecha a priori.

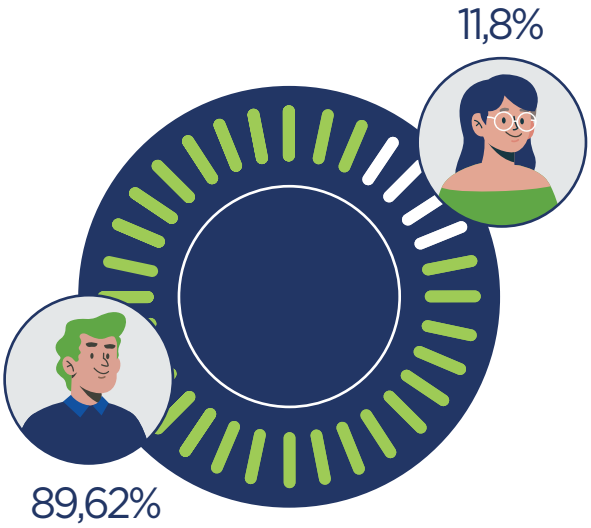
Esta opción es donde se encasilla el porcentaje más alto (35.65%) de los encuestados. Con esto se infieren dos cosas: que un porcentaje de quienes contestaron la encuesta se desempeña en cargos que sí están dentro de la lista de opciones pero no se reconocen como ninguno de ellos; y que otro porcentaje importante se desempeña en una variedad de cargos especializados.

Los porcentajes por cargo fueron:

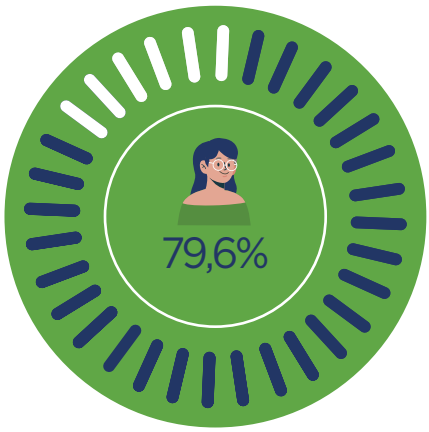


GÉNERO

En cuanto a género, se repite lo que ocurre en otras áreas de TI donde la gran mayoría de los puestos de trabajo los desempeñan hombres. Esta situación se repite en nuestro estudio:



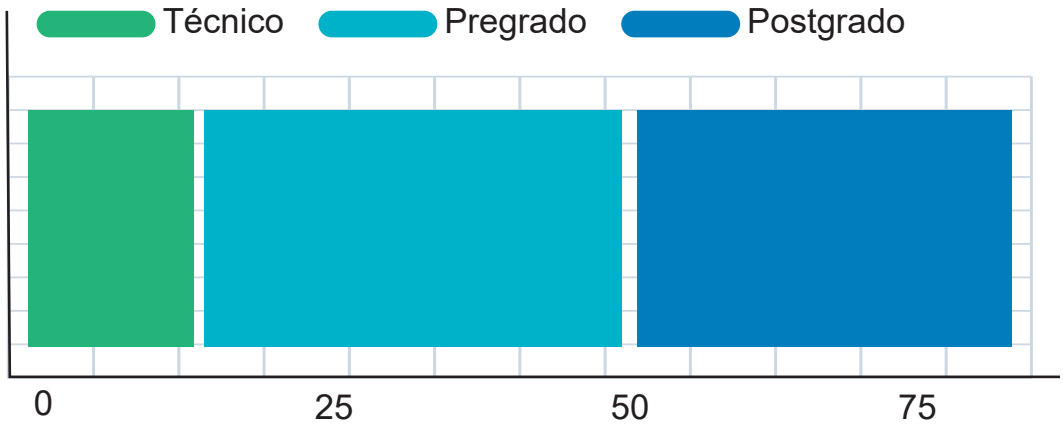
En los puestos de Ciberseguridad, el 89,62% pertenece a hombres y el 11,8% a mujeres.



La mayor presencia femenina está en los puestos de Gestión de Ciberseguiridad y Auditoría TI (alrededor de 80%), mientras que la menor proporción (10%) se encuentra en la categoría Otros.

FORMACIÓN ACADÉMICA

Uno de los puntos focales del estudio es la formación académica y la importancia de las certificaciones en las áreas de ciberseguridad. Los descubrimientos fueron:



75%

DE LOS CARGOS EN CIBERSEGURIDAD CORRESPONDE A LOS PROFESIONAES CON ESTUDIOS DE PREGRADO.

60,5%

DE LOS PROFESIONALES TI QUE SE DESEMPEÑAN EN CIBERSEGURIDAD POSEE AL MENOS UNA CERTIFICACIÓN.

32,2%

DE LOS LOS CARGOS GERENCIALES CUENTAN CON UNA MAESTRÍA



Cómo marcamos diferencia en lo profesional para el rubro de la ciberseguridad

Hoy en día, en un mundo tan dinámico y versátil en relación a lo tecnológico, donde la ciberseguridad no está al margen, no es un misterio ni algo desconocido que los ciberataques están aumentando cada vez más en el mundo y en Chile.

Por lo mismo, la necesidad de profesionales del rubro es muy alta, tanto así que tal como Ricardo Céspedes de EY indica en “seguridaddigital.emol.com”, se calcula que en Estados Unidos hay 700 mil profesionales empleados actualmente en puestos de ciberseguridad, y estima que se necesitan 350 mil profesionales más para cubrir las necesidades de las empresas en ese país. “En Chile la realidad no es muy diferente e incluso estamos más atrasados que Estados Unidos y otras potencias”, asegura.

Asimismo, la urgencia nos indica que debemos como líderes en el ámbito intentar disminuir está brecha de profesionales del rubro tanto en Chile como en Latinoamérica. Vemos que muchos profesionales buscan potenciarse en ciberseguridad, con distintas certificaciones internacionales tanto a nivel técnico como de gestión. El problema es que en muchas ocasiones el costo es muy elevado y, en algunos casos, tiene un costo equivalente al de una maestría universitaria. Un valor muy alto que, en muchos casos, les impide a nuestros profesionales mejorar.

Siendo así, la pregunta es ¿Cómo mejoramos los perfiles de nuestros profesionales para intentar cerrar la brecha en ciberseguridad en Chile?

Estimo que instituciones de excelencia en la continuidad educativa como Capacitación Usach y la Universidad de Santiago de Chile, entregan aprendizajes y herramientas a los profesionales y técnicos, que desean y se obligan a mantenerse actualizados. O bien, quieran extender su horizonte profesional con los conocimientos, habilidades y destrezas que demanda la ciberseguridad en el contexto actual.

Dichas instituciones, a través de su completa oferta programática en el área de la ciberseguridad, representan una plataforma de intercambio y encuentro entre profesionales de Chile y en Latinoamérica, para especializarse a nivel técnico, de gestión y normativo, con un alto estándar y visión global.

Es importante resaltar que en su staff académico cuenta con destacados profesionales y expertos docentes, tanto chilenos como internacionales.

Los programas ofrecidos son de valor accesible y de alta calidad, lo cual es un enorme valor agregado. Gracias a ello creo que hay muchas posibilidades de acortar esas brechas en el mediano plazo y contribuir al crecimiento profesional de los alumnos.



