Uruguay Presidencia | agesic

Ecosistema de Ciberseguridad en Uruguay

Un análisis cualitativo

Seguridad de la Información
Versión 1.0
Junio, 2020

KPMG

Contenido

1. Sobre el estudio

El uso masivo de los servicios de Gobierno Digital en Uruguay, así como la implementación y uso de nuevas tecnologías (TIC), han permitido lograr mayor eficiencia, calidad y agilidad en diversos ámbitos. Ha influido tanto en el gobierno como en la economía, la industria, el agro, la salud, la educación y algunos de los sectores claves para el país que se encuentran atravesando una fuerte transformación digital. Esto podemos visualizarlo, a nivel global, en el informe Consumer Loss Barometer, en donde se señala la importancia de que la ciberseguridad logre equipararse con la agilidad de la organización digital, adaptándose para satisfacer las necesidades cambiantes de las partes interesadas y permitiendo así la transformación digital requerida (KPMG, 2019).

El crecimiento exponencial en TI en la última década ha sido y es un claro facilitador del negocio y una herramienta de desarrollo académico, permitiendo innovar en la relación entre el gobierno y la ciudadanía, entre otros dominios, manteniendo a Uruguay como referente en el uso de las TIC.

A medida que se desarrolla el uso de las TIC, tanto en lo relativo a la trasformación digital como en la universalización de su empleo, también lo hacen las amenazas en ciberseguridad en cuanto a su cantidad, su sofisticación y su impacto en diferentes niveles. En este sentido, el estudio de Allianz Risk Barometer, realizado en 86 países, identifica que el riesgo de incidentes de ciberseguridad se encuentra segundo en el Top 10 de riesgos empresariales (Allianz Global Corporate & Specialty 2019).

El papel de la ciberseguridad radica en permitir el adecuado logro de los objetivos de las organizaciones y, cada vez más, promover una ventaja competitiva. Debe agregar valor a una organización en lugar de obstaculizar su progreso. Esto requiere una cultura de ciberseguridad positiva y una inversión y gestión adecuada. Las organizaciones enfrentan desafíos persistentes en el reclutamiento de profesionales calificados en ciberseguridad capaces de proteger sus sistemas contra la amenaza de ciberataques.

Sin embargo, tanto a los sectores público y privado como a las instituciones educativas les está resultando difícil cubrir la necesidad de talento en ciberseguridad; es posible, en este sentido, evidenciar la brecha que hay entre los especialistas disponibles y los que realmente se necesitan en la materia.

Esta situación determina varios desafíos, no solo el mantenerse actualizado en cuanto al uso de las TIC, sino en desarrollar, especializar y mantener a su equipo de profesionales para hacer frente a estos desafíos. **El objetivo de este estudio es analizar la situación del mercado laboral relacionando los principales retos que enfrenta la industria local, fundamentalmente, en lo que respecta a la demanda de profesionales especializados, desarrollo y oferta académica.**

Este estudio fue elaborado por la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic) y KPMG, con colaboración de Datasec.

Para su realización, se definió un enfoque de trabajo basado en entrevistas a:

- Empresas nacionales de los sectores financiero, salud, tecnología y telecomunicaciones.
- Empresas proveedoras de servicios de ciberseguridad.
- Instituciones de educación.

Se trabajó con **40 empresas nacionales pertenecientes a los sectores financiero, de salud, de tecnología y de telecomunicaciones,** ya que ellos, en general, engloban organizaciones que identifican los riesgos provenientes de la ciberseguridad como relevantes para el negocio. En ese sentido, el estudio realizado por Harvey Hash y KPMG al indagar sobre la frecuencia de ataques mayores por industria concluye que en telecomunicaciones es del 44%, en salud del 33%, en servicios financieros del 33% y en tecnología del 26% (Elis y Bates, 2019).

En términos generales, se trata de sectores que utilizan y gestionan información sensible y además están atravesando procesos de transformación digital en donde los riesgos inherentes a la ciberseguridad deben ser gestionados.

Asimismo, estas empresas contratan servicios de ciberseguridad a empresas proveedoras especializadas; por lo tanto, en el contexto del trabajo se entrevistó a **16 empresas proveedoras de servicios de ciberseguridad** en el mercado local, cubriendo servicios de estrategia y gobernanza, ciberdefensa, ciber respuesta y transformación. Algunas de estas empresas brindan exclusivamente servicios de ciberseguridad y otras tiene una amplia oferta de servicios de consultoría.

Adicionalmente, se consideró relevante indagar sobre la oferta académica local, por lo que se ha entrevistado a universidades y centros educativos que brindan cursos, especializaciones y formación en ciberseguridad con el objetivo de conocer el tipo de formación disponible en la materia y su detalle, características del cuerpo docente y el abordaje de la investigación en ciberseguridad. En ese sentido, se entrevistó a **8 instituciones educativas** durante el estudio.

Por otra parte, cabe destacar que acorde al estudio de Harvey Hash y KPMG las 5 habilidades más escasas, a nivel mundial en ciberseguridad, actualmente son:

- Big Data y Analytics.
- Ciberseguridad.
- Inteligencia Artificial.
- Arquitectura Empresarial.
- Análisis de negocio.

(Ellis y Bates, 2019).

Esta escasez de profesionales y habilidades de ciberseguridad es algo que se ha mencionado en diferentes publicaciones, tales como:

- Estudio de Ciberseguridad de Deloitte-NASCIO, en donde se indica que, en Estados Unidos, al consultar sobre las barreras para abordar el desafío de la ciberseguridad, aparece como segunda barrera el inadecuado personal de ciberseguridad, detrás de falta de suficiente presupuesto y antes de que el aumento de la sofisticación de las amenazas (2018).
- Estudio de ISC Cybersecurity Workforce Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens, en donde se indica que el 51% de los profesionales de ciberseguridad dicen que la organización está en riesgo moderado o extremo debido a la escasez de personal de ciberseguridad. A su vez, detalla que la escasez de profesionales en ciberseguridad es cercana a los 3 millones a nivel mundial (2018).
- FinancesOnline estima que para 2021 habrá un total de 3,4 millones de empleos en seguridad cibernética vacantes (Chang, 2020).
- Según el Banco Interamericano de Desarrollo, Uruguay necesita 600 especialistas en ciberseguridad (BID, 2019).
- El Estudio de Consumer Loss Barometer 2019 de KPMG consulta sobre la veracidad de la guerra por talentos de ciberseguridad; un 51% de las encuestas responden que están de acuerdo sobre la existencia de esta. Adicionalmente, se comenta que la escasez de personal puede abordarse mediante una mayor automatización, crowdsourcing y el uso de contratistas calificados.

La gran mayoría de las organizaciones en nuestro país dependen de la tecnología digital para poder operar. Una buena ciberseguridad protege esa capacidad de funcionamiento y garantiza que las organizaciones puedan aprovechar las oportunidades que brinda la tecnología. Por lo tanto, la seguridad cibernética es fundamental para la capacidad de recuperación de una organización.

2. Hallazgos

2.1. No hay suficiente concientización de los riesgos asociados a la ciberseguridad.

Aún no se visualiza a la gestión de la ciberseguridad como parte de la estructura organizativa de las empresas nacionales. Las organizaciones suelen reaccionar luego de sufrir incidentes serios y, aun así, en su gran mayoría no incluyen a la ciberseguridad como un eslabón que integre su estructura.

Si bien la gestión de la ciberseguridad es un tema que debería estar presente en la agenda de todas las empresas nacionales, casi la mitad de las empresas que participaron de este estudio **(45%) no cuentan con un área específica que trabaje en ciberseguridad**. Sin embargo, no siempre esto indica que no cuenten con algún recurso que pueda apoyarlos en la temática, pero sí demuestra que aún no se ha incorporado estructuralmente en las organizaciones un área que cumpla dicha función.

Según el National Cyber Security Center de Reino Unido, existen dos razones por las que es tan importante integrar la ciberseguridad a los objetivos y riesgos de una organización. En primer lugar, la ciberseguridad impacta en todos los aspectos de una empresa. Por lo tanto, para gestionarla adecuadamente debe integrarse en la gestión de riesgos organizacionales y la toma de decisiones. En segundo lugar, la ciberseguridad debe integrarse para que tenga éxito. Su correcta gestión no implica solamente la implementación de tecnología; se trata de que las personas tengan una buena relación con la seguridad y tengan los procesos adecuados en toda la compañía para administrarla (2019).

Adicionalmente, es relevante analizar la temática presupuestal habiendo detectado que un 33% de las empresas entrevistadas ven como un desafío la **falta de presupuesto adecuado**. A su vez, hemos identificado que existen empresas que no tienen un presupuesto exclusivo de seguridad, siendo más favorable la situación en aquellas donde el área de seguridad no depende de TI. En relación con el presupuesto de ciberseguridad, ISC revela que la mayoría de las empresas participantes de su estudio perciben al presupuesto asignado a ciberseguridad como insuficiente, representando una de las preocupaciones principales en el área junto a la falta de habilidades y experiencia del personal de ciberseguridad (2018).

Asimismo, se debe considerar que las empresas tienden a desarrollar proyectos de transformación digital que buscan modificaciones en los modelos de negocio, por lo que deben hacer un uso más eficiente de sus presupuestos de forma de poder viabilizar estos proyectos, lo que podrá determinar que los responsables de seguridad deban optimizar costos. Además, se adicionan las presiones para reducir costos de cumplimiento, automatizar las funciones de seguridad y hacer uso de soluciones de seguridad.

Es una realidad la creciente brecha de habilidades y la necesidad de reclutar más talento como uno de los principales desafíos de nuestros días, pero también se debe evaluar que gran parte de los procesos repetitivos de seguridad e infraestructura, como parches, escaneo de vulnerabilidades, administración de configuración y revisión de firewall, podrían ceder ante la automatización, con especialistas que actúen con capacidad de supervisión. Las herramientas automatizadas podrían generar inteligencia sobre grupos de atacantes y malware para ayudar a los ataques dirigidos. La respuesta a incidentes podría convertirse en prevención de incidentes a través del monitoreo de ecosistemas basado en Big Data y la prevención detectiva y analítica de fraudes.

Sin embargo, cuando se omite la ciberseguridad dentro de la cadena de valor del negocio digital, no se lograr un ecosistema de confianza y se pierden oportunidades comerciales significativas, por lo que el manejo de presupuesto de ciberseguridad debe ser lo más eficiente posible considerando los temas de cumplimiento y de transformación.

2.2. La percepción de la ciberseguridad

Es de destacar que un **80% de las empresas entrevistadas** perciben que el **riesgo de la ciberseguridad puede ser catalogado en Alto o Medio**. Esta percepción es un buen inicio a la hora de mejorar la gestión de la ciberseguridad y, a su vez, se ve acompañada con una tendencia de mayor inversión por parte de las empresas.

En esta línea, acorde al estudio ISC Cybersecurity Workforce Study. Strategies for Building and Growing Strong Cybersecurity Teams, un 51% de los profesionales de ciberseguridad perciben a su organización como expuesta a un riesgo de ciberseguridad entre moderado y alto. Esto responde a diversos factores, tales como la falta de personal capacitado, de recursos y de presupuesto a invertir en iniciativas de ciberseguridad, así como de una terminología compartida que habilite la eficiente comunicación (2019).

Del mismo modo, en Uruguay actualmente la mayoría de las empresas no cuentan con áreas exclusivamente dedicadas a ciberseguridad, con un presupuesto adecuado a ser invertido en iniciativas de la materia, así como con profesionales suficientemente capacitados.

Por otra parte, las áreas de ciberseguridad más críticas son la concientización y el entrenamiento de la gobernanza y la gestión y análisis de riesgos.

Esta percepción sobre la ciberseguridad puede explicar que un 84% de los entrevistados perciben que el grado de dificultad al momento de convencer a la Alta Dirección de invertir en seguridad es fácil o algo difícil dentro de la escala: “muy difícil”, “algo difícil”, “fácil” y “muy fácil”.

Sin embargo, es relevante considerar lo señalado por el informe Consumer Loss Barometer, que revela que muchas empresas todavía consideran que la ciberseguridad y la respuesta a la violación son un problema de TI, en lugar de un problema comercial crítico que puede afectar las operaciones, la confianza del cliente y el crecimiento futuro. El mensaje clave para las organizaciones es claro: habilitar e integrar la ciberseguridad en todas las verticales de su negocio (KPMG, 2019).

A su vez, en su mayoría las empresas contratan servicios de ciberseguridad. Un 74% de las empresas entrevistadas suelen acudir a la contratación en la búsqueda de especializaciones y experiencia que no poseen. Se enfrentan a la carencia de recursos internos o visualizan la contratación de servicios de ciberseguridad como una alternativa más redituable que la contratación de recursos internos. Los servicios que más se contratan son hacking ético y análisis de vulnerabilidad, seguidos de monitoreo, gestión y respuesta de incidentes.

El sector financiero es el que más contrata servicios de ciberseguridad y denota un grado de madurez mayor que los otros sectores participantes del estudio.

