ekojobs

EKOPARTY

INFORME EKO ENCUESTA 2023

ESTUDIO DEL MERCADO LABORAL EN CIBERSEGURIDAD PARA AMÉRICA LATINA

ÍNDICE

1. INTRODUCCIÓN

En Ekoparty, estamos motivados por la oportunidad de generar más oportunidades laborales en ciberseguridad para los talentos de América Latina. Para enfocar este propósito, hemos creado Ekojobs, un espacio diseñado para conectar a la comunidad con oportunidades laborales en esta industria, facilitando tanto el desarrollo profesional de los individuos como la identificación de talentos por parte de las organizaciones.

Con este objetivo en mente, decidimos impulsar este estudio. Reconocemos la enorme necesidad de desarrollar talento en ciberseguridad a nivel global. **Según el informe más reciente y especializado del mercado laboral de ISC2 de 2023, existe una brecha de más de 4 millones de profesionales de ciberseguridad que las organizaciones necesitan para defender adecuadamente sus activos críticos.**

Esta información nos proporciona una perspectiva y un panorama global que requieren acciones y esfuerzos conjuntos para abordar este gran desafío. A partir de este estudio, observamos que en el análisis del mercado laboral de Latinoamérica, solo se han considerado los países de Brasil y México, que se destacan como ejemplos en este sector, pero no representan la realidad y necesidades del resto de la región.

Esto reforzó nuestra intención de comprender el campo laboral en la región e integrar las perspectivas de los profesionales y organizaciones. La falta de información impacta tanto a los profesionales, que desean aplicar a un puesto y no encuentran referencias confiables para comparar pretensiones salariales, beneficios, descripción de tareas, tipo de contratación y demás variables vitales para entender el valor de sus conocimientos y experiencia dentro de la industria, como a las organizaciones, que enfrentan dificultades no sólo para encontrar talentos, sino también para entender el alcance y las necesidades de los equipos profesionales dedicados a la ciberseguridad.

Esperamos que este estudio, construido colectivamente, beneficie a todos, proporcionando información valiosa que permita entender mejor las necesidades y motivaciones de cada parte, y así generar más y mejores oportunidades laborales para esta industria en pleno desarrollo.

2. INSIGHTS

De la investigación realizada con los profesionales de ciberseguridad, podemos destacar los siguientes puntos que desarrollaremos en el informe:

- 44% posee una segunda ocupación relacionada con ciberseguridad (CS)
- 70% desarrolló su conocimiento en CS fuera de la educación formal
- El atributo más valorado de un trabajo es "Posibilidad de desarrollo profesional"
- 53% no posee certificaciones
- 79% trabaja en relación de dependencia (por cuenta ajena)
- El mal clima de trabajo es el motivo más mencionado para decidir un cambio. La baja remuneración, el segundo
- El atributo que más valoran de una organización es "Que se preocupe por el bienestar integral"
- Al momento de evaluar una oferta de empleo los dos ítems más observados son: Que el trabajo resulte interesante y enriquecedor y que el paquete de compensación resulte atractivo
- 50% visualiza su trabajo ideal en una organización del sector privado
- 49% imagina su trabajo ideal en una empresa de base tecnológica
- 44% poseen estudios universitarios completos. 82% en ciencias duras.
- 88% considera que su trabajo está relacionado con CS. 61% se considera especialista en CS.
- 35% posee menos de tres años de experiencia laboral en CS
- Las áreas de especialización con mayor prevalencia son: Gestión de Ciberseguridad / CISO y Respuesta a Incidentes / SOC / Blue Team

3. TRABAJO

El enfoque laboral de los especialistas en ciberseguridad en América Latina es notablemente diverso, reflejando una amalgama de habilidades técnicas especializadas y una visión estratégica de la seguridad digital. Aunque esta comunidad de profesionales se destaca por su experiencia técnica en áreas como la seguridad ofensiva, la detección de amenazas, la gestión de incidentes y la ciber inteligencia, también comparten similitudes sorprendentes en cuanto a sus perspectivas laborales y expectativas.