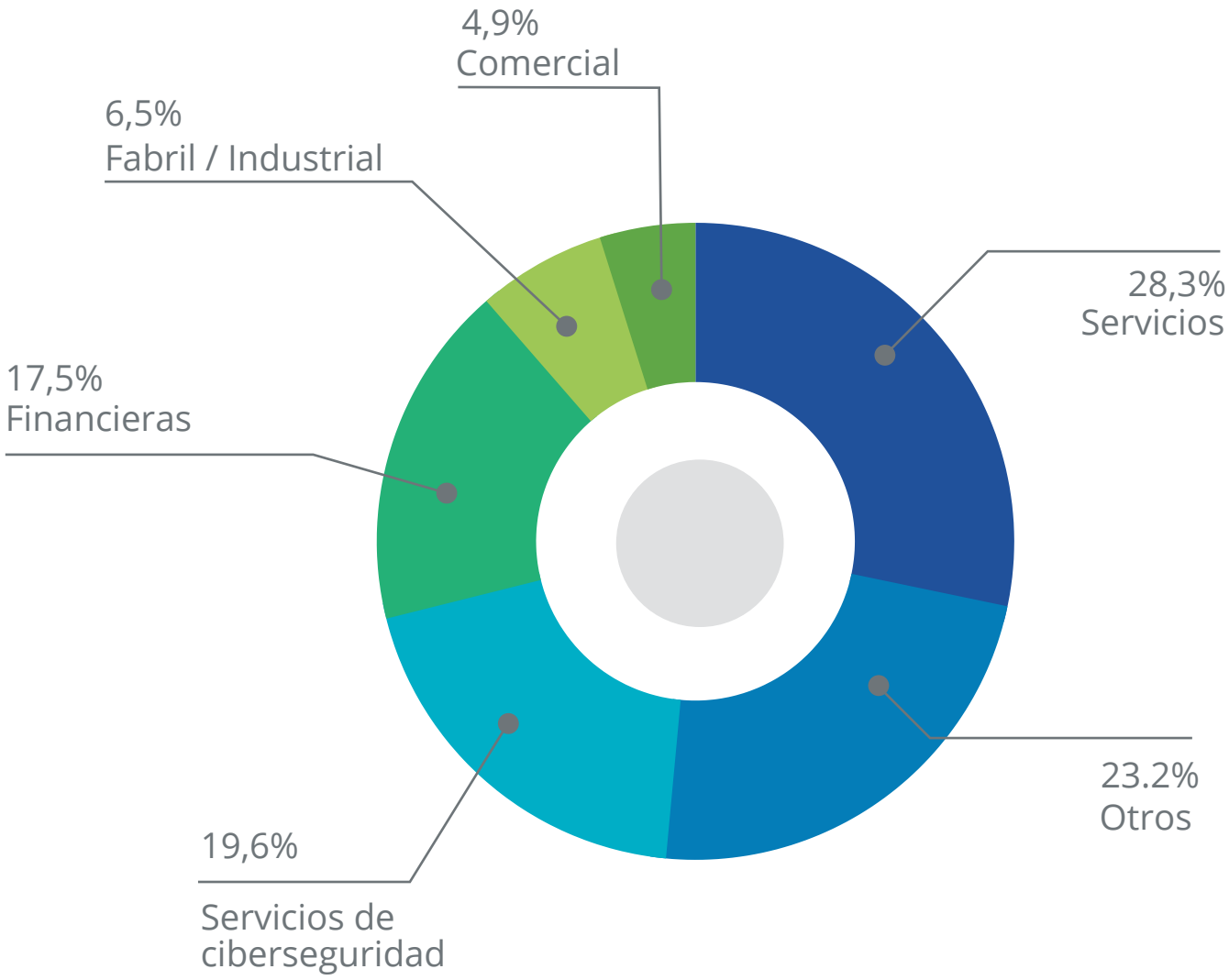
Julio Briones

CISO-Ciberseguridad ISA Intervial &
Consultor Senior Ciberseguridad
IT-Talent

ANÁLISIS DEMOGRÁFICO

Cantidad de empleados

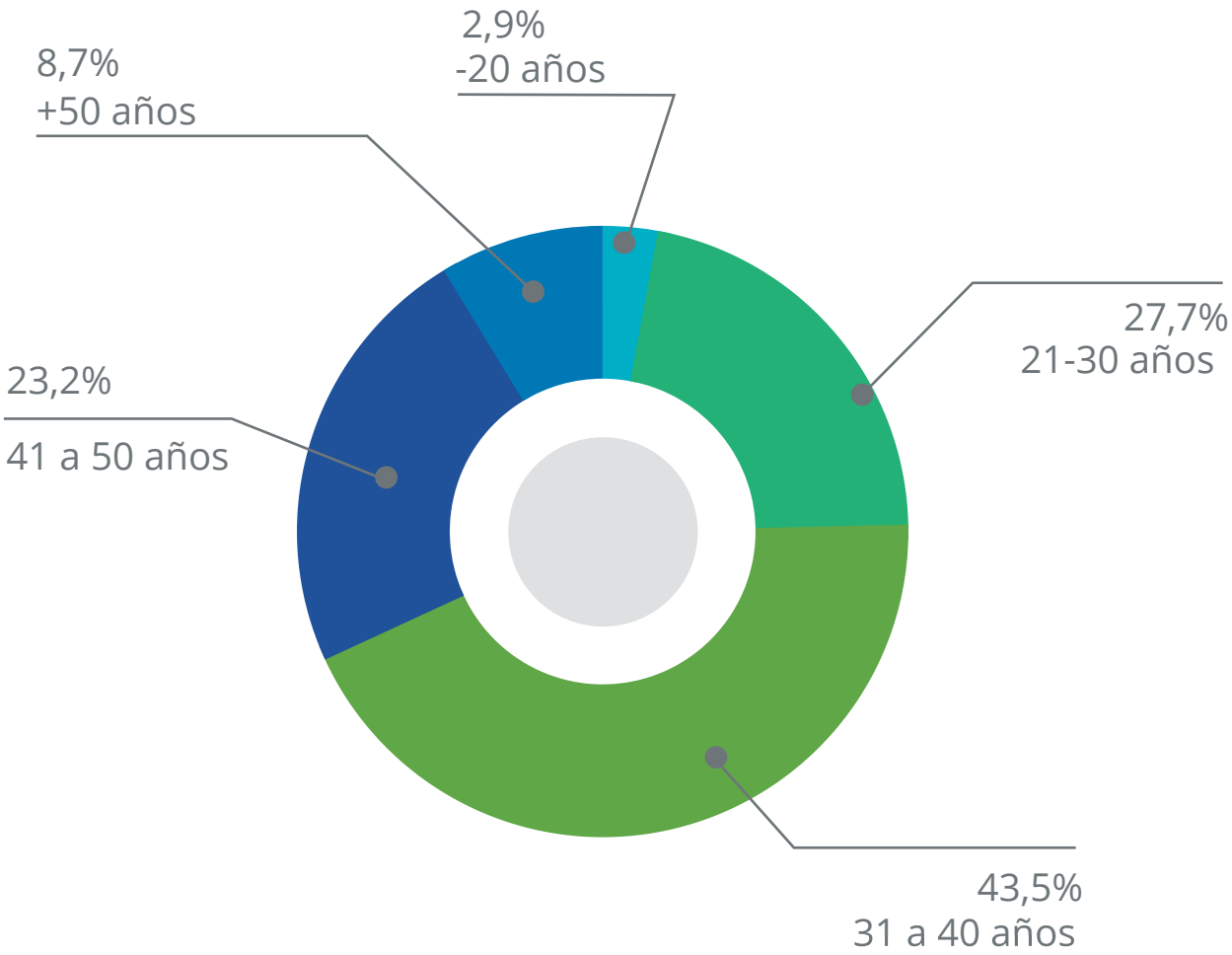
Lo más interesante de estas cifras es notar cuántos empleados hay en las áreas de Ciberseguridad en cada empresa. Es así como se ve que en las empresas de servicios una gran cantidad del total de empleados se desempeñan en departamentos pequeños (1 a 4 trabajadores). Esa misma proporción se repite en el rubro Fabril/Industrial y Comercial.



ANÁLISIS DEMOGRÁFICO

Distribución etaria

En este segmento se observa que aquellas empresas que invierten menos en ciberseguridad son aquellas que tienen una fuerza laboral de mayor edad. Mientras, aquellas como las de servicios de ciberseguridad tienen una mayor cantidad de empleados jóvenes. Esto es importante dado que en áreas que mantienen un estado de avance constante, mantener una base de trabajadores jóvenes permite mantener un nivel de conocimientos actualizados. Asimismo, permite contar con propuestas innovadoras, que mejoran las prácticas de ciberseguridad.