El sector de la salud está empezando a contratar servicios de ciberseguridad, seguido por consumo masivo.

La contratación de servicios de ciberseguridad en algunos casos se ve acompañada por la falta de un área de seguridad formalmente establecida en las empresas o por el hecho de contar con capacidades limitadas dentro de las empresas.

Adicionalmente, considerando una serie de predicciones para el 2020 de David Ferbrache, Leadership, Global Head of Cyber Futures considera un aumento de la velocidad y escala de explotación de vulnerabilidades favorecido por problemas de configuración de servicios cloud, sitios web e internet de las cosas, entre otros. Además, se incrementa el uso de herramientas automatizadas para detectar y aprovechar vulnerabilidades (Security, 2019).

La percepción sobre la ciberseguridad no debe ser vista solo desde la óptica de las empresas, sino que debe ser analizada también sobre la óptica de los consumidores. La confianza que estos últimos tengan sobre la gestión de la seguridad que hacen las empresas puede determinar su grado de fidelización y participación en los servicios que dichas empresas ofrecen (Harán, 2019).

Citando nuevamente el informe de Consumer Loss Barometer, podemos observar que un 48% de los consumidores creen que sus instituciones financieras tienen la responsabilidad total o compartida de garantizar que los dispositivos móviles utilizados para la banca sean seguros y estas instituciones deben demostrar que toman en serio la seguridad de la información personal de sus clientes. Si esto se analiza a la luz del comercio minorista, un 71% de los consumidores están más preocupados por el uso indebido de su información personal por parte de los minoristas que por la información que pueden tomar los hackers (68%) (KPMG, 2019).

2.3. Fuerza laboral especializada en ciberseguridad

El 27,5% de las empresas participantes no tienen un recurso especializado en seguridad y un 12,5% tiene algún recurso que trabaja en forma parcial. En relación con las empresas que cuentan al menos con un especialista en ciberseguridad, un 76% tiene entre 1 y 3 y un 60 % tiene al menos un recurso asignado. Estas compañías que al menos cuentan con un recurso en ciberseguridad se corresponden, en su mayoría, con empresas del sector financiero y con organizaciones multinacionales.

A su vez, a nivel local El Observador destaca la falta de profesionales en ciberseguridad como una problemática clave en nuestro país, estimando que en Uruguay existen 650 profesionales de ciberseguridad, extendiéndose la brecha con la necesidad de duplicar dicha cifra en los próximos dos años (2019).

Las cualificaciones más importantes al momento de cubrir una vacante son experiencia relevante y conocimiento avanzado. Ambas habilidades son de igual modo respaldadas como relevantes en el estudio ISC; un 49% de las compañías participantes subrayan la experiencia relevante como cualificación central y un 47% los conocimientos avanzados en conceptos de ciberseguridad (2018).

Por otro lado, se encuentra que un 22% de las empresas participantes tienen demanda de profesionales de ciberseguridad y un 74% contrata servicios de ciberseguridad a empresas especializadas.

Acorde al estudio ISC, existe una brecha relevante y creciente generada debido a un aumento global en la demanda de contratación de profesionales de ciberseguridad entre los profesionales que trabajan en ciberseguridad y los que sería necesario que se desempeñaran efectivamente en el área. Dentro de América Latina, esta brecha es mayor, existiendo aún más demanda de recursos de ciberseguridad en empresas de mediano y gran porte en relación con los recursos disponibles en el mercado (2019).

Asimismo, conforme con la publicación de Welivesecurity el crecimiento de las vacantes en ciberseguridad se espera crezca en un 350% para 2021. Sin embargo, se espera que la falta de profesionales capacitados para cubrir estos puestos deje 3 millones y medio de puestos sin cubrir alrededor del mundo (Harán, 2019).

En esta misma línea, se observó que entre las empresas que actualmente se encuentran con demandas de perfiles de ciberseguridad un 55% manifiesta que no ha logrado satisfacer la demanda debido a la dificultad para encontrar aspirantes con la formación y experiencia adecuada para el cargo.

Un 44% de las empresas proveedoras de ciberseguridad participantes se encuentran en una búsqueda activa de perfiles de ciberseguridad y han incorporado recientemente. A su vez, un 88 % prevé un aumento de la demanda de especialistas y un 94% considera que tiene necesidades mayores de recursos aun no estando en una búsqueda activa. Al momento de contratar nuevos recursos estas empresas suelen realizar contactos utilizando LinkedIn, portales laborales, universidades y/o promociones internas. Adicionalmente, un 69% de estas empresas han intentado contratar en los últimos tiempos, pero sin éxito, siendo la alta remuneración pretendida y la poca formación y experiencia lo que imposibilita la incorporación de recursos.

Si bien hemos identificado una demanda aún no satisfecha, claramente es más profunda en las empresas proveedoras de ciberseguridad que en el resto de las empresas participantes. Considerando las tendencias presentadas en diferentes publicaciones analizadas para este estudio, es probable que, a futuro, localmente la demanda aumente en el sector empresarial ya sea por temas de gestión de riesgo, cumplimiento y/o procesos de transformación del negocio. Esto podrá generar un crecimiento en la contratación de servicios de ciberseguridad, principalmente, en los sectores de servicios financieros, gobierno y salud, seguidos por consumo masivo, sector industrial y telecomunicaciones y tecnología.

2.4. Formación en ciberseguridad

Hemos identificado que a nivel universitario son varias las instituciones en Uruguay que dentro de sus planes de estudio han incorporado la seguridad de la información, permitiendo a los alumnos un acercamiento a la temática, aunque es necesaria la formación adicional en caso de querer lograr el conocimiento que les permita desempeñarse como especialistas en ciberseguridad.

Sin embargo, al consultar sobre la percepción de la oferta académica local, las empresas proveedoras de ciberseguridad consideran que no es suficiente, optando por formación externa al país tanto presencial como a distancia.

El Observador destaca en este sentido la pobre oferta formativa en seguridad informática dentro de nuestro país como una de las principales causantes de la falta de profesionales capacitados en el mercado (2019).

Sin considerar las asignaturas de seguridad de la información incluidas dentro de las formaciones de grado universitario, la oferta local relevada incluye dos posgrados de especialización en ciberseguridad, cursos cortos enfocados en aspectos técnicos y una especialización en gestión de la seguridad.

Una preocupación relevante en el contexto de la formación es el enfoque práctico de entrenamiento de los estudiantes, faltando recursos y herramientas que lo hagan posible. Esto puede generar un excesivo énfasis en la teoría y un insuficiente entrenamiento práctico para el marcado laboral. Aspecto a su vez destacado por Crumpler y Lewis, quienes señalan que el excesivo énfasis en la teoría resulta una de las críticas más comunes en el área de educación en ciberseguridad, pues dicho enfoque termina privando a los estudiantes de crear habilidades prácticas necesarias (2019).

En relación con el crecimiento de la oferta académica se denotan dos impedimentos: primero, la falta de recursos económicos y docentes calificados; y segundo, la falta de estudiantes interesados en la especialización en ciberseguridad. Respecto del primer punto, los centros de estudio identifican que deben ampliar la plantilla de docentes calificados, pero es un desafío poder reclutarlos en el mercado local, sea por formación, experiencia y aspiraciones salariales. El segundo desafío exige analizarlo en profundidad y ver qué acciones pueden promover el interés de jóvenes y profesionales en especializarse en el tema.

En referencia al segundo desafío, Meera Rao expresa la necesidad de motivar a los jóvenes dentro del área de ciberseguridad, dando a conocer sobre seguridad cibernética, realizando talleres para estudiantes y elaborando publicaciones que destaquen historias de éxito y el prometedor futuro que esta industria les depara (Meera Rao en Armerding, 2018).

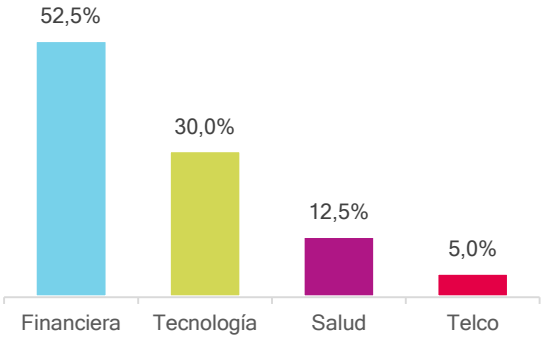
A modo de resumen, es posible destacar los siguientes conceptos claves a partir de los hallazgos:

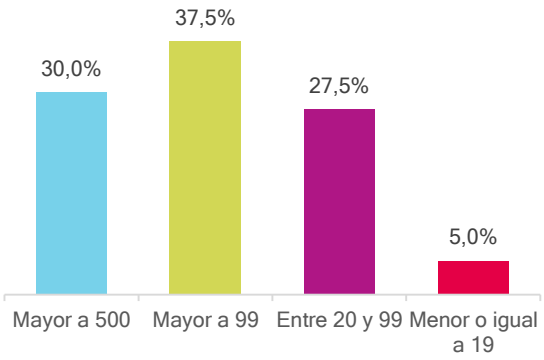
- Dificultades para integrar la ciberseguridad como parte de la estructura organizativa de las empresas nacionales, generando impactos desfavorables en la organización como una globalidad.
- Falta de presupuesto adecuado a ser invertido en iniciativas de ciberseguridad y las consecuentes pérdidas de oportunidades comerciales significativas.
- Percepción del riesgo de ciberseguridad en la mayoría de las empresas nacionales como alto o medio.
- A nivel de desarrollo en los sectores investigados, el financiero es el que posee mayores niveles de contratación de servicios de ciberseguridad y mayor grado de madurez. Los sectores de salud y comercio masivo se ubican en proceso de crecimiento en materia de ciberseguridad.
- La complejidad en los procesos de contratación de recursos de ciberseguridad responde a los elevados salarios pretendidos y a la falta de formación y experiencia de los perfiles disponibles en el mercado.
- En el mercado educativo uruguayo, a nivel universitario se identifica la incorporación de la ciberseguridad dentro de los planes de estudio, si bien se detecta necesidad de formación adicional para alcanzar niveles de formación de especialización en el rubro.
- El excesivo énfasis de la formación en elementos teóricos resulta en un insuficiente entrenamiento práctico de los estudiantes en el campo de la ciberseguridad.
- El crecimiento de la oferta educativa se ve desafiado por la falta de recursos económicos, la escasez de docentes calificados y el volumen de estudiantes que se acercan a las ofertas formativas de ciberseguridad.

3. Análisis del sector empresarial sin incluir a proveedores de servicios de ciberseguridad

Como hemos mencionado, durante el estudio se entrevistó a **40 empresas del mercado** de los rubros finanzas, salud, tecnología y telecomunicaciones; adicionalmente, se contactó a 16 empresas proveedoras de servicios de ciberseguridad. **A continuación, se analizan los resultados obtenidos para las empresas de los rubros financiero, tecnología, salud y telecomunicaciones**, para luego analizar los resultados logrados para las empresas proveedoras de servicios de ciberseguridad.

3.1. Empresas participantes

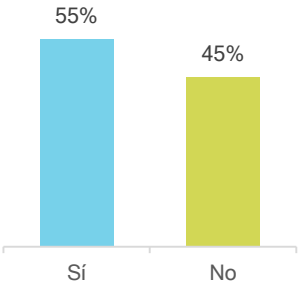




En el estudio realizado han participado empresas de la cuales el **52,5%** pertenecen al sector de **servicios financieros**, un **30%** al sector de la **tecnología**, **12,5%** son organizaciones de **salud** y el **5%** pertenecen a **telecomunicaciones**.

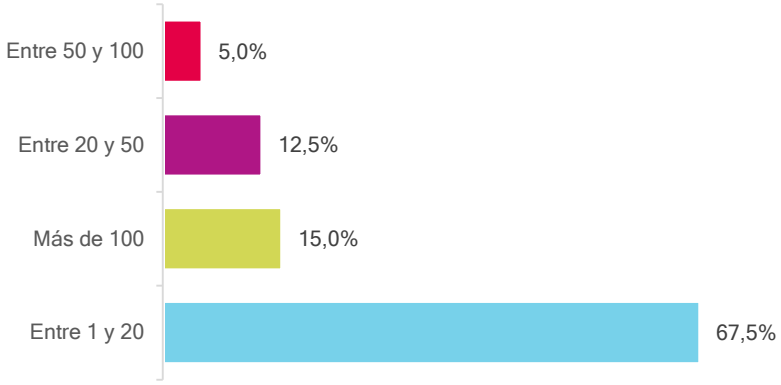
De estas empresas, el **37,5%** son empresas de **más de 99** colaboradores, el **27,5%** cuentan con una fuerza laboral que oscila **entre 20 y 99** personas, otro **30%** representa a empresas con **más de 500** empleados y un **5%** corresponde a empresa con **menos de 19 personas**.

