Ciberseguridad: empresas, sector público e instituciones de salud

Uruguay – 2022

Línea de base para la evaluación de resultados

Principales resultados

Uruguay Presidencia | agesic

Introducción

Este informe refleja los principales resultados de un estudio de línea de base sobre la situación de la Ciberseguridad en Uruguay, que se continuará de forma periódica para poder analizar la evolución de los principales indicadores sectoriales.

Para ello, se ha relevado información de:

- Empresas
  - Sector manufacturero, comercio y servicios mayores de 20 empleados –excluyendo sector tecnologías de la información (TI)
  - Sector TI
  - Sector financiero
  - Sector servicios de ciberseguridad.
- Instituciones de salud
- Sector público

Consideraciones metodológicas

- Se aplicó una encuesta autoadministrada en los sectores TI, financiero, ciberseguridad y sector público. En el caso de la encuesta a empresas de más de 20 empleados, se aplicó un cuestionario telefónico. Las encuestas fueron enviadas por correo electrónico, con seguimiento por correo y teléfono.

- Las encuestas fueron dirigidas a gerentes y a directores de TI, y fueron aplicadas entre los meses de octubre y diciembre de 2021.

- Si bien es esperable que los consultados ostenten conocimiento en la materia, el cuestionario no tenía definiciones de los términos utilizados. Por ende, es una encuesta de percepción, y los indicadores como, por ejemplo, incidentes de ciberseguridad sufridos, no deben analizarse sin considerar ese detalle.

- El diseño metodológico y las características de cada sector estudiado -tamaño del sector, de las empresas que lo integran, el nivel de digitalización de las mismas, habilidades digitales de las personas que las integran, entre otros-, inhabilita el estudio intersectorial comparado.

Consideraciones metodológicas (ii)

- Dada también la cantidad de casos realizados por sector, que varía enormemente, se deben analizar los casos en contexto. En el caso de sector financiero, por ejemplo, las empresas consultadas representan una porción mayoritaria de la población bancarizada; no obstante, cuantificar a partir de esas empresas consultadas es ciertamente riesgoso, ya que son muy pocas en número y la inclusión –o exclusión- de un solo caso hace variar sensiblemente los datos.

- En vista de que, como se mencionó al principio, este es un estudio de línea de base, el real potencial de análisis del mismo está atado a futuras mediciones.

Empresas privadas

La encuesta de Ciberseguridad en el sector empresas se realizó a partir de **una muestra representativa de las empresas de 20 empleados y más**.

Los resultados se analizan por tamaño y tipo de empresa, según la siguiente distribución:

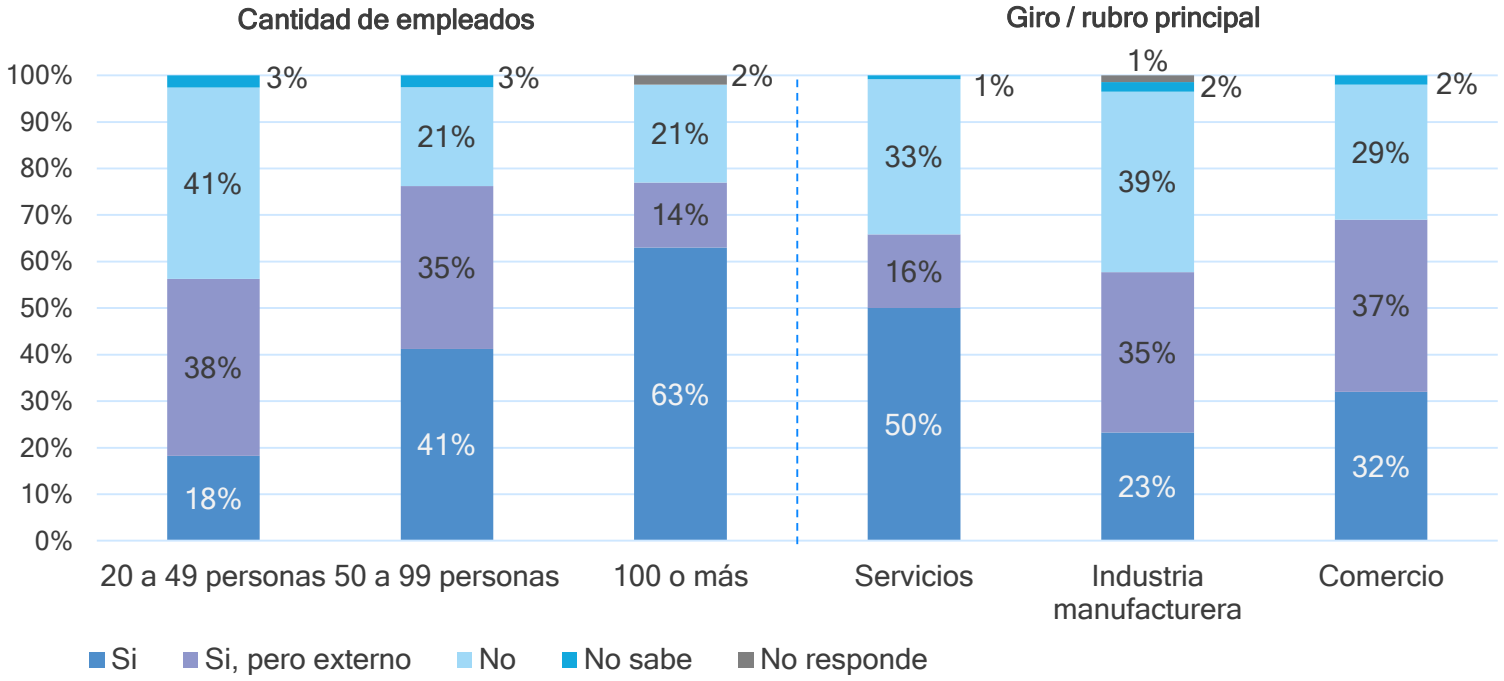
Tamaño

20 a 49 personas – 192 casos
50 a 99 personas – 80 casos
100 o más personas – 100 casos