A pesar de la alta especialización requerida en sus roles, los profesionales de ciberseguridad comparten, en muchos casos, expectativas laborales que se alinean con tendencias observadas en estudios más amplios y en diferentes contextos geográficos. **La búsqueda de un equilibrio entre la vida laboral y personal, la aspiración de un entorno laboral colaborativo y la necesidad de oportunidades continuas de aprendizaje y desarrollo profesional son preocupaciones comunes que trascienden las fronteras de la ciberseguridad y se entrelazan con las expectativas laborales generales.**

En este contexto, resulta interesante observar cómo estos profesionales altamente especializados no solo buscan la excelencia técnica en sus campos, sino también un ambiente de trabajo que fomente la creatividad, la innovación y el desarrollo personal. Esta convergencia de expectativas sugiere no sólo la madurez creciente del campo de la ciberseguridad en la región, sino también la importancia que los profesionales asignan a la calidad de vida laboral y al continuo enriquecimiento de sus habilidades.

En última instancia, aunque la ciberseguridad exige un nivel excepcional de experiencia y dedicación, los especialistas en la región no son ajenos a las dinámicas laborales generales, y su visión del futuro refleja un deseo colectivo de construir carreras significativas y equilibradas en un campo en constante evolución.

A. ¿QUÉ HACEN?

De acuerdo a nuestro estudio, el 79% de los especialistas en ciberseguridad se encuentran actualmente empleados bajo relación de dependencia, desafiando una creencia popular que sugeriría una preferencia hacia el trabajo freelance o por cuenta propia dentro de esta población. Este dato cobra especial relevancia al considerar que, históricamente, se ha asociado a los profesionales de la ciberseguridad con roles más independientes. Esta percepción podría deberse a un cambio en la dinámica del mercado laboral o a una mayor valoración de la estabilidad asociada con la relación de dependencia.

Las responsabilidades vinculadas con los puestos de trabajo en relación de dependencia muestran un cambio notorio en su alcance geográfico. **Actualmente, el 63% de estos profesionales que participaron del estudio se dedican principalmente a tareas de ciberseguridad a nivel local, marcando una reducción significativa en comparación con una estimación del 90% que surge de estudios sobre puestos globales y regionales registrada hace 10 años**. Este cambio podría reflejar una evolución en la naturaleza del trabajo en ciberseguridad hacia un enfoque más globalizado.

El 88% de los encuestados considera que su trabajo está vinculado a la ciberseguridad y el 61% se autodefine como especialista en el campo. Este dato resaltaría la creciente especialización en temas específicos de ciberseguridad en comparación con unos años atrás, cuando las responsabilidades relacionadas con la ciberseguridad estaban integradas en roles más genéricos de tecnología. **Actualmente, los roles de especialización más destacados incluyen Gestión de Ciberseguridad / CISO, Respuesta a Incidentes / SOC / Blue Team, y Arquitectura de Ciberseguridad / Cloud Security / Seguridad en Infraestructura.**

Al examinar la distribución de años de experiencia laboral, observamos que **el 35% de los profesionales tiene menos de 3 años de experiencia en ciberseguridad, mientras que el 27% cuenta con más de 7 años de experiencia**. Esto podría indicar que en el campo de la ciberseguridad, derivada durante la última década de la seguridad informática y la seguridad de la información, el rol y el área dentro de las organizaciones es aún jóven y va ganando creciente relevancia.

Un aspecto notable es **la brecha de género en el ingreso al mercado laboral formal en ciberseguridad, ya que las mujeres parecen ingresar entre 7 y 10 años después que los hombres**. Este hallazgo destaca la necesidad de abordar las barreras de entrada y promover la diversidad de género en el campo.

Además, **el 44% de los especialistas en ciberseguridad que respondieron desempeñan una segunda ocupación relacionada con la ciberseguridad, mayormente vinculada a actividades como investigación (research), docencia y participación en programas de bug bounty**. Este dato subraya la alta demanda de conocimientos y habilidades en el mercado laboral formal, extendiéndose a otros ámbitos profesionales. La participación en áreas como la investigación y la enseñanza no solo refuerza la expertise del profesional, sino que también contribuye al desarrollo y la difusión del conocimiento en el campo de la ciberseguridad. Es esencial prestar especial atención a esta dualidad ocupacional, ya que evidencia la versatilidad y la aplicabilidad de las habilidades en ciberseguridad en diversas industrias y sectores, consolidando así la posición estratégica de estos expertos en el panorama laboral actual.