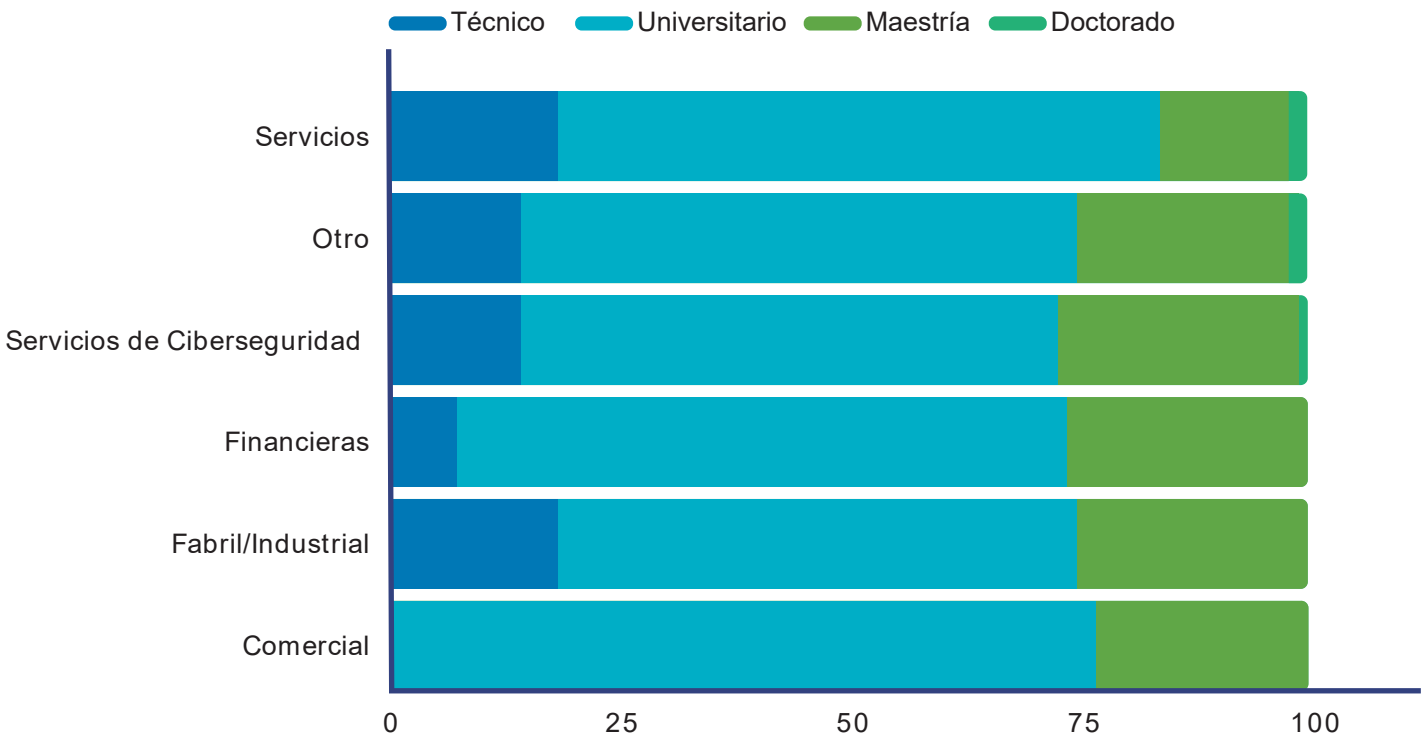
En la mayoria de todos los rubros tienen una cantidad similar y mayoritaria de trabajadores entre 31 y 40 años

DISTRIBUCIÓN ACADÉMICA

Esta parte se muestra la predominancia de empleados con estudios de pregrado, seguidos por los de grados de maestría. En los rubros de servicios y servicios de ciberseguridad, se nota la presencia de grados doctorales, lo que concuerda con lo visto anteriormente en tanto a qué servicios es el rubro que posee mayor cantidad de empleados de ciberseguridad. Llama la atención también que Servicios de Ciberseguridad es un rubro dedicado. Sin embargo, es notable la poca representación que este último grado presenta en el mercado en general.

En casi todos los rubros al menos un 40% de los empleados tienen por lo menos una certificación.

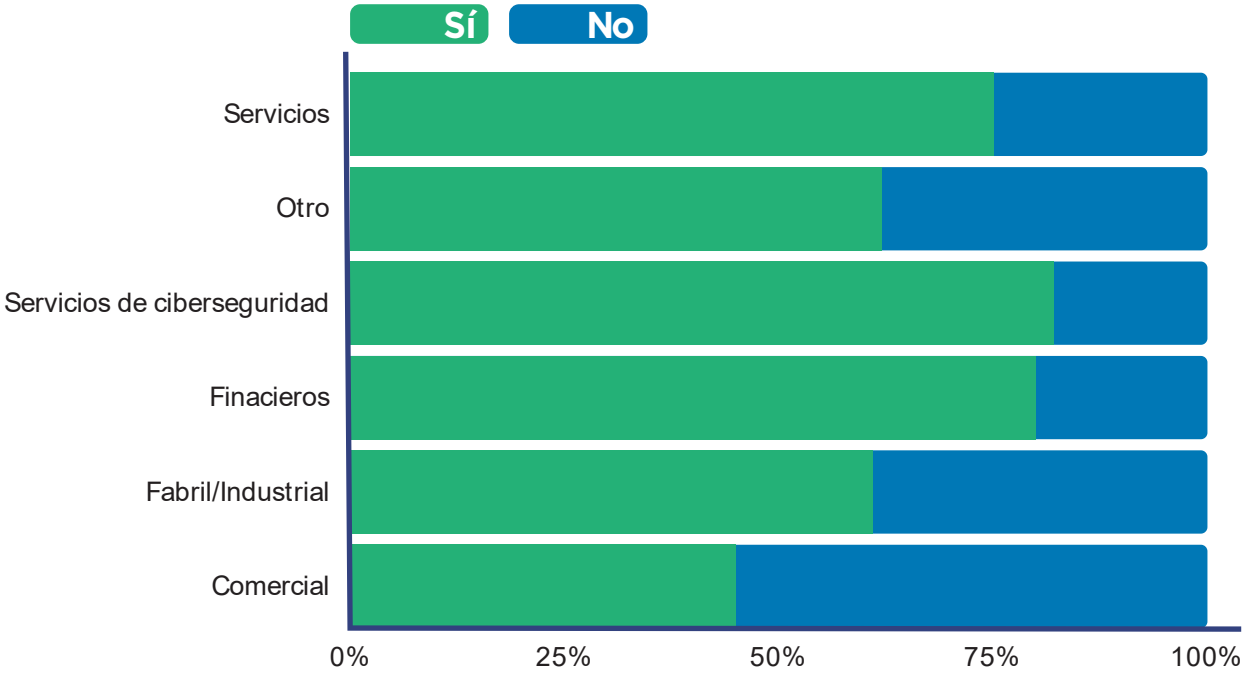




Existe una fuerte tendencia a la adquisición de certificaciones en los trabajadores de ciberseguridad. Más del 50% de los empleados están certificados, en todo tamaño de empresas.



Empleados con certificación por área



Pese a la necesidad de un aumento de dotación, existe de manera transversal una baja percepción de la cantidad de empleados de ciberseguridad. Este es un fenómeno que se da entre todos los tipos de empresas, sin variaciones apreciables.

¿CÓMO OPERAN LOS INCENTIVOS EN LA REGULACIÓN DE CIBERSEGURIDAD?

Cuando el legislador se enfrenta al problema de la ciberseguridad, a diferencia de muchos otros escenarios, lo hace obligando no solo a quien genera el daño, sino también –y con mucha mayor complejidad– a quien lo sufre.

En la pregunta sobre la regulación de la ciberseguridad, intuitivamente pensamos de inmediato en los delitos informáticos. Recientemente, en junio de 2022, se promulgó finalmente en Chile la nueva Ley de Delitos Informáticos N° 21.459, ajustando los nuevos tipos penales a escenarios actualizados y en coherencia con el Convenio de Budapest que nuestro país había suscrito el 2017. Las leyes de delitos informáticos, como toda ley penal, generan un desincentivo al potencial delincuente al asociar la conducta que se busca evitar, con un castigo.

Sin embargo, el problema de la ciberseguridad tiene características particulares, que hacen que un enfoque puramente penal (es decir, de solo castigo al delincuente) esté lejos de ser eficiente. Por un lado, el impacto asociado al riesgo es alto para la víctima: un daño en la continuidad operacional derivado de la indisponibilidad de los sistemas informáticos, puede ser devastador para una empresa.

En segundo lugar, la probabilidad del riesgo de la víctima es alta, pues la delincuencia informática es un negocio de altos retornos y muy baja exposición. Además, y en forma particular, este es un daño con efecto expansivo, pues afecta también a otros stakeholders, como los titulares de los datos personales a los que se acceda con ocasión de una brecha, la disponibilidad de servicios de un organismo público o la cadena de pagos.

Por esta razón, sea cual sea la motivación del ciberdelincuente (financiero, político, espionaje industrial, entre otros), el efecto desincentivador de una robusta ley de delitos informáticos tiene una profundidad muy limitada.

Es allí donde nacen las obligaciones para las potenciales víctimas, relacionadas con cuidarse y organizarse (a través de obligaciones de implementar medidas técnicas y organizacionales de seguridad en los sistemas y en la cultura) y avisar (a través de obligaciones de notificación de brechas de seguridad a los reguladores, y en ciertos casos, a los afectados). El incumplimiento de estas obligaciones, en legislaciones sofisticadas, traen aparejadas sanciones severas.

El sancionar a la víctima y el obligarla a cuidarse es correcto y es económicamente eficiente, pues ésta debe proteger sus sistemas no solo para sí, sino para custodiar la indemnidad de otros, como los titulares de datos personales, o la salud en la cadena de pagos, o la continuidad operacional del país.

Nuestro país, en este segundo aspecto (el de la regulación que incentiva conductas preventivas), muestra un atraso evidente en relación con legislaciones más sofisticadas. La punta de flecha de la implementación de regulación de seguridad y notificaciones de brechas la lleva el mercado bancario y financiero, con las obligaciones derivadas de las RAN 20-8 y 20-10; y, más tímidamente, ciertos mercados regulados como seguros, telecomunicaciones, AFP o eléctrico, entre otros.