3.2. Situación de ciberseguridad y tecnologías de información

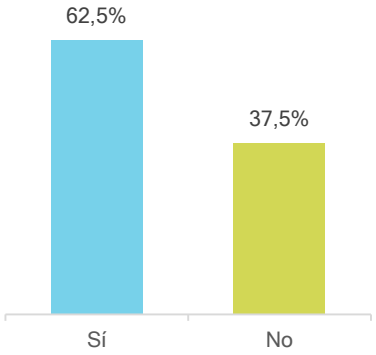


Al ser consultados sobre sí poseen un área dedicada a la seguridad de la información, el 55% de los entrevistados respondió que cuentan con dicha área mientras, que un 45% no han establecido aún un área de seguridad de la información, lo cual no siempre significa que no posean profesionales dedicados a tareas de ciberseguridad.

En aquellos casos en que se cuenta con un área de seguridad, el 56% depende de una gerencia del negocio que no es tecnologías de información, el 22% depende de TI, el 16,5% de gerencia general y un 5,5% es independiente, reportando al directorio.



El **67,5%** de las empresas entrevistadas tienen un área de tecnologías de la información compuesta por **entre 1 y 20 profesionales de TI;** en su gran mayoría, el área de TI **depende de la gerencia general.**



Abordando el tema sobre sí habían sufrido **incidentes de ciberseguridad** en los 3 últimos años, el **62,5% afirmo que así fue** y un 37,5% señaló que no hubo incidentes de ciberseguridad en la empresa.

Según Agesic, en promedio cada incidente de severidad "alto" o "muy alto" tiene un costo de US$ 40.000 (impuestos excluidos) en gastos operativos para su remediación; en 2018 hubo un total de 2.046 incidentes detectados, 43 de los cuales eran de severidad alta o muy alta (2,10%), lo cual totalizó la suma de dos millones de dólares.

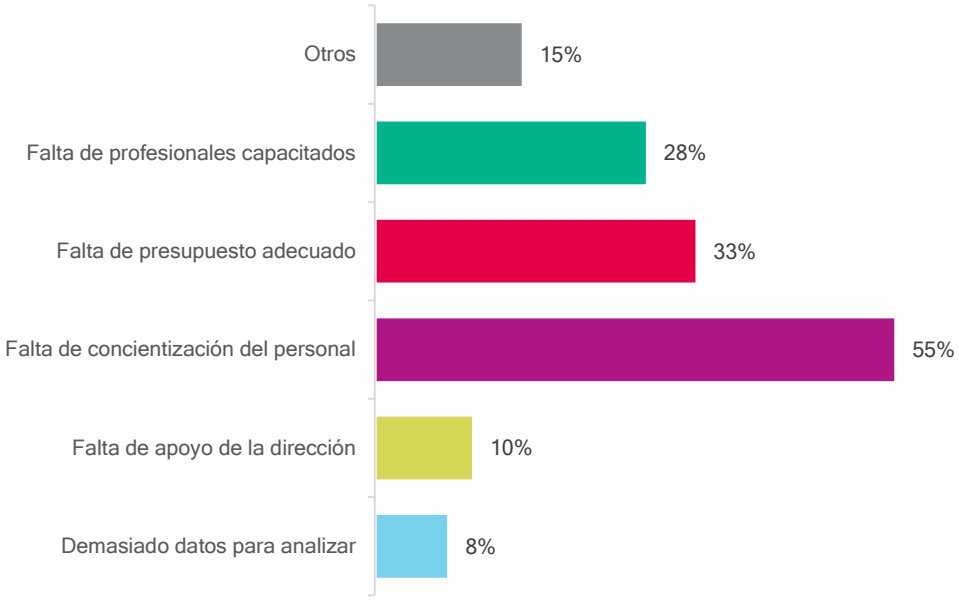
El **56%** de las empresas que sufrieron algún incidente de ciberseguridad cuentan con un área de seguridad formalmente establecida. Las acciones que derivaron luego de los incidentes fueron diseñar nuevos controles, concientización al personal, incorporar herramientas de monitoreo, alinearse con procedimientos de la norma ISO 27001, mejora de factores de autenticación y contratar a empresas especializadas en ciberseguridad, entre otras acciones.

3.3. Percepción de la ciberseguridad

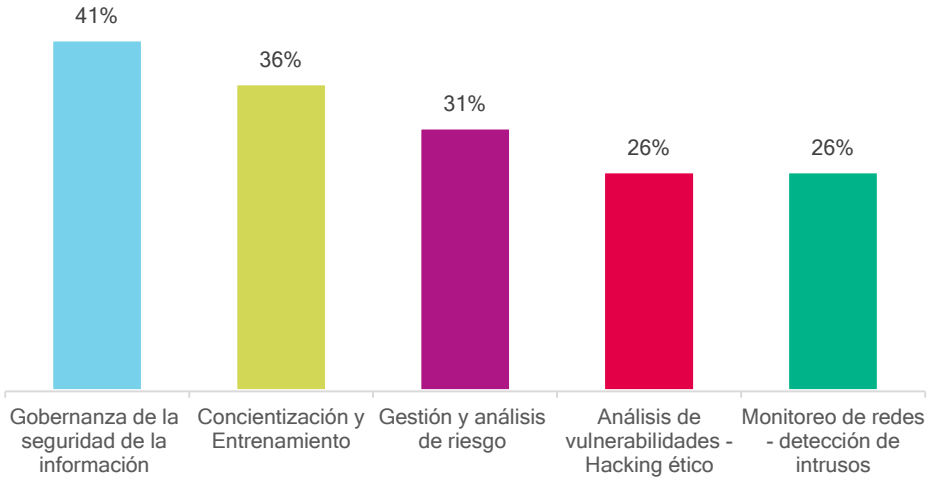
En relación con la percepción al **riesgo a la ciberseguridad**, un **50%** de los entrevistados lo consideran **alto**, un **30% medio** y el restante **20% bajo**.

El 60% de las empresas que participaron en el estudio de ISC alegan encontrarse con un nivel de riesgo de ciberseguridad de moderado a alto debido a la escasez de recursos (2018).

Los desafíos que no permiten el debido enfoque sobre las iniciativas a la ciberseguridad son varios, siendo la **falta de concientización del personal** el mayormente referido por los entrevistados (**55%**), seguido por la **falta de presupuesto adecuado** (**33%**) y **falta de profesionales capacitados** en ciberseguridad (**28%**). Al comparar estos datos con el análisis realizado por ISC en 2018 se arriba a conclusiones similares.



Al ser consultados por las **áreas de ciberseguridad más críticas** o relevantes para la organización, los entrevistados consideraron que **concientización y entrenamiento** de usuarios, **gobernanza** de la seguridad de la información y **gestión y análisis de riesgo** son las principales.



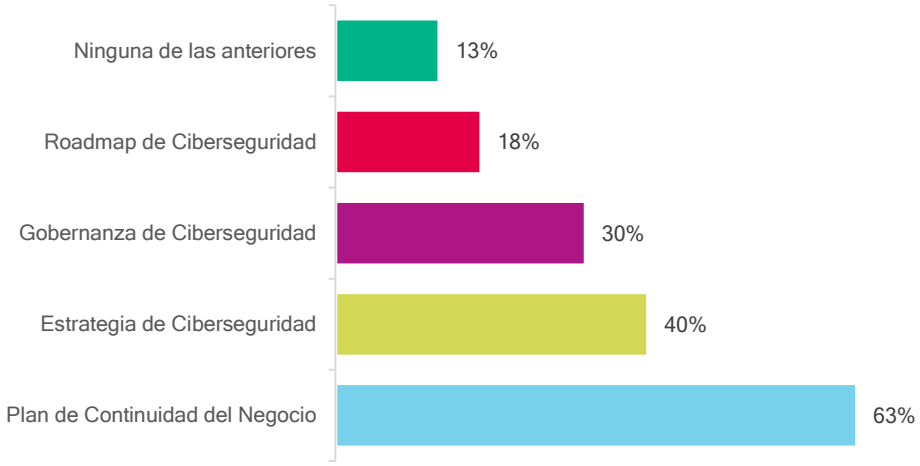
3.4. Grado de madurez de la ciberseguridad

El **80%** de las empresas entrevistadas considera que la organización tiene **necesidades de ciberseguridad y** un **95%** cuenta con **políticas y procedimientos definidos.** Asimismo, el **85% no** cuenta con **seguro de ciberseguridad contratado.**

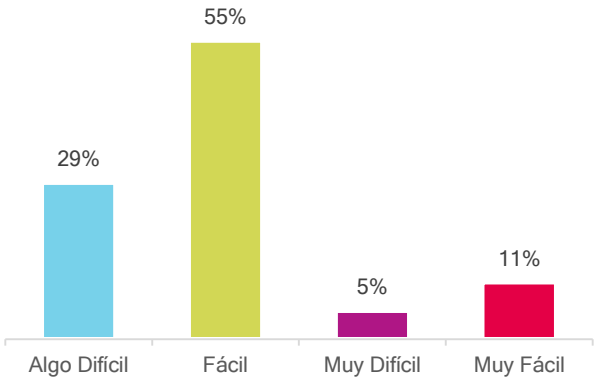
David Ferbrache, Leadership, Global Head of Cyber Futures ha realizado una serie de predicciones para 2020 en relación con la ciberseguridad; en particular, ha comentado que la creatividad del cibercrimen continúa siendo un desafío para las organizaciones, por lo que recurren cada vez más al sector de seguros cibernéticos para cubrir posibles pérdidas,

esperando que las aseguradoras se vuelvan más selectivas en cuanto a qué y a quién están asegurando (Security, 2019).

En relación con los procedimientos implementados, un **63% cuenta con Plan de Continuidad.**



En cuanto a la **inversión** en **seguridad,** se consultó sobre el grado de dificultad al momento de tener que **convencer** a la alta dirección, el **55%** entiende que es **fácil** y un **29%, algo difícil**.



En las empresas en que el área de Seguridad **depende de TI** encontramos que un **23% no tiene presupuesto** de seguridad, un **23% no sabe** si se cuenta con uno y un **27%** estima que el presupuesto de seguridad está entre **5% y 10%** del presupuesto de TI. Adicionalmente, se ha identificado que un 33% de los entrevistados considera como un desafío la falta de un presupuesto adecuado.

En aquellas empresas en que el área de Seguridad de la Información **no depende de TI,** un **82%** de ellas mencionan tener un **presupuesto exclusivo** para seguridad.

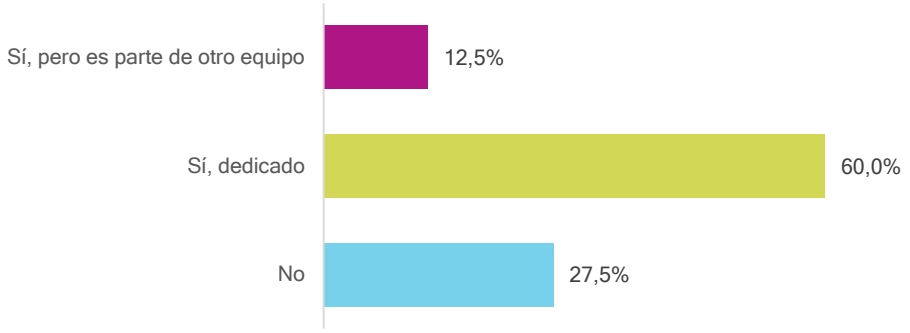
Adicionalmente, en los casos en que tienen presupuesto y lo conocen, encontramos que a un **81%** le parece **adecuado el porcentaje** asignado para las **necesidades de ciberseguridad de la organización** y un **54%** informó que el **presupuesto aumentó** con respecto al **año anterior**.

En la publicación CIO Survey 2019. A Changing Perspective realizada por Harvey Nash y– KPMG se detectó una mayor proporción de empresas invirtiendo en tecnología y los principales

motores detrás de estas inversiones corresponden con inversiones en ciberseguridad (14%), data analytics, automatización (17%) y trasformación (44%) (Elis y Bates, 2019).

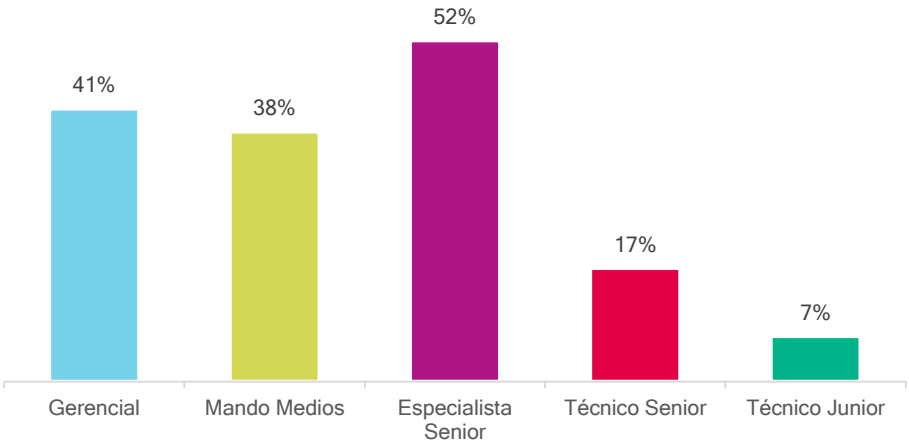
3.5. Roles de ciberseguridad en la empresa

Las empresas entrevistadas en un **60%** tienen **al menos un especialista en seguridad,** mientras que un 27,5% no cuenta con un rol específico y un **12,5% únicamente en forma parcial**. En ese sentido, podemos citar a Gary McGraw que menciona que la ciberseguridad debe ser entendida no como un solo trabajo, sino como una larga y variada lista de trabajos. Así como en el campo de la medicina, es necesario contar con distintos profesionales para alcanzar un sistema de salud eficiente; en ciberseguridad, de igual modo, se requieren diversos especialistas para lograr el éxito (Gary McGraw en Armerding, 2018).