B. ¿QUÉ BUSCAN?

Los especialistas en ciberseguridad que participaron del estudio respondieron que visualizan su empleo ideal en diversos entornos laborales, siendo las organizaciones privadas la preferencia para el 50% de ellos, seguido de un emprendimiento propio con un 22%, y empresas u organismos públicos con un 20%. Otros profesionales imaginan su contribución en sectores menos convencionales, como Organizaciones No Gubernamentales (ONGs). Al considerar el sector de actividad, **el 49% de estos profesionales concibe su empleo ideal en organizaciones con base tecnológica. El restante 51% distribuye sus preferencias en sectores como Bancos y Entidades Financieras (10%), Empresas u Organismos Públicos (7%), y Organismos de Defensa y Seguridad (5%)**.

Cuando los especialistas en ciberseguridad ponderan las cualidades de su organización laboral ideal, priorizan cinco atributos clave:

1. Buscan un entorno que se preocupe por su bienestar integral (16%)
2. Que les brinde flexibilidad para optar por su propio esquema de trabajo (presencial, teletrabajo o mixto) (15%)
3. Que valore la trayectoria profesional y el conocimiento individual (15%)
4. Que proporcione seguridad y estabilidad en el empleo (14%)
5. Donde prevalezca una cultura de trabajo colaborativa (12%)

Al consultar sobre los atributos fundamentales que deberían caracterizar su trabajo ideal, los especialistas destacan tres elementos principales:

1. La posibilidad de desarrollo profesional (20%)
2. Un equilibrio adecuado entre la vida personal y laboral (19%)
3. La presencia de objetivos de trabajo desafiantes e interesantes (15%)

Cuando reflexionan sobre los **motivos que podrían llevarlos a cambiar de empleo, surgen consideraciones clave, como un mal ambiente de trabajo (23%), no estar satisfechos con la paga y beneficios (19%), y sentir desequilibrio entre la vida personal y laboral (12%).** Este contraste entre lo que desean en un trabajo ideal y las cosas que podrían hacerlos considerar un cambio muestra lo mucho que valoran los profesionales un buen ambiente y condiciones de trabajo.

Finalmente, al evaluar una oferta de trabajo, los especialistas en ciberseguridad ponen énfasis en ciertos aspectos:

- Buscan trabajos que les resulten interesantes y desafiantes (25%)
- Paquetes de compensación atractivos (19%)
- La posibilidad de elegir cómo quieren trabajar (ya sea en la oficina, desde casa o mixto) (17%)
- Sentir que son valorados y respetados durante todo el proceso de selección (9%)

Este análisis destaca la importancia de que las ofertas de trabajo se alineen con lo que buscan estos profesionales en el competitivo mundo de la ciberseguridad.

4. LOS INGRESOS ECONÓMICOS

Cuando indagamos sobre los ingresos económicos de los profesionales en ciberseguridad, es clave tener en cuenta la diversidad de esta población, compuesta por individuos de diferentes países y contextos económicos. Esta diversidad podría generar distorsiones al comparar los ingresos pero, a pesar de ello, hemos identificado algunas tendencias y parámetros generales que ofrecen hallazgos valiosos.

En primer lugar, observamos una **marcada diferencia en los ingresos entre los profesionales que trabajan de manera independiente, con ingresos que oscilan entre 500 a 2000 dólares mensuales, y aquellos que están bajo relación de dependencia, con un rango de 1000 a 3000 dólares mensuales.**

Un punto destacado es la relación entre los ingresos de los profesionales en relación de dependencia y su experiencia en ciberseguridad. Los datos revelan un **crecimiento proporcional en la compensación salarial a medida que aumenta la experiencia en el campo de la ciberseguridad.** Esta tendencia se ilustra de la siguiente manera:

- Menos de 1 año de experiencia: 500 dólares
- Entre 1 y 3 años de experiencia: 500 a 1000 dólares
- Entre 3 y 5 años de experiencia: 1000 a 2000 dólares
- Entre 5 y 7 años de experiencia: 2000 a 4000 dólares

Este análisis sugiere que la experiencia laboral en ciberseguridad es un factor crucial para el crecimiento salarial, especialmente para aquellos que trabajan bajo relación de dependencia. La correlación entre la experiencia y la compensación destaca **la valoración de la especialización y el conocimiento acumulado en el campo, proporcionando una guía valiosa tanto para los profesionales como para los empleadores en la configuración de las estructuras salariales.**

El conjunto de empresas que participaron en este estudio se caracteriza por su heterogeneidad en términos de ubicación geográfica, sector industrial, tamaño estructural y alcance operativo. A pesar de estas diferencias, comparten una **visión estratégica unánime sobre la ciberseguridad y reconocen su importancia vital en**

el desarrollo de sus respectivos negocios. Todas las empresas contribuyeron con información detallada sobre sus prácticas salariales relacionadas con los puestos de ciberseguridad. Esta información nos brinda un parámetro general orientador respecto a los salarios que el mercado ofrece para roles específicos en ciberseguridad:

- Puestos de menor jerarquía organizacional: 1000 a 2000 dólares
- Puestos de mayor jerarquía organizacional: 4000 a 6000 dólares

Al consultar a este conjunto de empresas sobre sus **expectativas de crecimiento para la estructura de puestos de ciberseguridad específicos, se proyecta un aumento del 13% para el año 2024. Este dato resulta alentador para los profesionales de la ciberseguridad, ya que es casi diez veces superior a la estimación de crecimiento de empleos realizada por la Organización Internacional del Trabajo (OIT) para la región de América Latina**. Este contraste subraya la creciente demanda y valoración de los roles especializados en ciberseguridad en el mercado laboral actual, proporcionando un panorama prometedor para el talento en este campo.

5. RECOMENDACIONES PARA LAS ORGANIZACIONES

Los datos recopilados indican claramente que la competencia por el talento especializado en ciberseguridad se intensificará en el futuro. En consecuencia, **las organizaciones deberán esforzarse por lograr un posicionamiento específico orientado a este sector**. Dejar atrás las ofertas de empleo genéricas y adoptar un enfoque de propuesta de valor diseñado específicamente para atraer y fidelizar este tipo de talento se vuelve esencial. Este enfoque personalizado puede marcar la diferencia en un mercado laboral cada vez más competitivo.

Es innegable que el salario o la propuesta de compensación integral desempeña un papel crucial en la atracción y retención de talento en ciberseguridad, sin embargo, la diferenciación va más allá de una simple cifra. Dada la alta demanda de este talento especializado, las organizaciones compiten no sólo entre sí, sino también con la creciente preferencia de algunos profesionales de no comprometerse con

ninguna organización en particular. En este escenario, **el factor económico a menudo se sitúa en segundo plano** frente a consideraciones más amplias, como el bienestar general y la calidad del entorno laboral.

Más allá del salario competitivo, las organizaciones deben esforzarse por **construir un ambiente que valore y promueva el bienestar** de sus profesionales. Ofrecer beneficios que aborden las necesidades holísticas, como programas de salud mental, flexibilidad laboral y opciones de desarrollo personal, puede marcar la diferencia. Al crear un entorno donde los empleados se sientan valorados y respaldados, las organizaciones no solo atraen talento, sino que también fomentan un sentido de lealtad y compromiso a largo plazo.

En última instancia, el conocimiento y la posibilidad de desarrollo son aspectos altamente apreciados por la comunidad de ciberseguridad. Al destacar oportunidades tangibles para el aprendizaje continuo, la formación especializada y el crecimiento profesional, **las organizaciones pueden distinguirse como empleadores comprometidos con el avance y la excelencia en el campo**. Invertir en el desarrollo de habilidades y ofrecer una trayectoria clara de crecimiento no solo fortalece la posición de la organización en la competencia por el talento, sino que también contribuye al fortalecimiento del equipo y al éxito a largo plazo en un sector en constante evolución.

6. FORMACIÓN

Antes de entrar en detalles sobre cómo los participantes del estudio adquieren o construyen conocimiento, es importante resaltar que el **70% indicó que obtuvo su formación específica en ciberseguridad a través de medios informales, como cursos en línea (18%), experiencia laboral (17%) y laboratorios virtuales o entornos virtuales (16%).** Este dato sugiere que la educación formal institucionalizada tiene oportunidades concretas para adaptar o modificar programas de estudio que pueden no resultar completamente atractivos para la adquisición de estos conocimientos. Asimismo, las empresas tienen una excelente oportunidad de enriquecer su propuesta de valor para los empleados al considerar

de manera orgánica la adquisición de conocimientos concretos como parte de su oferta, considerando además, por este mismo estudio, que es uno de los puntos que más valoran los profesionales de ciberseguridad como principal atributo de un empleo ideal.

En cuanto a la educación formal universitaria, esta muestra una representación significativa en el estudio. De hecho, **un 44% de los encuestados posee un título universitario, y el 82% de estos están en disciplinas consideradas duras**, como ingeniería, matemáticas y tecnología. Esto refleja un alto nivel de especialización, posiblemente motivado por la búsqueda de mejores oportunidades laborales en el mercado formal.