Rubro / Giro

Servicios - 120 casos
Industria manufacturera – 142 casos
Comercio – 100 casos

Empresas con responsable de tecnología



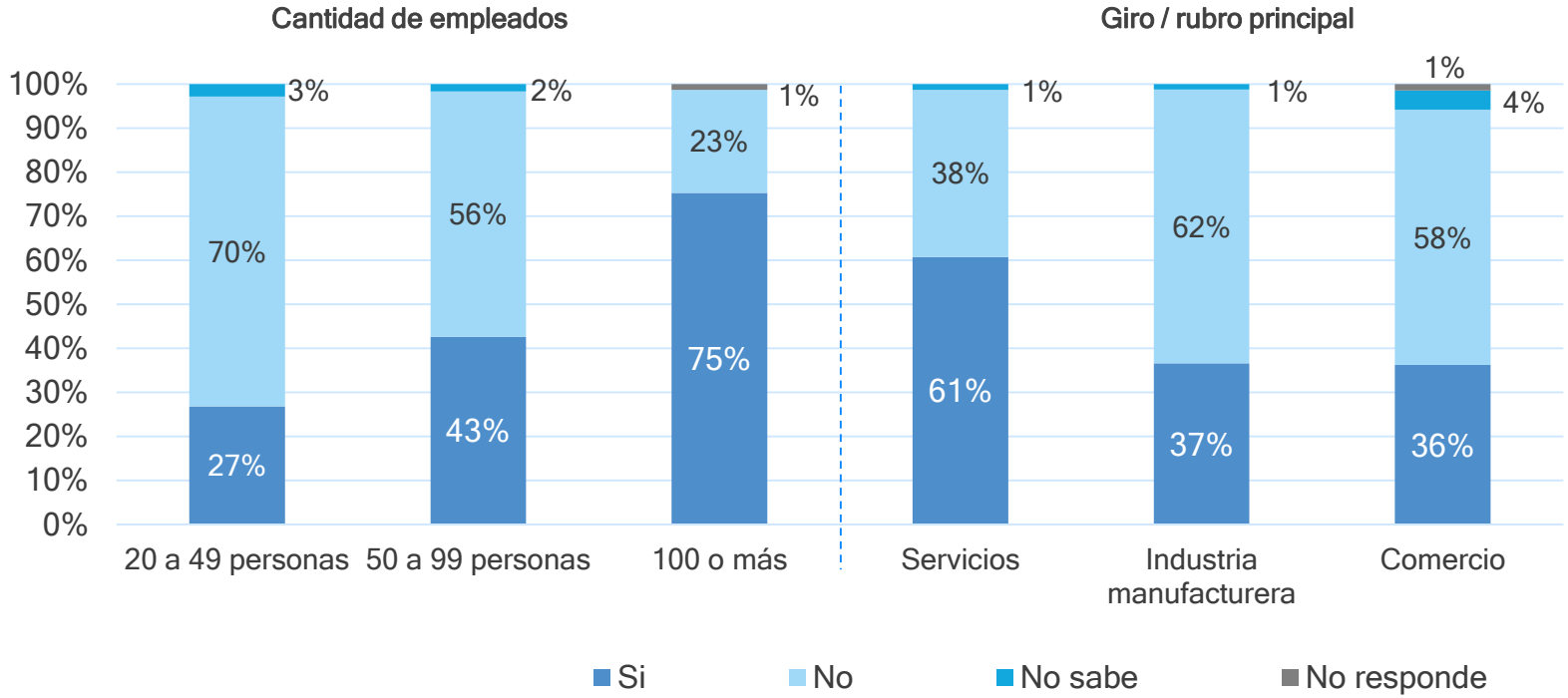
¿La empresa cuenta con un responsable de tecnologías de la información o de informática CTO *Chief Technology Office* o similar?

- La mayoría de las empresas cuentan con responsable de Tecnología (TI), aunque no necesariamente es parte del personal interno de la empresa.

- Como se visualiza en el gráfico, la presencia de una persona responsable aumenta de la mano del tamaño de la empresa. En el caso de las empresas de 100 empleados y más, el 63% cuenta con responsable interno, el 14% lo soluciona con tercerización y el 21% no lo tiene.

- Entre los rubros analizados, el sector manufacturero es el que presenta el porcentaje más bajo.

Empresas con área de tecnología



¿En esta empresa existe un área de tecnologías de la información o de informática?

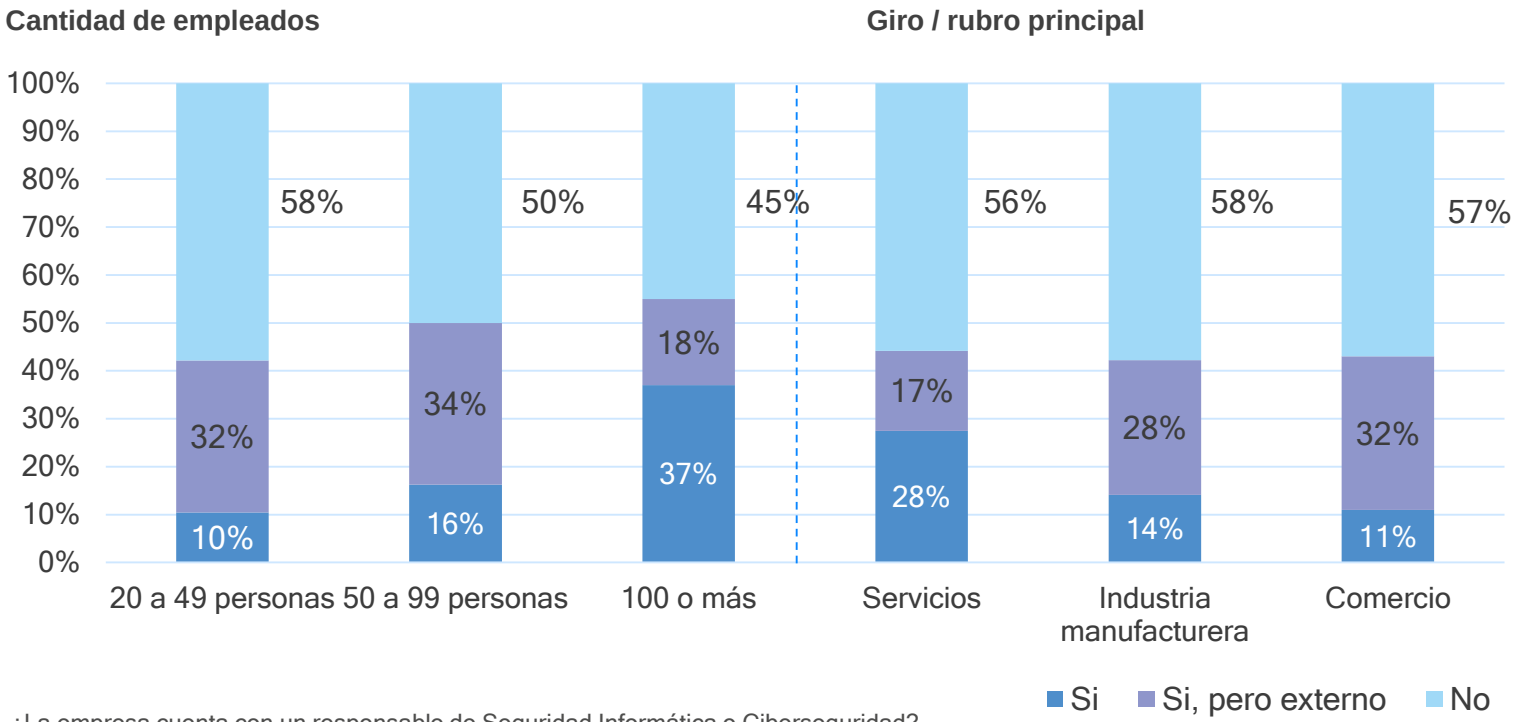
En cuanto a la existencia en la empresa de áreas de TI, se encuentra también muy marcada la correlación con el tamaño de la misma.

- 1 de cada 4 empresas de entre 20 y 49 empleados tiene área de TI.
- 3 de cada 4 empresas de 100 empleados o más, tiene un área de TI.

El **sector servicios* presenta niveles mayores de existencia de área de TI que el de comercio o manufactureras**, con un 61% de sus empresas con esta área frente a 36% y 37%, respectivamente.

*Debemos considerar, como vimos, que no están representados los sectores como tales, dado que la encuesta es a empresas de 20 empleados y más. El sector servicios que se representa aquí es una porción muy específica dentro del sector servicios general.

Empresas con responsable de Seguridad de la Información



¿La empresa cuenta con un responsable de Seguridad Informática o Ciberseguridad?

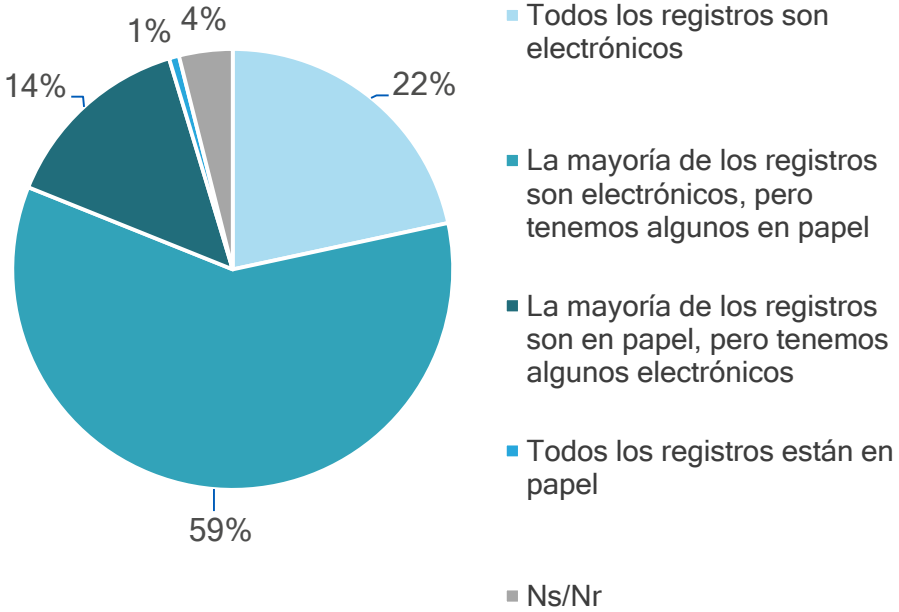
- El responsable de TI y de Seguridad es el mismo en 3 de cada 4 empresas.
- Organismos públicos con responsable de Seguridad: 6 de cada 10 (56% - 9 casos)

Las empresas que cuentan con responsable de Seguridad de la Información (SI) no llegan a ser mayoritarias, en ninguna de las aperturas del análisis con excepción de las de 100 empleados y más. De forma esperable, la proporción de empresas que cuentan con responsable de SI aumenta con el tamaño de la empresa.

Además de eso, a medida que aumenta el tamaño de la empresa también aumenta la proporción de responsables de seguridad que son personal interno de la empresa. En las más chicas (20 a 49 empleados), la tercerización es la forma más frecuente.

En conjunto, la figura de responsable de Seguridad de la Información coincide, en 3 de cada 4 casos, con la de responsable de TI.

Registros electrónicos



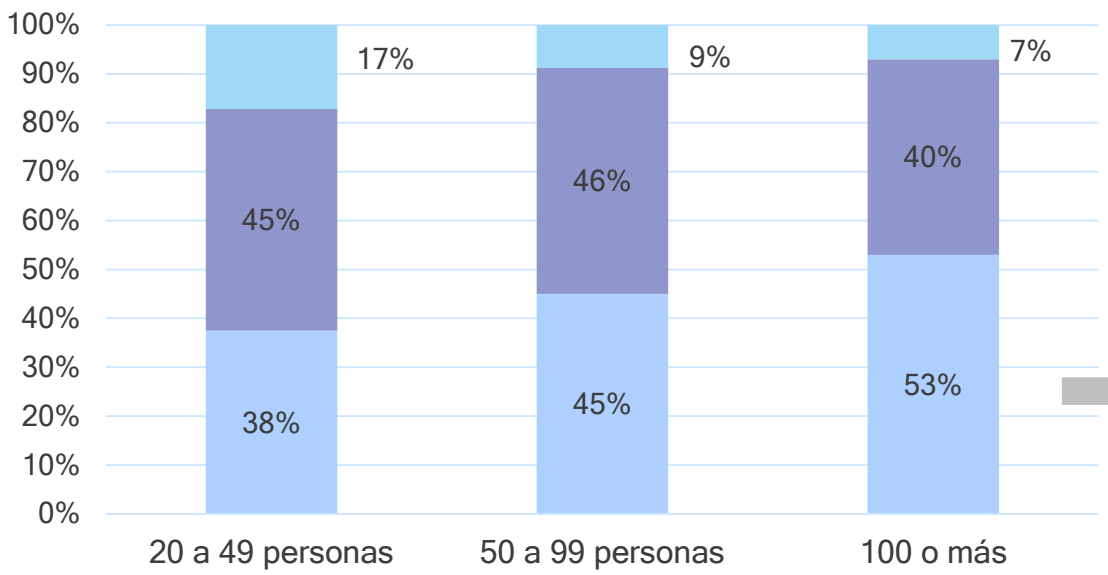
No se perciben diferencias destacables ni significativas por tamaño de empresa o rubro en relación a la forma de generar y almacenar registros.

En la mayoría de las empresas, conviven registros electrónicos y registros papel.

Una quinta parte de las empresas tiene todos los registros electrónicos.

¿De qué forma son almacenados los registros de la empresa como balances, contratos, etc.?

Intranet



Cámara Uruguaya de Tecnologías de la Información (CUTI)

6 de cada 10
accede desde cualquier lugar
(56% - 9 casos)

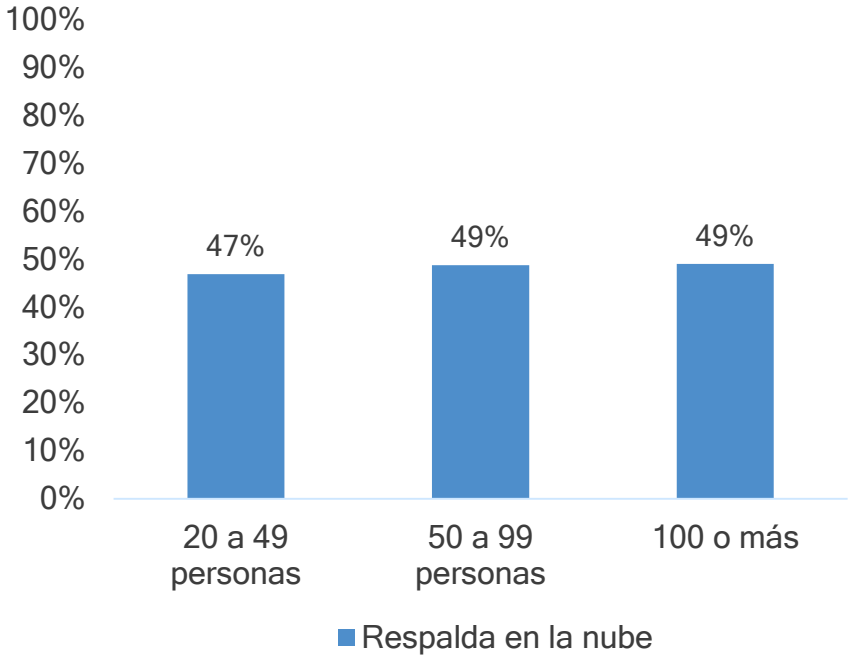
La red interna/intranet de la empresa puede ser consultada...

- La existencia de una intranet, o red interna, es algo muy extendido dentro de las empresas analizadas.

- En las empresas más chicas en estudio el valor es de 83%, mientras que en las de 100 y más empleados llega a 93%.

- Entre la mayoría de empresas que cuenta con intranet, se divide de forma similar la proporción que tiene una intranet que se puede consultar desde cualquier lugar, frente a los que tienen intranet que sólo se consulta desde la empresa.

Backup de la información - Nube



CUTI

75% Respalda en la nube
(12 casos)

No existen diferencias significativas entre los segmentos de empresas estudiados, con excepción de CUTI. De todas formas, las estimaciones para CUTI están apoyadas en un número de casos pequeños que no permite hacer afirmaciones concluyentes.