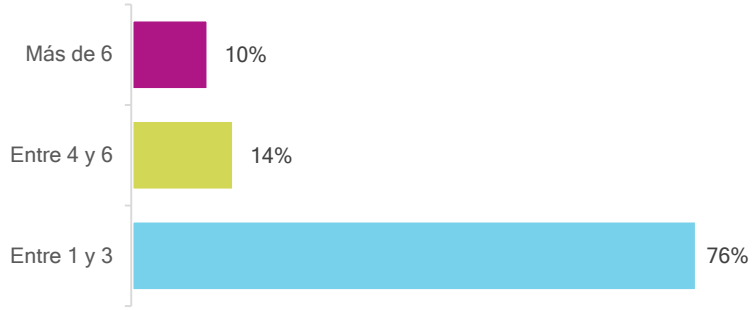
Contar con escasos recursos para la actividad puede determinar que las empresas no puedan cubrir todas las funciones necesarias para gestión de la ciberseguridad. Esto puede generar vulnerabilidades en la gestión, no abordándose áreas de la seguridad relevantes para el negocio.

Un **41%** de los recursos de ciberseguridad son de rango **gerencial**, **38%** corresponde a **mandos medios** y un **52%** a **especialistas senior.**



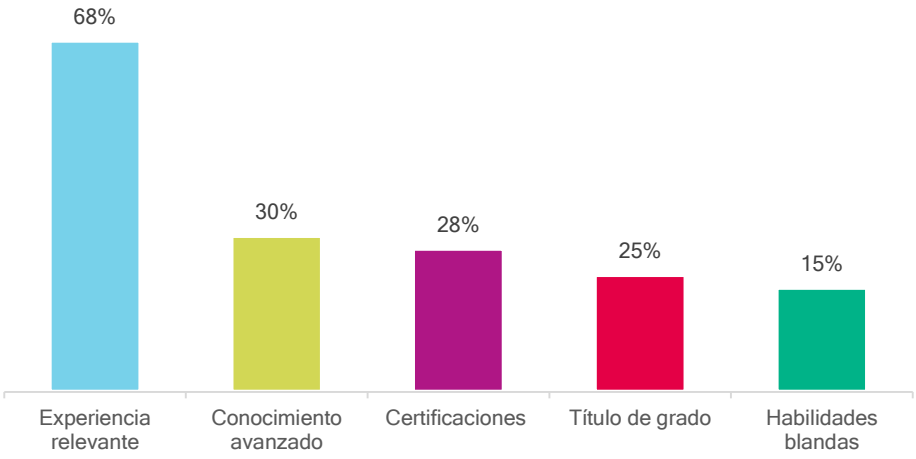
El 27,5% de las empresas que no cuentan con un especialista en ciberseguridad son en su mayoría (64%) empresas medianas de hasta 99 empleados.

En aquellos casos que cuentan con especialistas en seguridad, un **76% cuenta con menos de 3.**

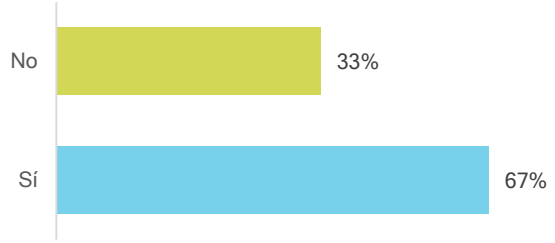


En aquellas empresas que tienen recursos asignados a ciberseguridad durante los últimos 5 años se ha mantenido relativamente constante la cantidad de recursos y un sector de las empresas se apoyan con la contratación de servicios brindados por empresas especializadas; como veremos más adelante, un 74% de las empresas entrevistadas contratan servicios de ciberseguridad.

Según las empresas entrevistadas, la **experiencia relevante** y el **conocimiento avanzado** en ciberseguridad son las cualificaciones más importantes al momento de cubrir una vacante en ciberseguridad.



El **58%** de los entrevistados mencionaron tener recursos de ciberseguridad **certificados**. A la hora de enumerar las certificaciones, **CISSP** y **CISM** fueron las referidas.



En relación con la **capacitación** del personal en ciberseguridad, el **67%** contestó que invierten en capacitación. Más adelante, en este estudio se analiza la oferta académica local.

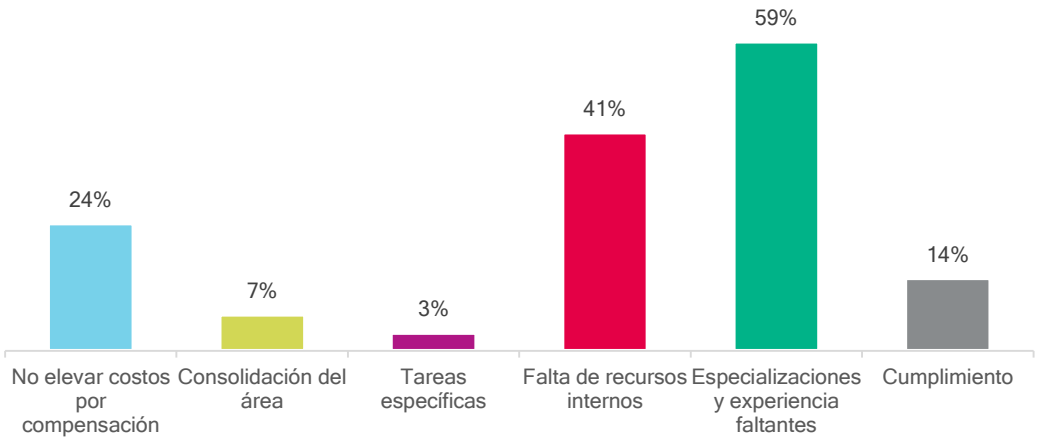
En la publicación de ISC se encuesta a profesionales de ciberseguridad y estos detallan que sus preocupaciones son: 36% la falta de personal capacitado, 28% falta de terminología estándar que permita una comunicación eficiente, 27% la falta de recursos para llevar adelante el trabajo, 24% falta de balance trabajo-vida y en un 24% la falta de presupuesto para invertir en iniciativas de ciberseguridad. Adicionalmente, se presentan como principales preocupaciones la falta de habilidades y experiencia del personal de ciberseguridad (37%) y el presupuesto inadecuado para dedicarles a las iniciativas claves de ciberseguridad (28%) (2019).

Este estudio detalla también que, generalmente, los profesionales en ciberseguridad cuentan con varios años de experiencia en el rol.

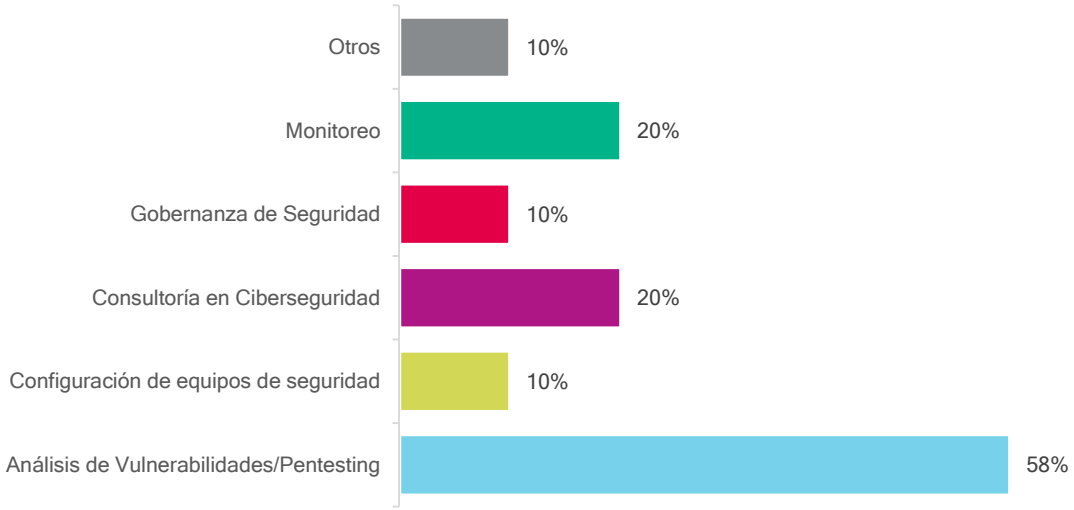
3.6. Contratación de servicios de ciberseguridad

El 74% de las empresas entrevistadas suele contratar servicios de ciberseguridad a empresas especializadas. Al ser consultados por los motivos que los llevan a contratar, mencionaron:

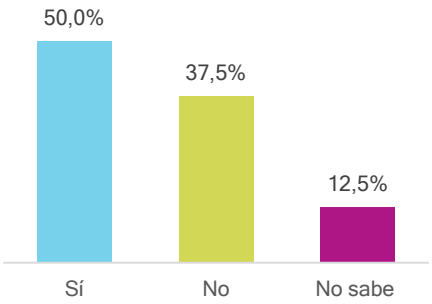
- Buscar especializaciones y experiencia que la empresa no tiene actualmente.
- La carencia de recursos internos.
- Evitar contratar nuevos recursos para eludir el aumento de los costos por compensación.
- Cumplir con aspectos normativos o de certificaciones.



En cuanto a los servicios que en mayor grado contratan, encontramos que análisis de vulnerabilidades, hacking ético, monitoreo y consultoría en ciberseguridad son los que lideran.



Las **horas contratadas** por las empresas que contratan servicios se han **mantenido** o han **aumentado** en los últimos 5 años.



El **50 %** de los entrevistados entienden que a futuro habrá un **aumento** de contratación de horas, mientras que un **37,5%** entiende que no **aumentarán** las horas contratadas.

Un aumento en las horas de contratación parece razonable considerando el uso intensivo de la tecnología en las empresas, los procesos de transformación, el cumplimiento de normativas y regulaciones y que las áreas de seguridad internas no siempre cuentan con los recursos para el desarrollo de las funciones requeridas no solo por la cantidad, sino también por el conocimiento y la experiencia.

Estimaciones y previsiones

Al evaluar las previsiones del presupuesto de ciberseguridad en los próximos años, un **80%** consideran que **aumentará** y un **20%** que se **mantendrá**.

80% considera que aumentará el presupuesto de ciberseguridad.

20% considera que se mantendrá el presupuesto de ciberseguridad.

Ante un contexto de complejos desafíos en materia de seguridad y oportunidades digitales, se hace necesario contar con altos niveles de compromiso por parte de los líderes para estar completamente informados y capacitados en temas de ciberseguridad. Sin embargo, mientras el compromiso ejecutivo con la seguridad informática ha ido en aumento, la encuesta “The economics of trust

de Consumer Loss Barometer", de KPMG, encontró que la mayoría de los CEO aún mantienen un involucramiento escaso o relativo con temáticas de ciberseguridad.

El estudio de ISC considera que la escasez de profesionales de ciberseguridad a nivel global es cercana a los 3 millones; un 63% de quienes contestaron la encuesta reportan que su organización tiene escasez de profesionales de TI dedicados a ciberseguridad (2019).

Al consultar a las empresas entrevistadas si **actualmente tienen demanda de profesionales de ciberseguridad, un 22% contestó en forma afirmativa** y prevé que esta aumentará, mencionando áreas como seguridad en la nube. Adicionalmente, recordemos que un 74% de las empresas suelen contratar servicios de ciberseguridad a proveedores especializados.

Según la publicación de Cybersecurity Workforce Gap, en la encuesta de CSIS de tomadores de decisiones de TI en 8 países, 28% de los empleadores reportan escasez de habilidades en ciberseguridad y 71% cree que esta brecha en el talento causa un daño directo y medible en sus organizaciones (Crumpler y Lewis, 2019).

Los casos en donde no se ha logrado satisfacer la demanda se deben a que no han logrado encontrar un aspirante con la formación y experiencia adecuada para el cargo. En el estudio profesionales en seguridad informática surge que, entre la formación académica y la autodidacta, se plantea que se espera un crecimiento del 350% de las vacantes de ciberseguridad; sin embargo, la falta de profesionales para cubrirlas se espera dejen 3 millones y medio de puestos vacantes a nivel mundial. Además, en el estudio ISC 2019 se menciona la falta de profesionales capacitados con habilidades y experiencia pertinente en ciberseguridad como la preocupación principal del 65% de las empresas encuestada (Harán, 2019).