Sin embargo, no existen leyes que se hagan cargo en forma transversal de esta estructura obligacional para incentivar el autocuidado; pero sí existen como proyectos de ley: el Proyecto de Ley de Protección de Datos establece obligaciones concretas y transversales de implementación de medidas de seguridad y notificación de brechas; y el proyecto de Ley Marco de Ciberseguridad e Infraestructura Crítica organiza administrativamente el esqueleto institucional de la ciberseguridad y provee a la continuidad operacional de áreas esenciales de la economía.



Paulina Silva

Abogada Universidad de Chile
LLM University of Melbourne
Socia, Bitlaw

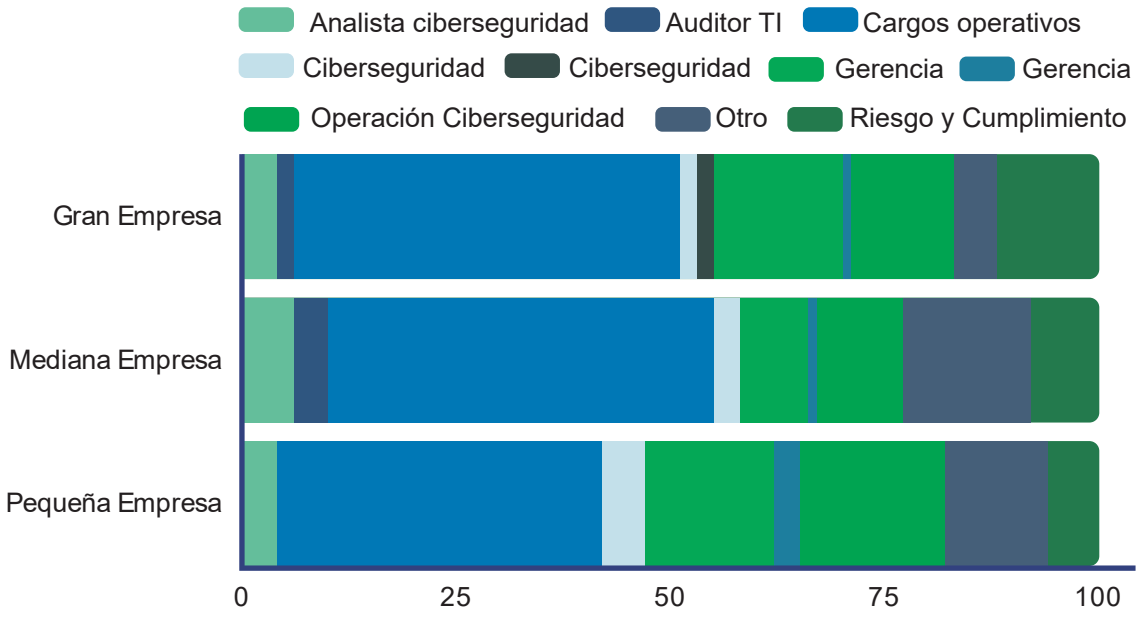
ANÁLISIS DEMOGRÁFICO: **TAMAÑO DE EMPRESA**

Distribución de cargos

Se realizó este mismo análisis, esta vez analizando como el tamaño de la empresa influye en su composición. Sin embargo, la información no varía de manera substancial entre cada categoría.

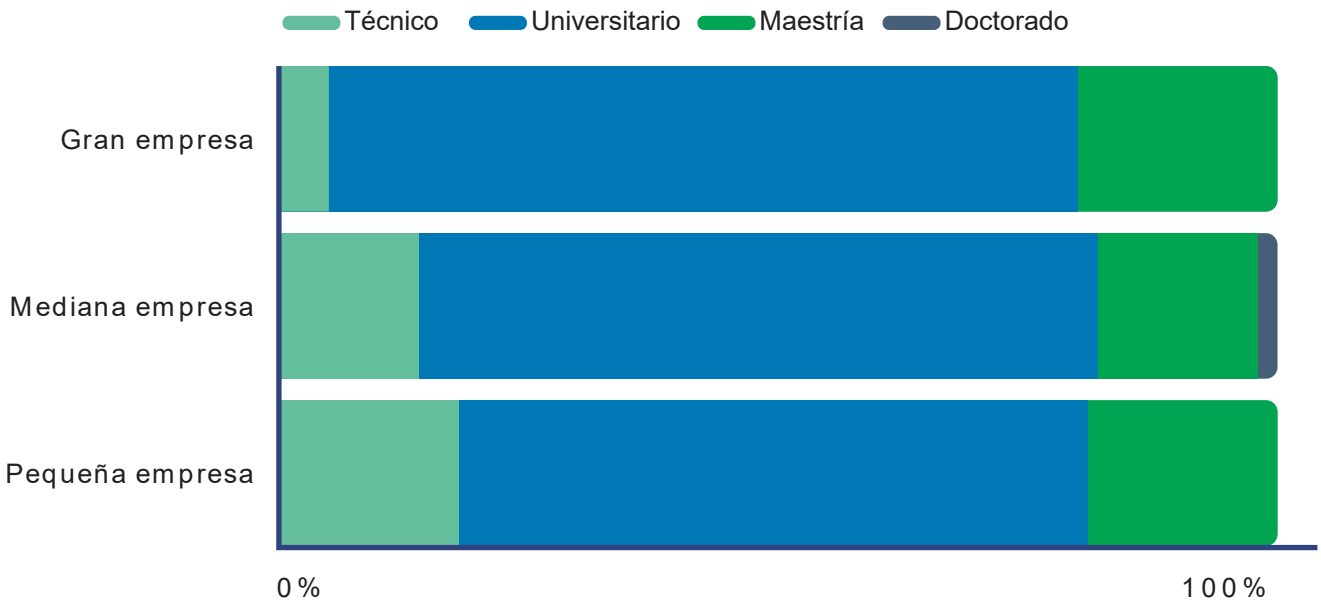
Con respecto a la presencia de cargos, nuevamente operación ciberseguridad es el cargo que tiene mayor presencia entre las distintas categorías. A diferencia del análisis previo, no se observa una falta de cargos a medida que se pasa de empresas pequeñas a otras más grandes.

Destaca sí la disminución gradual de la cantidad de cargos de Ciberseguridad Ofensiva a medida que el tamaño de la empresa aumenta; así como un aumento en cargos de Gestión de Ciberseguridad; y un mayor foco en cargos de Gerencia de Ciberseguridad en empresas grandes comparadas a las más pequeñas.



DISTRIBUCIÓN ACADÉMICA

En términos de nivel educacional existe una interesante mezcla de personal con grados doctorales y otros sin estudios universitarios en microempresas. Sin embargo, incluso en éstas se observa una predominancia de profesionales con estudios de pregrado.