Esta especialización se deduce como respuesta a las demandas del mercado laboral. Un dato relevante que las organizaciones proporcionan es que, además de las especializaciones más solicitadas mencionadas en el capítulo específico sobre empleo, también se requiere conocimiento en otras áreas, como pueden ser la Inteligencia de Ciberamenazas, la Investigación (Research), y la Educación en Ciberseguridad. Este dato puede ser de particular interés tanto para los proveedores de capacitación como para las personas que deseen adquirir habilidades técnicas sobre las que el mercado está poniendo su atención.

En el capítulo dedicado al trabajo, también se destaca que **el 44% de los participantes menciona desarrollar ocupaciones secundarias especializadas en ciberseguridad**. Se observa que estas ocupaciones suelen estar orientadas hacia la investigación, el desarrollo, y/o a compartir de conocimientos, como mencionamos anteriormente. Estos espacios podrían definirse como un punto de encuentro entre el mercado laboral, los entornos de formación y los profesionales de ciberseguridad, generando así oportunidades y beneficios para todos los involucrados.

Las certificaciones desempeñan un papel relevante en el mundo laboral, siendo requisitos técnicos y, en ocasiones, comerciales en una amplia variedad de proyectos. Sin embargo, la valoración de su utilidad como método de formación varía según el punto de vista de cada individuo consultado. De hecho, el **53% de los encuestados en este estudio posee al menos una certificación activa, y en su mayoría son personas empleadas formalmente. Entre las certificaciones más comunes se encuentran el CEH (Certified Ethical Hacker), que abarca un 19%,**

seguido por el OSCP (Offensive Security Certified Professional), Auditor ISO 27.001 (International Organization for Standardization), CISM (Certified Information Security Manager) y el CISSP (Certified Information Systems Security Professional).

7. DEMOGRAFÍA

- **Cantidad de Participantes**: 605
- **Género**: 81% varones 19% mujeres
- **Edad promedio**: 36 (37% tiene entre 30 y 40 años)
- **Lugar**: 82% reside en Latinoamérica Sur
- **Situación familiar**: 52% convive con su pareja / 62% no tienen hijos

8. CONCLUSIONES GENERALES

El primer estudio del mercado laboral en ciberseguridad para América Latina, realizado por Ekoparty, ofrece una visión profunda y detallada sobre las condiciones, expectativas y desafíos que enfrentan los profesionales en este campo. Este informe revela varias tendencias y puntos clave que son de particular importancia tanto para los talentos como para las organizaciones de la región.

En primer lugar, destaca la **alta capacidad autodidacta entre los profesionales de ciberseguridad**, con un significativo 70% que ha desarrollado sus habilidades fuera de la educación formal. Esto sugiere una urgente necesidad de adaptar y expandir las ofertas educativas formales para alinearse mejor con las demandas del mercado y las preferencias de los estudiantes.

Además, la estabilidad laboral y el desarrollo profesional son atributos altamente valorados por los especialistas en ciberseguridad. La mayoría trabaja en relación de dependencia, lo cual contradice la percepción popular de una preferencia por el

trabajo independiente en este sector. Esta tendencia podría reflejar un cambio en la dinámica del mercado laboral y una mayor valoración de la estabilidad.

Otro hallazgo relevante es la **disparidad de género en el ingreso al mercado laboral** formal, donde las mujeres ingresan entre 7 y 10 años después que los hombres. Esto subraya la necesidad de abordar las barreras de entrada y promover la diversidad de género en el campo.

En términos de expectativas laborales, los profesionales buscan entornos que promuevan su bienestar integral, flexibilidad en el esquema de trabajo, y una cultura colaborativa. Al evaluar ofertas de empleo, los factores decisivos incluyen trabajos interesantes y desafiantes, así como paquetes de compensación atractivos.

Por último, el estudio evidencia una correlación directa entre la experiencia en ciberseguridad y la compensación salarial, destacando la importancia de la especialización y el conocimiento acumulado en el campo. Las organizaciones, por su parte, deben adaptarse a estas realidades ofreciendo ambientes laborales que no solo sean económicamente competitivos, sino que también promuevan el desarrollo profesional y personal de sus empleados.

Este estudio, al ofrecer una visión comprensiva de la situación actual y las expectativas de los profesionales de ciberseguridad en América Latina, espera servir como una guía para mejorar las oportunidades laborales y fortalecer la industria en la región.

Descubrí más en: ekoparty.org/ekojobs / **ekojobs@ekoparty.org**