Al cierre de las entrevistas, las empresas nos brindaron opiniones adicionales; a continuación, presentamos algunos de los aportes:

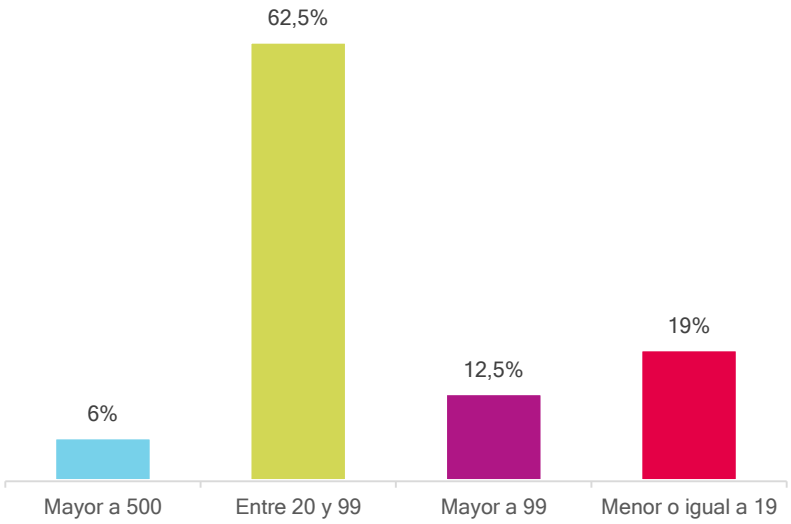
- "Importancia de incluir la ciberseguridad desde el momento en que se piensa el desarrollo de los sistemas y la gestión de los proyectos. Apoyar la diversidad y opciones de formación académica".
- "La idea en nuestra empresa es reforzar la seguridad entre los equipos, que haya una rotación dentro de cada equipo de responsables de los controles de seguridad. Hay una brecha entre lo académico y la práctica; es más rico asistir a ciclos de actualizaciones".
- "En Uruguay hay oportunidades en el sector de ciberseguridad, sobre todo por la exportación de productos, pero estamos muy en pañales aún y otros países nos superan en este punto".
- "Es necesario generar capacitaciones sobre la relevancia de ciberseguridad, en particular, en aquellos rubros ajenos a la tecnología, de modo de aumentar la conciencia".
- "El aumento de la demanda en los próximos años, la falta de talento en el mercado y la necesidad de tomar perfiles del exterior para las búsquedas realizadas".
- "Considero importante que desde Agesic se haga mayor seguimiento y apoyo a las empresas, que se generen grupos por tipo de empresas y que se pueda generar mayor intercambio".
- "Es relevante contar en el ámbito privado con políticas comunes y colaborativas de ciberseguridad".

- “Veo la falta de recursos humanos calificados como el principal obstáculo en ciberseguridad y la relevancia de la seguridad en la nube y la seguridad de las apps, especialmente móviles, como sectores de desarrollo”.

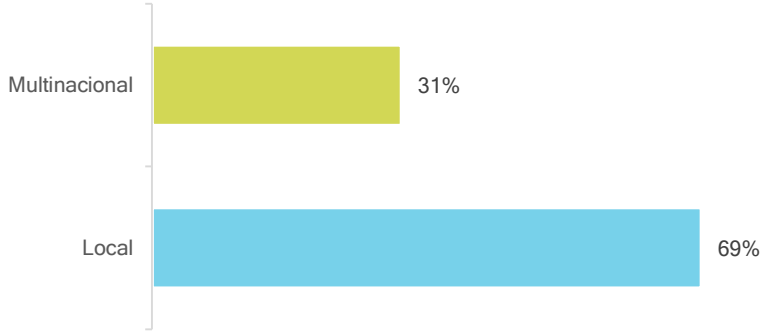
4. Análisis de empresas proveedoras de servicios de ciberseguridad

Anteriormente, hemos mencionado que el 74% de las empresas entrevistadas suelen contratar servicios de ciberseguridad a empresas especializadas. Es por tal motivo que, para el objetivo de este trabajo, ha sido relevante poder entrevistar a empresas que se especializan en proveer servicios de ciberseguridad.

En el estudio realizado han **participado 16 empresas que brindan servicios de ciberseguridad,** de las cuales un **12,5%** son empresas de **más de 99** colaboradores, el **62,5%** cuentan con una fuerza laboral que oscila **entre 20 y 99** personas, **6%** representa a empresas con **más de 500** empleados y un **19%** corresponde a empresa con **menos de 19 personas**.



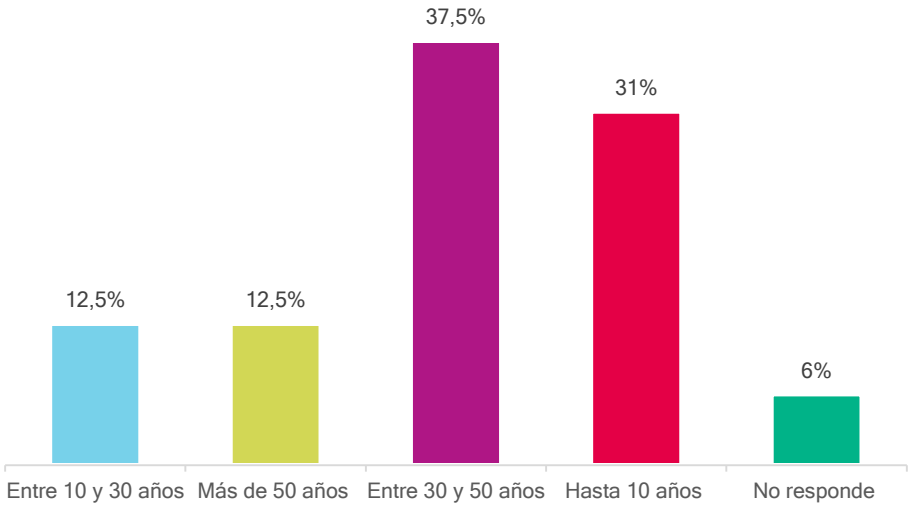
Dentro de los proveedores de ciberseguridad con menos de 19 personas, encontramos empresas que tiene hasta 4 empleados.



El **69%** de las empresas proveedoras participantes son empresas **locales** y un **31%** corresponde a empresas **multinacionales**.

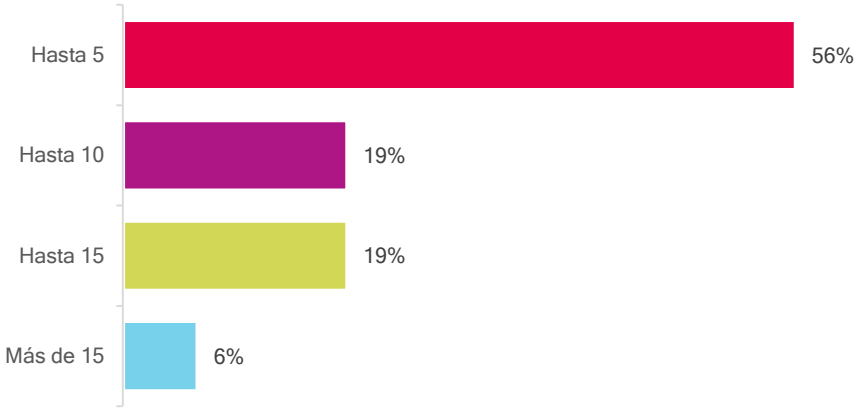
La mayoría de las empresas proveedoras de servicios de ciberseguridad entrevistadas están activas hace **menos de 10 años (31%),** mientras que un **37,5%** vienen brindando servicios **entre 30 y 50 años**, un **12,5%** desde hace **más de 50 años** y un **12,5%** tienen una antigüedad en plaza que va desde los **10 y los 30 años**.

En relación con proveer servicios de ciberseguridad, el **69% hace menos de 10 años** que los brinda y el resto hace menos de 20 años.

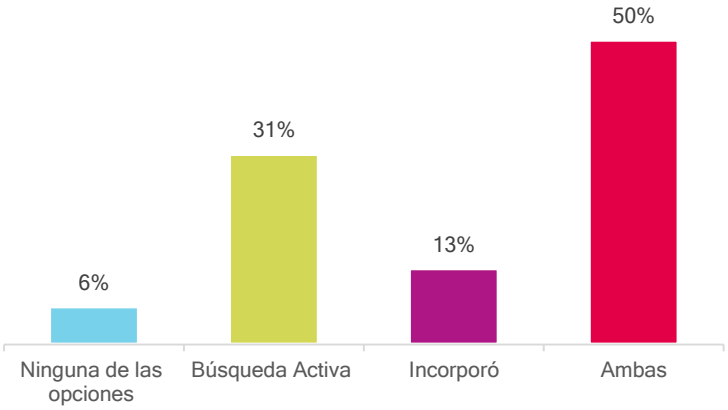


4.1. Profesionales de ciberseguridad

Las empresas tienen equipos de especialistas en ciberseguridad para brindar los servicios, un **56%** cuenta con hasta **5 profesionales**, un **19%** hasta **10 especialistas**, mientras que las empresas que tienen **hasta 15 profesionales** y **más de 15** representan el **19%** y **6%,** respectivamente.



Las empresas entrevistadas fueron consultadas respecto a si se encontraban en una búsqueda activa o si habían incorporado recientemente profesionales de ciberseguridad.



El 88% de los entrevistados prevé un aumento de la demanda de especialistas en ciberseguridad y un 94% considera que tienen necesidades mayores de recursos, pero aún no están en una búsqueda activa.

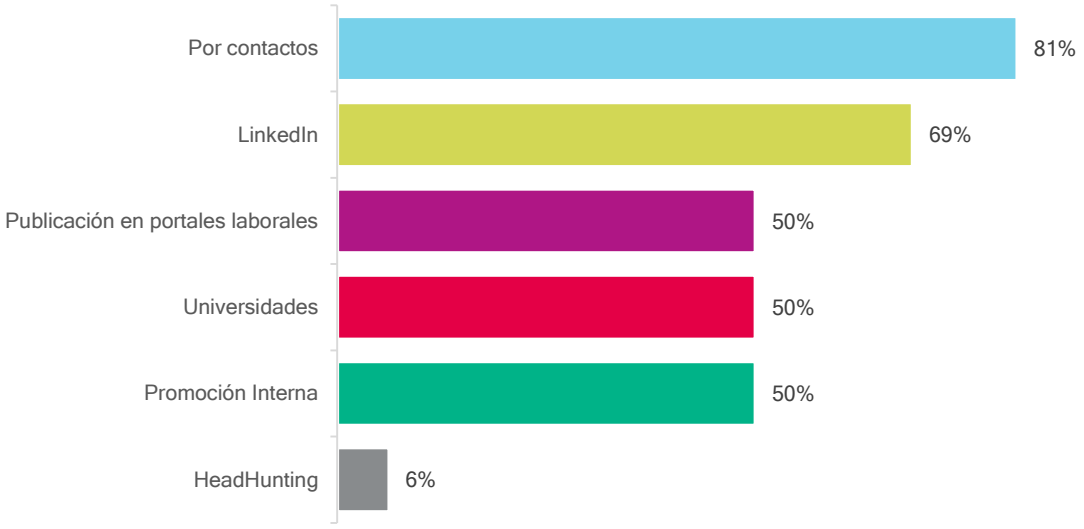
94% considera que tiene necesidades mayores de recursos, pero aún no están en búsqueda.

88% entiende que la demanda va a aumentar en los próximos años.

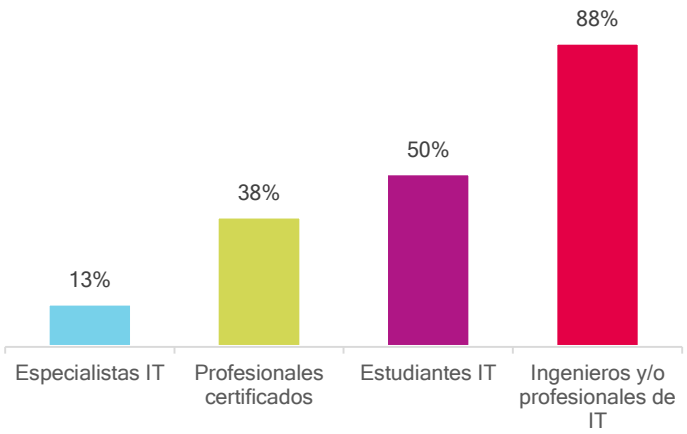
Al ser consultados por la rotación de personal, un 56% considera que es baja, mientras que un 25% considera que es media. En relación con el último año, un **56% ha tenido rotación de personal especializado en ciberseguridad**. En general, se han movido hacia empresas de la competencia o empresas de TI.

Al momento de contratar nuevos recursos, las empresas de ciberseguridad suelen realizarlos a través de contactos, utilizando LinkedIn, portales laborales, universidades y por las promociones internas.

El 50% indicó que actualmente se encuentra en una búsqueda activa y que ha incorporado recientemente especialistas a su equipo.

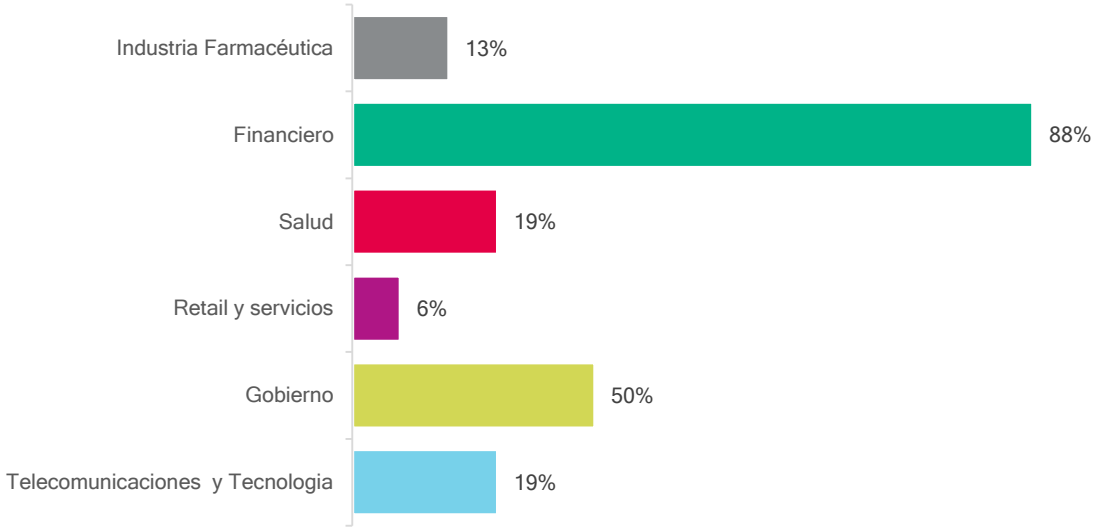


En relación con las contrataciones recientes la formación de esos recursos corresponde a Ingenieros u otros profesionales de TI y estudiantes de TI en su mayoría.



4.2. Entrega de servicios

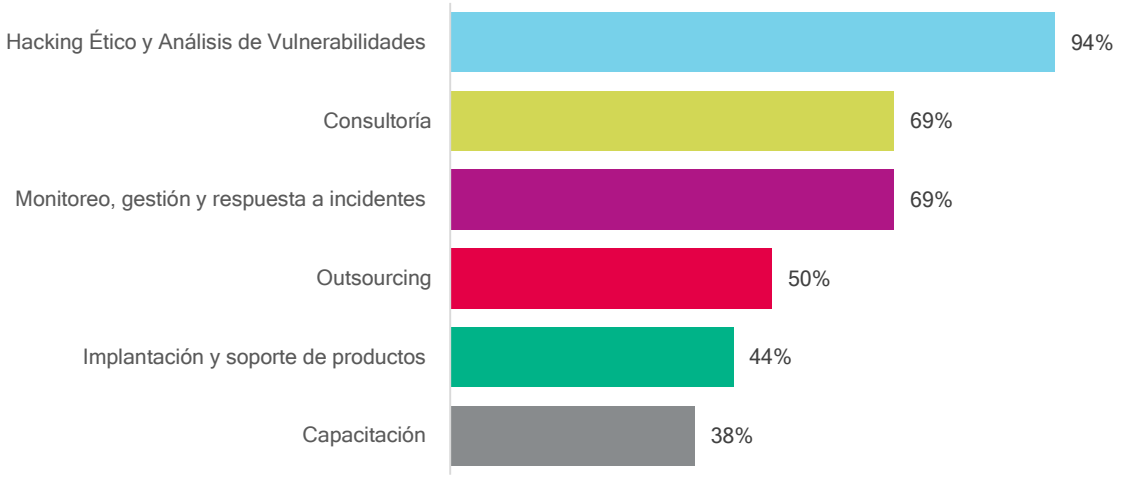
A conversar sobre los clientes que en mayor grado solicitan servicios de ciberseguridad, el **88%** de los entrevistados consideran que es en el sector **financiero** donde más son solicitados este tipo de servicios, seguido por **gobierno (50%)**, **salud (19%) y telecomunicaciones y tecnología (19%).**



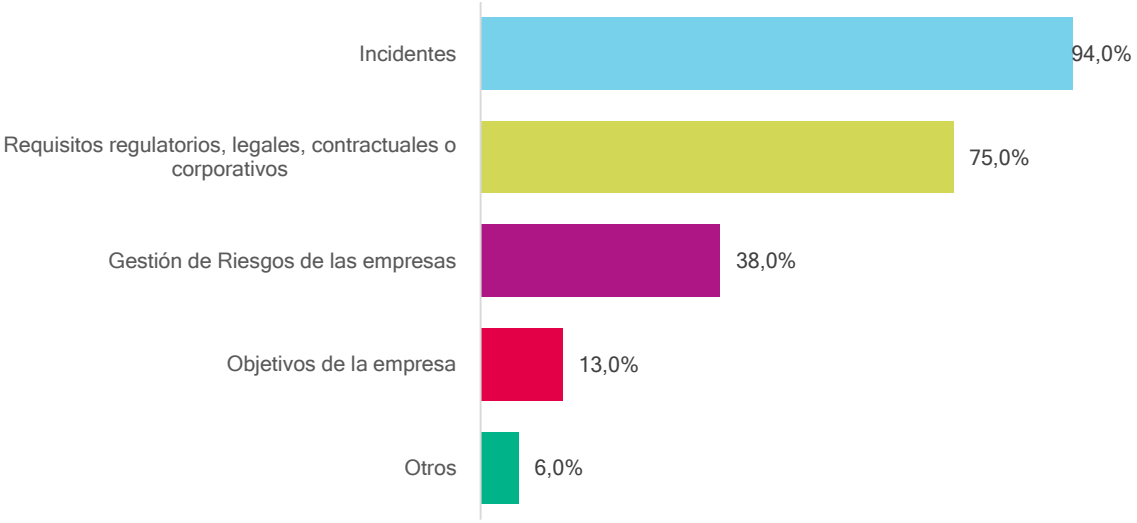
Adicionalmente, opinan que el sector **salud (56%)** es el sector que está empezando a contratar servicios de ciberseguridad, seguido por **retail y servicios (31%).**

El **69%** de las empresas entrevistadas **brindan servicios de ciberseguridad en el exterior** en países como Paraguay, Colombia y Argentina, entre otros.

En cuanto a los servicios que habitualmente son contratados, **hacking éticos y análisis de vulnerabilidad es el primero**, **seguido de monitoreo, gestión y respuesta de incidentes** y consultoría. En el apartado sobre empresa consumidora de servicios de ciberseguridad hemos visto que en mayor grado contratan **análisis de vulnerabilidades / pentest, monitoreo y consultoría en ciberseguridad,** lo que coincide plenamente con la opinión de los proveedores de servicios.



En cuanto a las razones que motivan a empezar a contratar servicios, el sufrir incidentes y los requisitos regulatorios son los principales catalizadores.

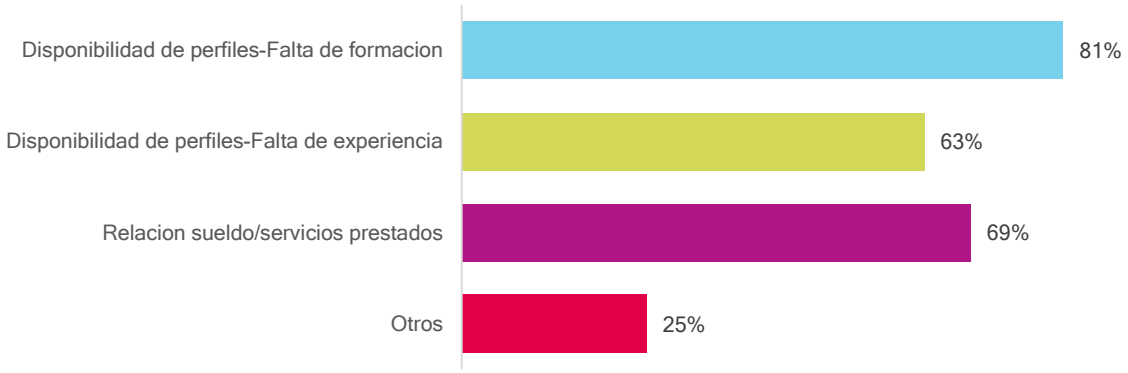


Al ser consultado sobre la evolución de horas contratadas, el 69% considera que va en aumento.

4.3. Contratación de profesionales

Como se mencionaba anteriormente, los medios utilizados para la selección y búsqueda de recursos son variados, utilizando contactos, LinkedIn, portales de laborales y universidades, entre otros. A su vez, al evaluar las últimas incorporaciones, son profesionales universitarios en TI o estudiantes.

Al momento de realizar una búsqueda y selección de personal, surgen ciertas restricciones entre las que podemos nombrar la baja de disponibilidad de perfiles con la formación y experiencia adecuada o la relación sueldo-servicios prestados.



Un **69%** de las empresas entrevistadas **ha intentado contratar en los últimos tiempos y no ha tenido éxito,** siendo la alta remuneración pretendida y la poca formación y experiencia lo que imposibilita la incorporación de recursos.

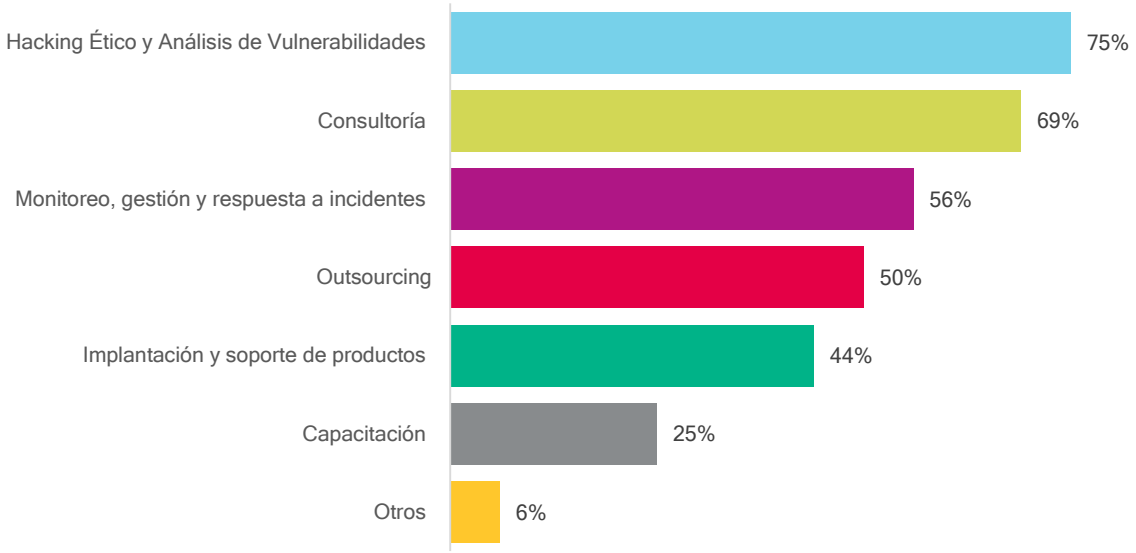
En esta misma línea, se observó que de las empresas que actualmente se encuentran con demandas de perfiles de ciberseguridad, un 55% manifiesta que no ha logrado satisfacer la demanda debido a la dificultad para encontrar aspirantes con la formación y experiencia adecuada para el cargo.

4.4. Formación en ciberseguridad y proyección de crecimiento del equipo

El **100% d**e los proveedores de ciberseguridad **invierten en capacitar** a sus recursos y un **81%** opta por **cursos** brindados desde el **extranjero,** ya que perciben que la oferta local no es suficiente. Estos cursos son tanto a distancia como presenciales.

En lo que respecta a proyectar un crecimiento del equipo de colaboradores, un 81% afirma que es necesario, con proyecciones de crecimientos que van desde un 20% a un 150%.

Los servicios que justificarán el crecimiento previsto se encuentran alineados, en gran medida, con los servicios que hoy son más demandados por el mercado.



En cuanto a los sectores que, entienden, ayudarán a que se lleve a cabo dicho crecimiento, proyectan que principalmente serán los sectores de servicios financieros, gobierno y salud, seguidos por retail y servicios, sector industrial y telecomunicaciones y tecnología.

5. Análisis de instituciones de educación

En el marco del estudio, se entrevistó **a 8 universidades y/o centros educativos** de nuestro país con el fin de conocer su oferta educativa en materia de seguridad informática, su cuerpo docente, estadísticas referentes al alumnado y el abordaje que se adopta en referencia a ciberseguridad.

Crumpler y Lewis subrayan una aparente falencia de la educación en ciberseguridad y de los programas de entrenamiento a la hora de preparar a los estudiantes para enfrentar la clase de roles técnicos altamente calificados que son actualmente tan necesarios y faltantes. En su estudio, se menciona que en 2018 profesionales asociados a ISACA encontraron que el 61% de las organizaciones creen que menos de la mitad de los postulantes a cargos abiertos de ciberseguridad cuentan realmente con las cualificaciones necesarias para ese trabajo/rol. Acorde a practicantes de ciberseguridad, los empleadores están insatisfechos debido a que perciben en los graduados falta de experiencia práctica y de entendimiento de los fundamentos de Computación y Seguridad de la Información. Como resultado, los graduados requieren una amplia capacitación en el ámbito laboral antes de que puedan comenzar a trabajar en el campo de la seguridad (2019)

Asimismo, acorde a la publicación de Security Predictions for 2020, las universidades no están logrando que se gradúen profesionales capacitados lo suficientemente rápido como para satisfacer la demanda de nuevos empleados dedicados a la seguridad de la información. La demanda de profesionales de ciberseguridad capacitados continúa en ascenso y no se detecta ningún cambio a nivel del reclutamiento ni de la educación que pueda potencialmente aumentar la oferta de estos perfiles. Es así como, entre otros factores, la falta de cursos de educación formal adecuados sobre ciberseguridad contribuye a la predicción de un crecimiento en la brecha de habilidades en ciberseguridad a un 15% para 2020 (2019).

Haciendo eco de esta misma preocupación, Robert Herjavec (Fundador y CEO en Herjavec Group) alega que hasta que no podamos rectificar la calidad de la educación y la capacitación que reciben los expertos cibernéticos, los terroristas virtuales continuarán superándonos y la oferta de talentos en ciberseguridad continuará siendo insuficiente (Cybercrime Magazine, 2019).

5.1. Oferta académica local

En el marco local, hemos identificado que a nivel universitario son varias las instituciones que dentro de sus planes de estudio han incorporado la seguridad de la información, permitiendo a los alumnos un acercamiento a la temática, siendo necesario formación adicional en caso de querer lograr el conocimiento que les permita desempeñarse como especialistas en ciberseguridad.

Adicionalmente, se han identificado cursos cortos, especializaciones y postgrados específicos dentro de la oferta local que se detallan a continuación.

En cuanto a la oferta educativa específica, la **Universidad ORT Uruguay** ofrece opciones de estudio vinculados a ciberseguridad en distintos niveles de formación. Dentro de sus carreras de grado, en Ingeniería en Sistemas se dicta la materia Seguridad Informática con carácter obligatorio, mientras que en la opción Licenciatura en Sistemas se cursa un Taller de Seguridad Informática al fin del sexto semestre de carrera. Ambas formaciones de grado abordan las siguientes materias electivas abocadas a la ciberseguridad: aspectos de seguridad de sistemas informáticos, arquitectura para datos seguros, seguridad en aplicaciones, tecnologías aplicadas a la seguridad de la información y gobernabilidad de la seguridad y gestión de riesgos.

Asimismo, dentro de sus planes de carreas cortas, ofrecen la formación de Analista en Infraestructura Informática, formando parte del plan la materia Fundamentos de Ciberseguridad en Redes y Datos. Por otra parte, la carrera corta denominada Administrador de Servidores y Aplicaciones imparte una materia directamente asociada a seguridad informática, conocida como Fundamentos en Ciberseguridad.

A su vez, en ORT es posible encontrar opciones educativas avanzadas en seguridad informática; se trata de dos cursos de Actualización Profesional, Hacking Ético y Gestión de Incidentes y Programa de Desarrollo Profesional en Seguridad Informática y actualmente, a nivel de educación de posgrado, la universidad estará dictando para el año 2020 el Diploma de Especialización en Ciberseguridad, enfocándose en una formación amplia y común a las diversas áreas de especialización en ciberseguridad.

Por otro lado, se relevó la oferta formativa de la **Universidad de la República, Facultad de Ingeniería**, en donde a nivel de formaciones de grado se imparten dos cursos dedicados a ciberseguridad como materias de la carrera Ingeniería en Computación y como electivas de las carreras de 5 o más años. Además, Udelar ofrece la posibilidad de formarse a nivel de posgrado con el Diploma de Especialización en Seguridad Informática, abocado a licenciados e ingenieros en Computación o formaciones equivalentes.

Se pude lograr una maestría a continuación del diploma de especialización desarrollando una tesis en la materia.

En otro orden, la **Universidad de Montevideo (UM)** cuenta con formación en ciberseguridad dentro de su carrera de grado Ingeniería en Informática, en donde se brinda una materia denominada Seguridad Informática. A su vez, la UM cuenta con un convenio firmado junto con

la empresa multinacional Fortinet que ofrece la oportunidad de certificarse en Fortinet Network Security Expert Level 4 – Professional (NSE 4) al cursar el Taller de Seguridad y Redes de la Facultad de Ingeniería de la Universidad de Montevideo (FIUM).

Por su parte, la **Universidad Católica del Uruguay (UCU)** habilita contenidos educativos en ciberseguridad en dos de sus formaciones de grado; en la carrera de Ingeniería se dictan dos materias vinculadas a la temática: Seguridad Informática, como asignatura obligatoria, y Programación Segura, que es electiva. A su vez, en Licenciatura en Informática se encuentra la materia denominada Seguridad Informática.

La UCU también ofrece a nivel de posgrado contenidos vinculados; en especial, el posgrado en Gerencia de Tecnología de la Información, que engloba dentro de su plan de estudios la materia Seguridad de la Información. Otros cursos u opciones de actualización profesional en ciberseguridad no se encuentran contemplados en su currícula.

En el plano internacional, la organización **Information Systems Audit and Control Association (ISACA)** en su capítulo Montevideo le permite a la comunidad global de profesionales acreditarse en diferentes campos del mundo digital; la certificación en CISA (Certified Information Systems Auditor) se encuentra directamente vinculada a la Seguridad Informática.

En la oferta formativa de la **Universidad Tecnológica del Uruguay** (**UTEC)** existen materias específicas abocadas a la seguridad de la información dentro de su carrera Licenciatura en Tecnología de la Información.

Asimismo, el **Instituto BIOS** permite cursar una formación específica de 4 meses de duración en ciberseguridad a través de la opción Técnico en Seguridad Informática.

Finalmente, el **Instituto Uruguayo de Normas Técnicas (UNIT)**, con el objetivo delimitado de contextualizar el significado de la seguridad para la gestión de la información, ofrece la titulación Especialista en Gestión de Seguridad de la Información UNIT-ISO_27000, integrando en consecuencia dentro de esta formación las principales normas del Comité Técnico de Seguridad de la Información.

5.2. Requisitos para acceder a educación en ciberseguridad

Cerca de la mitad de las instituciones entrevistadas solicitan conocimientos previos en TI, estudios avanzados y/o culminados de ingeniería en sistemas y aprobación de previaturas para acceder a una formación específica en ciberseguridad. Al igual que destaca el diario El País, el camino de formación en ciberseguridad inicialmente da comienzo con el estudio de carreras que aporten la base técnica, habitualmente, ingeniería en informática o telecomunicaciones, o también estudios expertos en matemática o física. Luego, a partir de estos cimientos, se puede cursar un máster o estudios especializados y avanzados en ciberseguridad (2019).

5.3. Modalidades de aprobación en la educación de ciberseguridad

Las modalidades de aprobación en las formaciones de ciberseguridad de nuestro país son diversas, exigiéndoseles a los estudiantes el empleo de un abanico amplio de habilidades. Se respalda la creación de proyectos, rendimientos de exámenes y parciales, experiencias vivenciales a través de prácticas obligatorias y un cierto porcentaje variable, según cada institución, de asistencia y participación en el aula.

5.4. Actividades educativas de ciberseguridad en modalidad práctica

Ante la consulta sobre la gestión de la parte más práctica de la formación en ciberseguridad, el 37,5% de las instituciones posee un entorno de simulación básico, utiliza Moodle y algunas herramientas simples prácticas. Sin embargo, este porcentaje de instituciones reportan necesidad y preocupación por fortalecer la parte práctica de la formación en ciberseguridad, enfrentando en este sentido falta de recursos y de herramientas para alcanzar sus metas educativas. Otros elementos que usan las instituciones entrevistadas para la gestión de la parte experimental de los estudios en ciberseguridad son ejemplos de casos prácticos, casos de estudio, proyectos con organizaciones del mercado y resolución de ejercicios en laboratorio, entre otros.

En relación con este aspecto, cabe destacar una crítica común en el área de educación de ciberseguridad, que es el excesivo énfasis en la teoría, lo cual termina privando a los estudiantes de crear las habilidades prácticas necesarias. La teoría sola no prepara a los graduados para las tareas que van a tener que enfrentar en el ámbito laboral. El entrenamiento y la experiencia prácticos son necesarios para equipar a los estudiantes con las habilidades tangibles esperadas en el mercado laboral (Crumpler y Lewis, 2019).

Es importante destacar que Agesic se encuentra en un proyecto de implementación de un Cyber Range con el fin de lograr una plataforma de simulación de ataques que permita la formación y el entrenamiento de profesionales, así como la experimentación, la prueba y la validación de nuevos conceptos, tecnologías, técnicas y tácticas de ciberseguridad y ciberdefensa.

5.5. Modalidad de dictado de cursos en ciberseguridad

El 100% de los centros educativos entrevistados ofrecen opciones formativas en ciberseguridad de forma presencial, siendo tan solo un 25% de estos centros lo que habilitan una opción educativa adicional en formato online en materia de ciberseguridad.

Respecto a estas opciones de educación presencial y/o remota, el investigador de ESET Daniel Cunha Barbosa destaca la enorme contribución de nuestro escenario actual para el aprendizaje autodidacta, lo que podemos observar en la oferta educativa y de calidad que ofrecen plataformas que brindan cursos online masivos y abiertos, además de la cantidad de recursos disponibles en YouTube, sitios web y demás repositorios. Si bien el aprendizaje por cuenta propia es un camino posible y muchos profesionales de la industria se formaron de esta manera, varios profesionales coinciden en el valor de la formación académica (Daniel Cunha Barbosa en Harán, 2019).

5.6. Previsiones a futuro respecto a la formación en ciberseguridad y el cuerpo docente

El 75% de las organizaciones educativas entrevistadas informaron que dictan sus cursos y opciones formativas en ciberseguridad de forma ininterrumpida.

Un 50% ti**ene pensado crear nuevas materias y o cursos a futuro**. Asimismo, el 75% prevé la apertura de más instancias de estos cursos para los próximos años.

Sin embrago, frente a las aspiraciones de continuar creciendo y ofreciendo más cantidad y diversidad de alternativas de estudio, las instituciones encuestadas reportan encontrar principalmente dos impedimentos para ello. El **primero** es la f**alta de recursos (37,5%) tanto sea de docentes calificados como económicos.** En relación con este punto, el 50% de las instituciones concuerdan en cuanto a la **necesidad de ampliar su plantilla docente** para dictar contenidos de ciberseguridad; sin embargo, el 50% de las instituciones identifican como un desafío a la hora de contratar nuevos docentes, la falta de formación y/o experiencia de los perfiles, inclusive más del 50% de estos centros se preocupa por ofrecer capacitación presencial y remota a su cuerpo docente en temáticas de actualización de ciberseguridad.

Adicionalmente, el sueldo requerido por estos perfiles profesionales en relación con los servicios brindados también surge como parte de las dificultades para ampliar el cuerpo docente de ciberseguridad.

Como **segundo** obstáculo para el crecimiento de la oferta educativa en ciberseguridad, se subraya la problemática de los **escases de estudiantes**, un 62,5% de las instituciones encuestadas reportan no contar con una cantidad mínima de estudiantes inscriptos que ameriten la apertura de algunos de sus cursos. En esta línea, Maite Villalba, investigadora y directora del máster en Seguridad de Tecnologías de la Información y Comunicaciones de la Universidad Europea, explica que la falta de promoción de las titulaciones STEM (las carreras de ciencia, tecnología, ingeniería y matemáticas) y la visión de los jóvenes, que consideran que se trata de carreras difíciles, atentan contra la decisión de los jóvenes de emprender estas formaciones (El País, 2019). De igual forma, Gary McGraw (vicepresidente de seguridad tecnológica en Synopsys) expone la necesidad de promover el estudio en el campo de todas las STEM, especialmente, entre las mujeres (McGraw en Armerding, 2018).

Como consecuencia, se subraya la falta de profesionales en estas disciplinas, lo cual implica problemas para las empresas, pero también para los ciudadanos y para el gobierno. Se genera un retroceso en el desarrollo de tecnologías emergentes, ya que los ciudadanos no se atreven a utilizarlas. A su vez, se recalca a nivel mundial una fuerza laboral en ciberseguridad de tan solo un 11% (El País, 2019).

De forma similar, Global Cyber Expertise Magazine destaca que mientras que la demanda de trabajo en el sector de telecomunicaciones, ciberseguridad y TI aumenta; los jóvenes deberían ser motivados a estudiar estas profesiones, lo que podría lograrse a través del desarrollo de iniciativas, programas de entrenamiento y otros (2017).

5.7. Perfil de los estudiantes de ciberseguridad

La mayoría de los centros educativos que participan reportan que los estudiantes o egresados de formación (terciara o universitaria) relacionada a tecnología de la información son el público objetivo de los cursos de ciberseguridad; si bien un porcentaje no desestimable (37,5%) mencionan la participación de un público mixto, en donde se incorporan con interés en seguridad informática y estudiantes de otras disciplinas y campos, destacándose el área de la economía principalmente.

5.8. Oferta de cursos de ciberseguridad a empresas

Las instituciones educativas entrevistadas no brindan cursos específicos de ciberseguridad a empresas del mercado. Generalmente, se imparten conocimientos genéricos del sector TI como parte de la demanda de empresas de diversos rubros entre los que se destaca el financiero y telecomunicaciones.

5.9. Investigación en ciberseguridad

Respecto a la presencia de equipos de investigación dedicados a ciberseguridad dentro de los organismos educativos, se reporta que tan solo la Udelar cuenta con un equipo de investigación dedicado propiamente a la ciberseguridad; las restantes organizaciones o no realizan investigación en la materia o cuentan con profesionales aislados que se involucran en investigaciones relacionadas a ciberseguridad y con la actualización de materiales.

A modo de resumen, es posible destacar los siguientes conceptos calves a partir de los hallazgos:

- La previsión a futuro de continuar dictando las formaciones en ciberseguridad desarrolladas, así como la creación de nuevos cursos y materias vinculadas.
- Escases de docentes cualificados para dictar formaciones de ciberseguridad, lo que, junto a la limitación de recursos, compromete el crecimiento de la oferta educativa en este sector.
- Los perfiles de estudiantes que mayormente optan por formarse en ciberseguridad cuentan con un background de IT, si bien existe cierta tendencia de involucramiento de perfiles de otras disciplinas.
- Necesidad de contar con más cursos específicos de ciberseguridad en las ofertas del mercado y un cuerpo de investigación de mayor porte en materia de ciberseguridad dentro de las instituciones educativas.
- El conocimiento previo en TI, estudios avanzados y/o culminados de ingeniería en sistemas y aprobación de previaturas como requisito de inscripción y acceso a formación en ciberseguridad.
- La necesidad y preocupación reportada por fortalecer la parte práctica de la formación en ciberseguridad.
- Tan solo un 25% de estos centros educativos entrevistados habilitan una opción educativa adicional a la presencial en formato online en materia de ciberseguridad.

6. Bibliografía

Allianz Global Corporate & Specialty. (2019). Allianz Risk Barometer. The 10 Global Business Risks for 2019. Recuperado de: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf

Armerding, T. (9 de octubre de 2018). Cybersecurity: Not Just "A" Job – Many Jobs Of The Future. *Forbes.* Recuperado el 20 de enero de 2020 de: https://www.forbes.com/sites/taylorarmerding/2018/10/09/cybersecurity-not-just-a-job-many-jobs-of-the-future/#6d8da9a93f2b

BID (2019). Fortalecimiento de la Ciberseguridad en Uruguay. Recuperado el 21 de enero de 2020 de: https://www.iadb.org/es/project/UR-L1152

Chang, J. (2020). 101 Impressive Cybersecurity Statistics: 2019 & 2020 Data & Market Analysis. *FinancesOnline.* Recuperado 17 enero de 2020 de: https://financesonline.com/cybersecurity-statistics

Cybercrime Magazine. (2019). Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally by 2021. Recuperado el 21 de enero de 2020 de: https://cybersecurityventures.com/jobs/

Crumpler, W. y Lewis. J. (2019). The Cybersecurity Workforce Gap. Center for Strategic & International Studies. Recuperado de Center for Strategic & International Studies (CSIS): https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf

Deloitte y Nascio. (2018). 2018 Deloitte-NASCIO Cybersecurity Study. States at risk: Bold plays for change. Recuperado de: https://www.nascio.org/wp-content/uploads/2019/11/2018DeloitteNASCIOCybersecurityStudyfinal.pdf

Ellis, A y Bates, S. (2019). CIO Survey 2019. A Changing Perspective. Harvey Nash. The Power of Talent y KPMG. [Publisher]. Recuperado de: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/07/harvey-nash-kpmg-cio-survey-2019.PDF

El Observador (11 de noviembre de 2019). "Uruguay necesita 600 especialistas en ciberseguridad; daños dejan pérdidas millonarias". El Observador. Recuperado el 20 de enero de 2020 de: https://www.elobservador.com.uy/nota/uruguay-necesita-600-especialistas-en-ciberseguridad-2019118144214

El País (16 de enero de 2019). "Se necesitan urgentemente expertos en ciberseguridad: ¿Qué estudiar para ser uno de ellos?". El País. Recuperado el 20 de enero de 2020 de: https://elpais.com/economia/2019/01/14/actualidad/1547486152_048652.html

Global Cyber Expertise Magazine. Volume 4, November 2017. GFCE: Putting Principles into Practice.

Harán, J.M. (2019). Profesionales en seguridad informática: entre la formación académica y la autodidacta. *Welivesecurity.* Recuperado el 17 de enero de 2020 de: https://www.welivesecurity.com/la-es/2019/11/11/profesionales-en-seguridad-informatica-entre-la-formacion-academica-y-la-autodidacta/

ISC. (2018). Cybersecurity Workforce Study. Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens. Recuperado de: https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx

ISC. (2019). Cybersecurity Workforce Study. Strategies for Building and Growing Strong Cybersecurity Teams. Recuperado de: https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

KPMG. (2019). *Consumer Loss Barometer. The economics of trust*. Recuperado de: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/03/consumer-loss-barometer-2019.pdf

National Cyber Security Center (2019). Cyber Security Toolkit for Boards. Recuperado de: https://www.ncsc.gov.uk/collection/board-toolkit

Security (30 de diciembre de 2019). Security Predictions for 2020. Recuperado el 20 de enero de 2020 de: https://www.securitymagazine.com/articles/91442-security-predictions-for-2020

7. Anexo: Metodología

7.1. Objetivo

El presente estudio se realizó entre agosto y diciembre del 2019 en la ciudad de Montevideo a partir de una iniciativa de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC).

Los objetivos de AGESIC en el marco del Estudio de Mercado de Ciberseguridad en Uruguay fueron:

Investigar y conocer el mercado laboral actual de ciberseguridad.

Investigar la potencial demanda de ciberseguridad en el mercado local a futuro.

Conocer lo sectores del mercado en los que potencialmente se espera un crecimiento destacado de la actividad de ciberseguridad.

Relevar y conocer la oferta formativa para ciberseguridad en el sector educativo público y privado.

7.2. Hipótesis e interrogantes iniciales

Se trabajó bajo la premisa de la escasez de profesionales de ciberseguridad dentro del mercado local y la comprensión de la existencia de un bajo grado de madurez de las empresas del mercado local en términos de ciberseguridad. Así como de la necesidad de generar mayor conocimiento y exposición de la oferta formativa en ciberseguridad.

Algunas de las preguntas medulares contempladas a la hora de estructurar la recolección de información fueron las siguientes:

- ¿La organización cuenta con un área dedicada a la seguridad?
- ¿Qué percepción tienen del riesgo a la ciberseguridad?
- ¿Cuáles de las siguientes áreas de ciberseguridad considera más críticas o relevantes para su empresa? (Gobernanza de la Seguridad de la Información, Gestión y Análisis de Riesgos, Auditorías de Seguridad, Concientización y Entrenamiento de Usuarios, Análisis de Vulnerabilidades – Pentesting – Hacking ético, Threat Intelligence Analysis, Monitoreo de Redes – Detección de intrusos, Endpoint Security Management, Respuesta a Incidentes, Análisis Forense, Investigación y Análisis de Malware u Otros)
- ¿Considera que la organización tiene necesidades de ciberseguridad?
- ¿Tiene al menos un especialista en seguridad contratado en la organización?
- ¿Cuáles considera son las cualificaciones más importantes para cubrir los cargos de ciberseguridad?
- ¿Se contratan servicios de ciberseguridad externos a la empresa?
- ¿Hoy en día tienen demanda de perfiles de ciberseguridad?
- ¿Qué sectores contratan servicios de ciberseguridad?
- ¿Qué tipo de servicios de ciberseguridad son los que se contratan o se solicita información actualmente?
- ¿Cuál es la principal restricción que enfrenta a la hora de incrementar su equipo de ciberseguridad?
- ¿Cómo perciben lo que es la oferta educativa de ciberseguridad en Uruguay?

- ¿Cuál es la proyección de crecimiento para su equipo de ciberseguridad en el 2020-2021?
- ¿Cuántos cursos de Ciberseguridad tienen?
- ¿Considera que es necesario abrir más cursos, pero no cuenta con los recursos y/o la cantidad mínima indispensable de estudiantes?
- ¿Necesita ampliar la plantilla de docentes en cursos de ciberseguridad?
- ¿Posee equipos de investigación en temas vinculados a ciberseguridad?

7.3. Metodología para la recolección de datos

AGESIC definió la lista de empresas e instituciones a invitar para que participaran del estudio. Los invitados se agrupan en:

- Empresas nacionales pertenecientes a los sectores: financiero, salud, tecnología y telecomunicaciones.
- Empresas proveedoras de servicios de ciberseguridad.
- Instituciones educativas públicas y privadas.

Se seleccionaron e invitaron a participar a empresas nacionales de los sectores mencionados dado que engloban organizaciones que identifican los riesgos de ciberseguridad como relevantes para el negocio; del mismo modo, se convocaron empresas proveedoras de servicios de ciberseguridad entendiendo que varias empresas locales tercerizan la gestión de la seguridad de la información, lo cual influye en gran medida en la demanda de perfiles de ciberseguridad y en los servicios que se prestan en el sector. Por último, la inclusión de las entidades educativas permite la evaluación de la oferta académica existente y las potenciales demandas formativas en el sector.

A partir de esta selección se extendieron invitaciones para la participación y con aquellas instituciones y empresas que expresaron interés en formar parte del estudio y visualizar resultados, se coordinaron instancias de entrevista para la recolección de datos.

Las entrevistas se condujeron en la mayoría de los casos en modalidad presencial, si bien también fueron utilizados los contactos telefónicos y de videollamada, empleando cuestionarios previamente elaborados para cada caso (empresas nacionales, empresas proveedoras de servicios e instituciones educativas).

Dichas instancias de entrevista fueron llevadas adelante por especialistas en IT, Ciberseguridad y en RRHH de KPMG, entrevistando figuras de niveles gerenciales dentro de las empresas provenientes del área de tecnología y/o ciberseguridad. En el caso de los centros de formación se recurrieron a coordinadores de carrera.

La información recolectada contempló datos estructurados de carácter cuantitativo, así como datos cualitativos espontáneamente compartidos e incorporados a modo de apreciaciones anónimas dentro de este informe.

Algunas de las temáticas abordadas en los cuestionarios formulados fueron:

- Identificación y clasificación del entrevistado.
- Preguntas estratégicas.
- Grado de madurez de ciberseguridad.
- Perfiles de ciber existentes.
- Necesidades a futuro de ciberseguridad
- Servicios de ciberseguridad solicitados.
- Perfiles buscados por las empresas proveedoras de servicios de ciberseguridad.
- Cantidad de recursos dedicados a brindar servicios de ciberseguridad.
- Crecimiento esperado para el área de ciberseguridad.
- Oferta formativa en ciberseguridad.

La totalidad de los datos recolectados fueron estructurados empleando Excel, se homogeneizaron y procesaron empleando diversas herramientas.

7.4. Metodología para el Procesamiento de la Información

El procesamiento de la información se contempló desde el inicio del proyecto, con el fin de determinar qué era lo que se deseaba medir. En ese sentido se utilizó el modelo Goal – Question – Metric (“GQM”) para la definición de mediciones asociadas al objetivo del estudio.

Goal/Objetivo – Objetivo de AGESIC en relación con el estudio del mercado de ciberseguridad en Uruguay. Investigar sobre el mercado laboral actual de ciberseguridad y la potencial demanda a futuro; así los sectores del mercado en donde se espera un crecimiento destacado de la actividad.

Question/Pregunta – Preguntas que permiten entender el estado de situación con respecto al objetivo y que fueron contempladas durante las entrevistas y selección de información secundaria. Por ejemplo: ¿Tiene al menos un especialista en seguridad en la organización?

Metric/Métrica – Conjunto de métricas que permitan responder a las preguntas considerando las empresas entrevistadas durante el trabajo. Por ejemplo: Porcentaje de empresas con especialista en ciberseguridad.

El procesamiento de la información fue soportado con herramientas de data analytics; donde se utilizó como repositorio de datos, las respuestas que surgen de los entrevistados durante el trabajo y se realizaba un análisis descriptivo con herramientas de visualización de datos.

7.5. Resultados

Los resultados luego fueron expuestos en el informe, agrupándolos de la siguiente manera:

- Hallazgos sobre concientización, percepción, fuerza laboral y formación en ciberseguridad.
- Análisis del sector empresarial sin incluir a proveedores de servicios de ciberseguridad.
- Análisis de empresas proveedoras de servicios de ciberseguridad.
- Análisis de instituciones de educación.