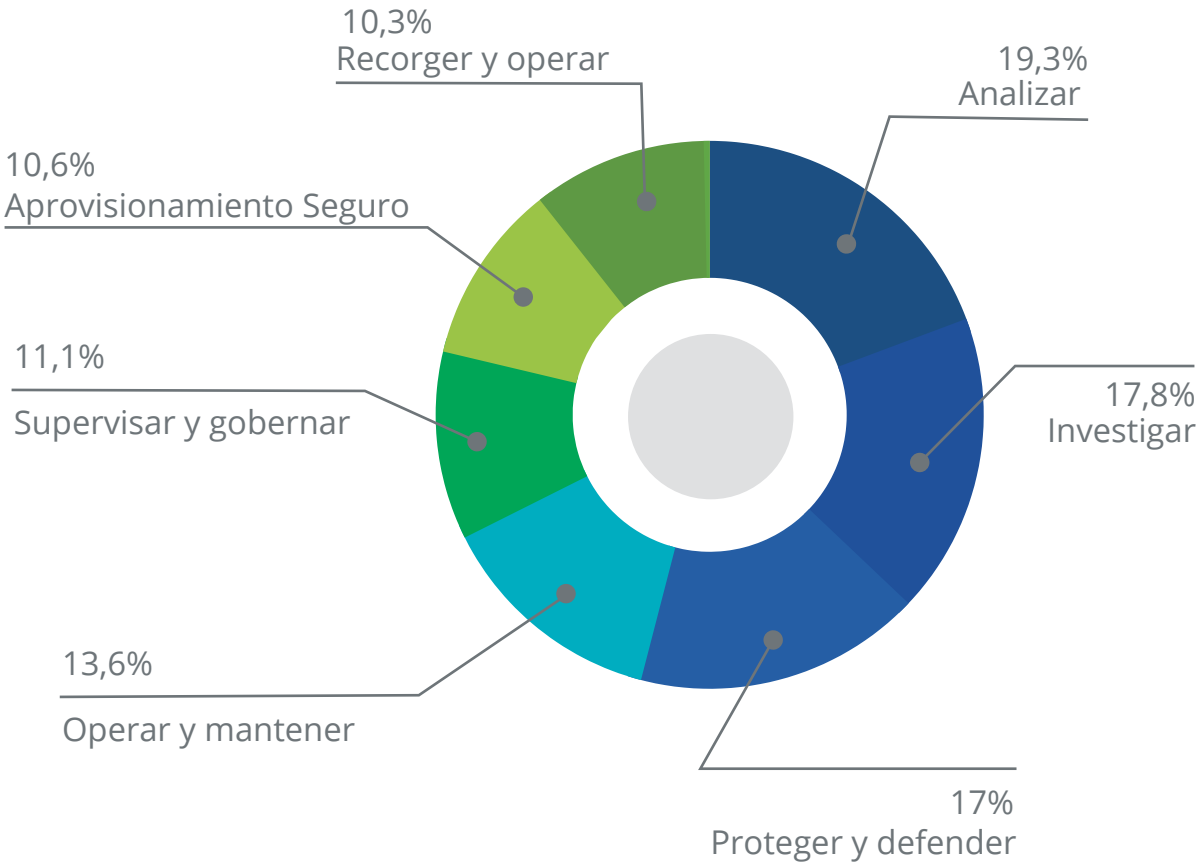
Conocimientos Estandarizados

GRUPO IT-TALENT® | ALIGNMENT | DIPLOMADO CIBERSEGURIDAD
CAPACITACIÓN USACH - UNIVERSIDAD DE SANTIAGO DE CHILE



CONOCIMIENTOS ESTANDARIZADOS

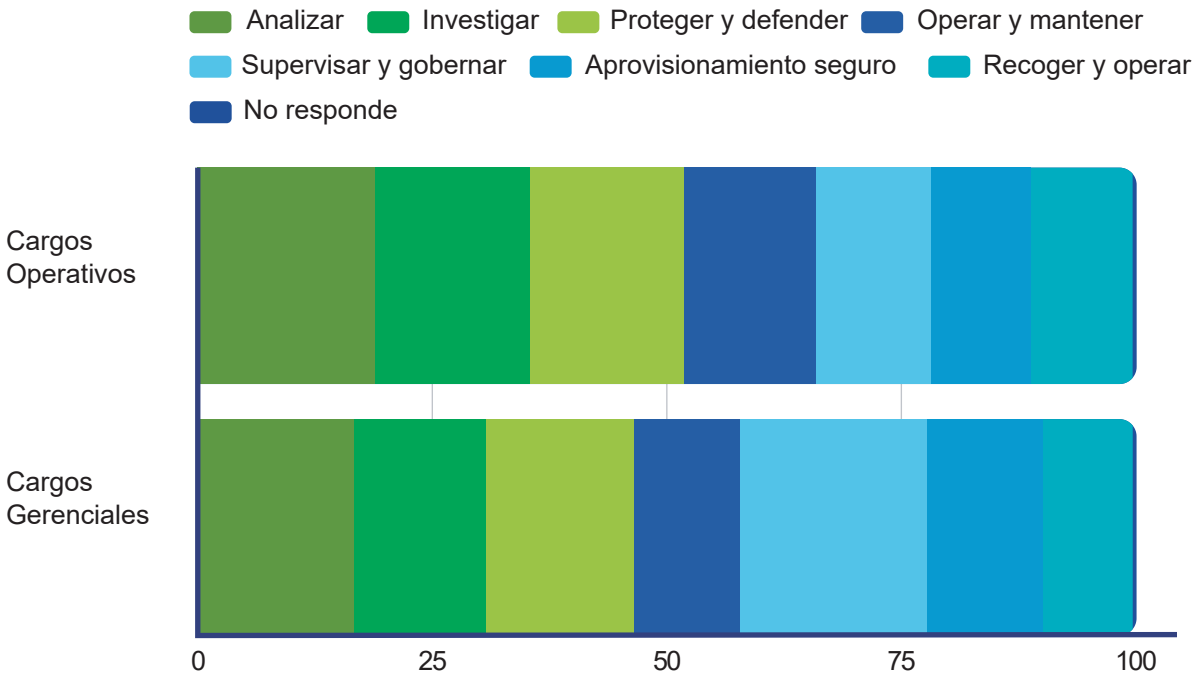
En este segmento se observa que aquellas empresas que invierten menos en ciberseguridad son aquellas que tienen una fuerza laboral de mayor edad. Mientras, aquellas como las de servicios de ciberseguridad tienen una mayor cantidad de empleados jóvenes. Esto es importante dado que en áreas que mantienen un estado de avance constante, mantener una base de trabajadores jóvenes permite mantener un nivel de conocimientos actualizados. Asimismo, permite contar con propuestas innovadoras, que mejoran las prácticas de ciberseguridad.



Esto indica que existe un mal perfilamiento de las funciones que debe cumplir cada cargo, ya que el estándar internacional indica que los distintos cargos se desempeñan a través de conocimientos estandarizados individuales, y no debería existir una representación tan pareja de ellos.

También se realizó una partición tomando en cuenta la cantidad de certificaciones y el grado académico. Sin embargo, estos también muestran una homogeneidad entre las categorías dadas.

Esto es evidencia de una mala caracterización en los cargos laborales, lo que implica una serie de dificultades para los profesionales de áreas de ciberseguridad. Esto porque requieren niveles de formación generalizada en vez de existir una situación que favorezca la especialización. Según la estandarización realizada por el NICSS considera que cada rol laboral cae dentro de una de las categorías mostradas.



CAMBIOS Y MEJORAS

De manera natural, las áreas de la ciberseguridad se han desarrollado con el paso de los años. Con esto ha aparecido el inevitable problema de la manera en la que se definen las crecientes habilidades y conocimientos requeridos para aquellos cargos que han ido especializándose más y más con el paso del tiempo.

Esto se ha reflejado en formas ineficientes, tanto en el reclutamiento de la fuerza laboral para las distintas empresas, así como también en el entendimiento de cuáles son las necesidades que solicitan los proyectos relacionados a ciberseguridad.



El síntoma más evidente de esto es el tema de las ofertas laborales publicadas en distintas plataformas, que han sido consistentes en no detallar las funciones de los cargos, y confundir a los solicitantes entre aquello que se les promete y aquello que últimamente se les solicita.

Este problema no solo afecta a los trabajadores, sino que además impacta directamente en cómo las empresas responden a la evolución de las tecnologías y los requerimientos de TI y ciberseguridad.



Haridas Umpierrez

Investigador – Científico de Datos en Alignment SpA -Académico Capacitación USACH – Universidad de Santiago de Chile

RENTAS



RENTAS

Las grandes empresas otorgan en promedio los sueldos más altos, sin que existan diferencias significativas entre los diferentes rubros de acuerdo al tamaño.

En cargos gerenciales, de riesgos y auditoría la mediana empresa presenta sueldos superiores a las grandes, lo cual se explica por una mayor cantidad de funciones realizadas en este tipo de organizaciones.

En cargos como de analista y operación ciberseguridad se percibe que las microempresas otorgan sueldos promedios similares en grandes empresas y microempresas, siendo esto menores en PYMEs.

En términos del efecto que las certificaciones tienen sobre el salario, se observa un claro aumento al adquirir más certificaciones de manera transversal.

Tabla mediana de salario por cantidad de certificaciones:

Cargo estandarizado	0	1 o 2	3 o más
Riesgo y cumplimiento	$2.563	$3.269	$3.329
Operación ciberseguridad	$1.484	$2.200	$2.216
Gerencia	$3.808	$4.054	$4.706
Auditor TI		$2.250	$2.500
Salario promedio	$2.618	$2.943	$3.187

Las rentas indicadas están expresadas en dólares y son después de impuestos y/0 descuentos legales. No incluyen bonos.

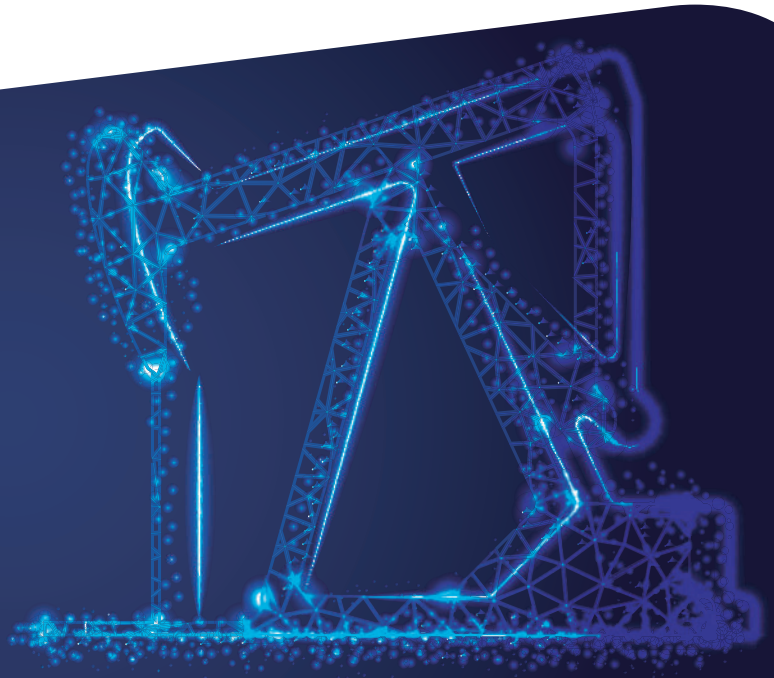
Tabla mediana de salario por empresa según cantidad de trabajadores:

Cargo estandarizado	Pequeña Empresa	Mediana Empresa	Gran Empresa
Analista de ciberseguridad	$1.250	$1.583	$1.750
Auditor TI		$2.625	$2.250
Gerencia	$3.864	$5.000	$4.221
Operación ciberseguridad	$1.872	$1.852	$2.398
Riesgo y Cumplimiento	$3.417	$3.375	$3.181
Salario Promedio	$2.369	$2.358	$2.779

Tabla de salario por rubro de empresa:

Cargo estandarizado	Comercial	Financieras	Industrial	Servicios	Servicios de Ciberseguridad
Gerencia	$3.918	$4.563	$5.200	$3.200	$5.133
Riesgo y Cumplimiento	$2.750	$3.958	$3.125	$3.071	$2.536
Operación ciberseguridad	$2.000	$2.785	$2.221	$2.116	$2.048
Analista de ciberseguridad		$1.583	$1.750	$2.464	$1.583
Salario Promedio	$2.426	$2.229	$2.229	$2.305	$2.603

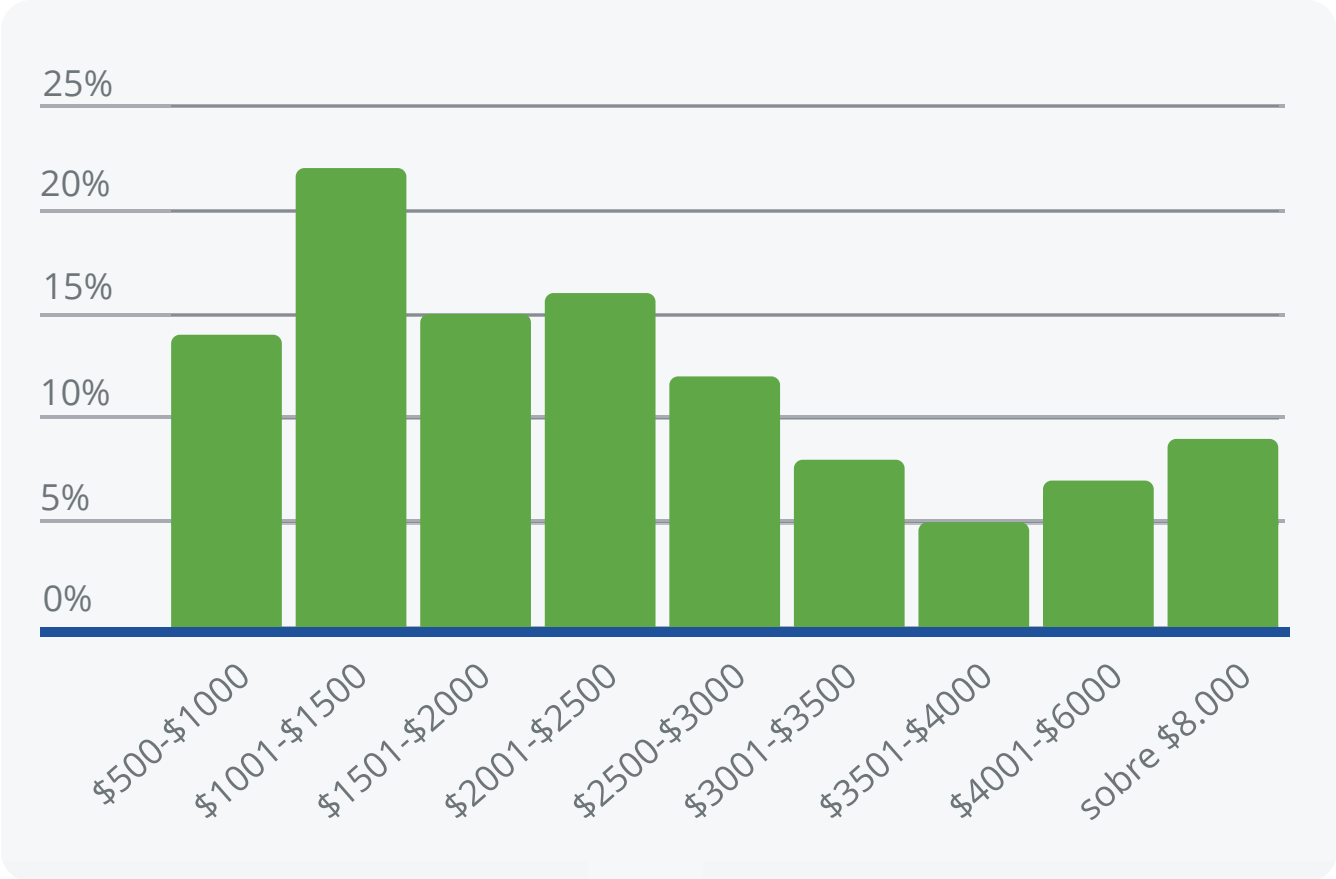
El sector industrial ha experimentado importantes avances en los salarios dadas las necesidades de continuidad y mayores regulaciones en el sector, sobre todo en los relacionados a Infraestructura Crítica.



SALARIOS SEGÚN CARGOS

En la encuesta se preguntó por el rango de salarios de $500 dólares, partiendo en $500 dólares y terminando en más de $8.000. Primero, en cuanto a la distribución sin filtrar de la renta de cargos de ciberseguridad, se observa una carga hacia los salarios más bajos con la mayor cantidad concentrada entre los $1.001 y los $1.500 dólares, que luego ve un descenso a medida que aumentan los salarios.

Asimismo, se da cuenta que existe una importante cantidad de trabajadores que ganan hasta $3.500 dólares mensuales. Además, la media de salario está en $2.376 dólares con una desviación de $1.616 dólares.



$2.376USD
Renta Promedio

$1.616USD
Desviación estándar de la renta.

Esta distribución cambia cuando se agrupa por cargos. En aquellos definidos como operativos, se observa que la distribución presenta mejoras en términos de cuáles son los rangos en donde se agrupa la mayor cantidad de empleados. Estos fluctúan entre los $1.501 y los $2.000 dólares, teniendo una concentración de ingresos superior en comparación a los ingresos generales.

Sin embargo, se ve una baja sustancial de salarios por encima de los $3.000 dólares en este tipo de cargos, los cuales son los más numerosos. En términos de renta promedio, se nota una leve baja con respecto a la renta promedio general, pero también mucha mayor certeza, con una desviación aún menor que en el análisis general, teniendo en el espectro más bajo de renta un valor mayor que en análisis de la distribución general.

$2.231USD
Renta Promedio

$1.394USD
Desviación estándar de la renta.

Los cargos de Manager de Ciberseguridad y DevSecOps son los de mayores salarios (US $4.230 aproximadamente)*.