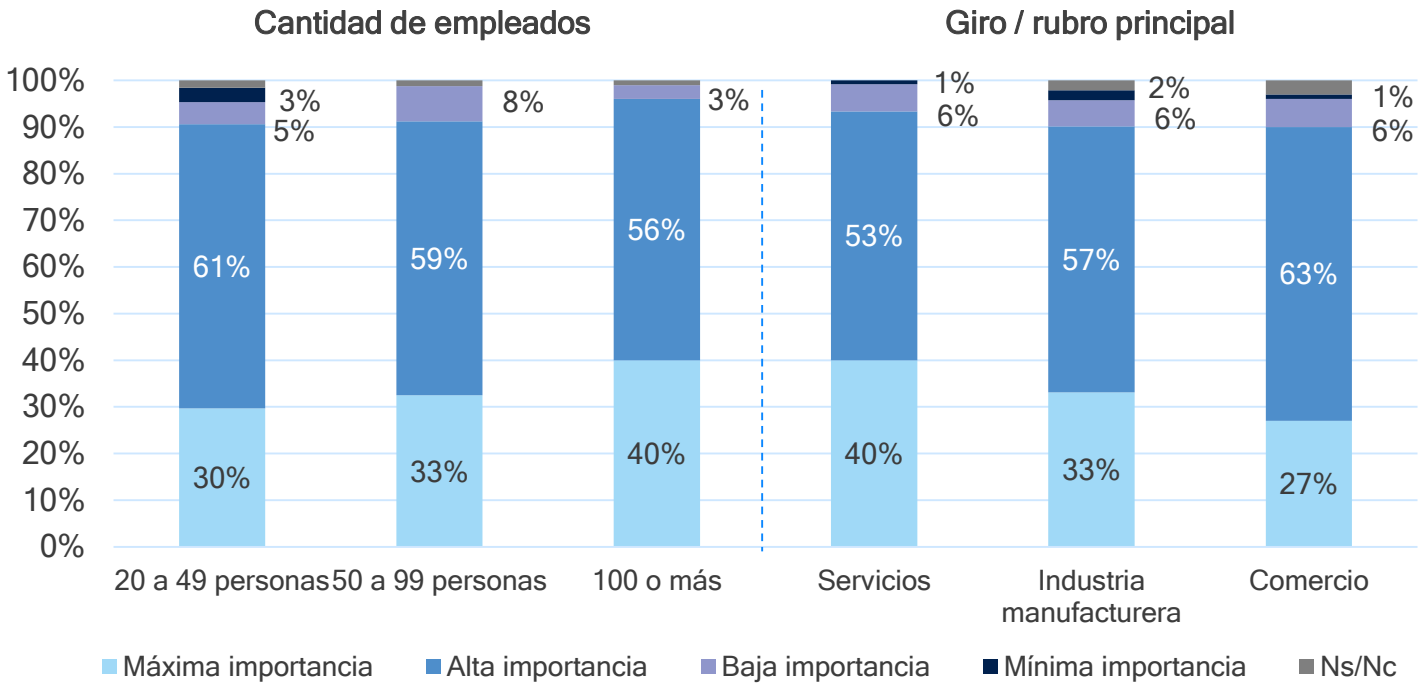
¿La empresa posee alguna de las siguientes estrategias de seguridad y respaldo?

- Todas las empresas utilizan algún tipo de respaldo de la información.

- La mitad de ellas utilizan mayoritariamente la nube como lugar de respaldo, no encontrándose diferencias según el tamaño de la empresa.

- En el caso de las empresas de la Cámara Uruguaya de Tecnologías de la Información (CUTI), el uso de la nube alcanza un 75%.

Importancia percibida de la Ciberseguridad



CUTI

La mitad de los encuestados considera que la seguridad es de *Máxima importancia*, y el resto considera que es de *Alta importancia.*

Pensando específicamente en su empresa y área de negocio, considera que la seguridad informática es algo de...

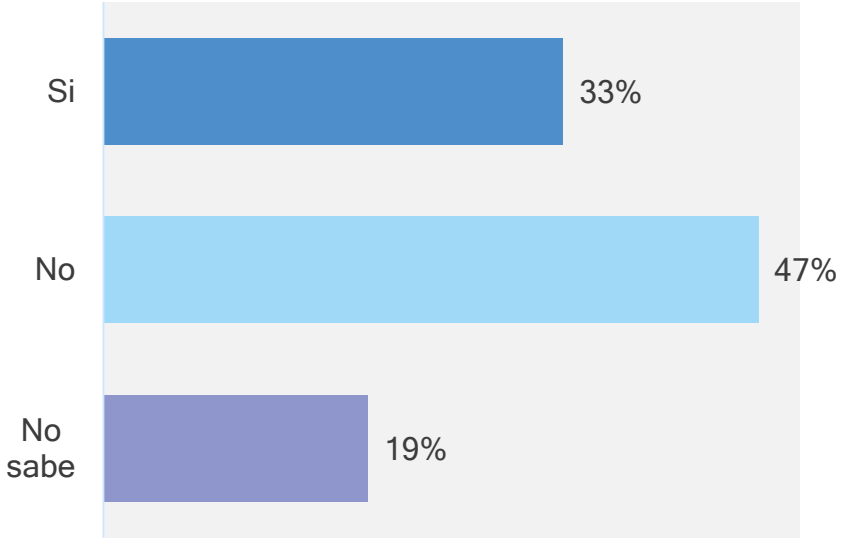
- Todos los entrevistados coinciden en la importancia de la seguridad informática.

- Existen muy leves diferencias según tamaño de la empresa y rubro/giro de la misma, pero en todos los casos la importancia es destacada. Las variaciones se registran entre los que dicen que es de máxima importancia; 30% entre las empresas de 20 a 49 empleados y 40% entre las de 100 y más.

- Las menciones a que la seguridad informática es de mínima importancia son casi inexistentes, y estadísticamente insignificantes.

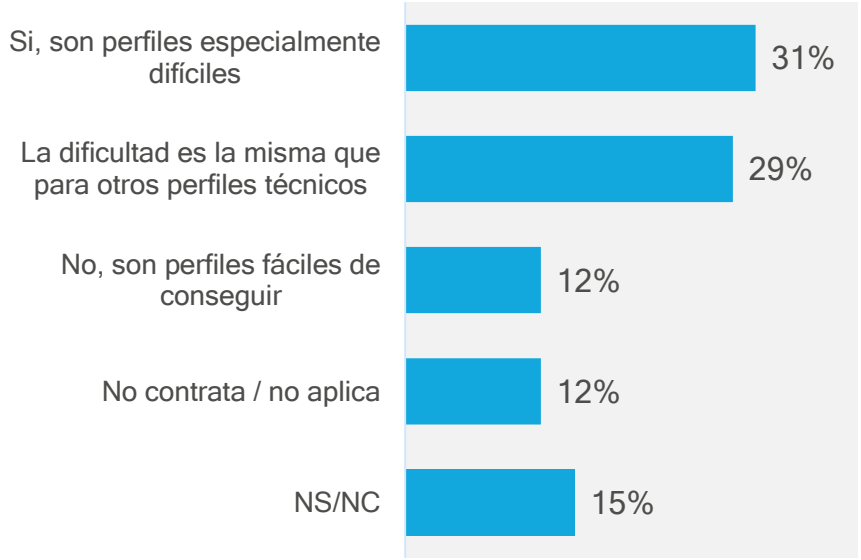
Perfiles de seguridad

Intención de incorporar perfiles



¿Le gustaría poder contratar más profesionales de ciberseguridad?
Total de empresas (372)

Dificultades para contratar



¿Cree usted que es difícil contratar perfiles vinculados al tema ciberseguridad para emplear de forma fija?
Total de empresas (372)

- Un tercio de los encuestados (33%) declara que le gustaría poder contratar más profesionales de seguridad.

- Casi en la misma proporción, un 31% de los encuestados dicen que éstos perfiles son especialmente difíciles de contratar, un 29% cree que son igualmente difíciles que los demás perfiles técnicos, y sólo un 12% cree que son perfiles fáciles de conseguir.

Sector público

La encuesta de Ciberseguridad en el sector Publico se realizó a **16 organismos**.

Muestreo por conveniencia, no probabilístico, no aleatorio, a instituciones relevantes del sector.

Percepción de la Seguridad en los organismos públicos

En su organismo, ¿existe un área o división de seguridad de la información o ciberseguridad?
Si: 9 casos
No: 7 casos

¿Su organismo cuenta con certificación ISO 27001 o se adecua al Marco de Ciberseguridad?
Si: 6 casos
No: 10 casos

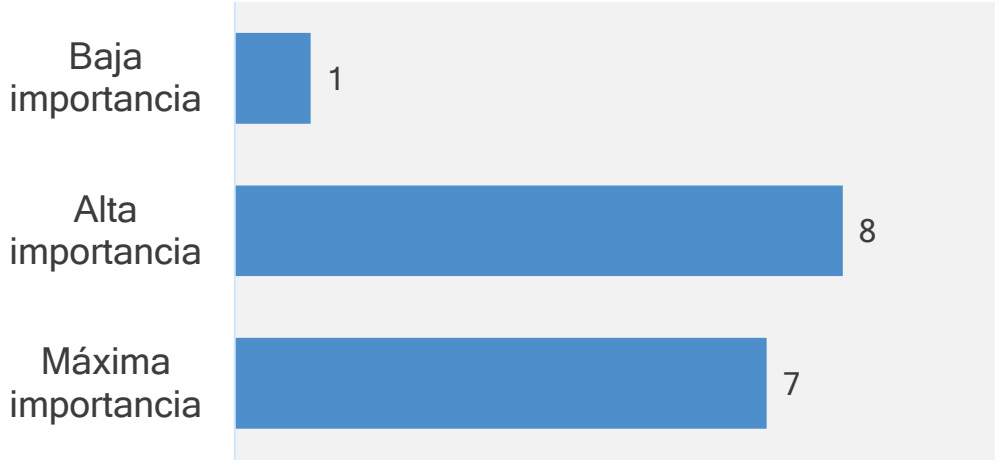
¿El organismo cuenta con un responsable de seguridad informática o ciberseguridad (CISO)?
Si: 9 casos
No: 7 casos

¿Existe en su organismo un equipo de respuesta de incidentes de seguridad o CSIRT?
Si: 6 casos
No: 10 casos

La situación de los organismos públicos respecto de la ciberseguridad está relativamente dividida: por un lado un grupo cuenta con una división específica y un responsable asignado, y otro grupo no las tiene.

6 de los 16 organismos cuenta con un equipo de respuesta a incidentes de ciberseguridad.

Importancia percibida de la Seguridad Informática



La importancia percibida entre los organismos alcanza niveles altos, similares a los vistos entre los encuestados de CUTI y de empresas de 100 empleados y más.

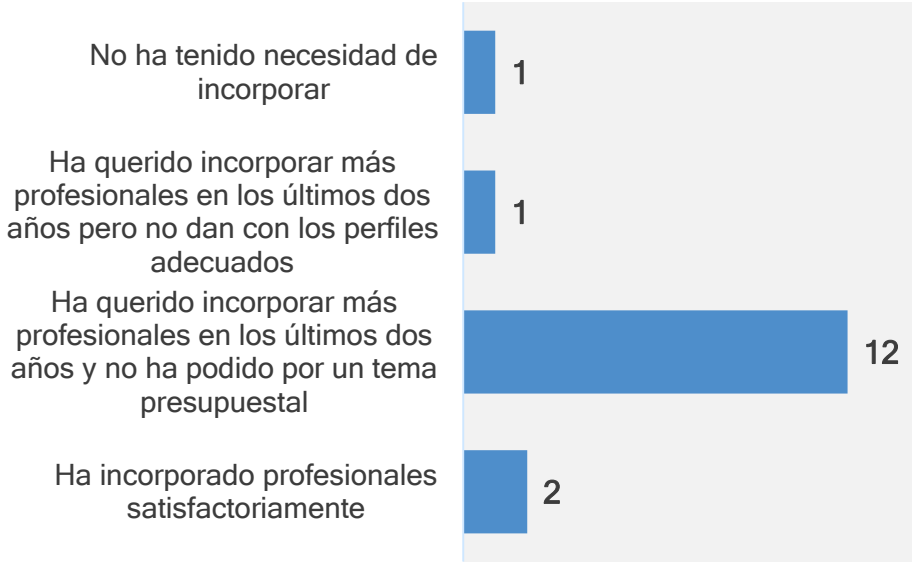
Pensando específicamente en su organismo y sus objetivos, considera que la seguridad informática es algo de...
N: 16 organismos

Mas allá de la existencia o no de una división específica y/o responsables de la temática, existe un consenso claro respecto de la importancia de la seguridad informática en relación a los objetivos de la institución.

La percepción de importancia presenta niveles similares a los encontrados para las empresas de mayor porte (100 empleados y más).

Perfiles de seguridad

Incorporación de perfiles



Respecto de los profesionales de ciberseguridad, su organismo...
N: 16 organismos

Dificultad para contratar

- Sí, son perfiles especialmente difíciles: 10 casos
- La dificultad es la misma que para otros perfiles técnicos: 6 casos

¿Cree usted que es difícil contratar perfiles vinculados al tema Ciberseguridad para emplear de forma fija?
N: 16 organismos

La incorporación de perfiles de ciberseguridad parece ser un desafío para las instituciones públicas.

La gran mayoría de estas organizaciones ha querido incorporar profesionales en estas áreas los últimos tiempos, pero no lo ha conseguido por temas presupuestales.

La mayoría de ellos (10 de 16) entiende, también, que los perfiles de ciberseguridad son específicamente difíciles para emplear de forma fija.

Incidentes de Seguridad

¿Ha tenido incidentes de seguridad en el último año?

Si: 12 casos
No: 2 casos
Ns/Nc: 2 casos

N: 16 organismos

¿Ha reportado al CERTuy los incidentes de seguridad?

Si, en todas las ocasiones: 8 casos
Si, en algunas ocasiones: 4 casos

N: 12 organismos

12 de 16 instituciones consultadas dice haber tenido incidentes de seguridad en el último año.

Aquellos que sufrieron incidentes se contactaron con el CERTuy, al menos para alguno de los incidentes sufridos.

Sector financiero

La encuesta de Ciberseguridad en el sector Financiero se realizó a **6 organizaciones,** a través de una encuesta por correo.

Muestreo por conveniencia, no probabilístico, no aleatorio, a instituciones relevantes del sector.

Estado de situación de la Seguridad en el sector financiero

¿La empresa cuenta con un responsable de tecnologías de la información o de informática (CTO o similar)?

Si: 5 casos
No: 1 caso

¿En esta empresa existe un área de tecnologías de la información o de informática?

Si: 5 casos
No: 1 caso

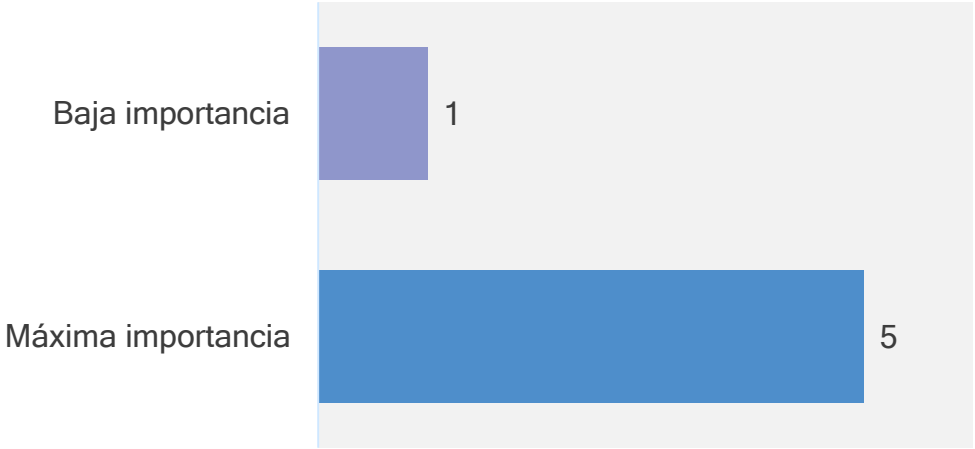
¿De qué forma son almacenados los registros de la empresa (balances, contratos, etc.)?

Todos los registros son electrónicos: 3 casos
La mayoría de los registros son electrónicos, pero tenemos algunos en papel: 3 casos

¿Con qué frecuencia el establecimiento realiza el “backup” o respaldo de la información electrónica almacenada?

Diariamente, formato físico: 5 casos
En la nube: 1 caso

Percepción de la importancia de la Seguridad Informática



La importancia percibida entre los organismos **alcanza niveles altos**, aunque no se pueden establecer comparaciones dada la cantidad de casos

Pensando específicamente en su organismo y sus objetivos, considera que la seguridad informática es algo de...
N: 6 instituciones financieras

Responsable de Seguridad Informática

¿La empresa cuenta con un responsable de seguridad informática o ciberseguridad?

Si: 5 casos
No: 1 caso

¿El responsable de Seguridad Informática, es el mismo que el responsable de TI o de Informática?

No: 5 casos

N: 6 instituciones financieras

N: 5 instituciones financieras

- Las empresas del sector financiero muestran altos niveles de preparación respecto de la Seguridad de la Información.

- En casi todos los casos, existe un área de Seguridad además de un área de Tecnologías de la Información; asimismo, todas ellas cuentan con un responsable de Seguridad específico para esa tarea.

- Esto coincide con la importancia percibida de la temática, en la que prácticamente todos los consultados declaran que la Seguridad es de máxima importancia.

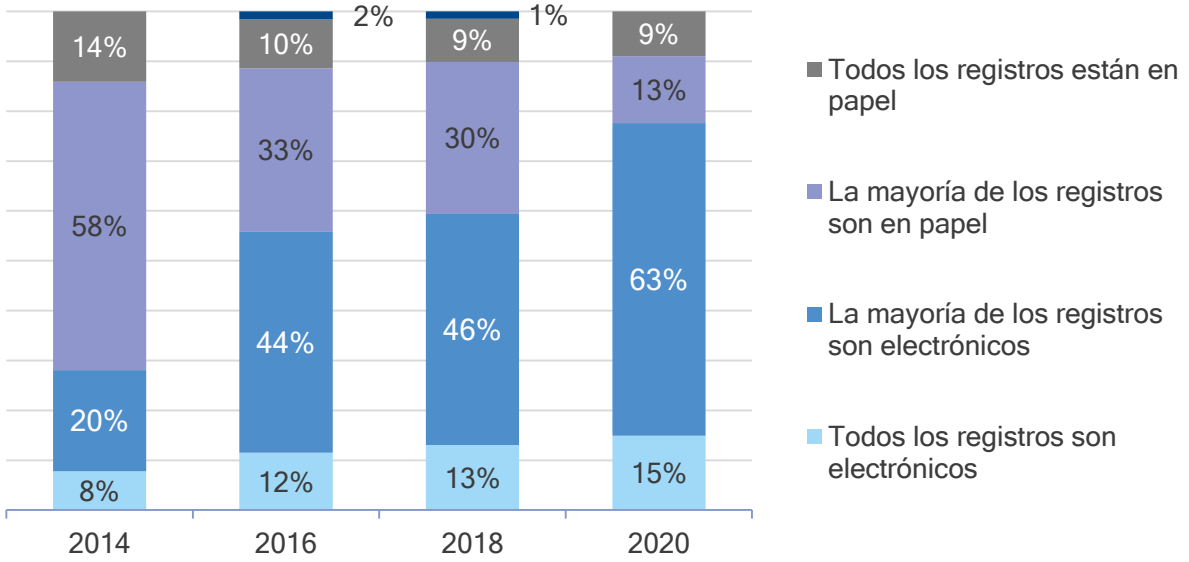
- La gran mayoría, a su vez, cuenta con una estrategia definida de seguridad, procedimientos documentados, planes de continuidad de negocio y estándares de referencia.

Instituciones de Salud

La encuesta de Ciberseguridad en el sector Salud se realizó a **68 prestadores,** a través de una encuesta por correo.

Muestreo por conveniencia, no probabilístico, no aleatorio, a instituciones relevantes del sector.

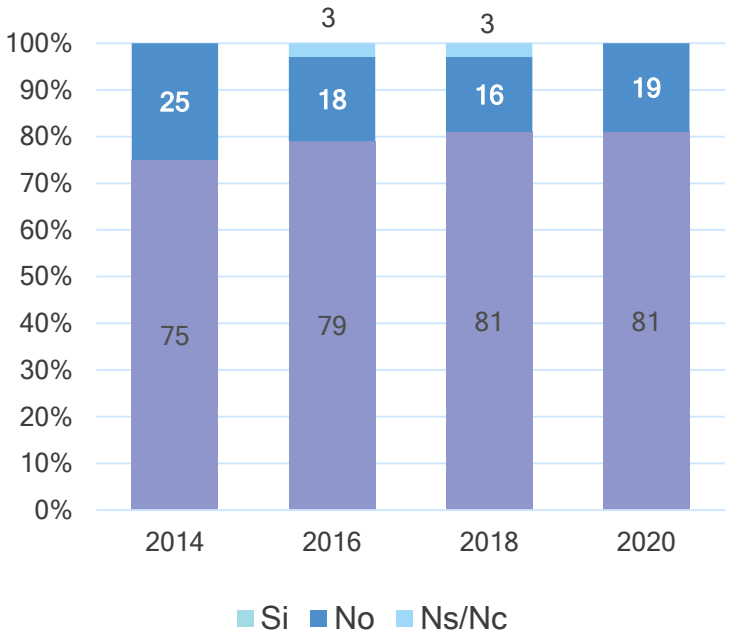
Grado de digitalización de los registros



Si bien existen instituciones que aún registran todo en papel, la tendencia a la digitalización es muy clara; de 2014 a 2020 se triplicaron los prestadores que tienen la mayoría o todos los registros de manera electrónica.

¿De qué forma son registrados los eventos de la historia de los pacientes de esta institución
N: 68 instituciones de salud (TIC y Salud 2020)

Área de Tecnología de la Información



¿En esta institución hay un área de tecnologías de la información y comunicación o informática a nivel central?
N: 67 instituciones de salud (TIC y Salud 2020)

Perfiles de ciberseguridad

% de instituciones que tienen en su equipo de TI personas con formación en seguridad de la información, seguridad informática o ciberseguridad

Año	Total Prestadores	Prestadores Integrales
2018	54%	64%
2020	58%↑	73%↑

¿Cuántas de las personas que trabajan en el área de tecnologías de la información o informática poseen formación en...?
N: 67 instituciones de salud (TIC y Salud 2020) / 41 prestadores integrales

- La gran mayoría de las instituciones de salud cuentan con área de TI, y este dato es de 100% para prestadores integrales. El porcentaje de instituciones que ha incorporado perfiles de ciberseguridad a los equipos de TI es de 58% para el total de los prestadores y de 73% entre los prestadores integrales.

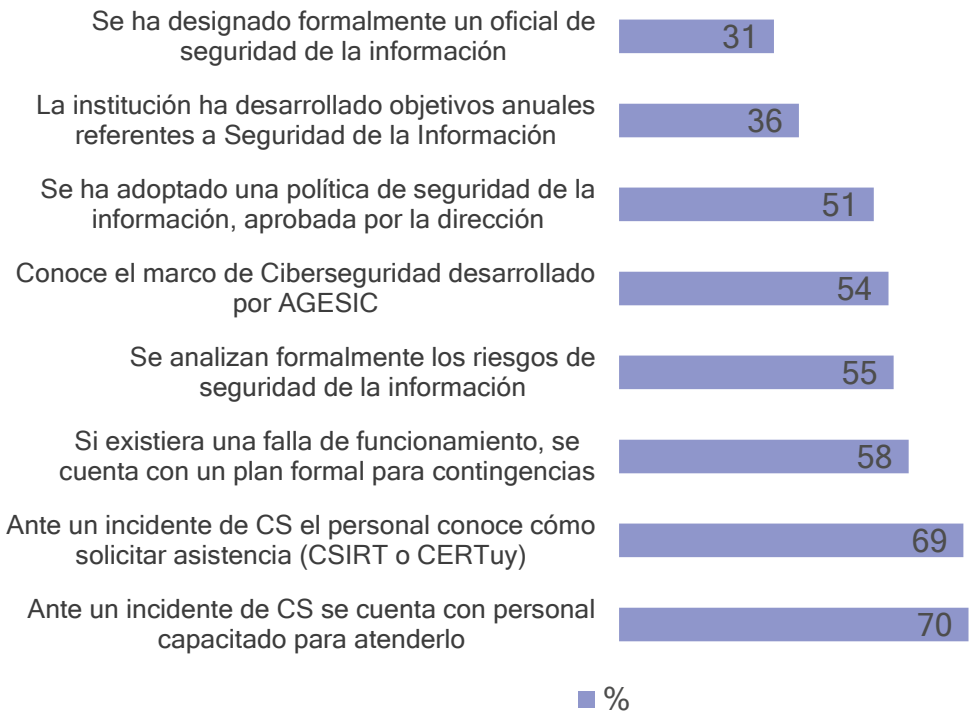
- Independientemente de lo anterior, una gran mayoría cuenta con servicios de TI de guardia las 24 horas del día: 78% del total de prestadores cuentan con este servicio, y entre los prestadores integrales, 9 de cada 10 lo hacen (88%).

Personal técnico de guardia

	TOTAL Prestadores		Prestadores INTEGRALES	
	2018	2020	2018	2020
Si	71%	78%↑	86%	88%
No	17%	12%	10%	5%
No brinda servicios las 24h	3%	3%	2%	5%
NS/NC	9%	7%	2%	2%

¿Tiene personal de TI que atienda las necesidades de la institución las 24h todos los días de manera presencial o a demanda guardia telefónica?
N: 67 instituciones de salud (TIC y Salud 2020) / 41 prestadores integrales

Líneas estratégicas en Ciberseguridad



La adopción de líneas estratégicas declaradas es relativamente alta, pero cae en cuanto se analizan acciones concretas, como por ejemplo, la designación formal del oficial de seguridad de la información (31%).

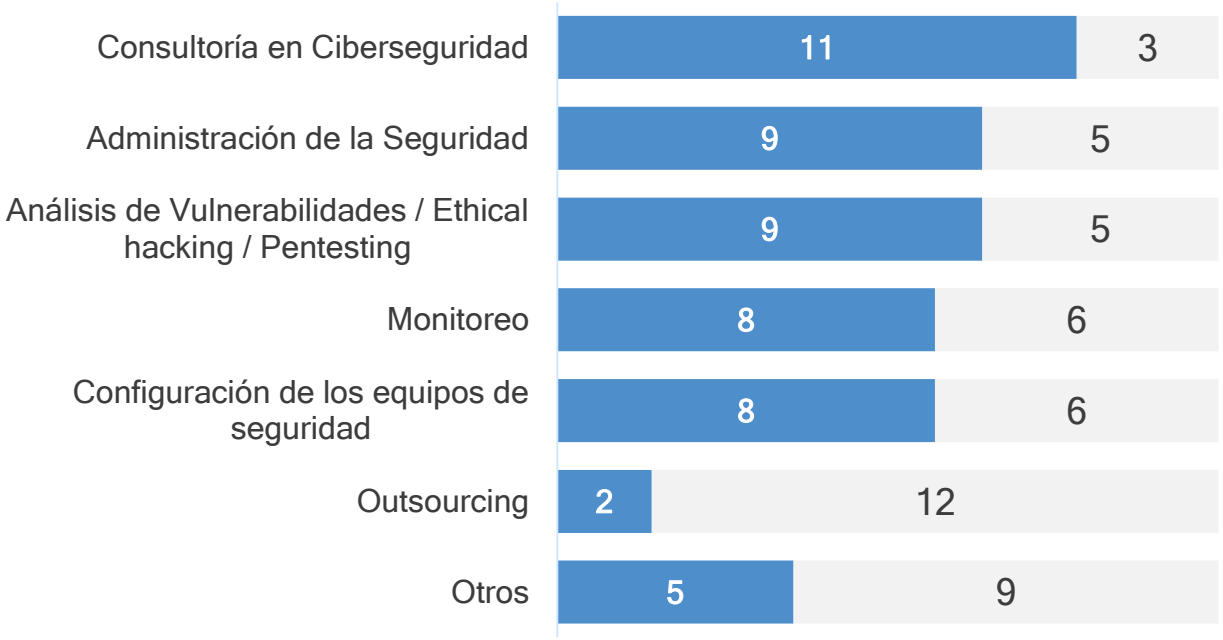
N: 67 instituciones de salud (TIC y Salud 2020) / 41 prestadores integrales

Servicios de ciberseguridad

La encuesta de Ciberseguridad en el sector Empresas vendedoras de servicios de Ciberseguridad, se realizó a **14 empresas,** a través de una encuesta por correo.

Muestreo por conveniencia, no probabilístico, no aleatorio, a instituciones relevantes del sector.

Servicios que provee



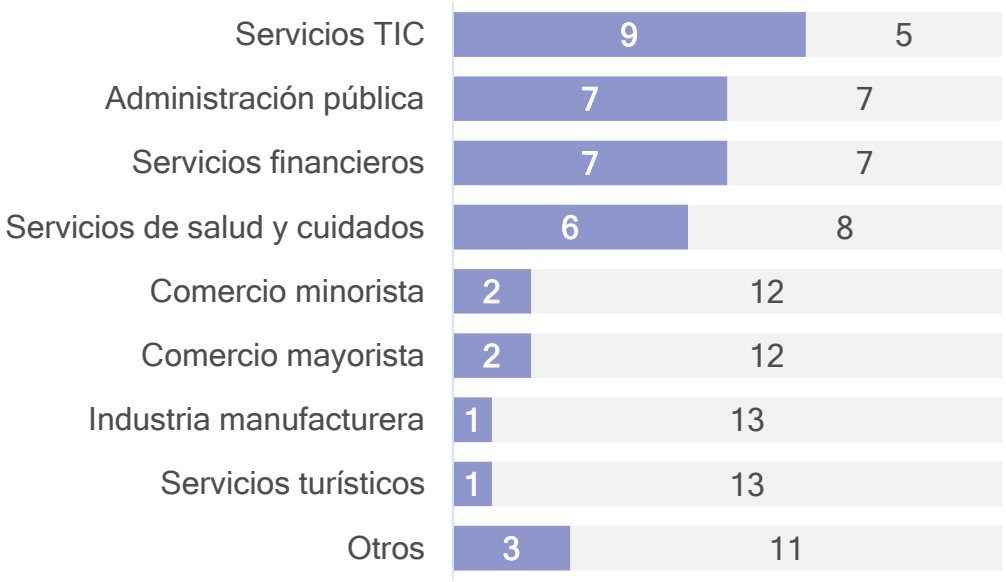
50%
de estas empresas vende servicios en el exterior.

Específicamente, ¿qué tipo de servicios provee/vende? Marque todas las que correspondan.
N: 14 empresas

Entre las empresas vendedoras de servicios de ciberseguridad, las consultorías son el tipo de servicio más comercializado. En segundo lugar, aparecen la administración de seguridad, el análisis de vulnerabilidades, el monitoreo y la configuración de equipos de seguridad.

La mitad de las empresas consultadas vende servicios también al exterior del país, aunque en todos los casos esa venta representa una fracción menor de la facturación total.

Sectores que contratan servicios



¿Qué sectores contratan servicios de ciberseguridad?
Marque todas las que correspondan.
N: 14 empresas

Razones que justifican esa demanda:

Requisitos regulatorios, legales, contractuales: 11
Gestión de Riesgos de las empresas:10
Incidentes: 9
Objetivos de la empresa: 5

¿Cuáles considera que son las razones que justifican la demanda de estos nuevos sectores? Marque todas las que correspondan.
N: 14 empresas

Los sectores que más contratan estos servicios son las empresas de servicios tecnológicos, organismos del sector público, organizaciones financieras y prestadores de salud.

Las razones que justifican esa demanda son varias, pero además de las específicas sobre seguridad para cada empresa o institución, se mencionan requisitos regulatorios, legales o formales que empujan esa demanda.

Perfiles de Ciberseguridad

¿Tuvo rotación de perfiles de ciberseguridad en el último año?

Si: 5 casos

No: 9 casos

¿Cuáles fueron las razones?*

- *"Actualización tecnológica, nuevas skills por tecnologías en los clientes"*
- *"Aumento de la demanda"*
- *"Falta de personal como en el resto de TI"*
- *"Nuevos requerimientos"*
- *"Se han incorporado nuevos colaboradores"*

*Respuestas textuales de los entrevistados

¿Cree usted que es difícil contratar perfiles de ciberseguridad?

- Si, son perfiles especialmente difíciles: **10 casos**
- La dificultad es la misma que para otros perfiles técnicos: **4 casos**

¿Por qué entiende que son perfiles difíciles?

- *"Competencia de otras empresas por los mismos perfiles y escasez de perfiles especializados."*
- *"En general, los especialistas son pocos en este campo y ya se encuentran comprometidos en cargos similares."*
- *"Hay perfiles con muy poca experiencia y perfiles con muchísima experiencia. Es difícil encontrar profesionales con experiencia media y con aspiraciones salariales acordes."*
- *"La capacitación especifica en Ciberseguridad aun está inmadura. La mayoría de los postulantes para estos cargos, son profesionales de TIC que tuvieron alguna experiencia práctica en sus trabajos anteriores."*
- *"Poca experiencia, poca preparación en general."*

¿Por qué entiende que son perfiles difíciles?

- *“Porque requieren de una alta capacitación continua, tanto técnica como de gestión y normativa, para tener un perfil que sepa comprender la problemática de los clientes (no solamente un conocimiento puntual para resolver algo técnico). Para los perfiles junior, si bien hay bastantes propuestas para capacitarse, es fundamental la experiencia y que la persona siempre esté capacitándose."*
- *“Requieren formación específica”.*
- *“Se necesita tener varios años de experiencia previa comprobada para mostrar conocimientos sólidos en seguridad en las áreas de consultoría en ciberseguridad.”*
- *“Sin cargos ya ocupados y con alto grado de demanda.”*
- *“Son muy especializados.”*

Carencias en la formación de recursos en ciberseguridad

¿Entiende usted que existen carencias específicas relativas a la formación en ciberseguridad?

- *Si: 9 casos*
- *No: 2 casos*
- *NS/NC: 3 casos*

¿En qué aspectos cree que hay carencias relativas a la formación en ciberseguridad?

- *“Analistas de seguridad, falta preparación para mitigar riesgos y ataques.”*
- *“Costo de certificaciones. Enfoque específico de las licenciaturas de TIC para ciberseguridad.”*
- *“Escasez de vocaciones científicas y tecnológicas entre los más jóvenes y dificultad para mantenerse capacitado, actualizado o reconvertirse hacia ciberseguridad en los profesionales de mediana edad. La velocidad de la transformación digital que provoca alta demanda de este tipo de profesionales no está acompasada con los ritmos de la formación existente, salvo excepciones (bootcamps, algunas certificaciones, etc.). Asimismo, la formación en ciberseguridad debe ser transversal en todas las profesiones para que los tomadores de decisiones de diferentes industrias comprendan los riesgos, ya que no es un tema tecnológico puro, sino de cualquier ámbito que usa tecnologías, me animo a decir, hoy en día, TODOS.”*
- *“Falta de prácticas operativas y escenarios reales de empresas, más transversal a la organización y no solo orientado a TI.”*

¿En qué aspectos cree que hay carencias relativas a la formación en ciberseguridad?

- *“Hay pocas carreras y formación específica. Hay perfiles muy avanzados, fruto de estudios en el exterior o mucha experiencia en el rubro, y por otro lado, perfiles muy junior con conocimiento específico a partir de alguna certificación o estudio autónomo.”*
- *“No forma parte de la currícula de la Universidad.”*
- *“No hay curso accesibles, ya sea por carga horaria o por aspectos económicos.”*
- *“Poca oferta de formación local.”*
- *“Pocos lugares de entrenamiento.”*

- Un tercio de las empresas consultadas declara tener cierto nivel de rotación de personal, y la mayoría de ellas coincide en que los perfiles de ciberseguridad requeridos son especialmente complejos de contratar.

- Entre las razones esgrimidas, entienden que son perfiles escasos, que requieren de una formación importante y específica, así como cierta experiencia.

- La mayoría de los consultados entiende que existen carencias específicas en la formación de estos profesionales, por escasa oferta o falta de contenidos en la misma curricula (por ejemplo: falta de prácticas operativas).

A modo de síntesis

La preparación de los organismos y empresas consultados está definida, en parte, por el porte de las mismas.

Entre las empresas de mayor tamaño, existe una proporción mayor que cuenta con áreas de TI. Los organismos públicos relevados, todos de más de 100 empleados, muestran un comportamiento similar a las empresas de ese tamaño.

En el caso específico de la existencia de un área de Seguridad Informática, esta situación se ve más marcada entre los segmentos de tamaño de empresas. Los organismos públicos marcan una clara diferencia a favor.

La importancia declarada de la seguridad para la institución o empresa es alta a nivel de todos los sectores consultados. Este punto genera un alto consenso, a pesar de que se perciben grandes diferencias en la preparación efectiva dentro de los segmentos estudiados.

A nivel de incidentes de seguridad, y atendiendo al hecho de que cada entrevistado reportaba incidentes según su propia definición y juicio, se encuentran importantes diferencias entre los segmentos analizados.

El sector público es el que reporta una mayor cantidad de incidentes, pero debe considerarse que es el de instituciones de mayor porte así como el de más capacidad de detección, dada la proporción mayoritaria que cuenta con área de Seguridad de la Información.

Próximos pasos

- Tal como se mencionó al inicio, este estudio constituye una línea de base para conocer la evolución de muchos indicadores estudiados.
- Dado eso, es esperable pensar que mucha de la información hoy relevada cobre otra dimensión a la luz de las futuras mediciones, que permitirían analizar en profundidad algunos datos que hoy son presentados de forma descriptiva.
- La siguiente evaluación esta planeada para realizarse durante el año 2023, y en ella se contempla la medición de una gran mayoría de los indicadores presentados anteriormente.
- Además de repetir los instrumentos aplicados en los segmentos en estudio, se incorporarán nuevos segmentos (por ejemplo, estudiantes de carreras de ciberseguridad) y se agregará una fase cualitativa (entrevistas en profundidad, grupos de discusión).

Muchas gracias

Uruguay
Presidencia

agesic

www.gub.uy/agesic