



O estado da Ciberseguridade en Galicia

Edición 2023



OBSERVATORIO
DA SOCIEDADE DA INFORMACIÓN
E A MODERNIZACIÓN DE GALICIA



AXENCIA PARA A
MODERNIZACIÓN
TECNOLÓXICA DE GALICIA

Índice

1. Introducción	3
2. Metodoloxía	4
2.1 Cidadanía	4
2.2 Empresas	4
2.3 Sector TIC	5
3. Resumo Executivo	6
Conclusións globais	6
4. Ciberseguridade na cidadanía galega	8
4.1 Incidentes de ciberseguridade na cidadanía galega	8
4.2 Cultura da ciberseguridade na cidadanía galega	16
5. Ciberseguridade nas empresas de Galicia	23
5.1 Incidentes de ciberseguridade nas empresas galegas	23
5.2 Cultura da ciberseguridade nas empresas galegas	28
6. O mercado da ciberseguridade en Galicia	30
6.1 O tecido empresarial galego de ciberseguridade	30
6.2 Incidentes de ciberseguridade nas empresas TIC	37
6.3 O teletraballo nas empresas TIC	43
6.4 Talento especializado en ciberseguridade en Galicia	44
7. Glosario de termos	48
8. Índice de gráficos	51

1. Introducción

Este documento **recompila, revisa e analiza os indicadores relacionados coa seguridade da información** dispoñibles nas fontes de información oficiais. Entre eles, o Instituto Nacional de Estatística (INE), o Instituto Galego de Estatística (IGE) e o Observatorio da Sociedade da Información e da Modernización de Galicia (OSIMGA).

Este informe, centrándose na ciberseguridade, busca coñecer o estado global da mesma na Comunidade Autónoma de Galicia . Para iso, e co fin de realizar unha análise máis detallada, o informe estrutúrase en dous grupos diferentes: o estado da ciberseguridade na **ciudadanía** galega e nas **empresas** da Comunidade (nas empresas en xeral e naquelas con actividade no sector TIC).

A Axencia para a Modernización Tecnolóxica de Galicia (Amtega), a través deste estudo no marco das iniciativas do Nodo Galego de Ciberseguridade CIBER.gal, elaborado polo Observatorio da Sociedade da Información e da Modernización de Galicia (OSIMGA), achega un **visión xeral do grao de adopción da ciberseguridade en cada un dos colectivos identificados, a cultura de boas prácticas en ciberseguridade, e como e en que medida os incidentes de ciberseguridade afectan a cada un dos colectivos**, entre outros.

Ademais, dada a relevancia do sector tecnolóxico na creación e implantación de medidas que contribúan a reforzar o nivel de seguridade dixital en Galicia, resérvase un punto específico para recoller e revisar indicadores do mercado laboral da ciberseguridade en Galicia, estruturándose na vertente da oferta e da demanda.

Finalmente, inclúese un glosario de termos empregados neste documento.

2. Metodoloxía

2.1 Cidadanía

Os indicadores que describen a situación da ciberseguridade con respecto á poboación en xeral están elaborados polo Observatorio da Sociedade da Información e da Modernización de Galicia (OSIMGA), adscrito á Axencia para a Modernización Tecnolóxica de Galicia (Amtega), en virtude do Convenio asinado entre o Instituto Galego de Estatística (IGE) e a Amtega.

Os microdatos proceden do módulo da Enquisa Estrutural a Fogares que realiza anualmente o Instituto Galego de Estatística (IGE) e facilita ao OSIMGA, como responsable de realizar o seu procesamento estatístico e análise.

No ano 2022, a enquisa recolleu información de 7.853 fogares galegos nos que residise, cando menos, unha persoa de 16 a 74 anos. Abarca así un total de 15.894 persoas pertencentes a este colectivo.

Nesta enquisa mídese a dixitalización a través da descrición do equipamento e uso das TIC nos fogares galegos nos que residen persoas de 16 a 74 anos e responde aos compromisos de seguimento e monitorización dos principais indicadores de dixitalización da sociedade galega, establecidos na Estratexia Galicia Dixital 2030 da Xunta de Galicia.

A enquisa ofrece datos desagregados por subconxuntos de idade, sexo, zonas xeográficas, hábitat, número de membros do fogar, convivencia no fogar con fillos/as, ingresos do fogar, nivel educativo e situación sociolaboral, obtendo unha perspectiva comparativa das distintas contornas socioeconómicas que conviven en Galicia.

2.2 Empresas

O apartado de empresas analiza detalladamente a información cuantitativa sobre ciberseguridade, tanto para microempresas como para empresas de 10 ou máis traballadores.

Os datos deste apartado obtivéronse no marco do convenio de colaboración asinado entre a Axencia para a Modernización Tecnolóxica de Galicia (Amtega), o Instituto Galego de Estatística (IGE) e o Instituto Nacional de Estatística (INE) para optimizar a recollida de datos relativos á Sociedade da Información nas empresas galegas.

O INE achega así as táboas de resultados para Galicia da Enquisa de uso das TIC e do comercio electrónico nas empresas realizada pola propia organización. A mostra desta operación estatística está formada por 1.473 empresas galegas de 10 ou máis traballadores con actividade en Galicia e 448 enquisas de microempresas galegas.

Ofrécese información diferenciada para dous segmentos de negocio:

- Empresas con sede en Galicia.
- Empresas con actividade en Galicia, aínda que a súa sede social non estea establecida na Comunidade galega.

Ademais, ofrécese información desagregada segundo o número de traballadores, a actividade económica e unha análise por provincias.

2.3 Sector TIC

Neste apartado preséntanse os datos do sector TIC en Galicia, recollidos a través da “Enquisa ás empresas TIC sobre a Sociedade da Información en Galicia”, realizada polo Observatorio Galego da Sociedade da Información e da Modernización de Galicia (OSIMGA), adscrito á Axencia para a Modernización Tecnolóxica de Galicia (Amtega).

O estudo inclúese no Programa Estatístico Anual da Comunidade Autónoma de Galicia para o ano 2022 e ten como obxectivo caracterizar o sector empresarial TIC galego, xa que é un sector estratéxico no desenvolvemento económico de Galicia e o seu efecto impulsor no conxunto do tecido empresarial.

A enquisa realizouse entre as empresas TIC galegas segundo os criterios metodolóxicos que se presentan a continuación:

- Ámbito territorial: Galicia.
- Universo: empresas e persoas físicas con actividade en Galicia, dedicadas a actividades relacionadas coas Tecnoloxías da Información e da Comunicación agrupadas en 5 grupos (Manufactureiras, Comerciais TIC, Telecomunicacións, Actividades Informáticas e Outros Servizos TIC).
- Tipo de enquisa: entrevista autoadministrada a través da web ou coa presentación dun cuestionario por correo postal, apoiada por teléfono ou persoalmente para a súa cobertura.
- Tamaño da mostra: 444 entrevistas.
- Asignación multietapa: estratificada proporcionalmente na primeira fase, en función do volume de emprego e da actividade específica da empresa TIC; nunha segunda fase, selección aleatoria da unidade de mostraxe dentro de cada un dos estratos definidos.
- Erro de mostraxe: cun nivel de confianza do 95,5% (2 sigmas) e $p=q=0,5$ como caso máis desfavorable, a marxe de erro de mostraxe para toda a mostra é de 4,3%.
- Traballo de campo: do 2 de maio ao 29 de xuño de 2022.

3. Resumo Executivo

Conclusións globais

Uso de ferramentas e medidas de seguridade:

A medida de seguridade para protexer o teléfono móbil máis habitual é o **pin ou patrón de desbloqueo**, cun uso do 90,4% da cidadanía galega. O uso da **pegada dixital ou outros datos biométricos** é a medida de seguridade que máis aumenta dende 2018 ata 2022, ata acadar o 50,4%.



Facer regularmente copias de seguridade da información persoal é a acción máis realizada para protexer a información. De entre a poboación que usou Internet no último ano en Galicia, o 49% leva a cabo esta acción, seguida da negación de permisos do uso da información persoal para fins publicitarios.

Nas empresas de máis de 10 traballadores/as é onde máis medidas de seguridade TIC se empregan, sendo un 86% das empresas con sede en Galicia. A medida máis empregada polo conxunto de empresas é a **autenticación mediante contrasinal forte**.



Apréciase unha tendencia negativa nos últimos dous anos no emprego de medidas de seguridade TIC nas empresas. Dende o ano 2020 ata o ano 2022 o emprego das medidas que se analizaron na enquisa evolucionou dende un 67,5% ata un 52% no caso das pequenas empresas.

O 96,9% das empresas TIC empregan medidas de seguridade que se analizan e, entre estas medidas, destacan **manter o software actualizado incluíndo o sistema operativo**. Outras medidas relevantes entre as empresas TIC son a **autenticación mediante contrasinal forte** e **copia de seguridade de datos nunha ubicación separada**.



Risco e materialización de incidentes de ciberseguridade:



A maior nivel de estudos maior é o risco de sufrir un incidente de ciberseguridade. Son as persoas con estudos de nivel superiores as que sofren máis incidentes deste tipo, pero tamén as que usan de forma máis frecuente e avanzada os servizos e produtos de internet.

Existen grandes diferenzas entre as principais cidades galegas na probabilidade de que os internautas sufran algún incidente de ciberseguridade coñecido. Pontevedra é a cidade de Galicia coa probabilidade máis alta, alcanzando unha cifra superior ao 75%, mentres que en Ferrol é onde menos probabilidade existe, cun porcentaxe do 42%.



Menos dun 5% das empresas de 0 a 9 traballadores/as con sede en Galicia tiveron algún incidente de ciberseguridade no último ano. Esta porcentaxe aumenta cando aumenta o tamaño da empresa e sitúase ao redor dun 16% nas empresas con máis de 10 traballadores/as

Ao longo do ano 2022, aproximadamente un 25% das empresas TIC de Galicia sufriron un incidente de seguridade informática.



4. Ciberseguridade na cidadanía galega



O 70,3% das persoas galegas usuarias da internet afirman que posúen coñecemento sobre o uso e funcións das cookies.

Un 58% da poboación actualiza periodicamente os produtos de seguridade informática



Entre as persoas galegas usuarias da internet, unha cifra próxima ao 27% asegura que sufriu algunha estafa ou intento de estafa nos últimos 12 meses.

Durante o ano 2022, pouco máis da metade da poboación galega con acceso a internet tivo algún incidente de seguridade nos seus dispositivos electrónicos.

Existe unha gran variedade de accións de protección empregadas polos cidadáns, dende restrinxir o acceso á súa localización xeográfica ata cambiar periodicamente o contrasinal do wifi do seu domicilio.

As Administracións Públicas, no seu labor de garantir que os cidadáns poidan exercer os seus dereitos, realizan tarefas de sensibilización e formación en materia de ciberseguridade. Con isto preténdese evitar que os riscos na navegación pola rede se materialicen, provocando graves consecuencias.

Co obxectivo de reflectir a situación actual en Galicia no que respecta ao uso de ferramentas e servizos de seguridade nos dispositivos privados dos usuarios, estúdanse os datos do ano 2022 tendo en conta as características sociais, económicas e xeográficas. Isto permítenos coñecer como impacta a cultura da ciberseguridade na poboación e que aspectos hai que reforzar no futuro co obxectivo de construír contornas seguras.

4.1 Incidentes de ciberseguridade na cidadanía galega

Enténdese por incidente de seguridade a aparición dun ou varios eventos que ameazan a confidencialidade, integridade, dispoñibilidade, autenticidade e trazabilidade da información. As consecuencias deses incidentes poden ser varias, como a subtracción de bens, o acoso, a extorsión ou a difusión de información persoal e confidencial.

Estes incidentes pódense producir pola existencia de vulnerabilidades que son explotadas, intencionadamente ou non, por terceiros. Tamén incluiremos a perda ou falta de accesibilidade a información por accidentes e avarías, sen o respaldo de seguridade axeitado. Entre os incidentes máis habituais atópanse infeccións por malware, roubo de información, espionaxe cibernética ou suplantación de identidade.

En ocasións, estes incidentes provocan graves prexuízos ás persoas que os sofren cunha reparación difícil. Por iso, a prevención mediante o uso de ferramentas de seguridade é un factor fundamental para evitar que se materialicen.

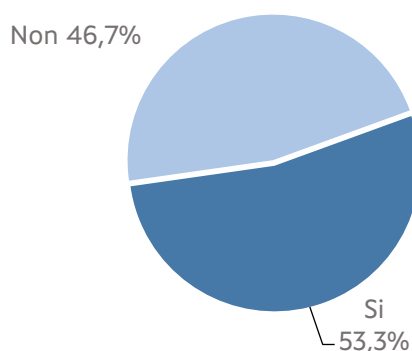
4.1.1 Incidencias rexistradas no colectivo da cidadanía

Durante o ano 2022, máis da metade da poboación internauta (o **53,3%**) da poboación galega que utilizou Internet declara que sufriu algún tipo de incidente de ciberseguridade nos seus dispositivos electrónicos. A última vez que se fixo esta enquisa detallada sobre ciberseguridade foi en 2018 e entón só o 28,5% declarara que sufrira algún incidente, a cifra case foi duplicada neste tempo.

Con todo, esta cifra debe ser tomada con precaución, xa que moitos destes incidentes pasan desapercibidos aos ollos dos usuarios e poden mostrar as súas consecuencias tempo despois de que se produzan. A cultura da ciberseguridade tamén implica maior capacidade de identificación dos incidentes a ameazas.

G. 1. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses

(% sobre as persoas de 16 a 74 anos que utilizaron Internet nos últimos doce meses)

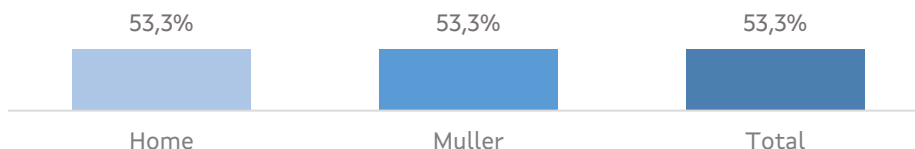


Fonte: OSIMGA + IGE (2022)

O xénero non é un factor determinante que condicione sufrir un incidente cibernético xa que non existen diferenzas significativas no impacto sufrido que identifican homes e mulleres.

G. 2. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses, segundo o sexo

(% do total de persoas de entre 16 e 74 anos que utilizaron Internet no último ano)



Fonte: OSIMGA + IGE (2022)

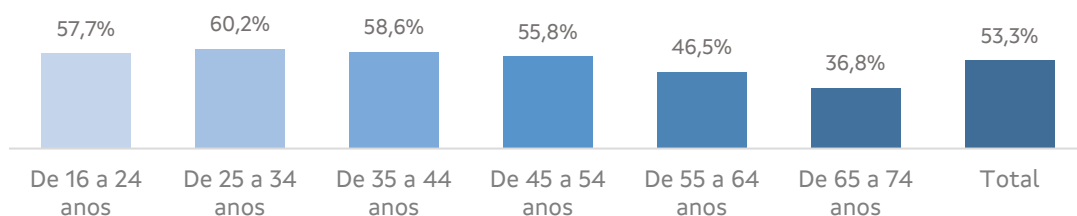
Canto maior sexa a exposición a Internet, a probabilidade de sufrir un incidente cibernético tamén aumenta considerablemente. **Só o 36,8% das persoas maiores de 65 anos usuarias de Internet, sufriron algún tipo de incidente nos últimos 12 meses**, sendo o valor máis baixo de todas as franxas de idade. En certa medida, este fenómeno

pode estar relacionado co feito de que o uso de Internet e da tecnoloxía por esta parte da poboación é menor e menos sofisticado que a que tenden a facer usuarios máis novos. É dicir, están menos expostos.

O colectivo de persoas **entre 25 e 34 anos** está á cabeza **dos que sufriron o maior número de incidentes de seguridade** en 2022, **o 60,2% da poboación**. Para explicar esta situación, enténdese que existen outros factores determinantes que inciden nesta casuística, como posuír competencias dixitais avanzadas, a prudencia adoptada e ser ou non nativo dixital.

G. 3. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses, segundo a idade

(% do total de persoas de entre 16 e 74 anos que utilizaron Internet no último ano)

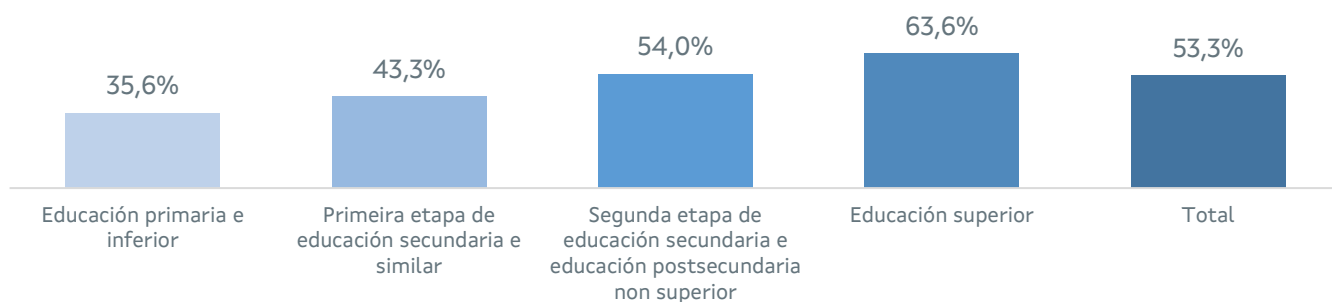


Fonte: OSIMGA + IGE (2022)

A nivel educativo superior, aumenta o número de incidencias sufridas. O uso da Internet é maior a medida que se avanza cara a contornas académicas superiores, polo tanto, a exposición aos riscos asociados aumenta. No lado oposto sitúanse aquelas persoas con educación primaria ou niveles de estudo inferiores, que presenta a cifra máis baixa.

G. 4. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses segundo estudos

(% sobre as persoas de 16 a 74 anos que utilizaron Internet nos últimos doce meses)



Fonte: OSIMGA + IGE (2022)

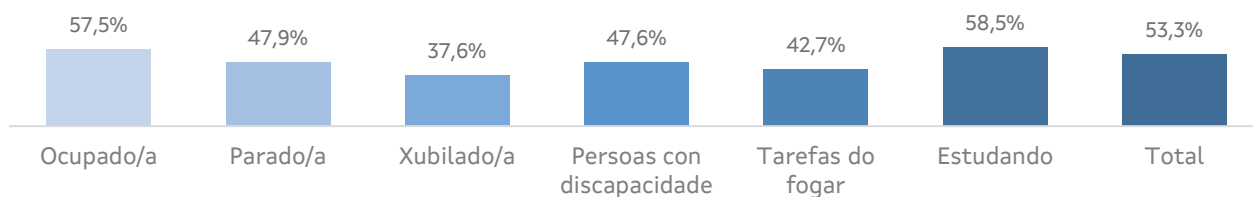
Tendo en conta a **situación social e laboral das vítimas deste tipo de incidentes, os/as estudantes e os ocupados/as están en cabeza** con maior porcentaxe de incidentes, seguidos dos que están en paro e das persoas con discapacidade. As

diferenzas entre as dúas últimas non son significativas xa que en ambos os casos aproxímanse ao 48%.

As persoas que realizan tarefas domésticas e os xubilados son os colectivos que menos incidencias deste tipo sufriron, nunha porcentaxe de case o 43% e 38% respectivamente.

G. 5. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos de uso privado nos últimos 12 meses segundo a súa situación sociolaboral

(% do total de persoas de entre 16 e 74 anos que utilizaron Internet no último ano)



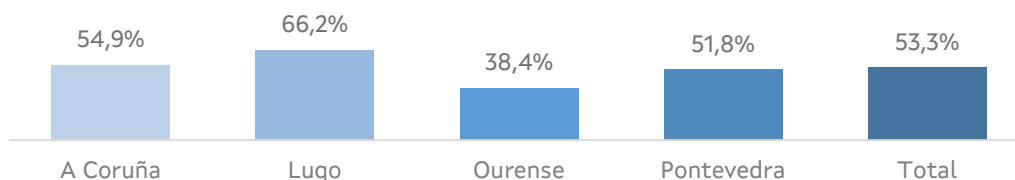
Fonte: OSIMGA + IGE (2022)

A pesar de que o uso de ferramentas de seguridade nas catro provincias galegas é similar, existe certa disparidade en canto aos incidentes de ciberseguridade producidos. **Lugo está á cabeza xa que algo máis do 66% dos enquisados sufriron algún incidente.**

A continuación, sitúanse no medio A Coruña e Pontevedra con cifras superiores ao 50%. Por último, Ourense é a provincia onde se producen menos incidencias, cunha incidencia de algo máis do 38%.

G. 6. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos de uso privado nos últimos 12 meses segundo a provincia

(% do total de persoas de entre 16 e 74 anos que utilizaron Internet no último ano)



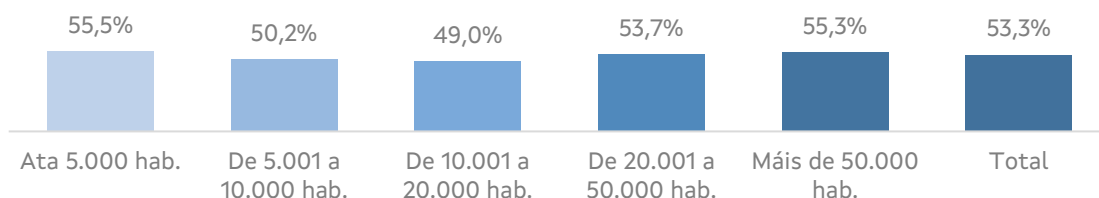
Fonte: OSIMGA + IGE (2022)

A pesar de que as cifras son similares en todos os tipos de hábitat, os municipios con menos de 5.000 habitantes teñen unha maior incidencia de ciberseguridade, cun 55,5%.

Séguenlle os municipios de máis de 50.000 habitantes, co 55,3%, ata o mínimo do 49% no caso dos núcleos de poboación de entre 10.001 a 20.000 habitantes.

G. 7. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos de uso privado nos últimos 12 meses, segundo o tipo de hábitat

(% do total de persoas de entre 16 e 74 anos que utilizaron Internet no último ano)



Fonte: OSIMGA + IGE (2022)

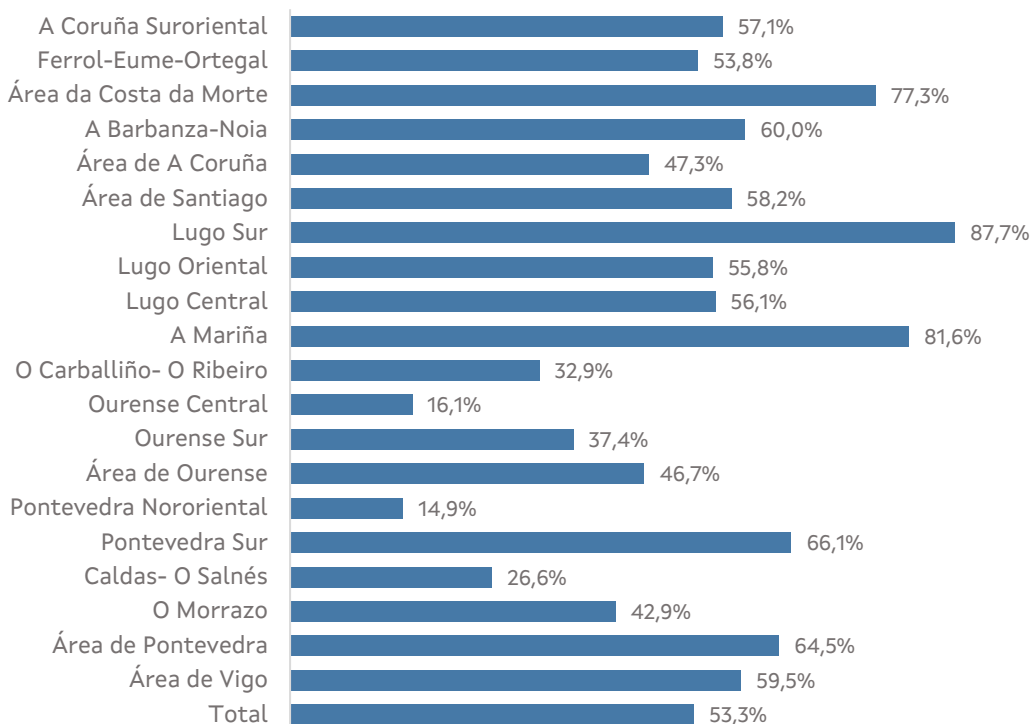
Pódense observar diferenzas significativas na distribución do número de incidencias de ciberseguridade dos internautas en función das distintas zonas de poboación.

Lugo Sur e A Mariña presentan a maior porcentaxe de poboación que sufriu un incidente, sendo as únicas zonas que superan a barreira do 80%.

No extremo oposto sitúanse **Pontevedra Nororiental e Ourense Central, que non chegan nin ao 20% dos incidentes** entre a súa poboación.

G. 8. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses por Área

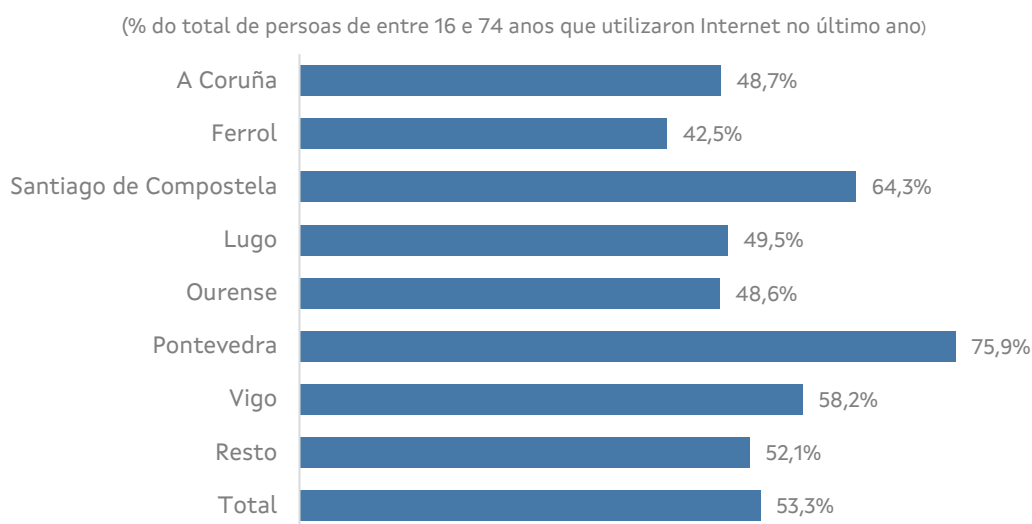
(% do total de persoas de entre 16 e 74 anos que utilizaron Internet no último ano)



Fonte: OSIMGA + IGE (2022)

Entre as sete principais cidades de Galicia preséntansenos diferenzas significativas en canto á probabilidade de sufrir un incidente de ciberseguridade. Por unha banda, **Pontevedra lidera este ranking cunha porcentaxe do 75,9% da poboación internauta que foi vítima dun incidente de seguridade no último ano**, mentres que Ferrol é a cidade con menos incidencias, cun 42,5%.

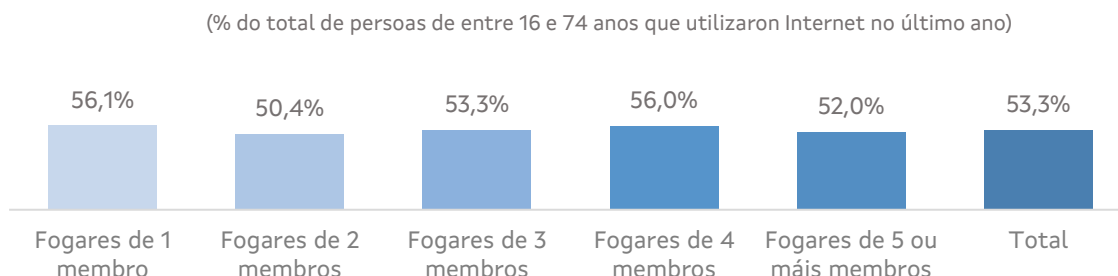
G. 9. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos de uso privado nos últimos 12 meses nos 7 concellos de maior poboación



Fonte: OSIMGA + IGE (2022)

Segundo o número de persoas que viven nun fogar, varía a probabilidade de sufrir un incidente de ciberseguridade, aínda que a tendencia non é clara. Por unha banda, están **os fogares unipersoais e os fogares de 4 membros, que son os que sufriron máis incidencias de seguridade**, arredor do 56%. No extremo oposto sitúanse os que están formados por 2 persoas, cunha proporción do 50,4%.

G. 10. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses segundo o número de persoas no fogar

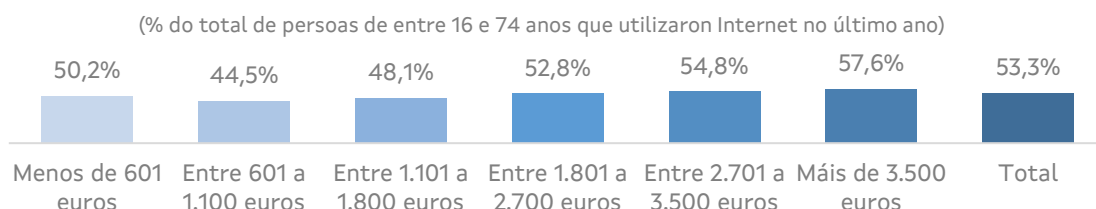


Fonte: OSIMGA + IGE (2022)

En xeral, e con algunha excepción, co aumento no nivel de ingresos das persoas usuarias da Internet que sofren incidentes de seguridade, aumenta tamén a probabilidade de identificar que se sufriu incidentes de ciberseguridade. As persoas con ingresos entre 601 e 1.800 euros sófrenos en menor proporción. Pola contra, os que teñen **ingresos**

superiores a 3.500 euros son os que **máis sufriron** este tipo de incidentes no último ano cunha porcentaxe do 57,6%.

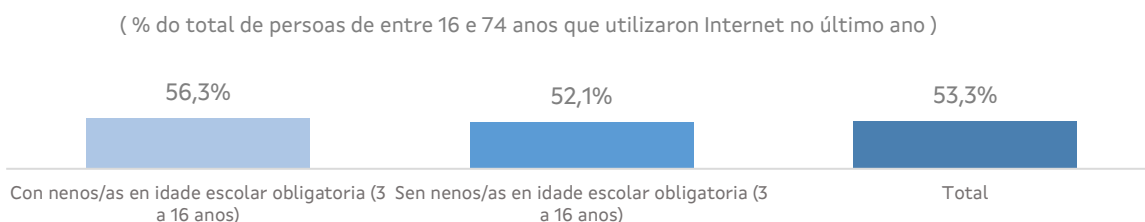
G. 11. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses segundo o nivel de ingresos do fogar



Fonte: OSIMGA + IGE (2022)

Ter fillos en idade escolar ten que ver coa idade e tamén coas necesidades de dixitalización no fogar. **As persoas con nenos/as en idade escolar superan en 3 puntos a media de incidentes de ciberseguridade, acadando o 56,3%.**

G. 12. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses segundo convivan con nenos



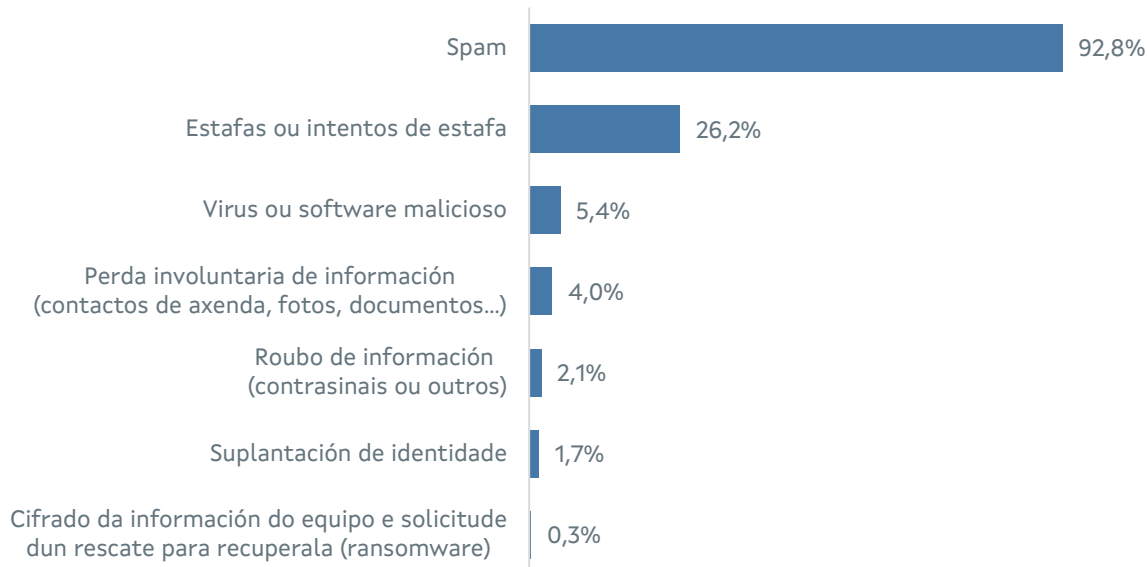
Fonte: OSIMGA + IGE (2022)

O incidente máis común entre a cidadanía galega que tivo algún problema de ciberseguridade é o spam ou correo malicioso, detectado polo 92,8% das persoas que sufriron algún incidente de ciberseguridade. Ademais, un 26,2% afirma que experimentou unha estafa ou un intento de estafa. Estes dous incidentes son os máis comúns durante este ano. A estafa ou intentos de estafa, sufriu un aumento de 18,7 puntos porcentuais dende 2018.

Os virus ou software malicioso e a perda involuntaria de información son incidentes menos comúns en comparación cos anos anteriores, xa que afectan a menos do 6% da poboación internauta con incidentes de ciberseguridade. É destacable a forte baixada da incidencia de software malicioso e da perda de información, a menos da terceira parte do detectado en 2018.

G. 13. Tipo de incidente de seguridade que sufriu en internet nos últimos 12 meses

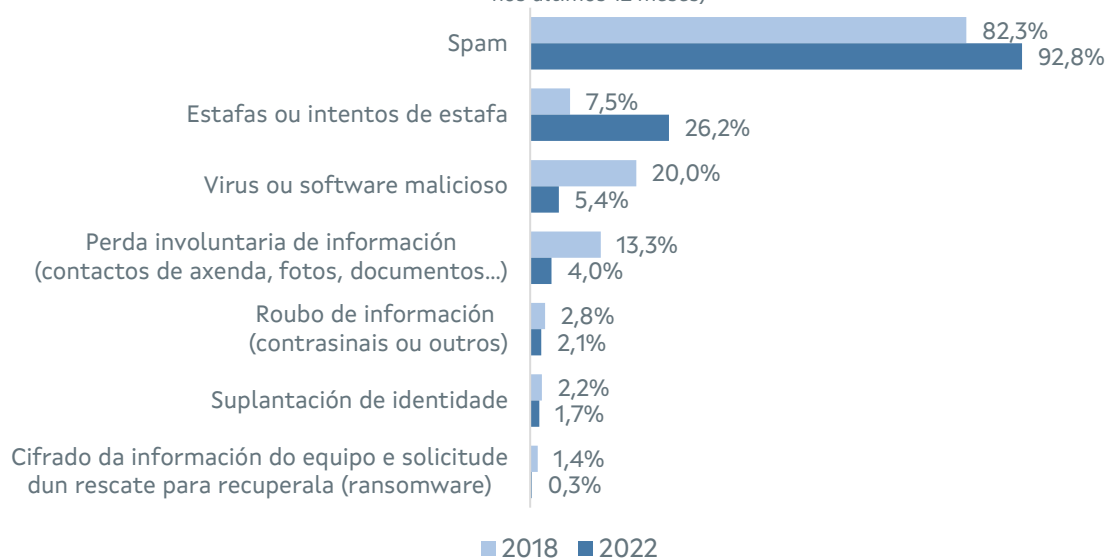
(% sobre o total de persoas de 16 a 74 anos que sufriron algún incidente de seguridade en internet nos últimos 12 meses)



Fonte: OSIMGA + IGE (2022)

G. 14. Tipo de incidente de seguridade que sufriu en internet nos últimos 12 meses. Evolución 2018-2022

(% sobre o total de persoas de 16 a 74 anos que sufriron algún incidente de seguridade en internet nos últimos 12 meses)



Fonte: OSIMGA + IGE (2022)

4.2 Cultura da ciberseguridade na cidadanía galega

Construír unha cultura da ciberseguridade que implique á cidadanía galega é un dos obxectivos prioritarios das políticas públicas. Coñecer a preocupación ou o nivel de coñecemento da poboación na materia, permite medir o grao de importancia que lle outorga unha sociedade.

As medidas e actuacións adoptadas pola cidadanía para combater ou previr posibles incidentes de ciberseguridade, actúan como un termómetro da vulnerabilidade ou fortaleza da poboación ante posibles ciberataques.

As competencias que posúe a poboación galega en materia de seguridade dixital mostran o avance cara a unha cultura da ciberseguridade arraigada no día a día.

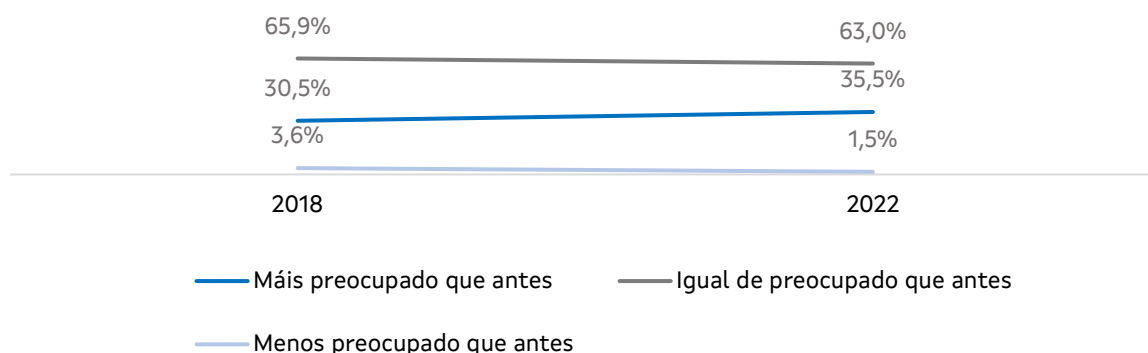
4.2.1 Nivel de preocupación pola ciberseguridade

Pódese comprobar que a poboación galega durante o ano 2022 amósase máis preocupada que no ano 2018 con respecto a seguridade de Internet, estando o 35,5% máis preocupada que antes.

Un 5% máis de poboación afirma estar máis preocupada que antes en temas de ciberseguridade (pasa do 30,5% ao 35,5%) mentres que se reduce nun 2% a que di estar menos preocupado en 2022 (do 3,6% ao 1,5%).

G. 15. Evolución do grao de confianza no uso de Internet en Galicia (Evolución 2018-2022)

(% sobre as persoas de 16 a 74 anos que utilizaron Internet nos últimos doce meses)



Fonte: INE (2022)

4.2.2 Principais medidas e actuacións adoptadas pola cidadanía en materia de ciberseguridade

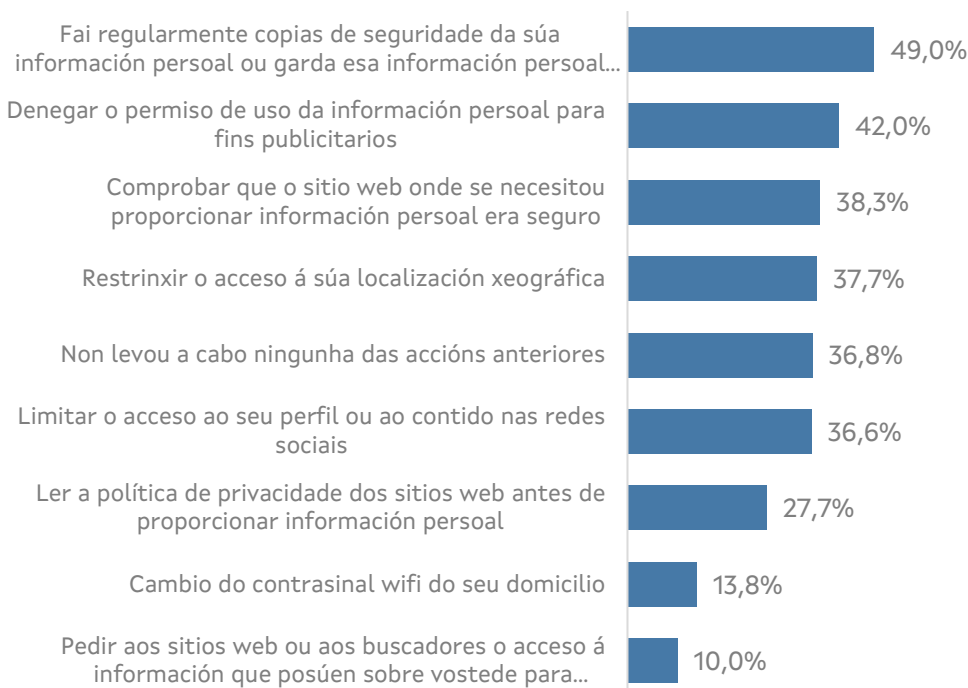
Facer regularmente copias de seguridade da súa información persoal é a acción que os galegos e galegas habitúan a desenvolver con máis frecuencia no que se refire a ciberseguridade.

Outra medida moi popular é **denegar o permiso de uso da información persoal para fins publicitarios**, onde a porcentaxe de poboación que leva a cabo este tipo de medida aumentou con respecto ao ano 2018 (dun 35,4% a un 42%).

Diminúe a porcentaxe de persoas que **non aplican ningunha das accións descritas**; mentres que no ano 2018 esta porcentaxe era dun 46,3% durante o ano 2022 esta porcentaxe baixa ata un 36,8%.

G. 16. Accións levadas a cabo para protexer o acceso a súa información persoal en internet nos últimos 12 meses

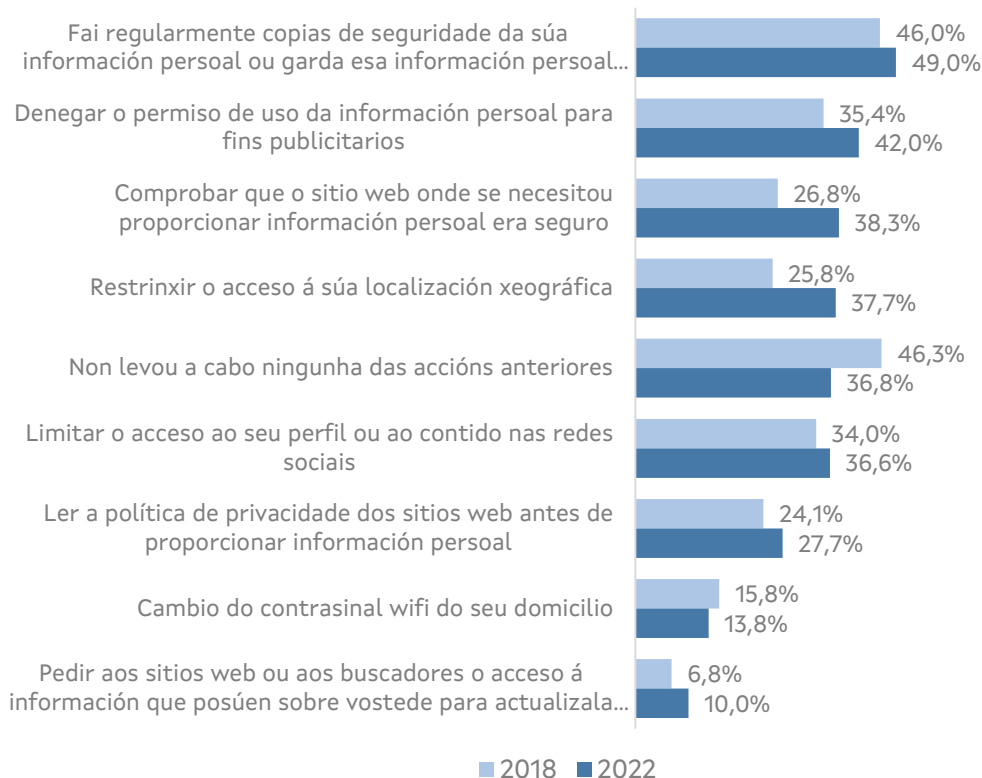
(% sobre o total de persoas de 16 a 74 anos que usaron internet nos últimos 12 meses)



Fonte: OSIMGA + IGE (2022)

G. 17. Accións levadas a cabo para protexer o acceso a súa información persoal en internet nos últimos 12 meses, evolución dos datos de 2018 a 2022

(% sobre o total de persoas de 16 a 74 anos que usaron internet nos últimos 12 meses)



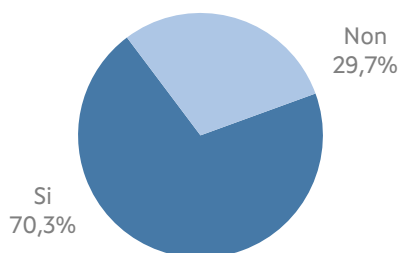
Fonte: OSIMGA + IGE (2022)

En Galicia, un 70,3% da poboación afirma saber como funcionan as cookies. Por outra banda, algo máis do 30% da poboación internauta galega realizou algunha modificación na configuración das cookies para restrinxilas.

G. 18. Porcentaxe de persoas que coñecen o funcionamento das cookies e/ou realizaron modificacións na configuración das cookies

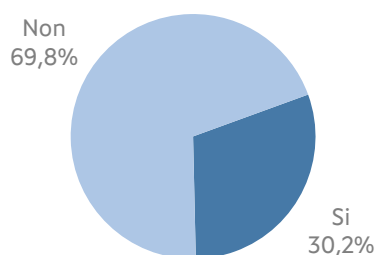
Coñecemento do uso e función das cookies

(% sobre as persoas de 16 a 74 anos que utilizaron Internet nos últimos doce meses)



Configuración do navegador de internet para previr ou limitar a cantidade de cookies

(% sobre as persoas de 16 a 74 anos que utilizaron Internet nos últimos doce meses)

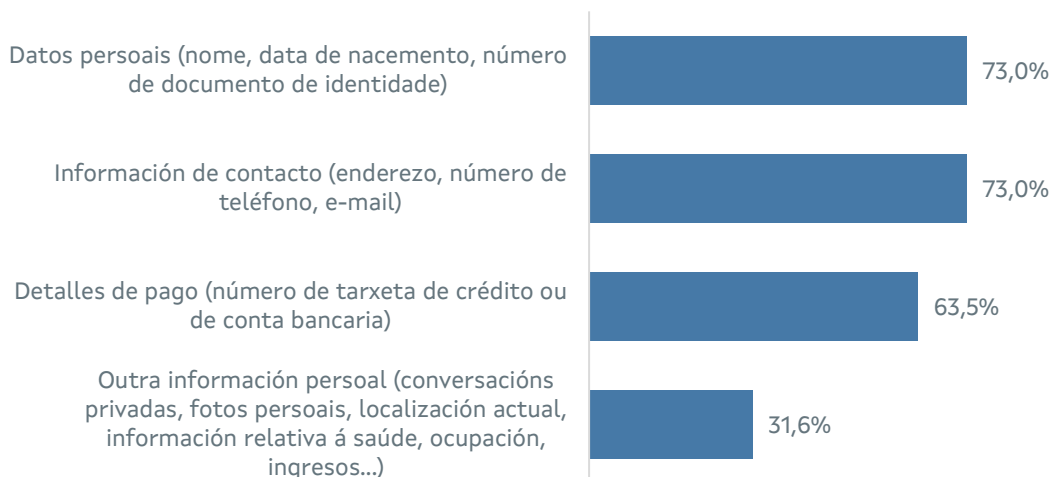


Fonte: OSIMGA + IGE (2022)

Os datos persoais e a información de contacto son as principais informacións persoais que os usuarios proporcionan a través de internet (un 73%). Por outra banda, un 63,5% proporciona **detalles de pago**, como o número da tarxeta de crédito ou a conta bancaria, e un 31,6% afirma ter dado **outro tipo de información persoal**.

G. 19. Información persoal proporcionada a través de internet nos últimos 12 meses

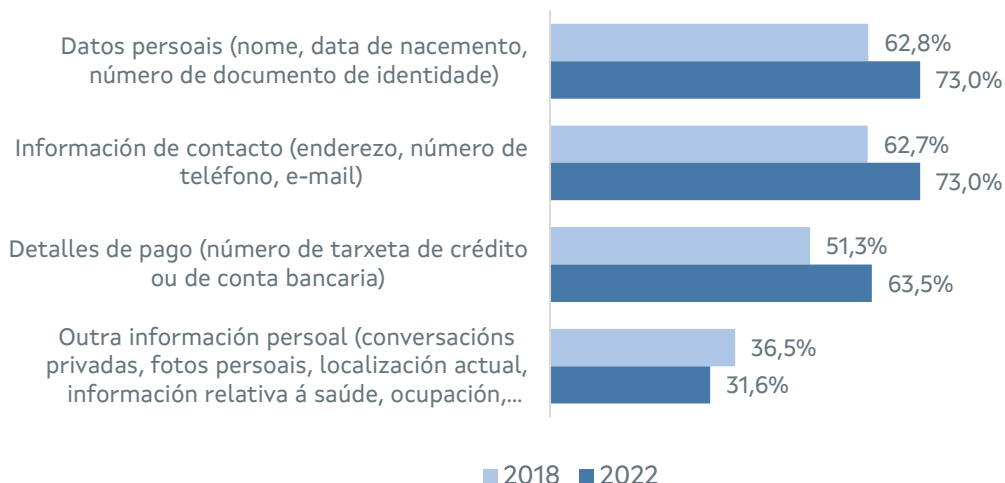
(% sobre o total de persoas de 16 a 74 anos que usaron internet nos últimos 12 meses)



Fonte: OSIMGA + IGE (2022)

G. 20. Información persoal proporcionada a través de internet nos últimos 12 meses. Evolución 2018-2022

(% sobre o total de persoas de 16 a 74 anos que usaron internet nos últimos 12 meses)

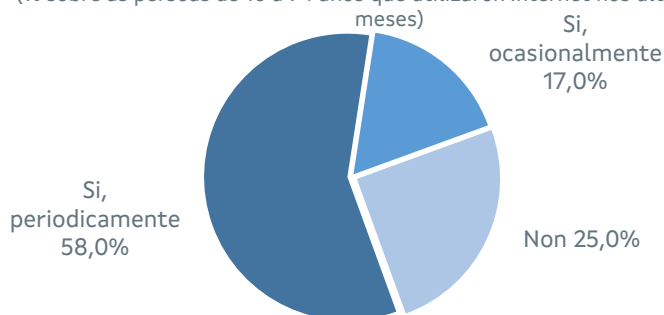


Fonte: OSIMGA + IGE (2022)

Un 58% da poboación mantén unha actualización periódica dos seus produtos informáticos fronte a un 25% que non os actualiza, situación bastante similar á de 2018.

G. 21. Actualización dos produtos de seguridade informática

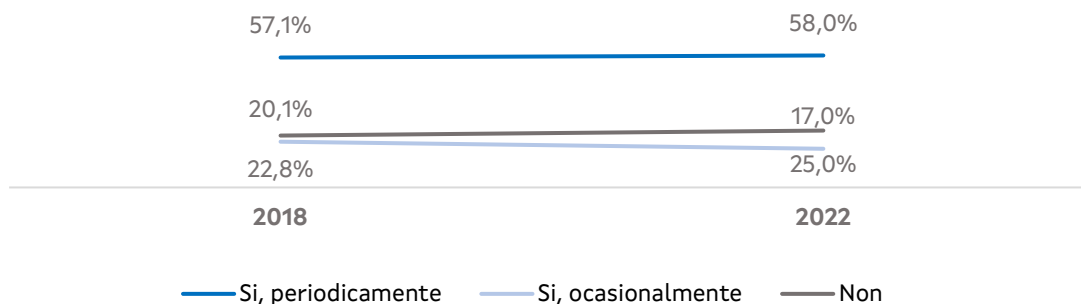
(% sobre as persoas de 16 a 74 anos que utilizaron Internet nos últimos doce meses)



Fonte: OSIMGA + IGE (2022)

G. 22. Actualización dos produtos de seguridade informática. Evolución 2018-2022

(% sobre as persoas de 16 a 74 anos que utilizaron Internet nos últimos doce meses)

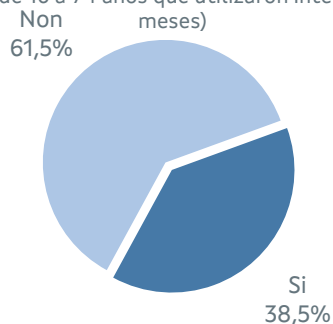


Fonte: OSIMGA + IGE (2022)

O 61,5% non accedeu a internet por unha rede wifi que non era a do seu domicilio algo moi diferente a anos anteriores, cando a maioría da poboación si accedía a redes wifi distintas as do seu fogar. Desta minoría que accede a redes que non son as do seu domicilio, un 59,4% só se conecta a redes con seguridade.

G. 23. Acceso a internet por unha rede wifi distinta á do seu domicilio

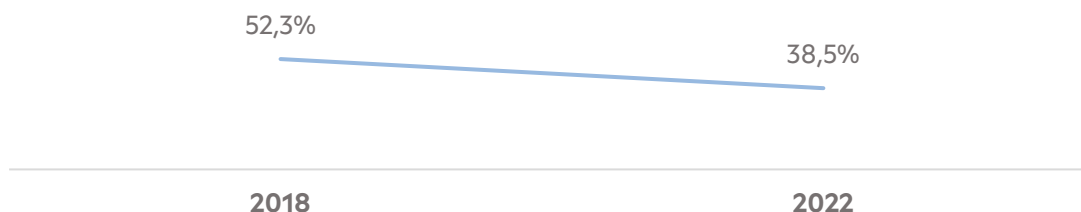
(% sobre as persoas de 16 a 74 anos que utilizaron Internet nos últimos doce meses)



Fonte: OSIMGA + IGE (2022)

G. 24. Acceso a internet por unha rede wifi distinta á do seu domicilio. Evolución 2018-2022

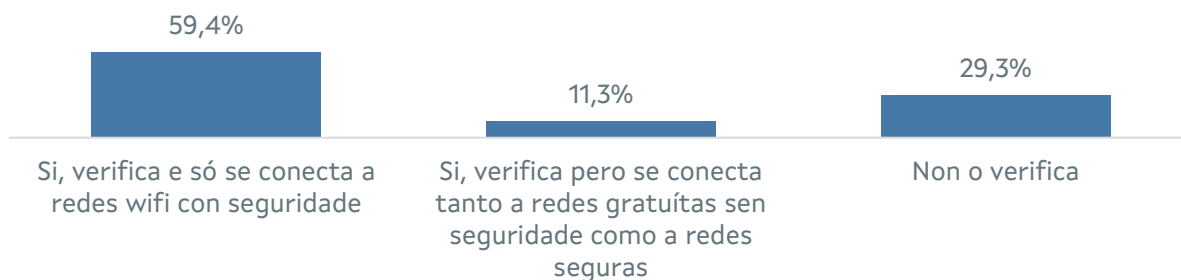
(% sobre as persoas de 16 a 74 anos que utilizaron Internet nos últimos doce meses)



Fonte: OSIMGA + IGE (2022)

G. 25. Verifica que a rede wifi á que accede a internet é distinta á do seu domicilio cumpre cuns requisitos mínimos de seguridade

(% sobre as persoas de 16 a 74 anos que acceden a internet por unha rede wifi distinta á do seu domicilio)

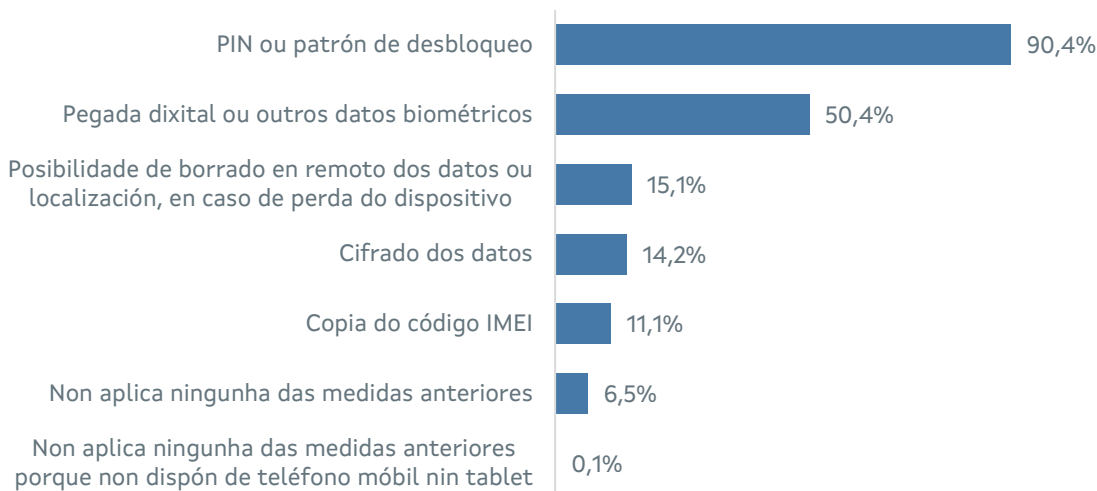


Fonte: OSIMGA + IGE (2022)

O pin ou patrón de desbloqueo do teléfono móbil é a medida de seguridade máis empregada polos usuarios/as de internet (90,4%). Cunha porcentaxe menor atópase a pegada dixital e outros mecanismos biométricos de seguridade (50,4%). Unicamente un 6,5% non aplica ningunha das medidas mostradas, o que supón unha baixada de case 4 puntos porcentuais con respecto ao ano 2018.

G. 26. Medidas de seguridade no teléfono móbil

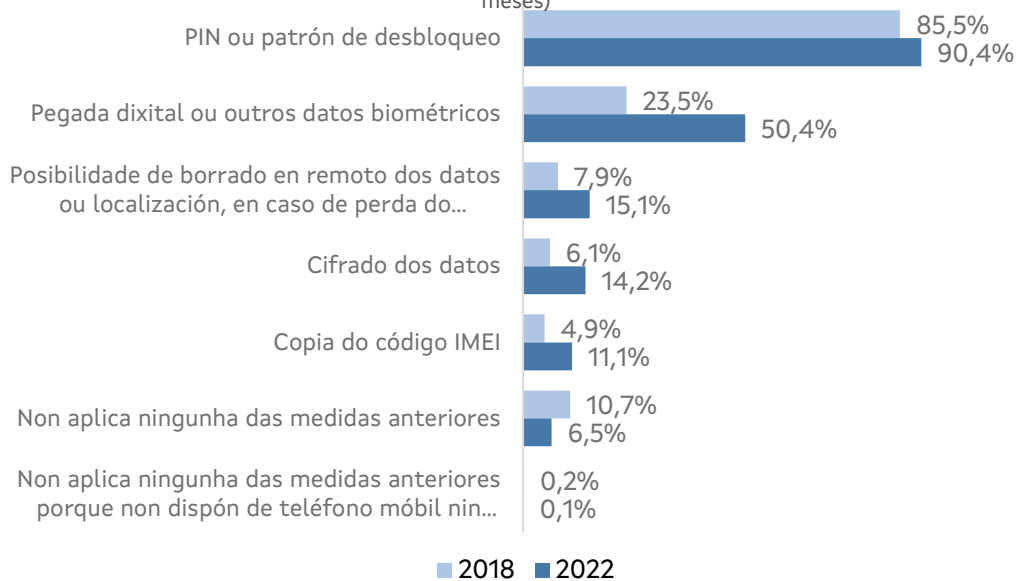
(% sobre o total de persoas de 16 a 74 anos que usaron internet nos últimos 12 meses)



Fonte: OSIMGA + IGE (2022)

G. 27. Medidas de seguridade no teléfono móbil. Evolución 2018-2022

(% sobre o total de persoas de 16 a 74 anos que usaron internet nos últimos 12 meses)



Fonte: OSIMGA + IGE (2022)

5. Ciberseguridade nas empresas de Galicia



O **8,2% das empresas** que contan con 10 ou máis traballadores e teñen a súa sede en Galicia dispoñen dun **especialista en ciberseguridade** dentro do seu persoal TIC.

O **86,2% das empresas con 10 ou máis traballadores e sede en Galicia** fan uso de medidas de seguridade TIC.



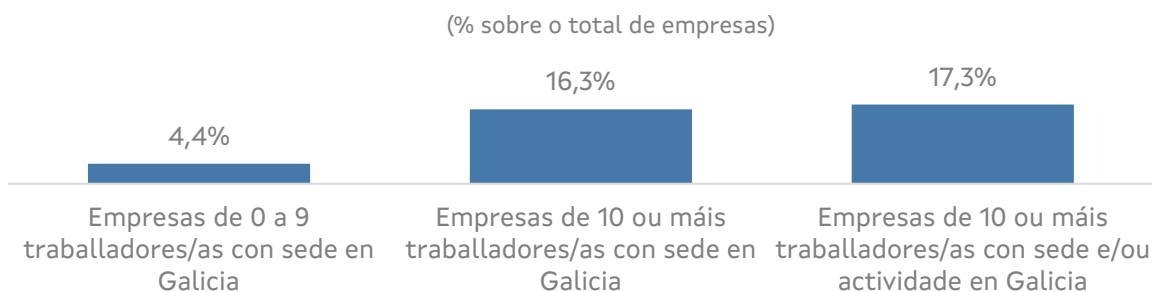
As empresas teñen un gran peso á hora de definir o ritmo da economía, afectando directamente á dixitalización. Un tecido empresarial altamente dixitalizado creará un ambiente favorable para que os cidadáns poidan acadar os seus obxectivos particulares arredor do sector TIC. A ciberseguridade gañou un lugar entre as preocupacións dos empresarios nos últimos anos. Isto xerou un incremento do investimento no sector, repercutindo tanto a nivel de gasto económico como de contratación de persoal especializado e medidas protectoras aplicadas. Á súa vez, unha forte cultura de ciberseguridade permite ás empresas tomar medidas ante calquera incidente que poida producirse para prevelas ou para que o seu impacto non sexa grave.

5.1 Incidentes de ciberseguridade nas empresas galegas

5.1.1 Incidentes de ciberseguridade rexistrados nas empresas

Ao longo do ano 2022, un **16,3% das empresas de máis de 10 traballadores/as con sede en Galicia tiveron algún incidente de seguridade informática**. Este dato é inferior no caso das empresas de 0 a 9 traballadores/as, no que a porcentaxe das que sufriron incidencias queda no 4,4%.¹ É comprensible que as empresas pequenas, por estar menos dixitalizadas, están menos expostas a este tipo de incidentes.

G. 28. Empresas con algún incidente de seguridade TIC)



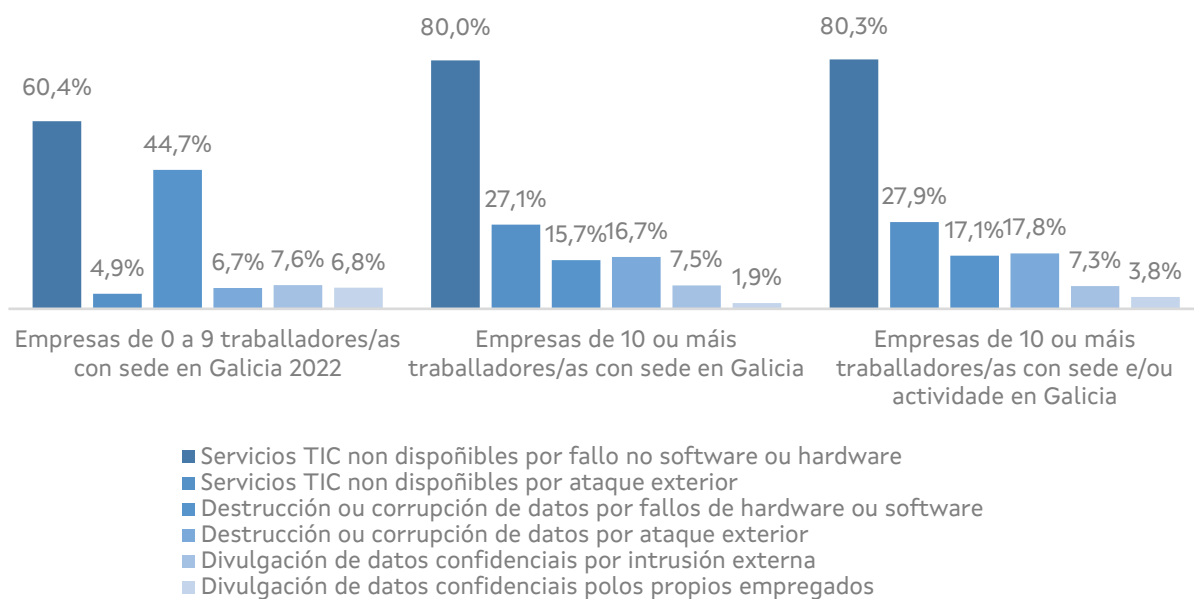
Fonte: OSIMGA Base: Empresas de Galicia

¹ En 2021 o INE non inclúe no seu cuestionario os incidentes de ciberseguridade, polo que non se dispón da comparación interanual.

No que respecta ao tipo de incidentes de ciberseguridade sufridos, nas tres categorías de empresas, a falta de dispoñibilidade de servizos TIC debido a fallos de software ou hardware é o incidente máis recorrente. É importante destacar que entre as empresas de 0 a 9 traballadores, a destrución de datos debido a fallos de software ou hardware ten unha porcentaxe particularmente superior en comparación coas empresas de máis de 10 traballadores. Isto podería deberse á posible falta de adquisición de equipos, ferramentas ou servizos externos TIC específicas nas empresas máis pequenas.

G. 29. Tipos de incidencias de seguridade informática

(% sobre o total de empresas que sufriron algún incidente de seguridade TIC)

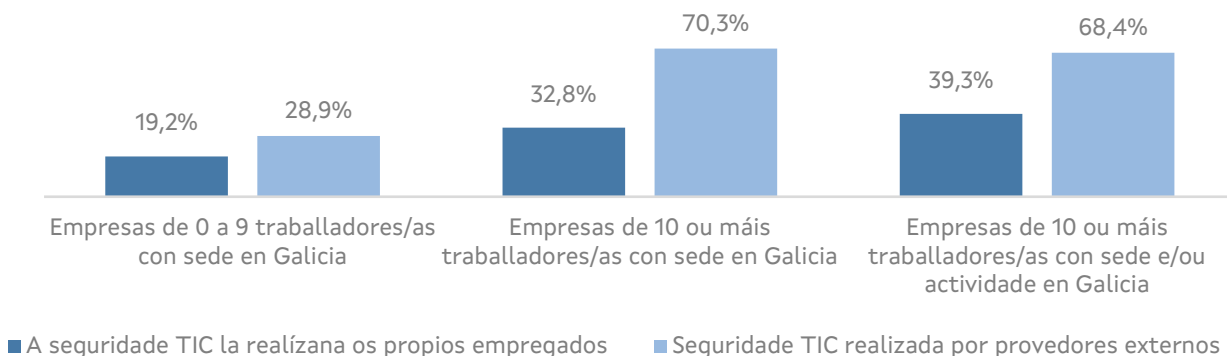


Fonte: OSIMGA Base: Empresas que sufriron incidencias de seguridade informática

Na maior parte dos casos, as empresas contan con provedores externos para a seguridade TIC. No caso das empresas pequenas, esta porcentaxe acada case un 30% dos casos mentres que nas empresas de máis de 10 traballadores con sede en Galicia esta porcentaxe ascende ata un 70%.

G. 30. Como realizan a seguridade TIC as empresas

(% sobre o total de empresas con conexión a Internet)



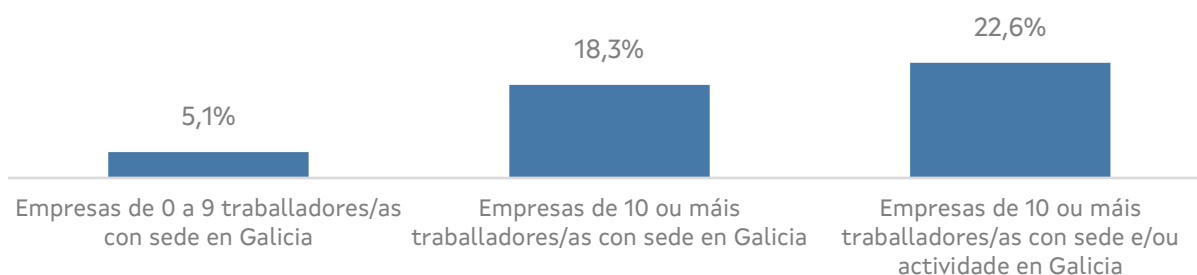
Fonte: OSIMGA Base: Empresas que sufriron incidencias de seguridade informática

A porcentaxe de empresas de 0 a 9 traballadores/as con sede en Galicia que contan cun seguro de seguridade TIC é dun 5,1%. Este dato aumenta cando se incrementa o número de traballadores/as das empresas, xa que no caso das que teñen máis de 10 e sede en Galicia, ascende ata un 18,3%.

Na maior parte dos casos, as empresas contan con **formación voluntaria sobre seguridade TIC, concretamente no 43,8% das empresas de máis de 10 traballadores/as** con sede ou actividade en Galicia. A porcentaxe de empresas que inclúen no contrato a obrigatoriedade de formación en seguridade TIC é moi inferior no caso das pequenas empresas (4%). Este dato aumenta notablemente cando as empresas teñen máis de 10 traballadores/as.

G. 31. Empresas con seguro fronte a incidencias de seguridade TIC

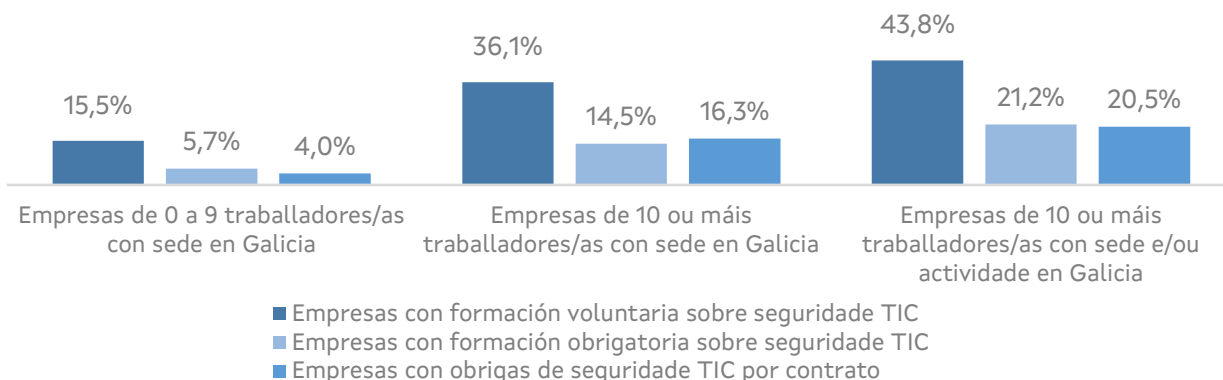
(% sobre o total de empresas con conexión a Internet)



Fonte: OSIMGA Base: Empresas que sufriron incidencias de seguridade informática

G. 32. Empresas con formación en seguridade TIC

(% sobre o total de empresas con conexión a Internet)



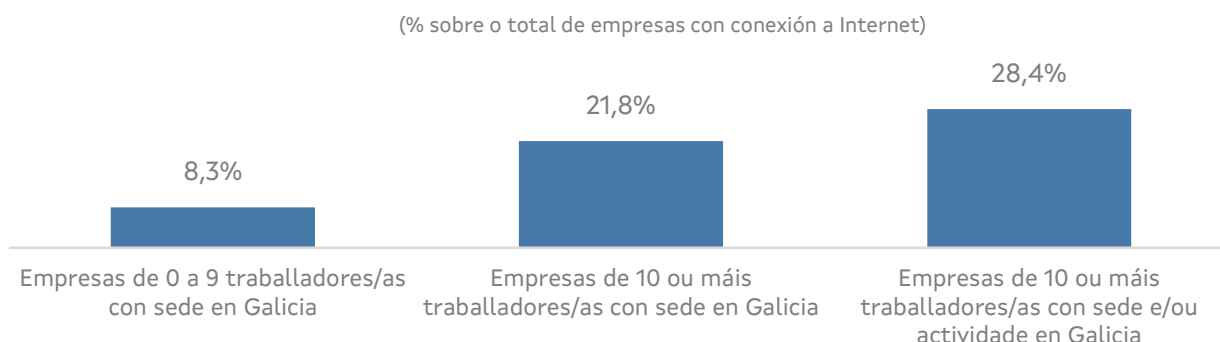
Fonte: OSIMGA Base: Empresas que sufriron incidencias de seguridade informática

A porcentaxe de empresas que dispoñen de documentación sobre seguridade TIC aumenta a medida co número de traballadores/as. Ademais esta porcentaxe é maior no caso das empresas de 10 ou máis, con sede e/ou actividade en Galicia.

No caso de contar con **documentación sobre seguridade, máis do 60% das empresas revisárona fai menos de 12 meses**. Nas pequenas empresas é nas que máis se observa casos nos que se revisou hai máis de 24 meses (21,9%).

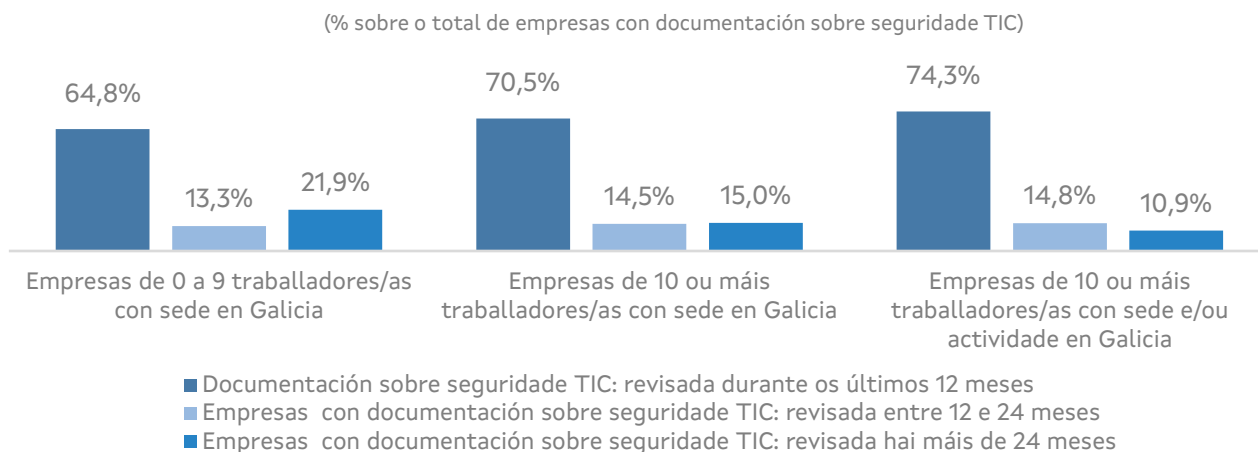
As novas formas de traballar (teletraballo) esixen tamén coñecer e difundir hábitos que eviten estar expostos a novos perigos. O acceso remoto é un punto crítico na prevención de ciberameazas. Unicamente o 27,7% das empresas de 0 a 9 empregados/as dispoñen de protocolos de seguridade para o acceso remoto. No caso das de 10 ou máis traballadores, supérase claramente o 50%.

G. 33. Empresas con documentación sobre seguridade



Fonte: OSIMGA Base: Empresas que sufriron incidencias de seguridade informática

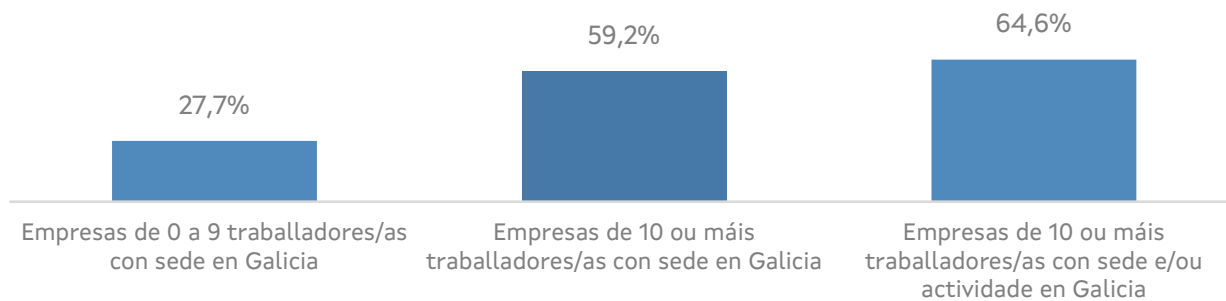
G. 34. Revisión da documentación sobre seguridade TIC



Fonte: OSIMGA Base: Empresas que sufriron incidencias de seguridade informática

G. 35. Empresas con algún protocolo de seguridad TIC para o acceso remoto

(% sobre o total de empresas con conexión a Internet)



Fonte: OSIMGA Base: Empresas que sufriron incidencias de seguridade informática

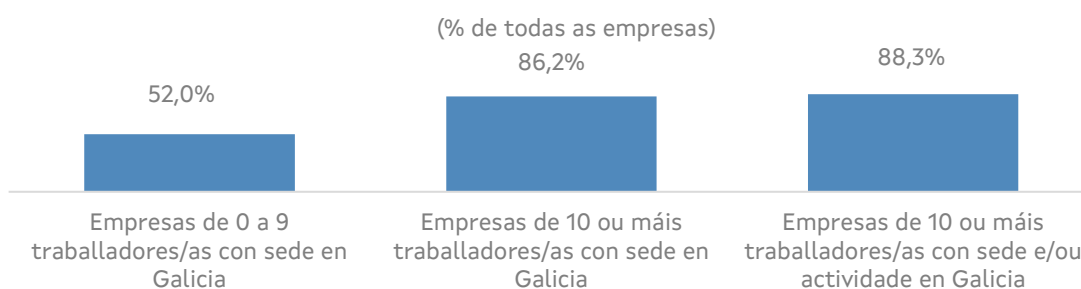
5.2 Cultura da ciberseguridade nas empresas galegas

5.2.1 Principais medidas e actuacións adoptadas polas empresas en materia de ciberseguridade

Para garantir un entorno dixital seguro é necesario adoptar as medidas correspondentes en materia de ciberseguridade.

En Galicia, o **88,3%** das empresas de 10 ou máis traballadores con sede e/ou actividade en Galicia utilizan medidas de seguridade TIC, e máis da metade das microempresas galegas fan o uso correspondente.

G.36. Empresas con medidas de seguridade TIC

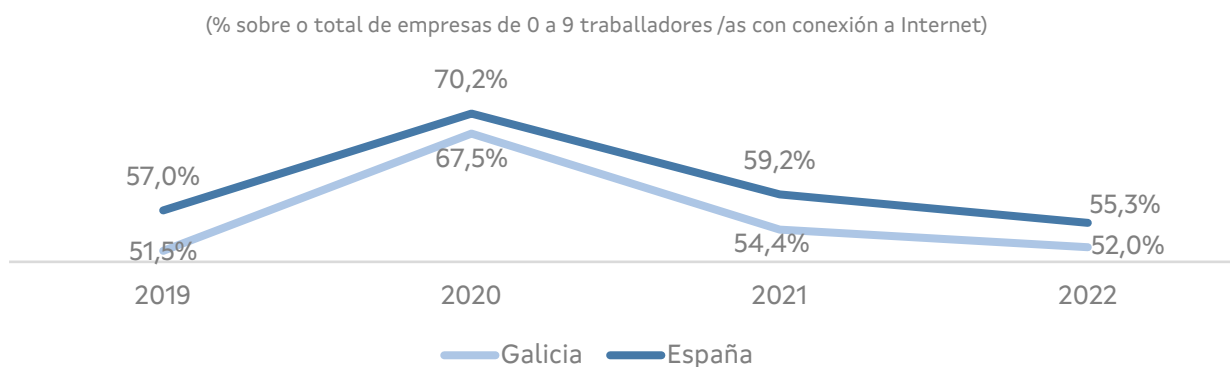


Fonte: INE (2022) Empresas de Galicia

Os datos de España e Galicia son moi similares e ambos seguen unha tendencia á baixa dende o ano 2020, onde un **67% de empresas galegas de 0 a 9 traballadores/as utilizaban medidas de seguridade TIC**. No ano 2022 este dato diminúe ata un 52%, pouco máis da metade do total de empresas.

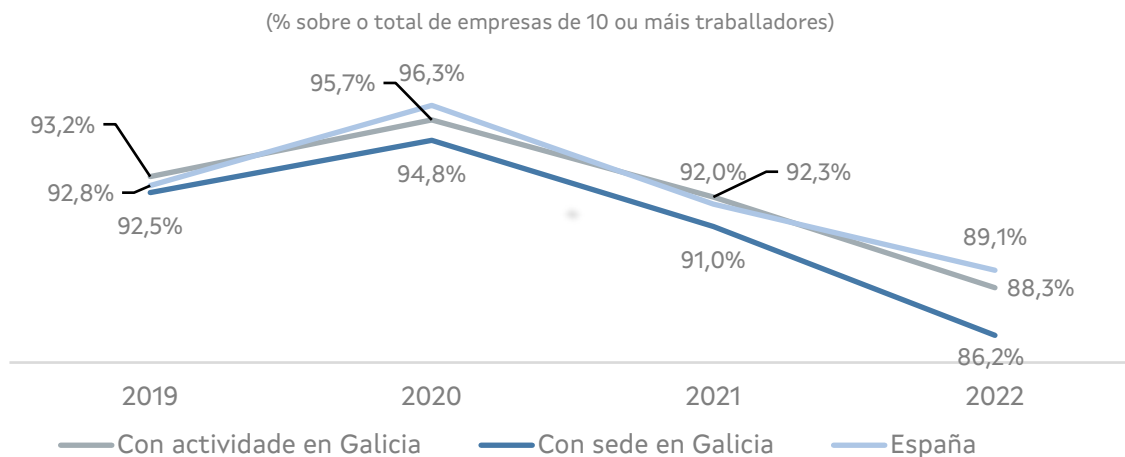
No caso das empresas de 10 ou máis traballadores a tendencia tamén é á baixa. No ano 2022, as empresas con medidas de seguridade son menos do 90% mentres que durante o ano 2020 os datos de empresas con medidas de seguridade situábanse ao redor dun 95%.

G.37. Empresas con medidas de seguridade TIC: evolución e comparativa (España e Galicia)



Fonte: OSIMGA Base: Empresas con sede en España

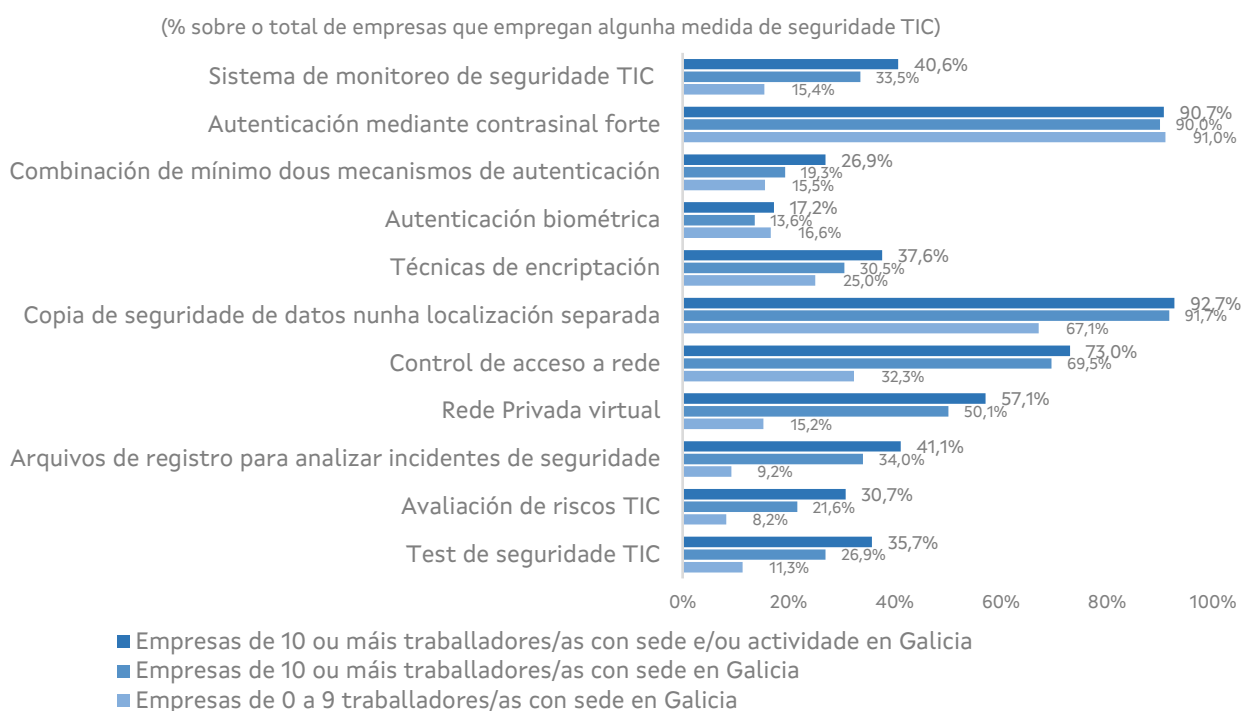
G.38. Empresas con medidas de seguridade TIC: evolución e comparativa (España e Galicia)



En 2022, a medida de seguridade máis utilizada entre as empresas galegas con 0 a 9 traballadores foi a autenticación mediante contrasinal forte. No caso das empresas con máis de 10 traballadores/as, a medida máis usada foi ter unha copia de seguridade de datos nunha localización separada. Estas dúas medidas son as máis empregadas polo total de empresas.

A estas medidas, séguelles o control de acceso á rede, aínda que está moito máis presente nas empresas que contan con máis de 10 traballadores/as. Menos común é o uso de autenticación biométrica e a combinación de mínimo dous mecanismos de autenticación, aínda que esta última medida aumenta no caso das empresas de 10 ou máis traballadores e con sede ou actividade en Galicia.

G.39. Tipoloxía de Medidas de Seguridade que empregan



6. O mercado da ciberseguridade en Galicia

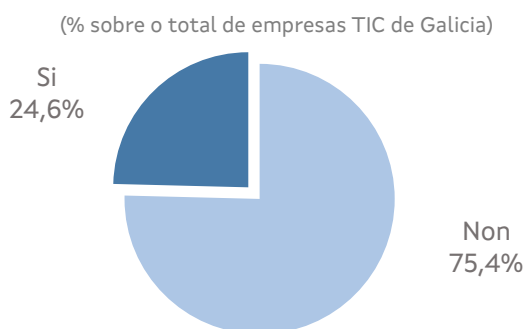
A ciberseguridade é unha parte moi importante do mercado para o sector tecnolóxico, converténdose hoxe nunha oportunidade para moitas start-ups e empresas xa consolidadas neste sector. Galicia non queda á marxe desta tendencia. O **tecido empresarial do hipersector TIC galego achega millóns de euros á economía autonómica e emprega a miles de persoas.**

6.1 O tecido empresarial galego de ciberseguridade

6.1.1 Empresas de ciberseguridade en Galicia e servizos ofertados

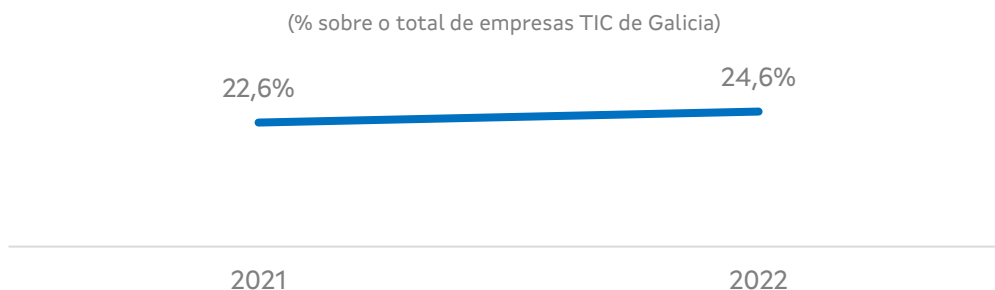
A porcentaxe de empresas TIC galegas que en 2022 ofreceron servizos e produtos de ciberseguridade é do **24,6%**. Sobe dous puntos sobre o ano anterior coincidindo co aumento da demanda de produtos de ciberseguridade altamente especializados. Esta cifra pode seguir aumentando paulatinamente nos próximos anos.

G. 40. Empresas que ofrecen produtos ou servizos de ciberseguridade



Fonte: OSIMGA Base: Empresas TIC de Galicia

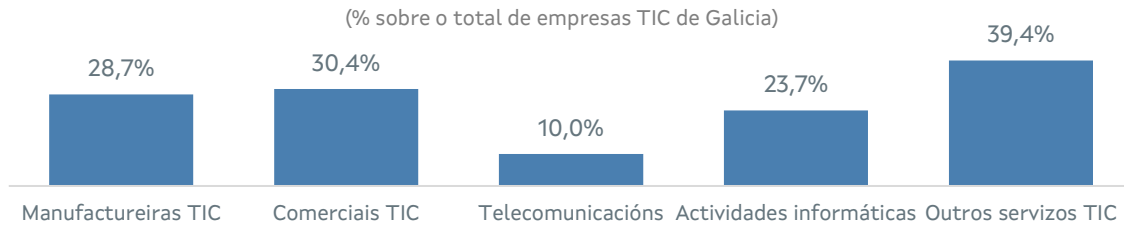
G. 41. Empresas que ofrecen produtos ou servizos de ciberseguridade en 2021 e 2022



Fonte: OSIMGA Base: Empresas TIC de Galicia

O 39,4% das empresas pertencentes ao subsector "Outros servizos TIC" comercializan este tipo de servizos, seguidas do 30,4% das empresas pertencentes ao sector de comerciais TIC. No extremo oposto sitúanse as telecomunicacións, nas que a ciberseguridade ten un peso específico do 10%.

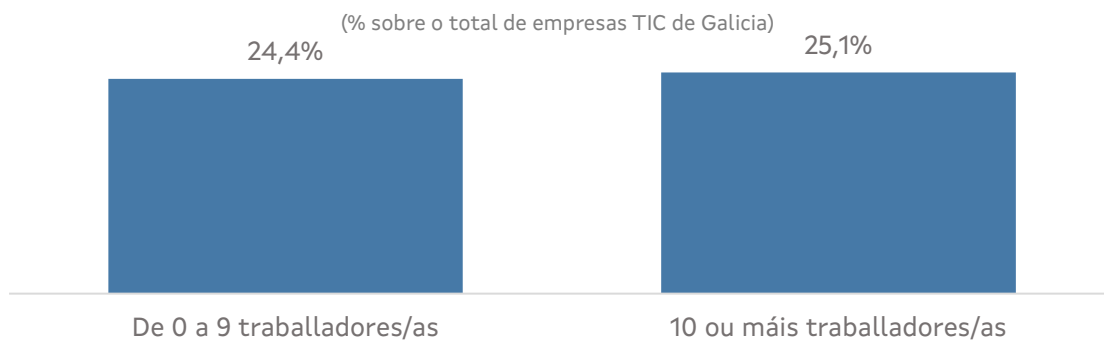
G. 42. Gráfica. Empresas que venden produtos ou servizos de ciberseguridade por sector de actividade.



Fonte: OSIMGA Base: Empresas TIC de Galicia

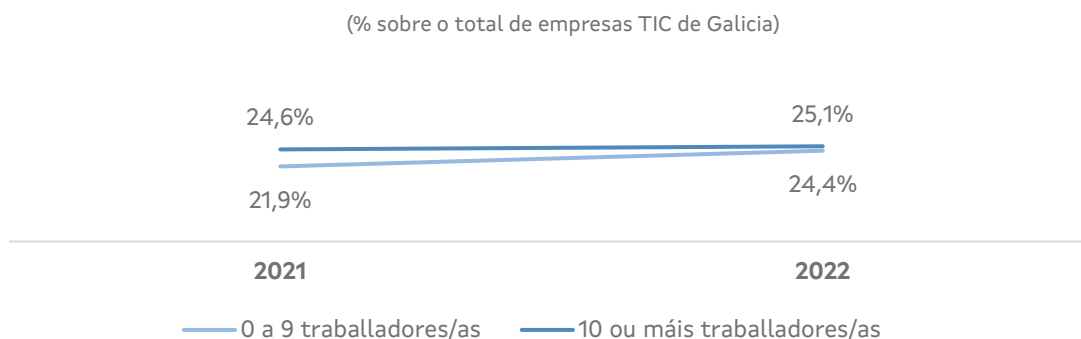
Considerando o tamaño da empresa TIC por **número de traballadores**, o 24,4% das empresas de 0 a 9 traballadores/as venden estes produtos e servizos e o 25,1% no caso das empresas de 10 ou máis, polo que se reduce a diferenza respecto ao ano anterior.

G. 43. Empresas que venden produtos ou servizos de ciberseguridade por número de traballadores.



Fonte: OSIMGA Base: Empresas TIC de Galicia

G. 44. Empresas que venden produtos ou servizos de ciberseguridade por número de traballadores (2021 e 2022)



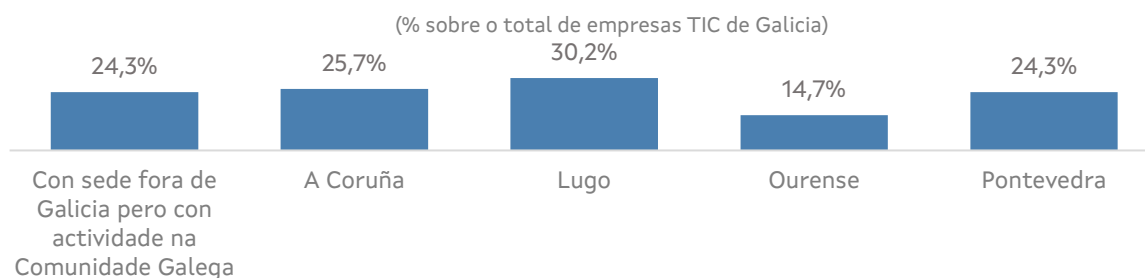
Fonte: OSIMGA Base: Empresas TIC de Galicia

Tendo en conta a situación xeográfica das empresas que prestan servizos TIC en Galicia, a **ciberseguridade ten maior presenza no sector TIC de Lugo, co 30,2%**. Dato que

cambia con respecto ó ano pasado, onde era máis común que vendesen ciberseguridade as que teñen sede fóra de Galicia (39,6%).

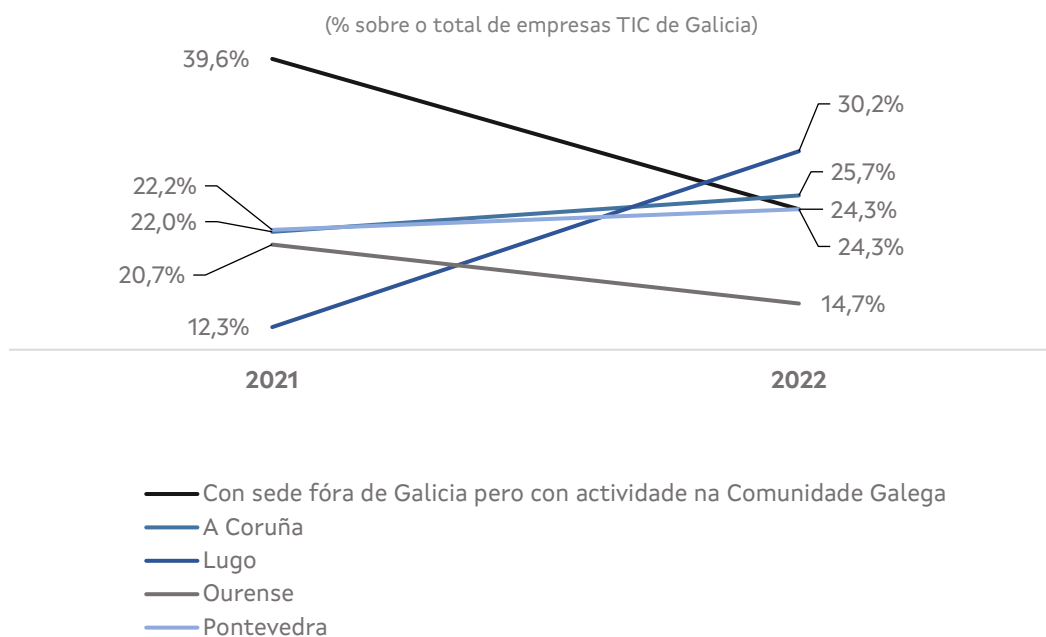
A Coruña é a provincia, ademais de Lugo, onde máis proporción de empresas TIC venden produtos ou servizos de ciberseguridade, cunha porcentaxe do 25,7%. Ourense ocupa o último lugar cunha porcentaxe de case un 15%. 3 das 4 provincias galegas aumentan a proporción de empresas tic que venden produtos ou servizos de ciberseguridade.

G. 45. Empresas que venden produtos ou servizos de ciberseguridade por sedes.



Fonte: OSIMGA. Base: empresas TIC en Galicia

G. 46. Empresas que venden produtos ou servizos de ciberseguridade por sedes (2021 e 2022)



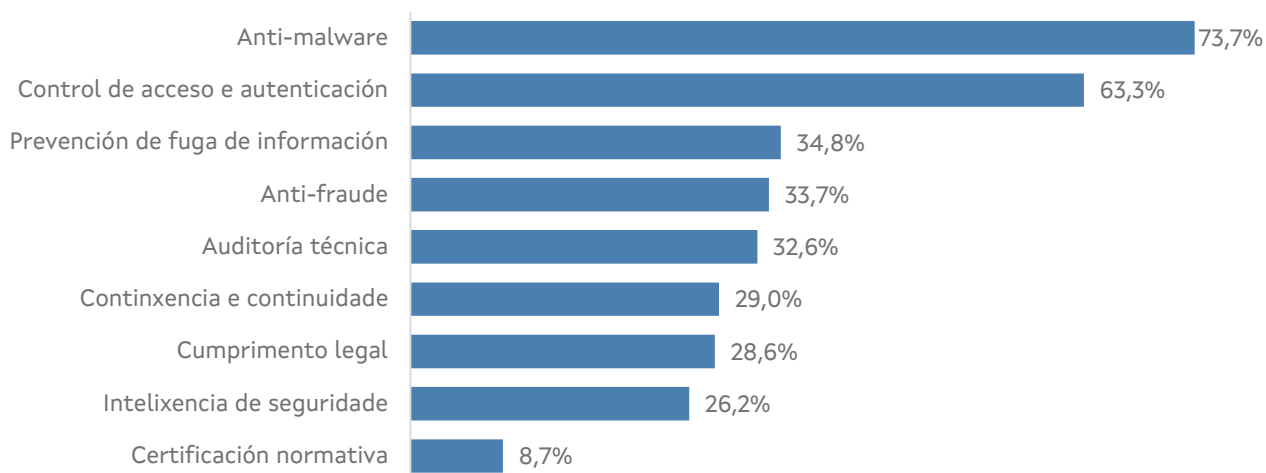
Fonte: OSIMGA. Base: empresas TIC en Galicia

Tendo en conta o tipo de **produtos ofertados**, destacan sobre todo o **antimalware** e o **control de acceso e autenticación**, con porcentaxes do 73,7% e do 63,3% respectivamente. O catálogo de produtos e servizos é moi amplo, tendo un gran peso específico e con porcentaxes superiores ao 30% produtos como **prevención de fuga da información, anti-fraude e auditoría técnica**.

En último lugar sitúase a **certificación normativa en normas como a ISO 27001 ou o RD 311/2022**, cunha porcentaxe de oferta do 8,7%.

G. 47. Tipo de produtos que ofrecen

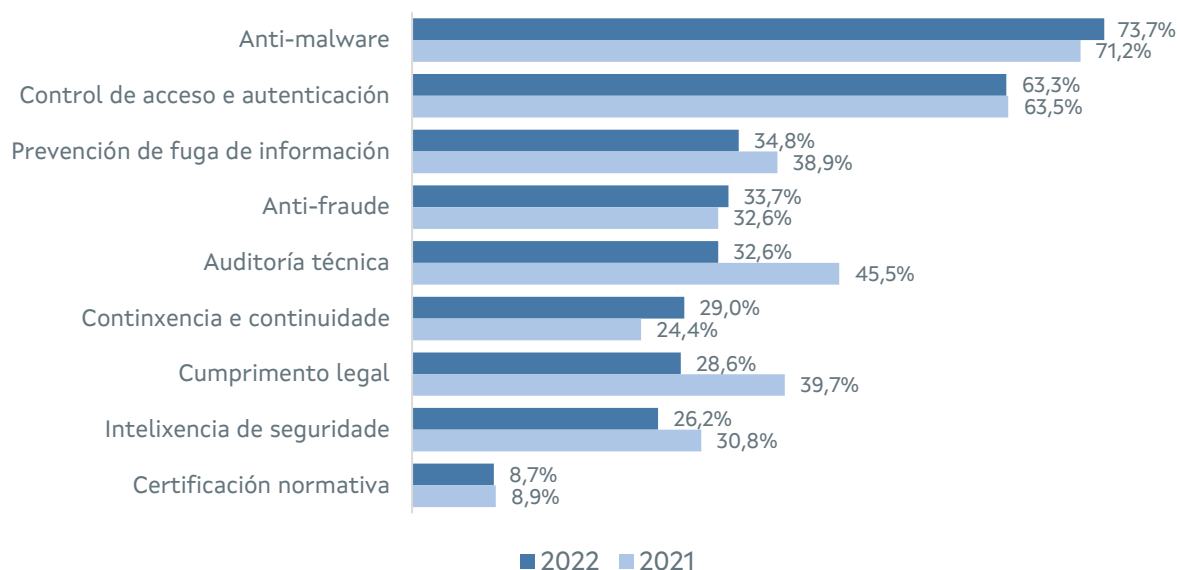
(% sobre o total de empresas TIC que venden produtos ou servizos de ciberseguridade)



Fonte: OSIMGA Base: Empresas TIC que comercializan produtos ou servizos de ciberseguridade

G. 48. Tipo de produtos que ofrecen (2021 e 2022)

(% sobre o total de empresas TIC que venden produtos ou servizos de ciberseguridade)



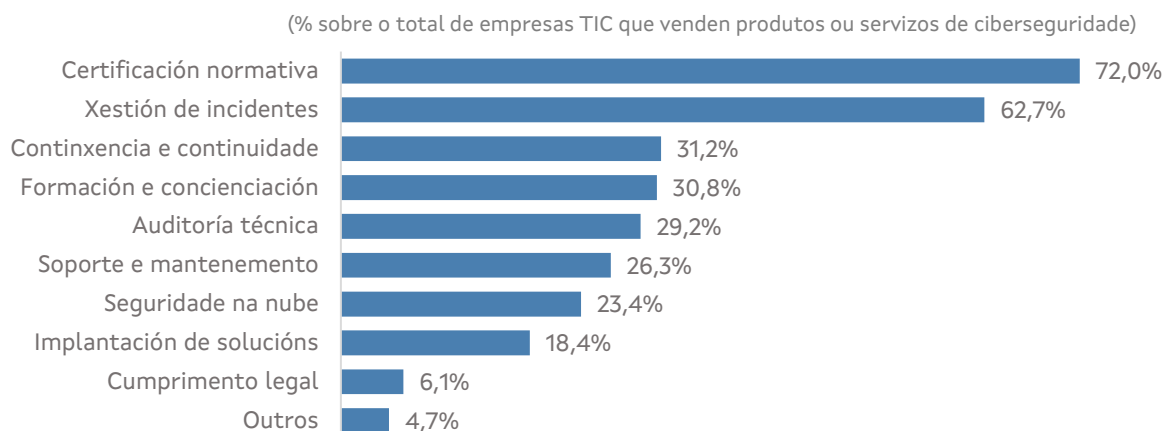
Fonte: OSIMGA Base: Empresas TIC que comercializan produtos ou servizos de ciberseguridade

Observamos como entre os **servizos de ciberseguridade ofrecidos destaca**, moi por riba de todos, a **certificación normativa**, cunha presenza do 72% entre as que ofertan ciberseguridade. Unha situación moi distinta se comparamos cos datos do ano anterior, onde este servizo non alcanzaba o 7%.

Outro servizo ofrecido que ten unha porcentaxe superior ao 50% é a **xestión de incidentes**, que aumenta case dez puntos porcentuais no último ano.

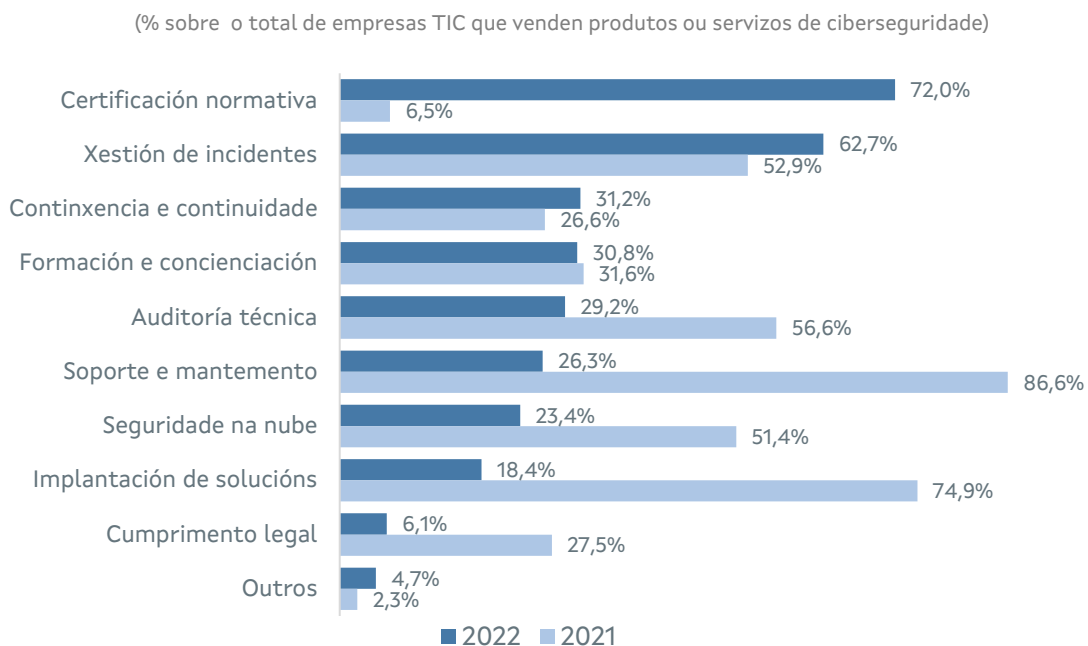
O cumprimento legal, nunha porcentaxe inferior ao 7%, é un dos servizos con menos oferta na actualidade, dato moi inferior ao do ano pasado (27,5%).

G. 49. Tipo de servizos ofertados.



Fonte: OSIMGA Base: Empresas TIC que comercializan produtos ou servizos de ciberseguridade

G. 50. Tipo de servizos ofertados (2021 e 2022)



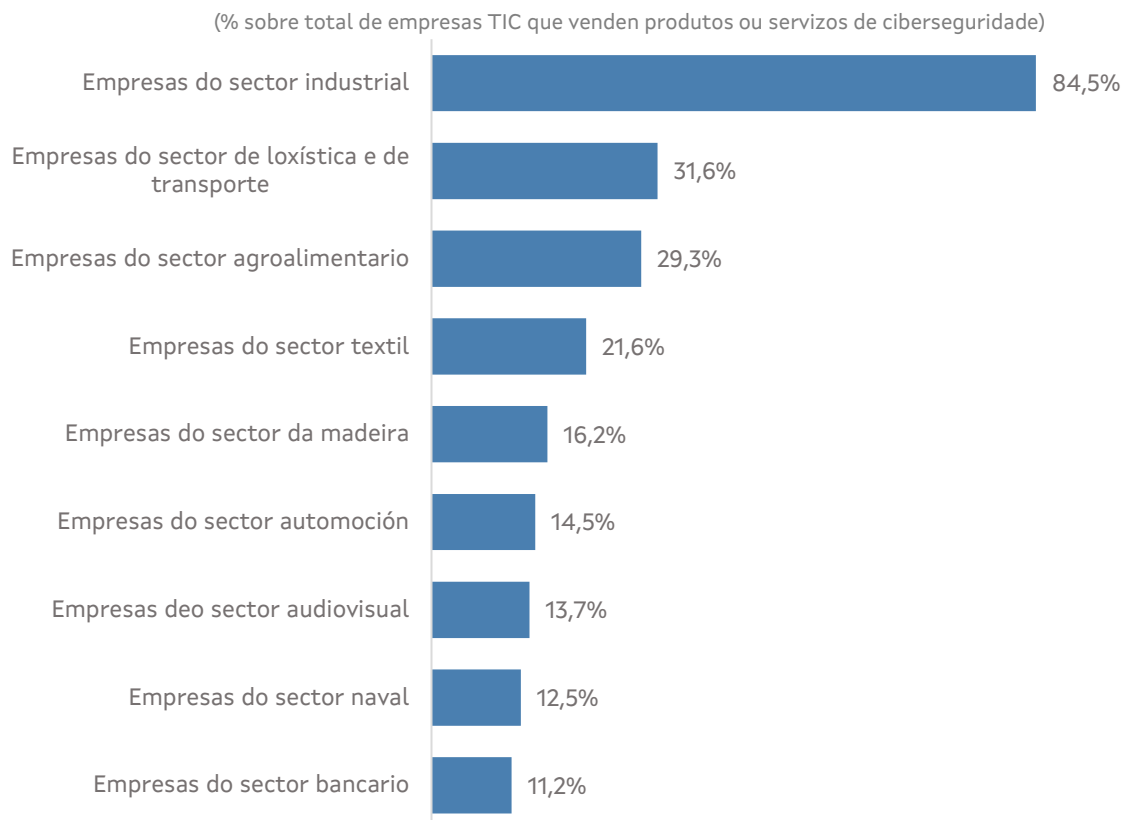
Fonte: OSIMGA Base: Empresas TIC que comercializan produtos ou servizos de ciberseguridade

O tipo de cliente é un factor determinante á hora de ir ao mercado para ofrecer este tipo de solucións tecnolóxicas.

Das empresas que vende servizos ou produtos de ciberseguridade, **o 84,5% ten entre a súa clientela ao sector industrial**. O resto dos sectores, xa moi detrás deste, son loxística e transporte, agroalimentario, téxtil e madeira.

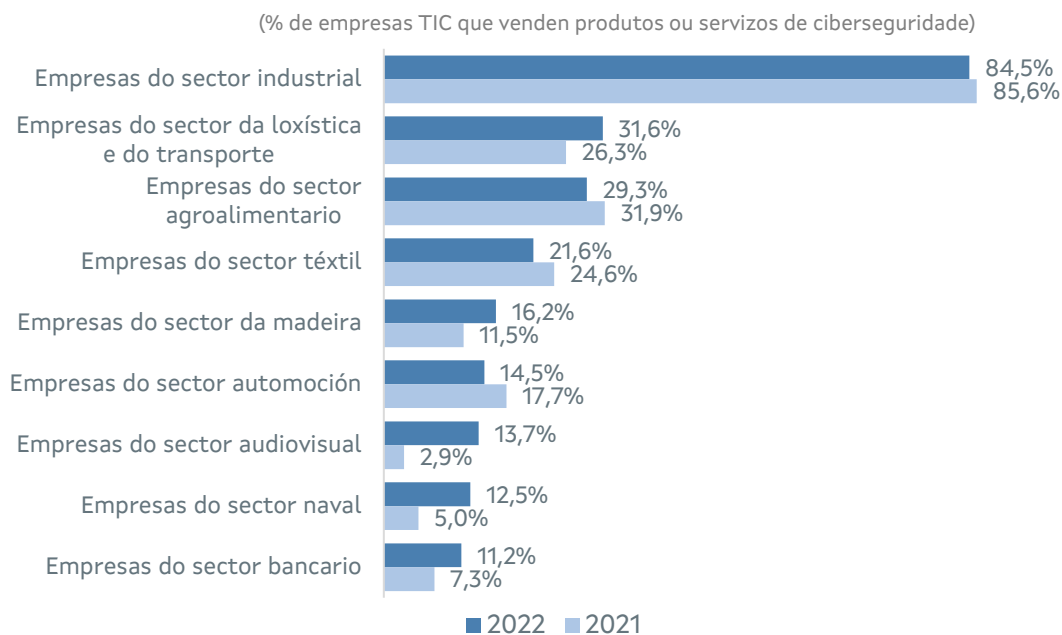
Os que máis crecen no peso da clientela no último ano son o sector audiovisual (+10,8 puntos), sector naval (+7,5 puntos) e o da loxística e transporte (+5,3 puntos).

G. 51. Comercialización de produtos ou servizos por tipo de cliente.



Fonte: OSIMGA. Base: empresas TIC que venden produtos ou servizos de ciberseguridade

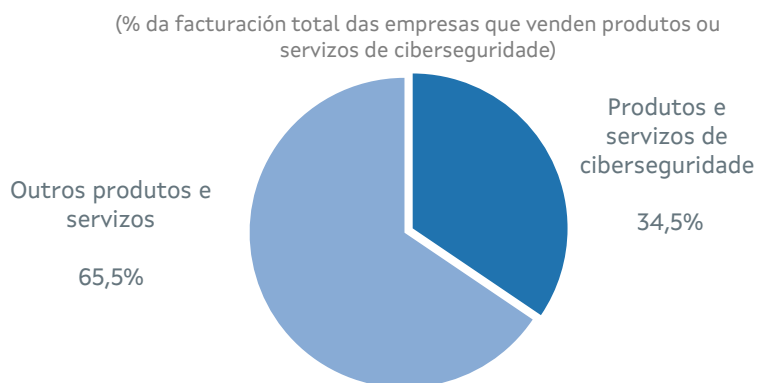
G. 52. Comercialización de produtos ou servizos por tipo de cliente (2021 e 2022)



Fonte: OSIMGA. Base: empresas TIC que venden produtos ou servizos de ciberseguridade

En Galicia, a porcentaxe derivada da venda de produtos e servizos de ciberseguridade é dun 34,5% sobre o total do importe neto da facturación das empresas TIC con produtos ou servizos TIC.)

G. 53. Porcentaxe derivada da venda de produtos e servizos de ciberseguridade sobre o importe neto da facturación .

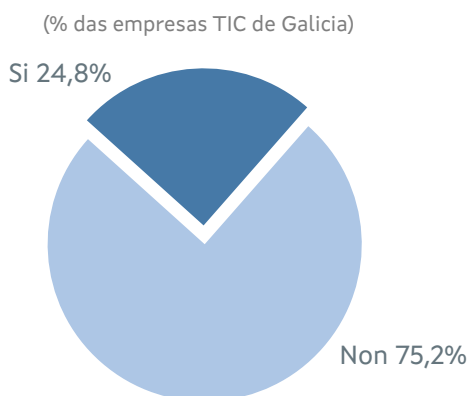


Fonte: OSIMGA. Base: empresas TIC en Galicia que venden produtos ou servizos de ciberseguridade

6.2 Incidentes de ciberseguridade nas empresas TIC

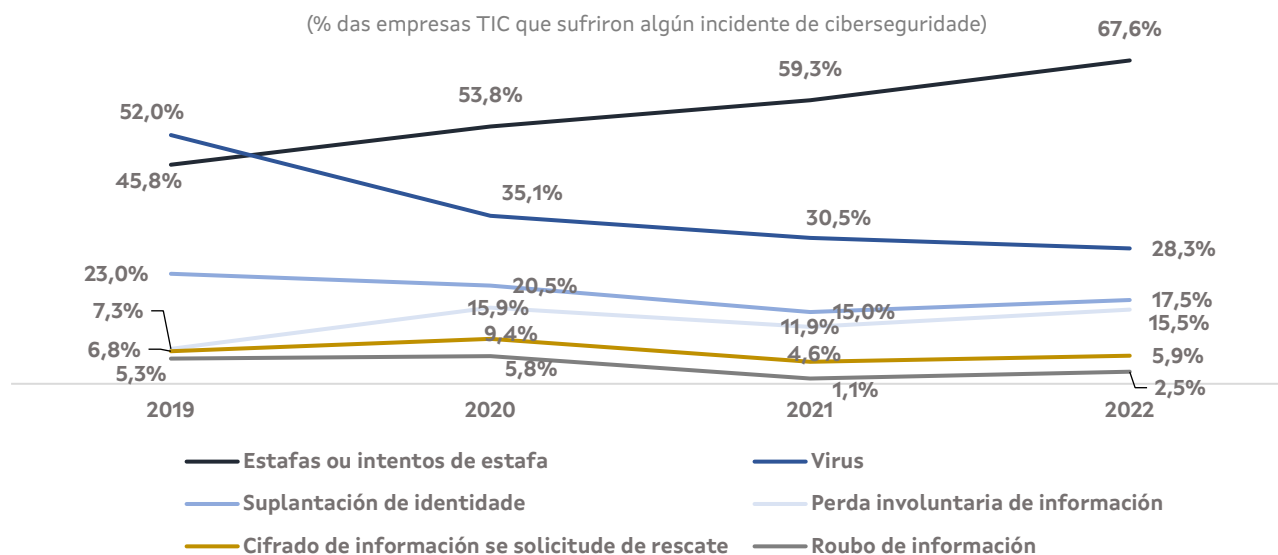
A porcentaxe de empresas TIC galegas que en 2022 sufriron incidentes de ciberseguridade é dun 24,8%. O incidente de seguridade máis común nas empresas TIC son as **estafas ou intentos de estafa**, que ademais aumenta continuamente dende o ano 2019 ata o 67,6%. Os **virus** son os segundos incidentes máis comúns nestas empresas pero a súa incidencia tende á baixa durante os últimos anos, ata o 28,3%. A suplantación de identidade acada o 17,5%, mentres a perda de información, co 15,5%, presenta tendencia irregular, máis ben ascendente.

G. 54. Empresas TIC que sufriron incidentes de ciberseguridade



Fonte: OSIMGA. Base: empresas TIC en Galicia

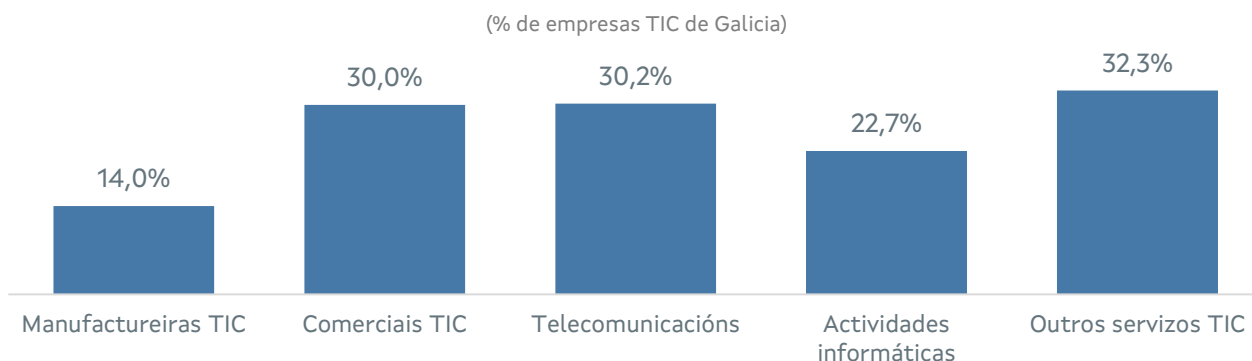
G. 55. Tipos de incidentes de ciberseguridade que sufriron as empresas TIC



Fonte: OSIMGA. Base: empresas TIC que sufriron algún incidente de ciberseguridade

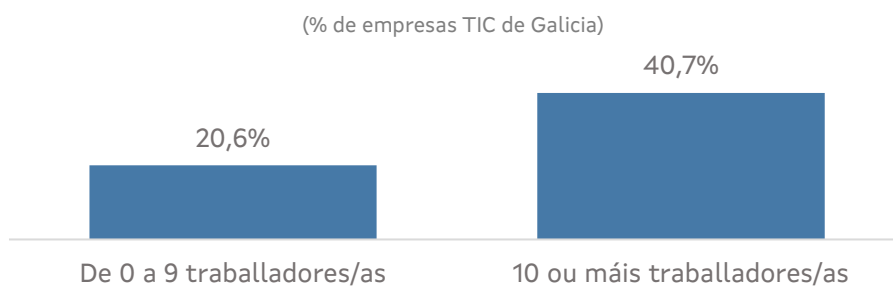
Outros servizos TIC é o subsector onde se observaron máis incidencias de ciberseguridade, cunha porcentaxe de 32,3%. Moi preto atópase **Comerciais TIC** e o sector das **telecomunicacións**, con porcentaxes do 30%. En último lugar, un 14% das **manufactureiras TIC** sufriron incidentes de seguridade.

G. 56. Empresas TIC que sufriron incidentes de seguridade por subsector



Fonte: OSIMGA. Base: empresas TIC en Galicia

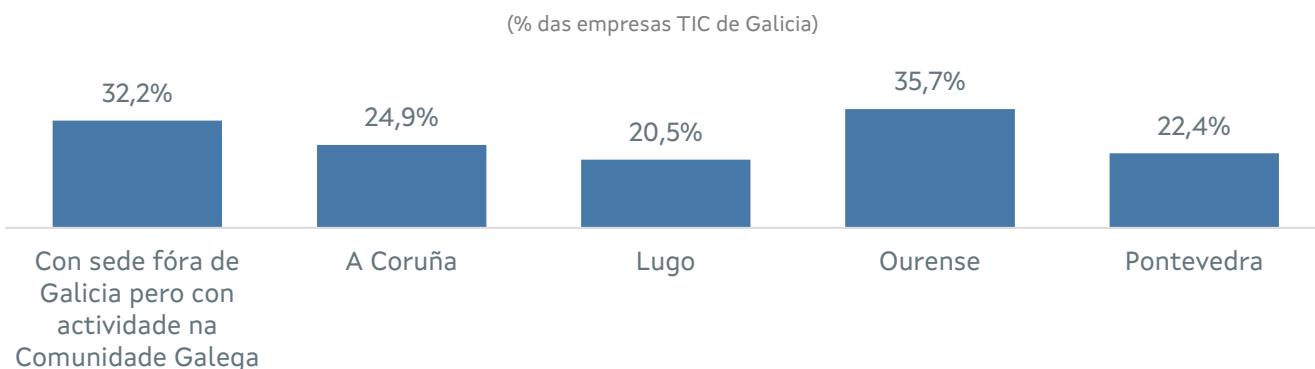
G. 57. Empresas TIC que sufriron incidentes de seguridade por tamaño



Fonte: OSIMGA. Base: empresas TIC en Galicia

Ourense posiciónase como a provincia onde hai máis empresas que sufriron algún incidente de seguridade mentras que en Lugo é onde hai menos incidencias relacionadas coa seguridade. Ademais vemos como as empresas con máis persoal son as que sufriron en maior medida máis incidentes de seguridade (un 40,7% fronte ao 20,6% das empresas de 0 a 9 traballadores/as).

G. 58. Empresas TIC que sufriron incidentes de seguridade por lugar da sede

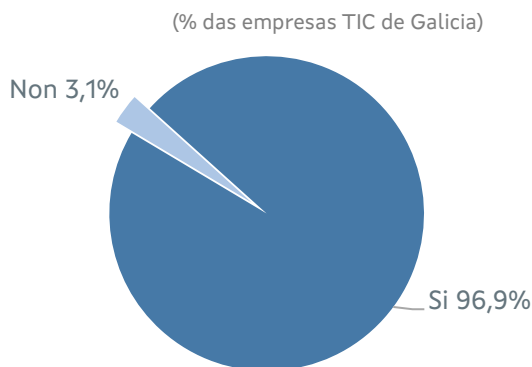


Fonte: OSIMGA. Base: empresas TIC en Galicia

Practicamente o total das empresas TIC empregan medidas de ciberseguridade. Entre estas medidas destacan as de **manter o software actualizado**, **autenticación mediante contrasinal forte** ou **facer unha copia de seguridade de datos nunha ubicación**

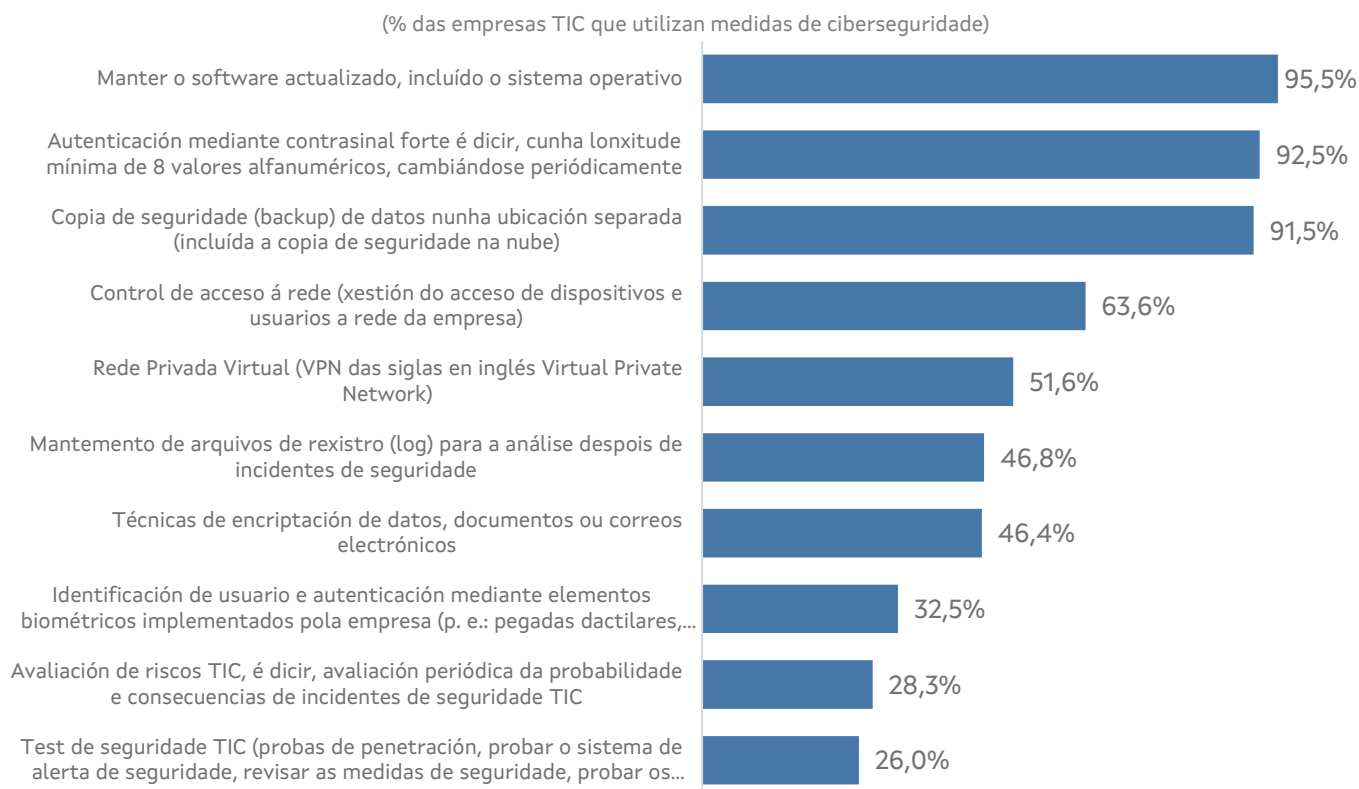
separada. Por outra banda, as medidas de seguridade menos utilizadas polas empresas TIC son os **test de seguridade e a avaliación de riscos TIC.**

G. 59. Empresas TIC que utilizan medidas de seguridade TIC



Fonte: OSIMGA. Base: empresas TIC en Galicia

G. 60. Medidas de seguridade TIC empregadas polas empresas TIC

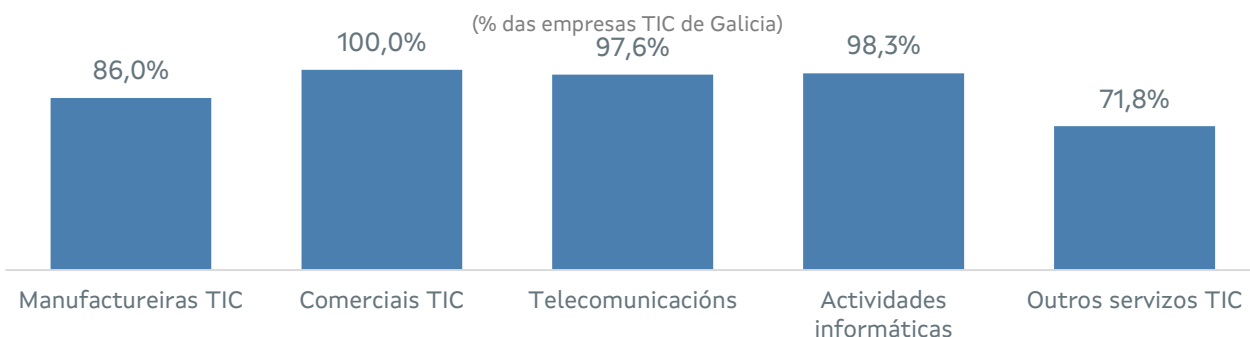


Fonte: OSIMGA. Base: empresas TIC que empregan medidas de seguridade TIC en Galicia

O total do sector de **comerciais TIC** empregan medidas de seguridade TIC. Moi seguido atópanse os sectores das **telecomunicacións** e das **actividades informáticas**. O subsector **outros servizos TIC** é o que menos porcentaxe presenta (71,8%).

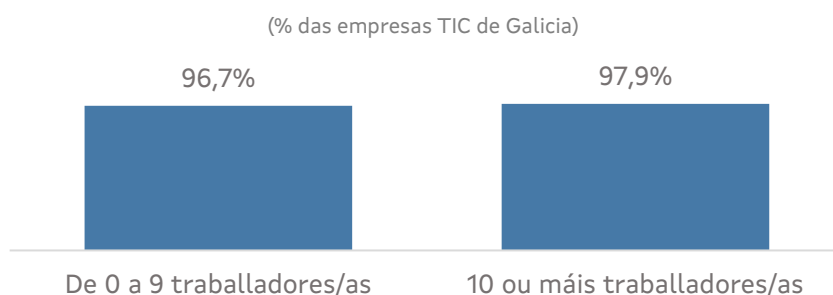
O uso da seguridade TIC amosa valores similares por tamaño de empresa e, tendo en conta a ubicación da sede, só a provincia de Ourense baixa do 90%.

G. 61. Empresas TIC que utilizan medidas de seguridade TIC por subsector



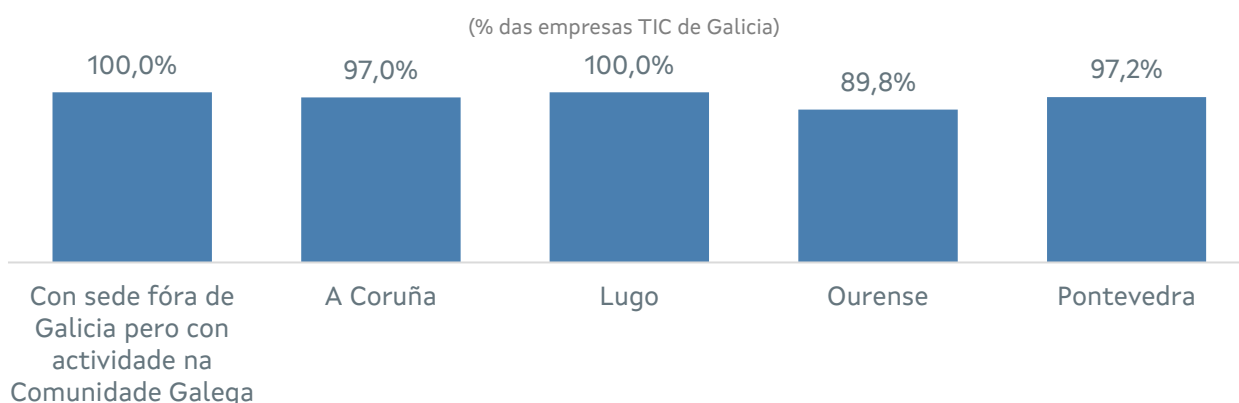
Fonte: OSIMGA. Base: empresas TIC en Galicia

G. 62. Empresas TIC que utilizan medidas de seguridade TIC por tamaño



Fonte: OSIMGA. Base: empresas TIC en Galicia

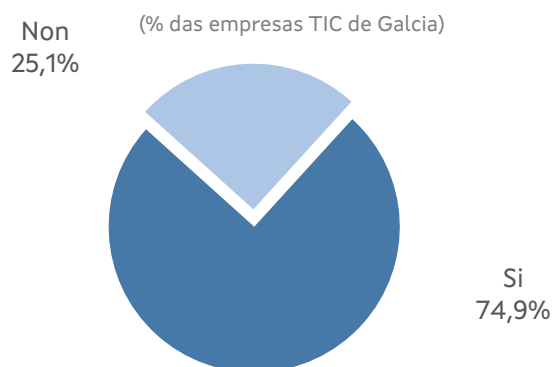
G. 63. Empresas TIC que utilizan medidas de seguridade TIC por provincia da sede



Fonte: OSIMGA. Base: empresas TIC en Galicia

A maior parte das empresas TIC realizaron compras por internet (74,9%), polo que están máis expostas a posibles ameazas na rede. Por esta razón pregúntase, ás que non compraron, se a seguridade foi un factor que o impediu. Só o 6,6 % das que non compraron indican que é porque lles preocupa a seguridade, e ao 4,5% preocúpalles a privacidade.

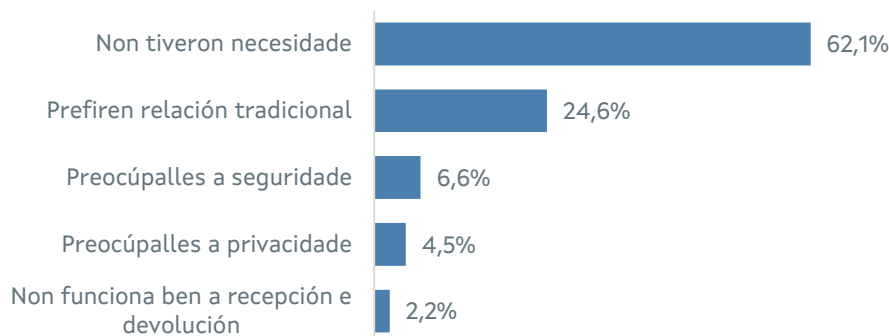
G. 64. Empresas TIC que realizan ou non compras por Internet



Fonte: OSIMGA. Base: empresas TIC en Galicia

G. 65. Razóns polas que non realizaron compras por internet

(% sobre as empresas TIC que non realizaron compras por internet)

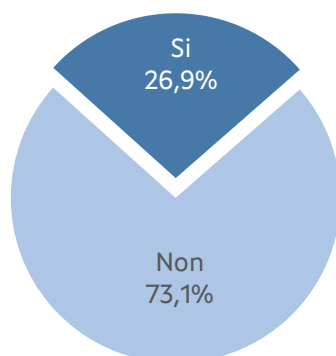


Fonte: OSIMGA. Base: empresas TIC que non realizaron compras por internet en Galicia

Se falamos de vendas pódese observar que case un 27% das empresas realizan vendas por internet, sendo o 73% restante aquelas empresas que non realizaron vendas a través deste medio. A principal razón é que os produtos que venden non son axeitados para vender por internet. Só o 1% das empresas TIC que non venden por internet sinalan que unha das razóns é a seguridade.

G. 66. Empresas TIC que realizan ou non vendas por Internet

(% das empresas TIC de Galicia)



Fonte: OSIMGA. Base: empresas TIC en Galicia

G. 67. Razóns polas que non realizaron vendas por internet

(% das empresas TIC que non venderon por internet)

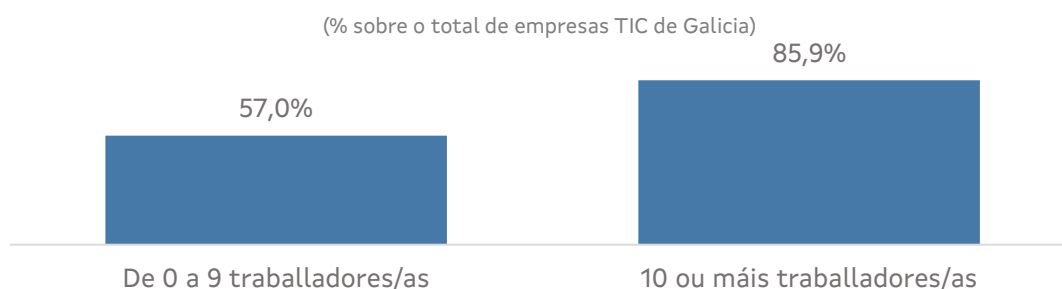


Fonte: OSIMGA. Base: empresas TIC que non realizaron vendas por internet en Galicia

6.3 O teletraballo nas empresas TIC

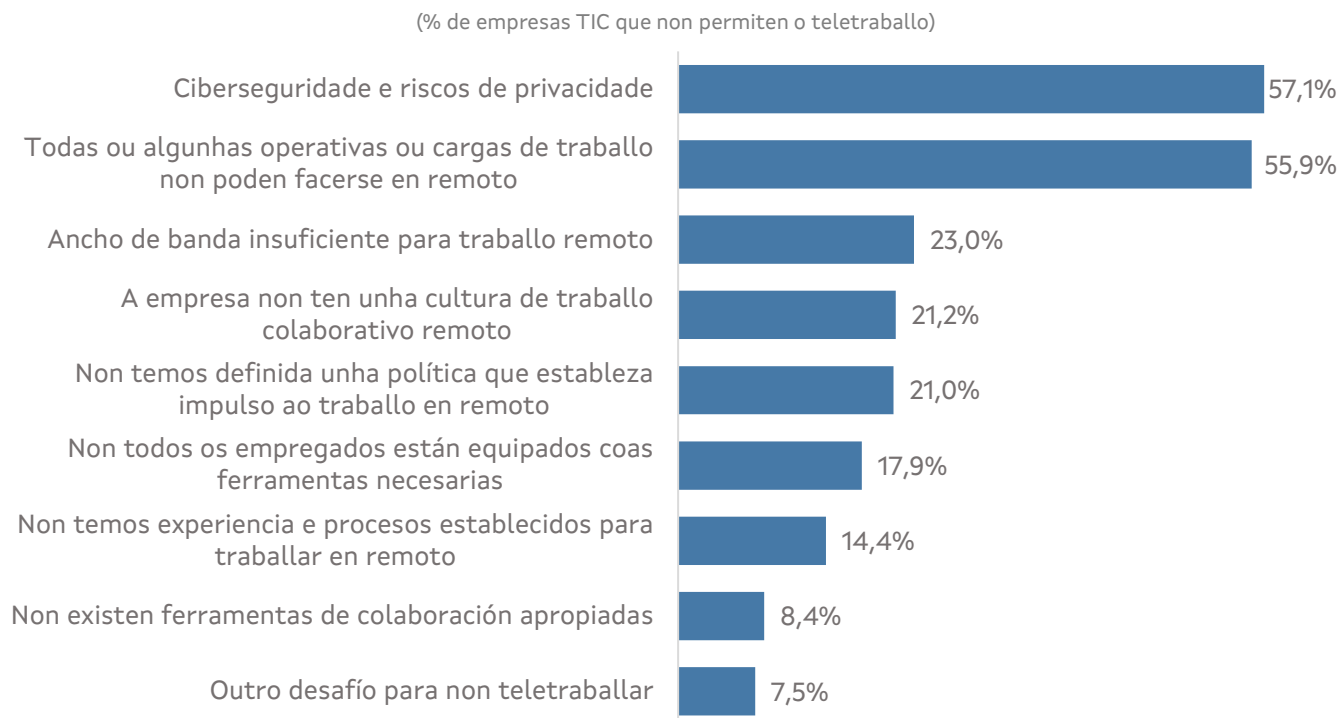
A maioría das empresas TIC permiten o teletraballo ós seus traballadores, polo que están expostos a novas ameazas, xa que precisan garantir o acceso a documentos, servizos e ferramentas aos seus traballadores. É máis habitual nas empresas de máis de 10 traballadores/as, onde esta porcentaxe alcanza case un 86%. Entre as principais razóns para non permitir o teletraballo atópanse a **ciberseguridade e riscos de privacidade, co 57,1%**, e que todas ou algunhas das operativas **non poden facerse en remoto, co 55,9%**.

G. 68. Empresas TIC que permiten o teletraballo por tamaño



Fonte: OSIMGA. Base: empresas TIC en Galicia

G. 69. Principais razóns para non teletraballar



Fonte: OSIMGA. Base: empresas TIC en Galicia que non permiten o teletraballo

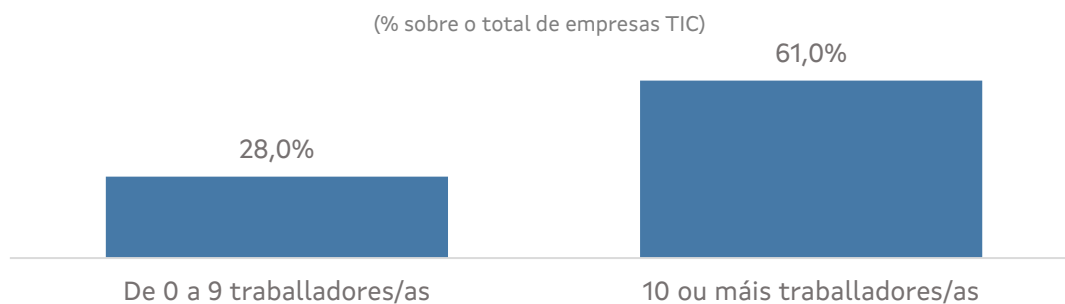
6.4 Talento especializado en ciberseguridade en Galicia

A **formación** é un elemento fundamentais á hora de prever incidentes de ciberseguridade. Entre os diferentes ámbitos nos que se desenvolven estas actuacións formativas, as empresas TIC priorizan **ciberseguridade, co 40,3% das empresas e as contornas de programación e desenvolvemento no 38,6%.**

As bases de datos e as metodoloxías de desenvolvemento e sistemas informáticos teñen á súa vez un gran peso.

Con algo menos de presenza na formación TIC atópase a xestión de Big Data, a Intelixencia Artificial, as tecnoloxías Cloud, a dirección de proxectos e as Infraestruturas TIC, con porcentaxes entre o 30% e o 20%. Por último, nesta lista figuran as tecnoloxías relacionadas coa economía verde que teñen unha dedicación algo inferior ao 5%.

G. 70. Empresas TIC que recibiron formación en TIC e ciberseguridade.



Fonte: OSIMGA. Base: empresas TIC en Galicia

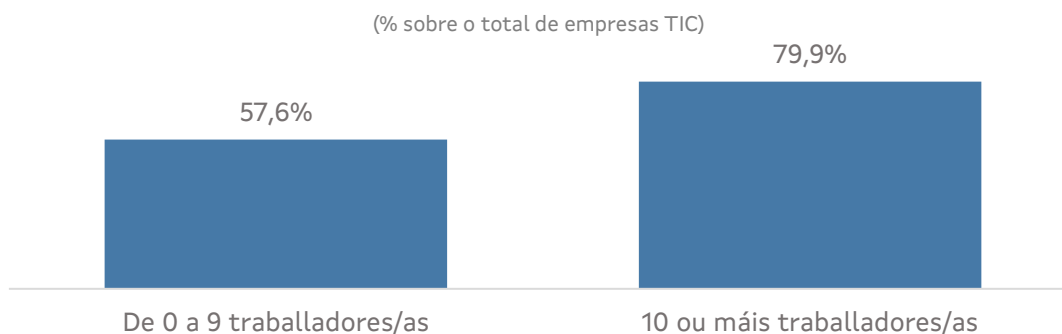
G. 71. Ámbitos da formación TIC de interese na empresa.



Fonte: OSIMGA. Base: empresas TIC interesadas en impartir formación TIC aos seus traballadores

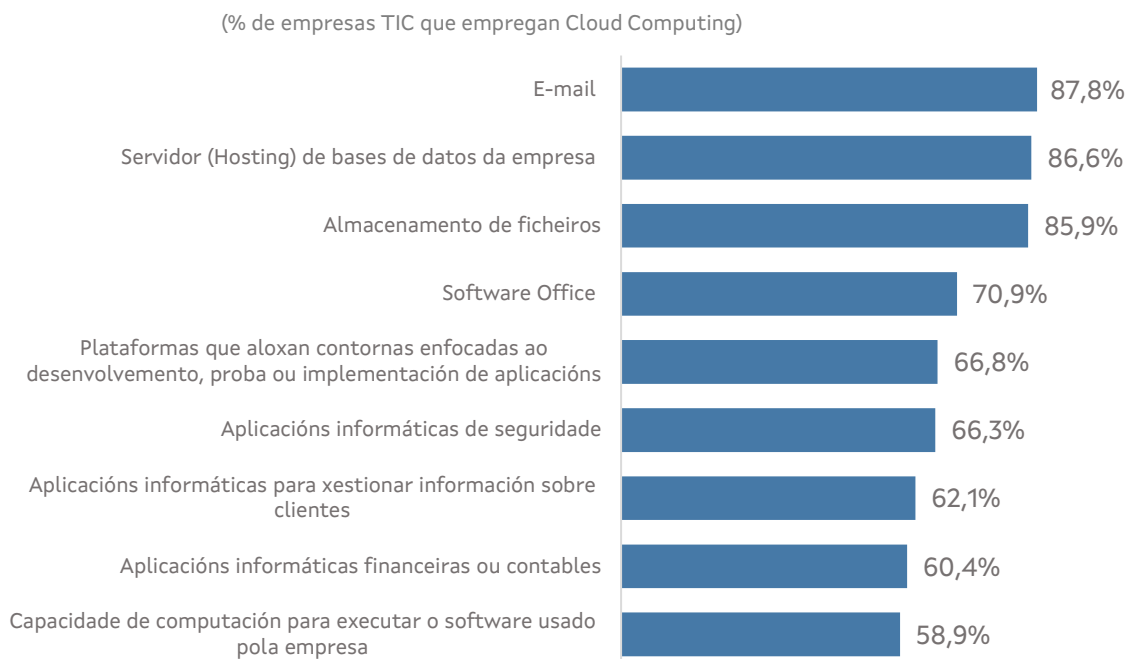
Máis da metade das empresas TIC empregan servizos de Cloud Computing. Os servizos máis utilizados, con porcentaxes maiores ao 80% son o e-mail, servidor de bases de datos da empresa e o almacenamento de ficheiros. **Tamén ocupa un lugar destacado as "aplicacións informáticas de seguridade", empregadas polo 66,3% das empresas que usan Cloud Computing.**

G. 72. Empresas TIC que empregan servizos de Cloud Computing



Fonte: OSIMGA. Base: empresas TIC en Galicia

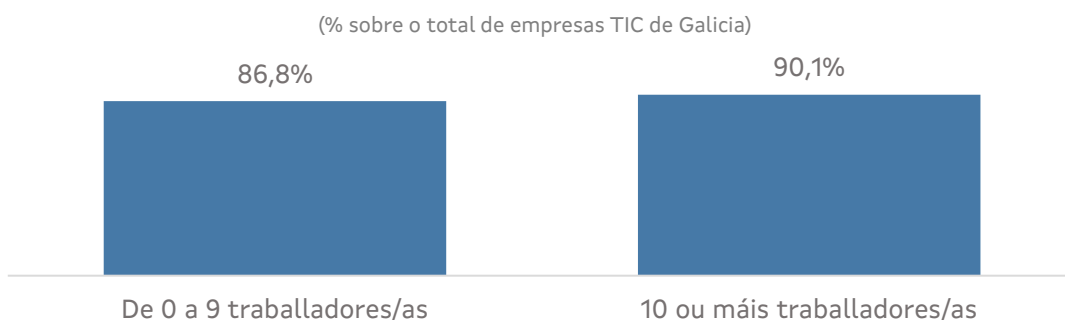
G. 73. Servizos de Cloud Computing que empregan as empresas



Fonte: OSIMGA. Base: empresas TIC que empregan Cloud Computing en Galicia

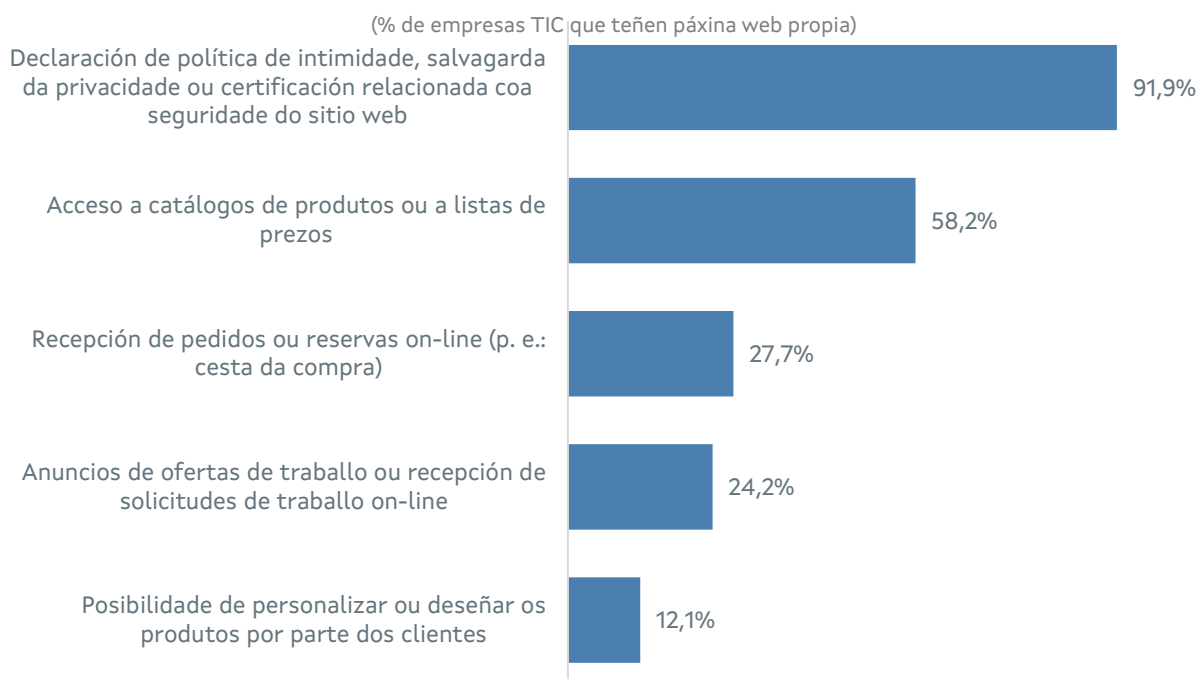
Máis do 85% das empresas TIC dispoñen dunha páxina web e o servizo máis común nestas páxinas é a **declaración de política de intimidade e seguridade da páxina**, presente en máis do 90% das empresas que contan cunha páxina web.

G. 74. Empresas TIC que dispoñen de páxina web



Fonte: OSIMGA. Base: empresas TIC en Galicia

G. 75. Servizos presentes nas páxinas web das empresas TIC

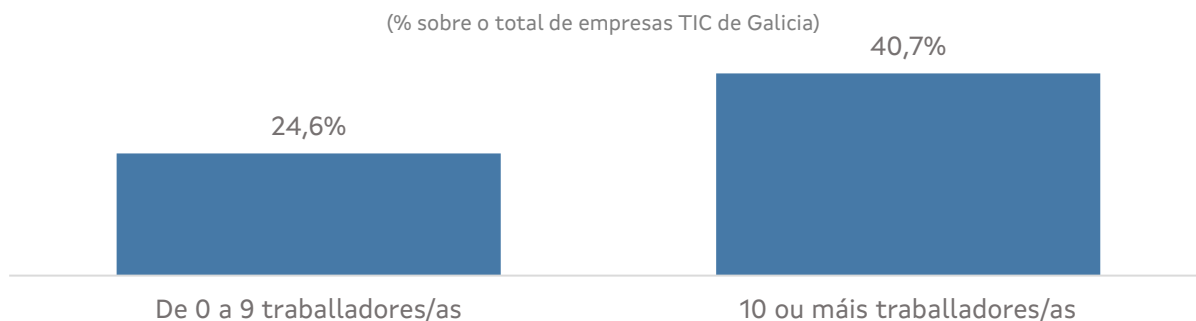


Fonte: OSIMGA. Base: empresas TIC que dispoñen de páxina web en Galicia

O uso da Intelixencia artificial nas empresas TIC galegas crece cada ano. Un 25% das empresas de 0 a 9 traballadoras/as empregan este tipo de servizo mentres que case un 41% das empresas de máis de 10 traballadores/as contan con servizos de Intelixencia Artificial.

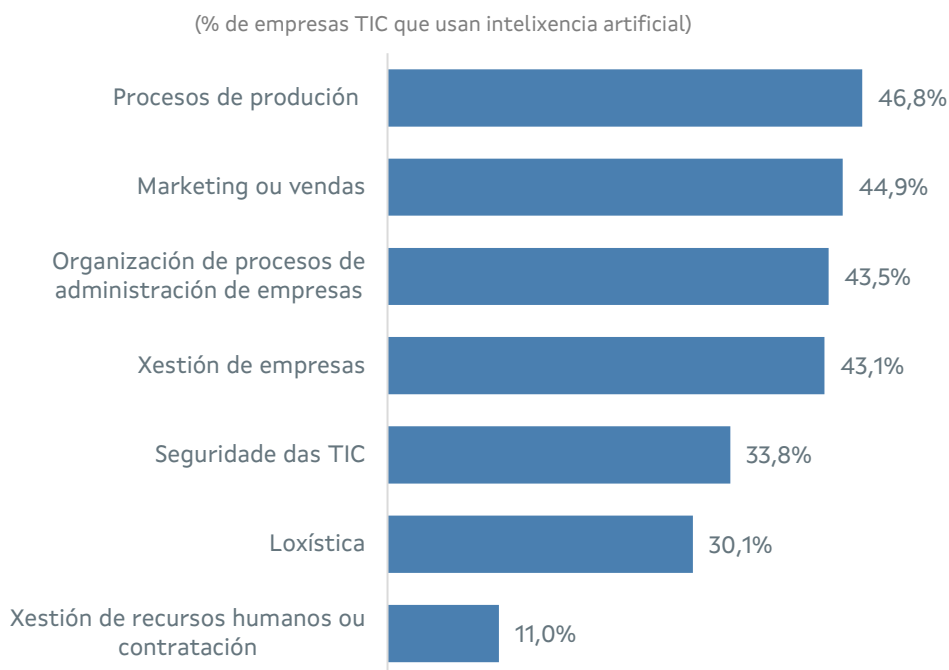
Os procesos de produción e marketing ou vendas son os usos máis comúns que as empresas TIC fan da IA. Destaca tamén usos relacionados coa organización de procesos de administración e a xestión de empresas (todos con porcentaxes superiores ó 40%). Pero tamén sobe con forza o uso da IA para "Seguridade nas TIC", acadando xa o 33,8%.

G. 76. Empresas TIC que empregan Intelixencia Artificial



Fonte: OSIMGA. Base: empresas TIC en Galicia

G. 77. Usos da Intelixencia Artificial



Fonte: OSIMGA. Base: empresas TIC que empregan intelixencia artificial en Galicia

7. Glosario de termos

Ameaza (ciberameaza): Circunstancia desfavorable na contorna dixital que se pode producir e cando sucede ten consecuencias negativas sobre os activos provocando a súa indispoñibilidade, funcionamento incorrecto ou perda de valor. Unha ameaza cibernética pode ser accidental ou intencionada. Se esta circunstancia desfavorable se produce ao mesmo tempo que existe unha vulnerabilidade ou debilidade nos sistemas ou se aproveita a súa existencia, pode dar lugar a un incidente de seguridade.

Antivirus (antimalware): Ferramenta de protección para evitar que calquera tipo de software malicioso se execute no noso ordenador.

Auditoría de seguridade: É o estudo que inclúe a análise e xestión de sistemas realizados por profesionais das tecnoloxías da información co obxectivo de identificar, enumerar e describir as distintas vulnerabilidades que se poidan presentar nunha revisión exhaustiva de estacións de traballo, redes de comunicación, servidores ou aplicacións.

Autenticación: Acción pola que se lle demostra a outra persoa ou sistema que somos quen realmente dicimos que somos, mediante un documento, contrasinal, trazo biolóxico, etc.

Backup: Copia de seguridade que se realiza en ficheiros ou aplicacións contidos nun dispositivo coa finalidade de recuperar os datos no caso de que o sistema de información sufra danos ou perda accidental/intencionada dos datos almacenados.

Brecha de seguridade: Violacións da seguridade que provocan a destrución, perda ou alteración accidental ou deliberada de datos persoais cando se transmiten, almacenan ou se someten a outro tratamento. As violacións de seguridade tamén afectan ás comunicacións ou accesos non autorizados a tales datos.

Centro Criptolóxico Nacional: Axencia encargada de garantir a seguridade das Tecnoloxías da Información e a Comunicación (TIC) nas distintas entidades do Sector Público, así como a seguridade dos sistemas que procesan, almacenan ou transmiten información clasificada.

CERT: É o equipo de expertos encargado de dar resposta ás incidencias de seguridade que se producen nas redes de comunicación e nos sistemas informáticos. O seu traballo consiste en desenvolver medidas preventivas e reactivas que ofrecen como resposta a incidencias, como publicar alertas sobre ameazas e vulnerabilidades ou ofrecer axuda para mellorar a seguridade dun sistema. En España é INCIBE e en Galicia é CSIRT.gal.

Certificado de autenticidade: Etiqueta de seguridade especial que acompaña ao software con licenza legal para evitar a falsificación.

Certificado dixital: Ficheiro informático xerado por unha entidade denominada Autoridade de Certificación que asocia datos de identidade cunha persoa física, organización ou empresa, confirmando así a súa identidade dixital en Internet.

Ciberataque: Intento deliberado dun cibercriminal de acceder non autorizado a un

sistema informático mediante diferentes técnicas e vulnerabilidades para realizar actividades con fins maliciosos, como roubo de información, extorsión ao propietario ou simplemente danar o sistema.

Ciberdelincuente: Persoa que realiza actividades delituosas na rede contra persoas ou sistemas informáticos, podendo causar danos económicos ou reputacionais mediante roubos, filtracións de información, deterioración de software ou hardware, fraude e extorsión.

Ciberseguridade: Protección dos activos de información, mediante o tratamento de ameazas que poñen en risco a información que é procesada, almacenada e transportada polos sistemas de información que están interconectados.

Confidencialidade: Propiedade da información, pola cal se garante que só é accesible ao persoal autorizado. A confidencialidade da información é a pedra angular da seguridade da información. Xunto coa integridade e dispoñibilidade representan as tres dimensións da seguridade da información.

Contrasinal: Forma de autenticación mediante unha clave secreta para controlar o acceso a algún recurso ou ferramenta. No caso de que non se facilite o contrasinal correcto, non se permitirá o acceso a ditos elementos.

Cookie: Pequeno ficheiro que almacena información enviada por un sitio web e que se almacena no ordenador do usuario, para que o sitio web poida consultar a actividade previa do usuario.

Cortalumes (Firewall): Sistema de seguridade composto por programas ou dispositivos hardware situados nos puntos fronteirizos dunha rede que teñen como obxectivo permitir e limitar o fluxo de tráfico entre as distintas zonas que protexe en función dun conxunto de estándares e outros criterios.

Documentos de seguridade TIC: no contexto das estatísticas procedentes na enquisa de uso das TIC e o comercio electrónico nas empresas, que realiza o INE, enténdese por documentos de seguridade TIC: "cobren a información dos traballadores no uso das TIC, medidas de seguridade TIC, avaliación das medidas de seguridade TIC, plans para actualizar os documentos de seguridade TIC, etc.)".

Esquema Nacional de Seguridade: Norma que establece a política de seguridade no uso dos medios electrónicos, constituída por principios básicos e requisitos mínimos que permitan unha adecuada protección da información.

Xestión de incidencias: Relación de procedementos previamente documentados sobre os pasos a seguir en caso de detectar unha ameaza de ciberseguridade na empresa. A xestión de incidencias ten como obxectivo mitigar un incidente de seguridade no menor tempo posible, identificándoo e asignando o persoal que atenderá dentro duns parámetros predefinidos.

Incidente de seguridade: Calquera evento que afecte á confidencialidade, integridade ou dispoñibilidade dos activos de información da empresa, por exemplo: acceso ou intento de acceso a sistemas, uso non autorizado, divulgación, modificación ou destrución de información.

Malware: É un tipo de software que pretende danar ou infiltrarse nun sistema de información sen o consentimento do seu propietario.

Rede privada virtual (VPN): É unha conexión virtual punto a punto entre dúas redes LAN utilizando unha rede pública como Internet para a conexión e facendo que esta conexión sexa segura grazas ao cifrado da comunicación.

Software: Conxunto de programas, instrucións e regras informáticas que permiten executar diferentes tarefas nun dispositivo. O software conforma todas aquelas accións que se poden realizar grazas ás instrucións previamente contempladas e programadas e incluídas dentro dun programa que permite ao usuario interactuar co sistema dun xeito sinxelo e intuitivo.

Virus: Malware cuxa principal característica é que infecta ficheiros executables ou sectores de arranque dos dispositivos de almacenamento.

Vulnerabilidade: Debilidade ou fallo dun sistema que pode ser explotado con fins maliciosos, normalmente a través dun programa chamado exploit. Cando se descubre, o programador do software ou hardware solucionarao lanzando unha actualización de seguraza para o produto.

Wifi: Rede de dispositivos inalámbricos interconectados que xeralmente tamén están conectados a Internet a través dun punto de acceso inalámbrico. Trátase por tanto dunha rede LAN que non utiliza un cable físico para o envío da información.

8. Índice de gráficos

G. 1. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses	9
G. 2. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses, segundo o sexo	9
G. 3. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses, segundo a idade	10
G. 4. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses segundo estudos	10
G. 5. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos de uso privado nos últimos 12 meses segundo a súa situación sociolaboral.....	11
G. 6. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos de uso privado nos últimos 12 meses segundo a provincia	11
G. 7. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos de uso privado nos últimos 12 meses, segundo o tipo de hábitat.....	12
G. 8. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses por Área	12
G. 9. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos de uso privado nos últimos 12 meses nos 7 concellos de maior poboación.....	13
G. 10. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses segundo o número de persoas no fogar	13
G. 11. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses segundo o nivel de ingresos do fogar	14
G. 12. Persoas que tiveron un incidente de ciberseguridade nos seus dispositivos para uso privado nos últimos 12 meses segundo convivan con nenos.....	14

G. 13. Tipo de incidente de seguridade que sufriu en internet nos últimos 12 meses	15
G. 14. Tipo de incidente de seguridade que sufriu en internet nos últimos 12 meses. Evolución 2018-2022	15
G. 15. Evolución do grao de confianza no uso de Internet en Galicia (Evolución 2018-2022)	16
G. 16. Accións levadas a cabo para protexer o acceso a súa información persoal en internet nos últimos 12 meses	17
G. 17. Accións levadas a cabo para protexer o acceso a súa información persoal en internet nos últimos 12 meses, evolución dos datos de 2018 a 2022.....	18
G. 18.Porcentaxe de persoas que coñecen o funcionamento das cookies e/ou realizaron modificacións na configuración das cookies.....	18
G. 19.Información persoal proporcionada a través de internet nos últimos 12 meses	19
G. 20.Información persoal proporcionada a través de internet nos últimos 12 meses. Evolución 2018-2022.....	19
G. 21.Actualización dos produtos de seguridade informática.....	20
G. 22.Actualización dos produtos de seguridade informática. Evolución 2018-2022	20
G. 23.Acceso a internet por unha rede wifi distinta á do seu domicilio	20
G. 24.Acceso a internet por unha rede wifi distinta á do seu domicilio. Evolución 2018-2022.....	21
G. 25.Verifica que a rede wifi á que accede a internet é distinta á do seu domicilio cumpre cuns requisitos mínimos de seguridade	21
G. 26.Medidas de seguridade no teléfono móbil.....	22
G. 27.Medidas de seguridade no teléfono móbil. Evolución 2018-2022.....	22
G. 28.Empresas con algún incidente de seguridade TIC).....	23
G. 29.Tipos de incidencias de seguridade informática	24
G. 30.Como realizan a seguridade TIC as empresas.....	24

G. 31. Empresas con seguro fronte a incidencias de seguridade TIC	25
G. 32. Empresas con formación en seguridade TIC	25
G. 33. Empresas con documentación sobre seguridade	26
G. 34. Revisión da documentación sobre seguridade TIC	26
G. 35. Empresas con algún protocolo de seguridade TIC para o acceso remoto	27
G.36. Empresas con medidas de seguridade TIC	28
G.37. Empresas con medidas de seguridade TIC: evolución e comparativa (España e Galicia)	28
G.38. Empresas con medidas de seguridade TIC: evolución e comparativa (España e Galicia)	29
G.39. Tipoloxía de Medidas de Seguridade que empregan	29
G. 40. Empresas que ofrecen produtos ou servizos de ciberseguridade	30
G. 41. Empresas que ofrecen produtos ou servizos de ciberseguridade en 2021 e 2022	30
G. 42. Gráfica. Empresas que venden produtos ou servizos de ciberseguridade por sector de actividade.	31
G. 43. Empresas que venden produtos ou servizos de ciberseguridade por número de traballadores.	31
G. 44. Empresas que venden produtos ou servizos de ciberseguridade por número de traballadores (2021 e 2022)	31
G. 45. Empresas que venden produtos ou servizos de ciberseguridade por sedes.....	32
G. 46. Empresas que venden produtos ou servizos de ciberseguridade por sedes (2021 e 2022)	32
G. 47. Tipo de produtos que ofrecen	33
G. 48. Tipo de produtos que ofrecen (2021 e 2022)	33
G. 49. Tipo de servizos ofertados.	34
G. 50. Tipo de servizos ofertados (2021 e 2022)	34

G. 51.Comercialización de produtos ou servizos por tipo de cliente.	35
G. 52.Comercialización de produtos ou servizos por tipo de cliente (2021 e 2022).....	35
G. 53.Porcentaxe derivada da venda de produtos e servizos de ciberseguridade sobre o importe neto da facturación	36
G. 54.Empresas TIC que sufriron incidentes de ciberseguridade	37
G. 55.Tipos de incidentes de ciberseguridade que sufriron as empresas TIC	37
G. 56.Empresas TIC que sufriron incidentes de seguridade por subsector.....	38
G. 57.Empresas TIC que sufriron incidentes de seguridade por tamaño	38
G. 58.Empresas TIC que sufriron incidentes de seguridade por lugar da sede	38
G. 59.Empresas TIC que utilizan medidas de seguridade TIC	39
G. 60.Medidas de seguridade TIC empregadas polas empresas TIC	39
G. 61.Empresas TIC que utilizan medidas de seguridade TIC por subsector.....	40
G. 62.Empresas TIC que utilizan medidas de seguridade TIC por tamaño	40
G. 63.Empresas TIC que utilizan medidas de seguridade TIC por provincia da sede	40
G. 64.Empresas TIC que realizan ou non compras por Internet.....	41
G. 65.Razóns polas que non realizaron compras por internet.....	41
G. 66.Empresas TIC que realizan ou non vendas por Internet	42
G. 67.Razóns polas que non realizaron vendas por internet.....	42
G. 68.Empresas TIC que permiten o teletraballo por tamaño.....	43
G. 69.Principais razóns para non teletraballar	43
G. 70. Empresas TIC que recibiron formación en TIC e ciberseguridade.	44

G. 71. Ámbitos da formación TIC de interese na empresa.	44
G. 72. Empresas TIC que empregan servizos de Cloud Computing.....	45
G. 73. Servizos de Cloud Computing que empregan as empresas	45
G. 74. Empresas TIC que dispoñen de páxina web	46
G. 75. Servizos presentes nas páxinas web das empresas TIC	46
G. 76. Empresas TIC que empregan Intelixencia Artificial.....	47
G. 77. Usos da Intelixencia Artificial	47