*Benchmark Profesionales TI Latam 2021 de IT-Talent

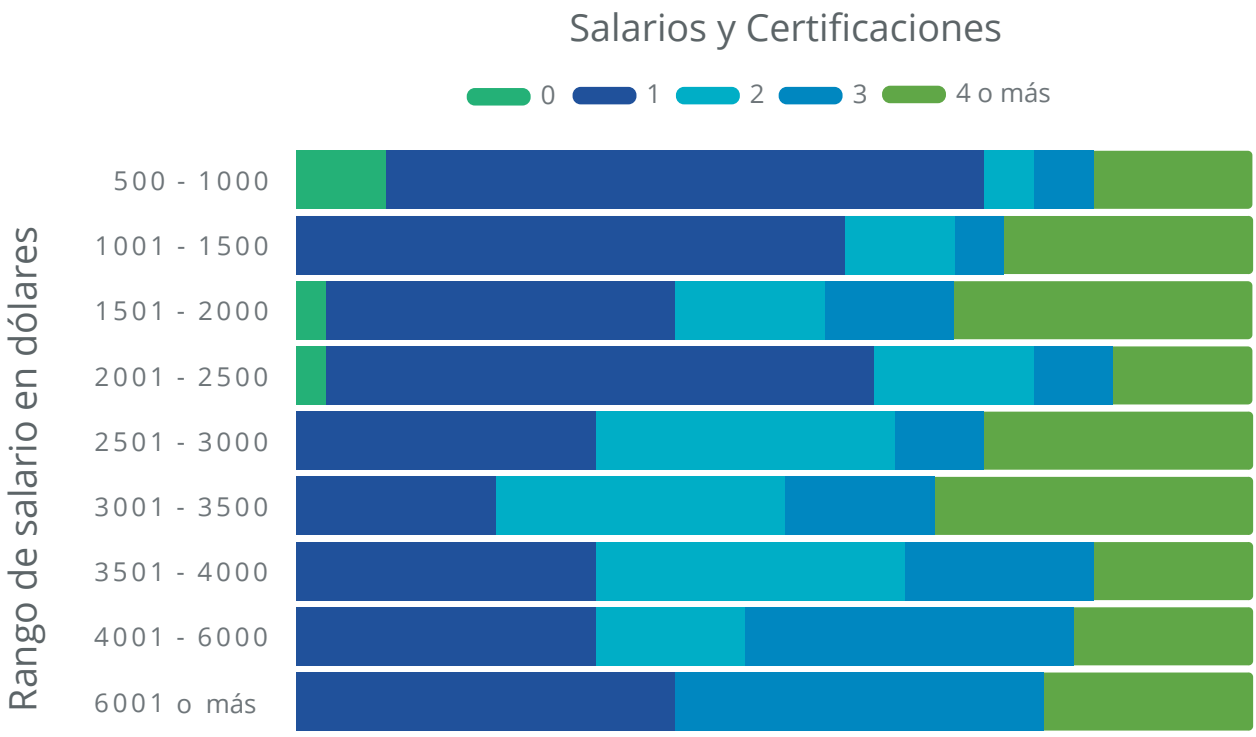
SALARIO SEGÚN EMPRESAS

En el sector financiero se concentra una mayor cantidad de personal con salarios altos y los cargos de mayor renta corresponden a gerentes y oficiales.

Se observa cierta regularidad en empresas de servicios de ciberseguridad, con rentas que pueden bordear los $6.000 dólares.



SALARIOS Y CERTIFICACIONES



Al analizar la posesión de certificaciones se ve que existe una clara relación entre un aumento salarial a medida que se adquieren certificaciones, siendo los rangos salariales más bajos los que muestran mayor cantidad de empleados sin certificaciones o con una sola certificación.

Sin embargo, a medida que sube el rango salarial, se da cuenta de que la cantidad de empleados con más de dos certificaciones aumenta proporcionalmente al resto. Sobre todo entre los $3.500 y los $6.000 dólares se observa que más del 40% de los trabajadores de esos rangos poseen 3 o más certificaciones.Esto indica que existe una tendencia a tener un mejor sueldo a medida que se obtienen más certificaciones.



OPINIÓN

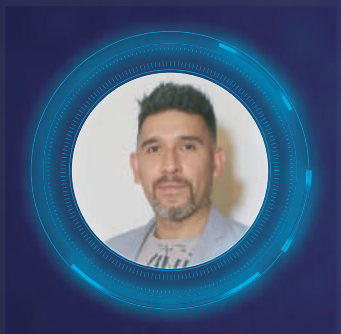
Muchos son los fenómenos que han posibilitado la necesidad de un aumento continuo de especialistas en materias de ciberseguridad, siendo algunos de los factores claves:

- Acelerada transformación digital de las organizaciones
- Aumento de ciberataques a nivel nunca vistos
- Mayor especialización de grupos criminales
- Nivel de especialización de especialistas
- Mayor efecto y visibilidad de los ciberataques
- Gran cantidad de regulaciones nacionales y sectoriales

Las empresas son cada vez más dependientes de sus tecnologías, por tanto la materialización de ciberataques genera efectos muy significativos en su operación, afectando el ámbito financiero, su reputación y también creando temas legales relacionados. La mayor especialización de grupos criminales, tanto en cantidad de ataques, técnicas, tácticas y procedimientos empleados, así como las capacidades tecnológicas, exige a las organizaciones una mayor especialización de la fuerza laboral en ciberseguridad, requiriendo elevar los niveles de capacitación y certificación en la materia, así como mayor inversión en infraestructura y servicios de ciberseguridad.

En prácticamente todos los países de la región se han impulsado iniciativas tendientes a fortalecer las capacidades de ciberseguridad, estableciendo a un nivel orgánico diversos tipos de instituciones (principalmente CSIRT), agendas de desarrollo de la ciberseguridad y principalmente la definición de regulaciones en torno a la protección de datos. Los avances son importantes, pero aún insuficientes, mientras que la cantidad de especialistas requerida es insuficiente.

La necesidad de especialistas es ahora, la ciberseguridad necesita de capital humano avanzado para abordar estos desafíos, siendo la transición de especialistas de diversas áreas de conocimiento a la ciberseguridad una materia clave para subsanar con la brecha existente.



Carlos Lobos de Medina

Académico y Director de Diplomados de Ciberseguridad
Capacitación USACH – Universidad de Santiago de Chile

FORMACIÓN ACADÉMICA

La proporción de grados de maestría crece a medida que se van moviendo a rangos de salario superiores, lo que refuerza la idea de que tener un grado más alto aumenta el prospecto de ganancia.

Doctorados

Los grados doctorales aparecen en el primer rango, luego en el cuarto y en los dos últimos, dando la impresión de que no son un buen indicador para el salario del trabajador.



Los grados técnicos suelen estar localizados en rangos de salario bajo los $2.500 dólares.

En cargos operativos el conocimiento **Analizar** es el más importante, por menos de un 2% sobre el siguiente, **Investigar.**

En los cargos de gerencia el conocimiento **Supervisar y Gobernar** es el más relevante, seguido muy de cerca por **Analizar.**



ANÁLISIS DE MOVILIDAD Y ESTABILIDAD LABORAL

Esta sección explora qué tan requeridos son los trabajadores dependiendo de distintas variables. Ellas incluyen género, edad, cargo, formación académica, y cantidad de certificaciones.

En cuanto a cantidad de ofertas recibidas por género, se observa que en términos relativos, no existe una diferencia significativa entre hombres y mujeres en tanto a la cantidad de ofertas laborales.

En lo que refiere a cargos, Gestión de ciberseguridad, Operación Ciberseguridad y Riesgo y Cumplimiento parecen tener una demanda más moderada, teniendo prevalencia el conjunto de trabajadores que han recibido hasta 4 ofertas laborales, con una baja proporción de quienes no han recibido ofertas.

Oportunidades

Entre los trabajadores que tienen una cantidad mayor de ofertas, los datos indican un aumento en cantidad a medida que aumenta la edad, siendo entre 41 a 50 años donde vemos que se da la mayor cantidad de ofertas.

Demanda

Los tres cargos que presentan mayor demanda son Ciberseguridad Ofensiva, Gerente TI y Auditor TI, los cuales presentan la mayor proporción de trabajadores con más de 7 ofertas recibidas. Los de menos demanda son Ciberseguridad defensiva, Gerencias de Ciberseguridad.

Por último, se consideró interesante saber cómo la cantidad de certificaciones afecta la cantidad de ofertas que se reciben. Se observa que a medida que se poseen más certificaciones, la proporción de trabajadores que no reciben ofertas laborales se reduce significativamente, comenzando con un 28.73% hasta llegar a solo un 3.13%.

Además, se ve que en los grupos con 2 o menos certificaciones, predominan los grupos de trabajadores que reciben 1 o 2 ofertas, con alrededor de un 39% en los tres grupos. En aquellos en los que se poseen 3 o 4 o más certificaciones, este segmento también se reduce, dando paso a una mayor demanda de trabajadores, viéndose en un aumento significativo de más de 3 ofertas. Esto hace evidente la ventaja competitiva que significa tener un mayor número de certificaciones.

Solo hay un 6.33% de desempleo en ciberseguridad, siendo un área bastante estable.

No se aprecian demasiadas diferencias entre rangos etarios o género.

Con respecto a formación y certificación, solo aquellos que poseen grados doctorales o cuatro o más certificaciones se encuentran en pleno empleo.



OPINIÓN

Tanto este estudio como las instancias que ocurren cada vez más no solo en el país, sino que más allá de las fronteras, creo que son necesarias todas las acciones posibles para que nuestras empresas, del tamaño que sean, logren cubrir la necesidad de recurso humano especializado en el resguardo de los bienes más preciados que una empresa posee: sus DATOS.

Es por eso que los profesionales relacionados a ellos deben estar en constante perfeccionamiento, conocimiento de las leyes y actualización de las mismas. En Chile aún existe carencia de esta toma de consciencia. Esto se da a todo nivel, desde el usuario base hasta el nivel de la gerencia.

En nuestro país la nueva ley de delitos informáticos obliga a plantear sistemas de especializaciones en ciberseguridad, pasando de los niveles de acceso más bajos de un sistema hasta los tomadores de decisiones.



Ello obliga a la búsqueda y preparación del recurso humano en cada uno de los niveles de la empresa. Hoy todos debemos ser responsables de estas acciones: el efecto de esta puesta en marcha no selecciona por género, por nivel académico o por alguna otra variable que se quiera agregar. Debemos educarnos y prepararnos pues es necesario potenciar la fuerza laboral en esta temática.

De acuerdo al movimiento que el mercado experimenta, cada vez son más y más las señales que nuestras empresas generan. Se requiere efectuar mejoras y cambios en todas las posibles instancias. Es necesario contar con mano de obra preparada y con espíritu de constante actualización.

Al mismo tiempo debemos educar a quienes ya forman parte de las empresas, y que en ellas se tome conocimiento de los procesos. Para este caso existen distintos framework que solicitan la capacitación y la sensibilización, que señalan lo que se debe contemplar. Por otro lado, si queremos aumentar el nivel de madurez se debe sumar concientización y capacitación. Según los expertos se debe dividir los equipos de trabajo, y hacer un levantamiento de cuáles son los perfiles con los cuales se cuenta y las habilidades que deben desarrollar.

Dado lo anterior hoy es necesario educar, capacitar y perfeccionar el recurso humano de nuestras empresas. Al mismo tiempo, al perfeccionarnos en esta área, los niveles de empleabilidad mejorarán a nivel país y, además, mejorarán las potencialidades de funcionarios ya vigentes en las empresas del país.



Lidia Herrera Mateluna

Directora Carrera Área Tecnologías de Información y Ciberseguridad - Telecomunicaciones Conectividad y Redes. INACAP Valparaíso

SELECCIÓN Y RETENCIÓN



Actualmente los profesionales TI son altamente cotizados en diferentes industrias. En los últimos 12 meses, más de un 40% de los profesionales TI* han cambiado de empleador. Además, 1 de cada 5 hoy gana más de un 20% que hace un año y un 72% está trabajando 100% remoto.

Considerando el mercado, desde IT-TALENT queremos entregar algunas recomendaciones para la contratación y hunting de estos talentos.

EL PERFIL CORRECTO

Es importante que definas correctamente qué perfil de profesional necesitas. En IT-Talent tenemos un equipo altamente capacitado para ayudarte a ajustar la búsqueda de la mejor manera.

EL DESAFÍO

Cuenta los hitos de la compañía y sus grandes aciertos en el mercado, en especial el desafío y la proyección tecnológica. Los buenos profesionales buscan saber esto.

BENEFICIOS

Una buena forma de diferenciarte y hacer que tu empresa sea más atractiva son los beneficios. Recuerda darlos a conocer desde el primer momento.

RESPONDE A TIEMPO

Muchos candidatos se bajan de los procesos cuando estos son muy extensos, por lo que es importante responder prontamente los resultados de las entrevistas.

RENTA

Contacta a nuestro equipo de investigación. Ellos constantemente realizan estudios y análisis de mercado para tener nociones con datos válidos sobre las rentas según el perfil y las tecnologías que requieras.

LA CARTA OFERTA

Éste es un documento sumamente importante y es necesario que contenga de forma clara los detalles, conversando entre ambas partes, lo que permitirá aclarar dudas.



*Fuente: Elaboración propia, IT-Talent Research.
Basado en encuestas digitales y entrevistas a candidatos durante los últimos 16 meses.

CONCLUSIONES

No es la primera vez que nos referimos a la escasez de profesionales TI y a la demanda cada vez más creciente de ellos en todas las áreas de la industria. En este estudio, donde abordamos el tema de la ciberseguridad, la situación se repite.

La creciente digitalización de personas y organizaciones requiere de una mayor fuerza laboral especializada y con conocimientos actualizados. La ciberseguridad es un tema que siempre debe ser primordial tanto para las grandes empresas, los bancos, el Estado como para la microempresa familiar.

En esta área que es crítica los profesionales necesitan estar al día con sus conocimientos. A la fecha del estudio más de la mitad cuenta con al menos una certificación. Sin embargo, mientras aumenta la cantidad de estas, y además la experiencia del profesional, los salarios suben de forma importante.

Los postgrados también son altamente demandados. Sin ir más lejos, poco más de un tercio de los cargos gerenciales están a cargo de profesionales con magíster. Quienes cuentan con un doctorado no solo se limitan a trabajar en corporaciones, sino que se desempeñan en empresas de tamaño pequeño y mediano también.

Los conocimientos sobre ciberseguridad forman parte de la mayoría de los curriculum académicos y de formación. Las opciones para capacitarse están disponibles. Las certificaciones entregan la posibilidad no solo de actualizar conocimiento sino también de hacerlo más específico, lo que resulta esencial para enfrentar las amenazas surgen a diario.

Desarrollo pero también auditoría, política y gestión de procesos son todas áreas que requieren de profesionales capacitados en ciberseguridad. Quien decida especializarse en este ámbito tendrá accesos a ofertas laborales cada vez más convenientes.

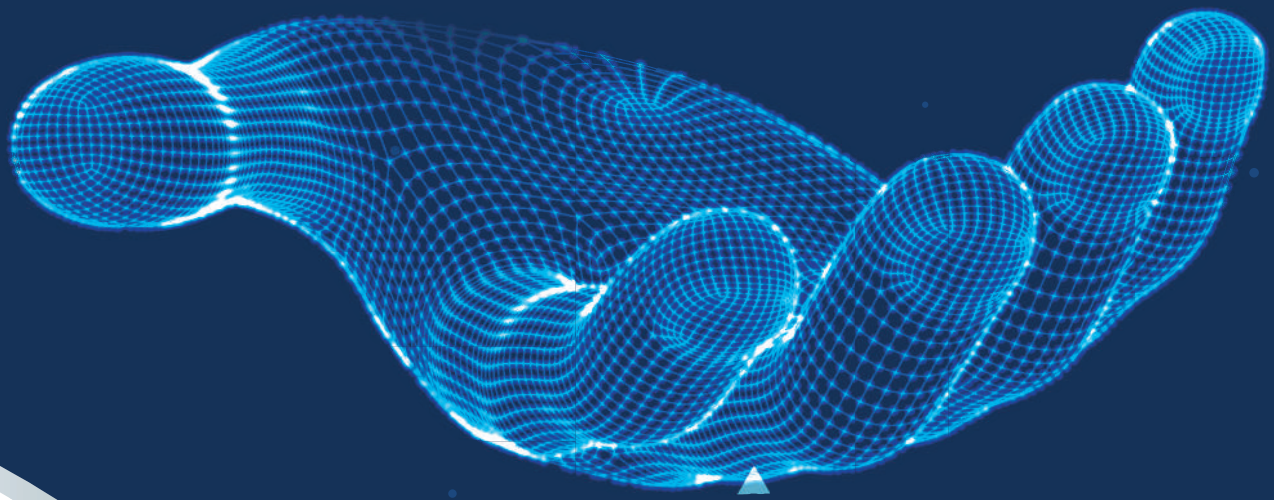
Por último, las capacitaciones de los profesionales pasan a ser clave para las empresas no solo por los conocimientos técnicos que se adquieren, sino también porque les permite acceder a certificaciones importantes dentro de la industria, como ISO.



Marco Muñoz

CEO Grupo IT-Talent Headhunter SENIOR IT

CONOCE NUESTROS SERVICIOS DE HEADHUNTER



Diseñamos una fórmula única para reclutar y contratar al profesional TI que tu empresa necesita.

GRUPO IT-TALENT®

www.it-talenthh.com

UNIVERSIDAD DE SANTIAGO DE CHILE

13 Diplomados y más de 60 cursos certificados



Metodología práctica, académicos certificados, pagos flexibles, respaldo de la Universidad de Santiago de Chile.

Contamos con la colaboración de:

HACKTHEBOX aws academy DevOps INSTITUTE

Reporte 2022 ciberseguridad

Diseñado por: IT-Talent Headhunter Senior TI - Mojito Marketing
Marco Muñoz, CEO IT-Talent
Ana Guajardo, Chief Marketing Officer
Paulina Bustos, Commercial Manager
Angelica Guzmán, Editora
Stephanie Rodrigues, Multimedia Designer

Con el apoyo de:
Haridas Umpierrez, Investigador, Científico de Datos en Alignment SpA,
Académico Capacitación USACH – Universidad de Santiago de Chile
USACH - Diplomado en Ciberseguridad

© 2022 IT-Talent Headhunter Senior TI

Copyright

Todos los derechos de esta publicación están reservados y no puede ser reproducida o transmitida, total ni parcialmente, de ninguna forma ni por ningún medio, electrónico o mecánico sin previa autorización de los autores. Cualquier uso no autorizado, compartido, reproducción o distribución quedan expresamente prohibidos.

Este informe NO INCLUYE ningún derecho de reventa.

Aviso Legal

Si bien se ha intentado verificar la información proporcionada en esta publicación, ni el autor ni la casa editorial asumen responsabilidad alguna por los errores, omisiones o información contradictoria que pudiese contener el documento.
El presente documento no debe interpretarse como un asesoramiento legal, ni de inversión o contabilidad. 2022

2022

REPORTE
CIBERSEGURIDAD

GRUPO IT-TALENT®

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT