Informe sobre a ciberseguridade nas empresas de Galicia

Edición 2025

AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA

Edita: Xunta de Galicia

Axencia para a Modernización Tecnolóxica de Galicia (Amtega)

Lugar: Santiago de Compostela

Ano: 2025

Informe sobre a ciberseguridade nas empresas de Galicia.

Edición 2025

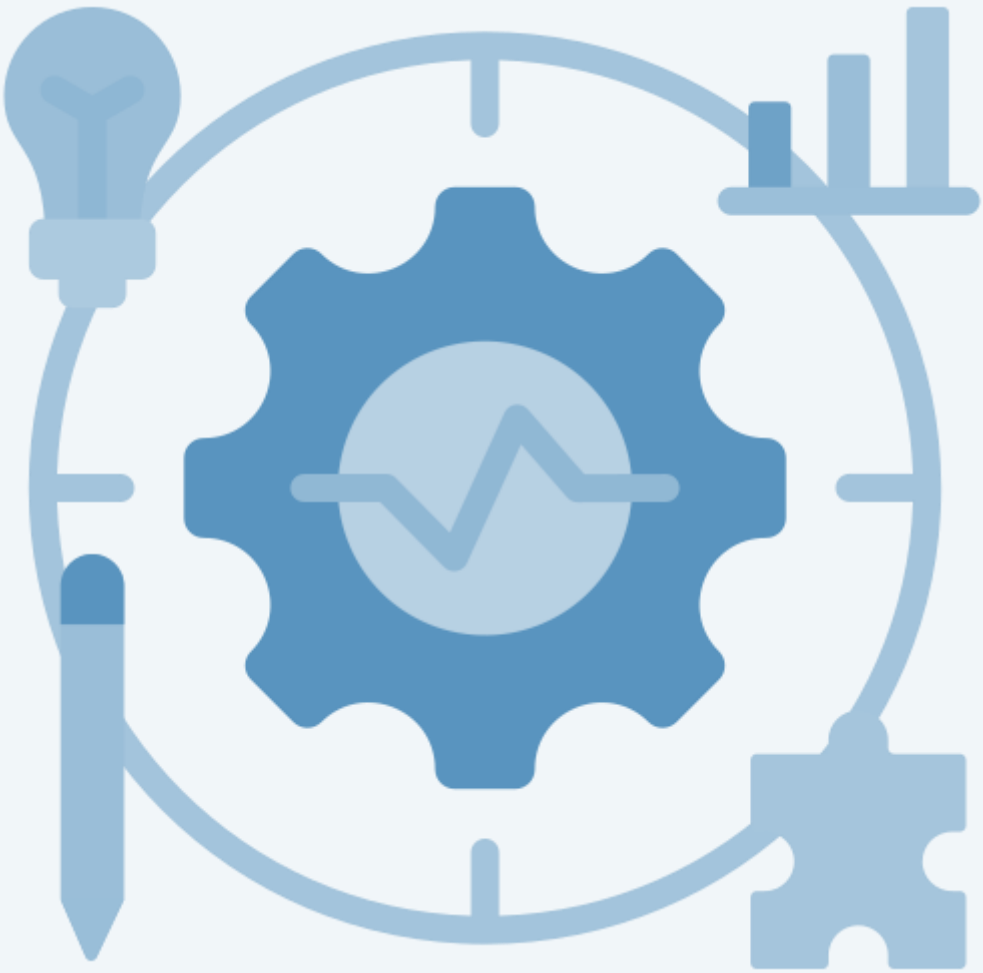
Observatorio da Sociedade da Información e a Modernización de Galicia (OSIMGA)

Xunta de Galicia

Consellería de facenda e administración pública

Axencia para a Modernización Tecnolóxica de Galicia (Amtega)
Santiago de Compostela
2025

ÍNDICE DE CONTIDOS



I. PRESENTACIÓN

1. PRESENTACIÓN

Este informe contén a análise dos resultados da Enquisa sobre ciberseguridade nas empresas Galegas en 2025.

A enquisa é froito da cooperación por unha parte da Subárea de Seguridade e OSIMGA, dependentes da Axencia para a Modernización Tecnolóxica de Galicia (AMTEGA), e do IGE mediante o "Convenio de colaboración entre a Axencia para a Modernización Tecnolóxica de Galicia e o Instituto Galego de Estatística para optimizar as estatísticas no ámbito da sociedade da información" polo que o IGE se encarga do deseño mostral, proxecto técnico presentado e aprobado no Consello Galego de Estatística, tarefas de traballo de campo e depuración de resultados. O deseño do cuestionario, planificación e análise faise en colaboración entre o IGE e OSIMGA.

Esta colaboración impulsou a redacción do proxecto técnico "4102-03 Enquisa de ciberseguridade nas empresas galegas", que será de aplicación en 2026. Con todo, en 2025 realízase a primeira edición desta enquisa, que ten previsto repetirse un ano máis, e permite a elaboración deste informe.

Segundo o Instituto Nacional de Ciberseguridade, a ciberseguridade defínese como o conxunto de mecanismos e prácticas destinadas a protexer os sistemas de información, as redes, os dispositivos e os datos da exposición na Rede ante ataques mal intencionados, o acceso non autorizado e a destrución ou alteración dos mesmos.

Os principais obxectivos da ciberseguridade inclúen:

- Confidencialidade: garantir que a información sensible sexa só accesible a usuarios autorizados.
- Integridade: asegurar a exactitude e fiabilidade dos datos, evitando modificacións non autorizadas.
- Dispoñibilidade: asegurar que os sistemas e a información estean accesibles e operativos cando se precisen.

Cando se consegue rachar con algúns deses obxectivos, as ameazas poden provocar roubos, extorsións, falta de dispoñibilidade de servizos, difusión de información ou acoso, entre outros.

Por iso, nun entorno cada vez máis dixitalizado, a ciberseguridade converteuse nun piar fundamental para as organizacións. A protección dos datos e os sistemas fronte

a ameazas dixitais é esencial para garantir a continuidade da actividade, a privacidade da información e a confianza dos clientes e empregados, entre outros. Galicia, como rexión cun tecido empresarial diverso, non é allea aos desafíos que supón a seguridade no espazo dixital.

Co fin de comprender mellor a situación actual e os retos que afrontan as empresas galegas en materia de ciberseguridade, deseñouse esta operación estatística co obxectivo de recompilar datos que permitan:

- Identificar a percepción das ameazas dixitais que teñen as empresas, e o coñecemento da regulación e normativa que lles afecta nesta materia.
- Coñecer as medidas adoptadas, os incidentes sufridos e as súas consecuencias na actividade da empresa ou na protección e integridade da información que manexan.
- Coñecer os recursos investidos e usados na protección contra ameazas cibernéticas e as razóns destes investimentos.
- Estudar a actuación das empresas ante ameazas ou incidentes cibernéticos a través da asistencia externa, accións de mellora, actividades formativas e persoal especialista.

Os resultados obtidos axudan a proporcionar un panorama máis claro do estado da ciberseguridade na comunidade autónoma e poderán servir como base para o desenvolvemento de políticas e estratexias que reforcen a resiliencia das empresas fronte a ciberataques.

1.1. Motivación do informe

Ante a crecente dixitalización das empresas e a interconexión de todos os sistemas tecnolóxicos, é preciso achegarse con maior detalle ás medidas e incidentes que acontecen, xa que poden afectar á seguridade e continuidade da actividade das empresas, e as persoas e a dereitos fundamentais.

Se ben existen enquisas que tratan o tema da ciberseguridade en Galicia, detectouse que o seu alcance non chegaba aos obxectivos do Nodo galego de ciberseguridade (CIBER.gal) e de OSIMGA sobre o análise da sociedade da información.

As limitación das fontes de datos actuais e que pretende superar esta enquisa son:

- A Enquisa sobre uso das TIC e o comercio electrónico que realiza o Instituto Nacional de Estadística (INE) achega a AMTEGA resultados desagregados para Galicia, mediante o convenio co IGE. Porén, o cuestionario non é tan amplo e non aborda en detalle outros aspectos de interese como son as consecuencias dos incidentes de ciberseguridade, as medidas tomadas tras sufrilos, autoavaliación, as fontes externas utilizadas tras sufrir ataques, as accións de mellora previstas, a inversión en ciberseguridade e a formación. Esta enquisa tampouco ofrece posibilidades de desagregación por sector da empresa, tamaño ou provincia ao presentar mostras insuficientes.
- A Enquisa ao sector TIC que realiza a propia OSIMGA comprende unicamente ás empresas galegas encadradas dentro dos servizos, o comercio e a industria TIC. Aínda que esta enquisa pregunte en detalle sobre ciberseguridade, comprende unha poboación de empresas distinta da deste informe, que inclúe todas as áreas de actividade, a excepción do sector primario.

1.2. Obxectivos específicos

A poboación obxecto de estudo: Empresas con sede social en Galicia e que conten con un ou máis asalariados no réxime xeral en polo menos un establecemento en Galicia e con actividade incluída nas seccións: B a J e L, M e N da CNAE-2009[1].

Exclúense aquelas empresas que realizan actividade TIC recollidas nos epígrafes: 26.1, 26.2, 26.3, 26.4, 26.8, 46.5, 58.2, 61.1, 61.3, 62.0, 63.1 e 95.1 da CNAE-2009.

No ámbito temporal, a información sobre incidentes de ciberseguridade fai referencia ao último ano, entendido como os últimos doce meses dende a realización da enquisa.

Este estudo pretende dar resposta aos seguintes obxectivos de investigación:

1. Nivel de preparación da empresa fronte a posibles ataques ou incidentes de ciberseguridade.
2. Medidas de seguridade TIC que aplica a empresa.
3. Incidentes de seguridade sufridos pola empresa.
4. Consecuencias dos incidentes de seguridade sufridos.
5. Fontes das que se recibe asistencia externa tralos incidentes.
6. Accións que se prevén levar a cabo para mellorar a ciberseguridade da empresa.
7. Actividades formativas en ciberseguridade ofertadas pola empresa aos seus empregados.
8. Persoas/ especialistas encargadas de realizar funcións relativas á ciberseguridade.
9. Recursos utilizados fronte ás amenzas de ciberseguridade.
10. Investimento da empresa en ciberseguridade.
11. Razón principal pola que inviste en ciberseguridade.
12. Existencia de revisións periódicas sobre a normativa de ciberseguridade.

[1] **No anexo figura a descrición dos códigos.**

1.3. Metodoloxía da enquisa

Neste estudo as unidades de mostraxe (elementos do marco sobre o que se toma a mostra) coinciden coas unidades elementais (elementos da poboación en estudo) e coas informantes.

Unidades de mostraxe: Empresas con sede en Galicia cun asalariado ou máis no réxime xeral en polo menos un establecemento en Galicia e con actividade incluída nas seccións: B a J e L, M e N da CNAE-2009. Exclúense aquelas empresas que realizan actividade TIC recollidas nos epígrafes: 26.1, 26.2, 26.3, 26.4, 26.8, 46.5, 58.2, 61.1, 61.3, 62.0, 63.1 e 95.1 da CNAE-2009.

Unidade informante: Empresas seleccionadas na mostra.

Unidades excluídas ou limiares: Empresas e autónomos sen asalariados, así como todas as empresas correspondentes ás seccións non incluídas anteriormente. O marco poboacional empregado foi o Directorio de empresas e unidades locais do IGE.

Dado que interesa saber cal é o nivel de ciberseguridade en distintos sectores económicos fíxose tamén a agrupación por:

a) Industria (Sectores B, C, D , E)

b) Construción F

c) Comercio G

d) Hostalaría I

e) Servizos (resto de)

Método de mostraxe: estratificada, no que as variables de estratificación son o tamaño das unidades definido polo número de asalariados, e os sectores de actividade.

Estratos considerados e criterios de estratificación: Consideramos 15 estratos definidos polo cruce de: empresas de 1 a 9 traballadores, de 10 a 49 e de máis de 50 traballadores cos 5 sectores de actividade: industria, construción, comercio, hostalaría e resto de servizos.

Determinación do tamaño da mostra: calcúlase o tamaño preciso de mostra en cada estrato utilizando a afixación de Neymann . O resultado para un erro relativo do 5% para o estimador do global e para o estimador en cada un dos cinco sectores sería:

Actividade	1-9 ASALARIADOS	10-49 ASALARIADOS	50 OU MÁIS ASALARIADOS
INDUSTRIA	66	55	425
CONSTRUCIÓN	247	130	84
COMERCIO	64	25	126
HOSTALARÍA	281	84	33
OUTROS SERVIZOS	97	56	240

Tamaño teórico da mostra: 2013 empresas e collen como marco o directorio de empresas do IGE.

1.4. Dixitalización nas empresas de Galicia

A dependencia das empresas duns servizos dixitais que funcionen axeitadamente vese reflexados nos datos de dixitalización. O Instituto Nacional de Estatística publicou os resultados da última Enquisa sobre uso das tic e o comercio electrónico o pasado mes de outubro de 2025, con datos sobre ese mesmo ano.

Segundo esa enquisa, o uso da Intelixencia artificial que fan as empresas galegas é do 15,7%, tras experimentar un crecemento do 51,1% no último ano. Crece tamén o uso do Cloud Computing, que pasou do 31,5% ao 38,2% no mesmo período de tempo. Outro dos indicadores do grao de dixitalización das empresas galegas é a incorporación dos especialistas TIC. O 13,1% das empresas de máis de 10 empregados conta con este perfil profesional, un 4% máis no último ano, o que converte a Galicia na novena comunidade autónoma con máis proporción de especialistas TIC no seu tecido empresarial.

A enquisa do INE apunta, tamén, a un maior gasto en ciberseguridade por parte das empresas galegas. No último ano, os recursos destinados á seguridade TIC en Galicia achegáronse aos 126 millóns de euros, o que supón un crecemento do 23,6%, case o dobre que media estatal.

Por outra banda, o 30,9% de las empresas galegas de 10 ou máis traballadores permiten o teletraballo e o 65,3% utilizan medios sociais na rede, o que as sitúa no oitavo lugar a nivel estatal.

O 85% das grandes empresas galegas dispoñen de páxina web. A maioría contan con descrición dos seus produtos e servizos (84,6%), e o 16% permite facer perdidos e reservas.

A maioría das empresas galegas de 10 e máis empregados usan o Software libre. Co 82,5%, superan en máis dun punto media estatal. Delas, o 93,6% dispón de navegadores de código aberto, o 71,4% de aplicación ofimáticas, o 49,2% de sistemas operativos e o 45,6% software de seguridade.

As microempresas

O 75,2% das microempresas galegas ten conexión a internet, e destas, o 79,1% dispón de banda larga móbil, 3G ou superior. Das que acceden á rede, o 33,3% empregan

medios/redes sociais con fins empresariais. Ademais, o 33,7% das empresas de menos de 10 traballadores ten páxina web.

Vendo todos eses datos, é doado comprender como a ciberseguridade debe ser un tema fundamental, que afecta a moitos ámbitos de actividade na maioría das empresas.

1.5. Datos sobre ciberseguridade

Fogares galegos

A Enquisa estrutural a Fogares do IGE, de 2024, amosa como a ciberseguridade no fogar consolidouse como unha necesidade esencial para todas as familias. No ano 2024, o 17 % das dos galegos e galegas que utilizaron Internet nos últimos 12 meses experimentaron algún incidente relacionado coa ciberseguridade nos seus dispositivos de uso persoal (+18,1% respecto ao ano anterior). Estes incidentes inclúen roubo de datos, intentos de acceso non autorizado ás súas contas, suplantación de identidade, acoso ou a recepción de correos electrónicos maliciosos, entre outros.

Sector tic en Galicia

O 14,2% das empresas galegas dedicadas ás tic sufriu un incidente de ciberseguridade durante o 2024. Os incidentes máis frecuentes foron os intentos de estafa e os ataque de virus informáticos.

As principais medidas adoptadas polas empresas TIC foron manter o software actualizado (93%), ter un sistema de autenticación mediante contrasinal forte (90,9%) e facer copias de seguridade de datos nunha localización separada (88,3%).

Empresas galegas (INE 2024)

Os últimos datos sobre ciberseguridade nas empresas dispoñibles a nivel galego proceden da Enquisa sobre uso das tic e do comercio electrónico nas empresas, do INE. As definicións de incidentes e medidas de seguridade difiren ás deste informe, polo que os datos non deben considerarse comparables. Reproducímolos aquí, a título informativo.

O uso de medidas de ciberseguridade continúa a ser máis habitual nas grandes empresas que nas microempresas galegas. No ano 2024 mantense arredor do 90% nas primeiras, ao crecer respecto a 2022 pero case o mesmo dato que en 2021.

En cambio, as empresas pequenas galegas manteñen a tendencia descendente no uso da ciberseguridade, quedando no 51%.

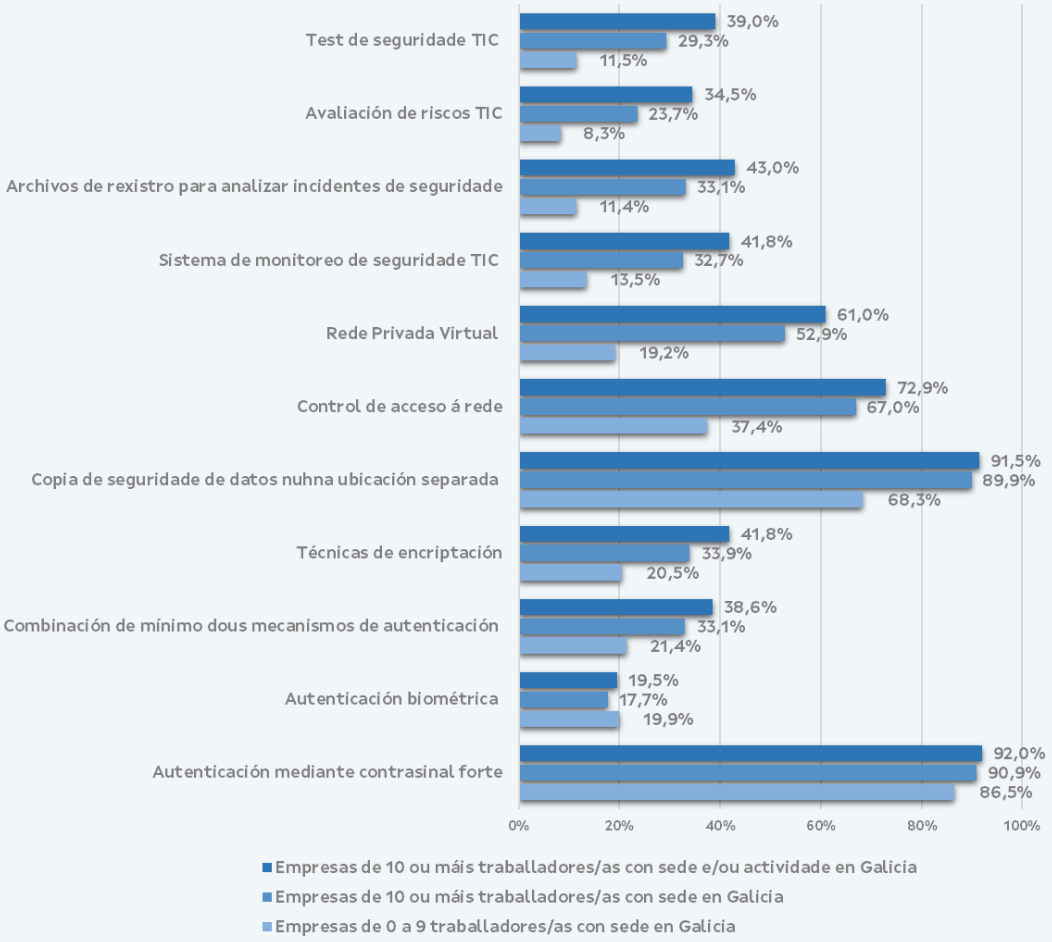
As medidas de seguridade TIC empregadas con maior frecuencia polas empresas galegas, tanto as grandes como as pequenas, son autenticación mediante contrasinal forte, seguida da copia de seguridade de datos nunha localización separada e en terceiro lugar control de acceso á rede.

Un 19,7% das empresas de máis de 10 traballadores con sede ou actividade en Galicia tivo algún incidente de seguridade TIC. O incidente máis repetido nestas empresas son a falta de dispoñibilidade dos servizos TIC por erros no software e hardware; en menor medida destacan os incidentes debidos a ataques exteriores.

No caso das microempresas, destaca tamén a destrución ou corrupción de datos por erros de hardware ou software.

G. 1. Tipoloxía de medidas de seguridade aplicadas por empresas galegas en 2024 (INE)

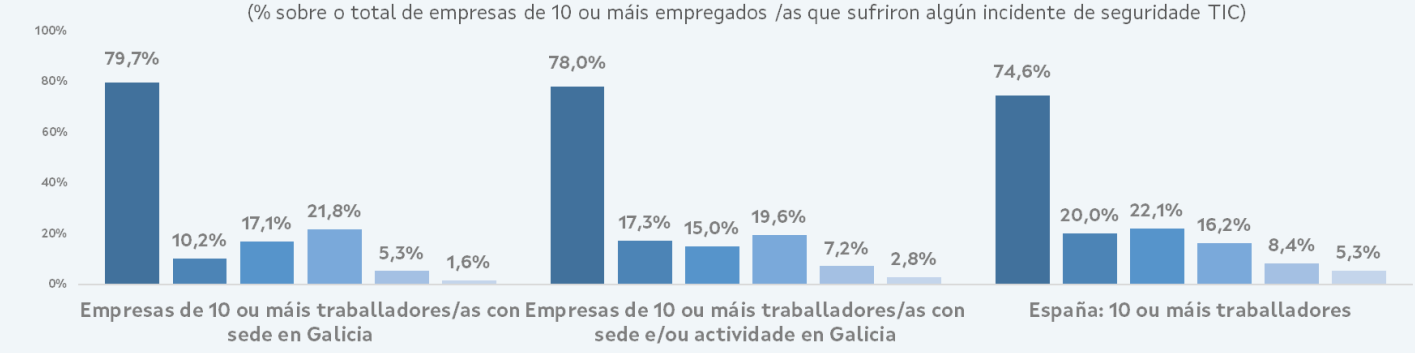
(% sobre o total de empresas que empregan algunha medida de seguridade TIC)

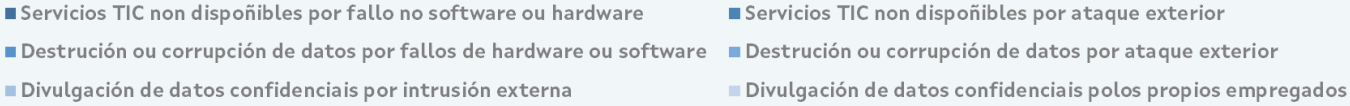


Fonte: INE (2024)

G. 2.Empresas de 10 ou máis traballadores/as con algún incidente de seguridade TIC: Galicia e España

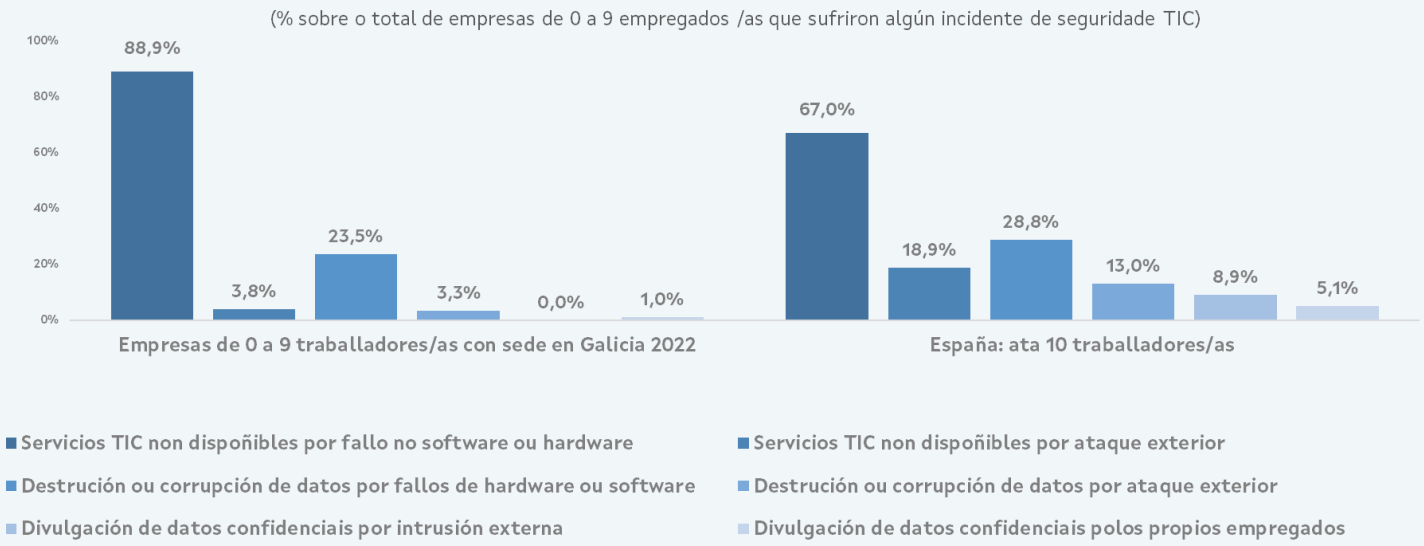
(% sobre o total de empresas de 10 ou máis empregados /as que sufriron algún incidente de seguridade TIC)





Fonte: INE (2024)

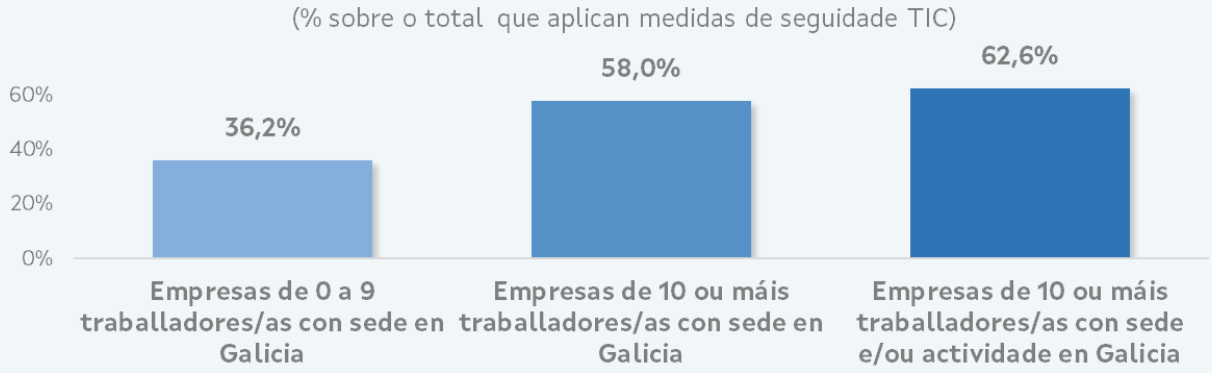
G. 3.Empresas de menos de 10 traballadores con algún incidente de seguridade TIC: Galicia e España



Fonte: INE (2024)

Máis do 58% das empresas de 10 ou máis empregados que aplican medidas de seguridade TIC fan que os seus empregados coñezan as súas obrigas en materia de seguridade. O principal medio é a formación voluntaria.

G. 4.Empresas que fan que os seus empregados coñezan as súas obrigas en materia de seguridade: Galicia



Fonte: INE (2024)

2. INCIDENTES DE CIBERSEGURIDADE

2. INCIDENTES DE CIBERSEGURIDADE

A partir deste punto, preséntanse os resultados da Enquisa sobre ciberseguridade ás empresas galegas. O traballo de campo fíxoo o IGE ao longo de 2025 a análise é efectuada por OSIMGA.

Neste primeiro bloque analízanse os incidentes de ciberseguridade. Aquí, a principal diferenza con outras enquisas é que se separan os incidentes (tipo de ataque sufrido) das consecuencias (prexuízos sufridos).

No seguinte bloque detallaranse as medidas preventivas aplicadas. Entenderase como tales a calquera tipo de recurso como servizos contratados, software, accións de protección, recursos humanos, formación, contratación de empresas, etc.

No último capítulo detállase a medida en que as empresas se consideran preparadas para enfrontarse á ciberseguridade.

Os resultados obtidos axudan a proporcionar un panorama máis claro do estado da ciberseguridade na comunidade autónoma e poderán servir como base para o desenvolvemento de políticas e estratexias que reforcen a resiliencia das empresas fronte a ciberataques.

Amosaranse todos os resultados estatísticos cruzados por sector e tamaño da empresa, o que nos permitirá amosar que son as empresas máis grandes as que utilizan máis medidas de seguridade e as que sofren máis incidentes (están máis expostos por ter máis equipos e servizos en liña), aínda que hai importantes matices por sector de actividade.

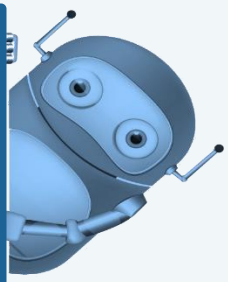
2.1. Incidentes de ciberseguridade

O 15,5% das empresas galegas sinalan que sufriron algún incidente de ciberseguridade no último ano.

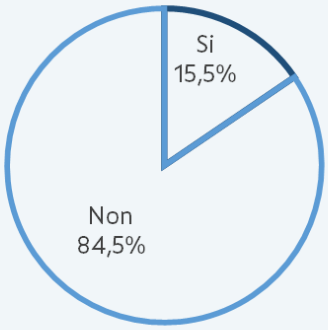
Nas empresas de máis de 49 traballadores, sufriu incidentes case a metade, o 47,8%.

Por sectores, todos superan o 14% de empresas con incidentes a excepción da hostalaría, que só se veu afectada no 7,6% dos casos.

O 15,5% das empresas galegas sufriron algún incidente de ciberseguridade no último ano

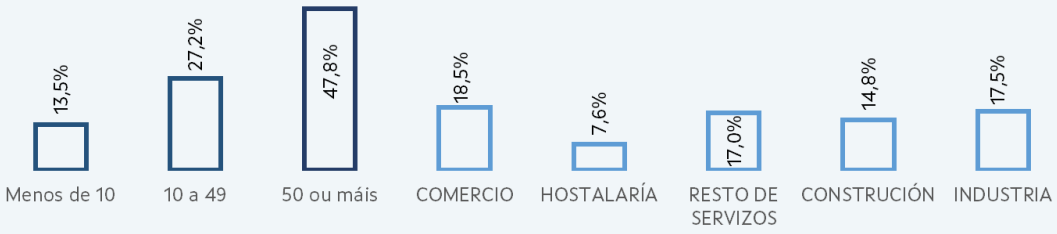


G. 5.Empresas incidentes de ciberseguridade no último ano



Fonte: OSIMGA-IGE

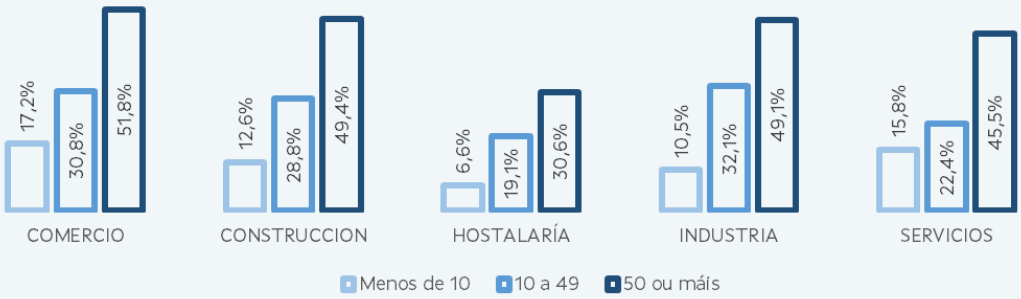
G. 6. Empresas que sufriron incidentes de ciberseguridade no último ano por sector e por tamaño



Case a metade das empresas de 50 ou máis traballadores sufriron incidentes

Fonte: OSIMGA-IGE

G. 7. Empresas que sufriron incidentes de ciberseguridade cruzadas por sector e por tamaño



Fonte: OSIMGA-IGE

A clase de incidente de seguridade que máis afecta ás empresas galegas é o phising, ou intentos de obter información suplantando unha identidade de alguén externo á empresa. Cabe subliñar que o segundo caso por incidencia ten semellanzas, ao tratarse de suplantación de identidade dentro da empresas, co 2,6%.

Os ataques por virus informáticos e de denegación de servizos afectaron a máis do 2% das empresas no último ano.

As intrusión en sistemas mediante accesos non autorizados afectaron ao 1,9% de empresas galegas.

A instalación de software malicioso para danar sistemas ou datos tamén supera o 1% de afectación a empresas.

G. 8. Clases de incidentes de ciberseguridade sufridos polas empresas

Fonte: OSIMGA-IGE

Por sectores e tamaños de empresas observamos como nas empresas grandes, a incidencia de calquera clase de incidencia de ciberseguridade é superior ás pequenas.

Por sectores de actividade, as principais ameazas afectaron máis ao sector do comercio. Máis adiante veremos que tamén está entre os peor preparados. A suplantación de identidade facéndose pasar por un empregado é máis frecuente na industria, e a perda ou roubo de dispositivos, na construción.

G. 9.Principais clases de incidentes de ciberseguridade sufridos por tamaño de empresa

Clase de incidentes	Menos de 10	10 a 49	50 ou máis
Ataques de phishing (intentos de obter información confidencial suplantando a identidade dun terceiro)	8,7%	18,1%	39,2%
Ataque de denegación de servizo (sobrecarga de sistemas para interromper o servizo ou facelo inaccesible)	2,1%	2,0%	3,2%
Infección por virus informático (introdución de virus que alteran ou destrúen datos e sistemas)	2,0%	3,5%	5,1%
Accesos non autorizados (intrusión en sistemas para obter información sen permiso)	1,9%	2,1%	3,3%
Suplantación de identidade (facerse pasar por un empregado para enganar e obteren acceso a información confidencial)	1,7%	7,1%	19,4%
Instalación de malware (software malicioso que se infiltra para danar sistemas ou datos)	1,1%	2,2%	4,4%
Perda ou roubo de dispositivos (dispositivos corporativos extraviados ou roubados)	0,5%	2,0%	10,8%

*Fonte: OSIMGA-IGE *Exclúense algunhas das categorías por razóns de segredo estatístico*

G. 10. Principais clases de incidentes de ciberseguridade sufridos por sector de actividade

Clase de incidentes	COMERCIO	HOSTALARÍA	OUTROS SERVIZOS	CONSTRUCIÓN	INDUSTRIA
Ataques de phishing (intentos de obter información confidencial suplantando a identidade dun terceiro)	14,6%	5,2%	8,9%	8,6%	10,7%
Ataque de denegación de servizo (sobrecarga de sistemas para interromper o servizo ou facelo inaccesible)	4,3%	0,0%	2,1%	0,3%	1,2%
Infección por virus informático (introdución de virus que alteran ou destrúen datos e sistemas)	3,2%	0,5%	2,3%	2,1%	1,8%
Accesos non autorizados (intrusión en sistemas para obter información sen permiso)	2,9%	0,9%	2,2%	1,2%	1,1%
Suplantación de identidade (facerse pasar por un empregado para enganar e obteren acceso a información confidencial)	3,9%	1,2%	1,4%	1,7%	4,8%
Instalación de malware (software malicioso que se infiltra para danar sistemas ou datos)	0,3%	0,4%	2,1%	2,2%	2,1%
Perda ou roubo de dispositivos (dispositivos corporativos extraviados ou roubados)	0,1%	0,6%	1,5%	1,8%	0,8%

*Fonte: OSIMGA-IGE *Exclúense algunhas das categorías por razóns de segredo estatístico*

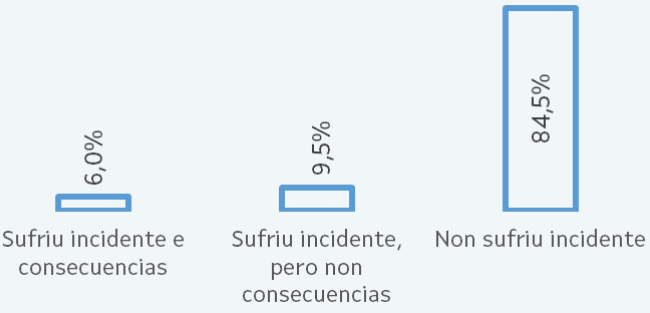
2.2. Consecuencias dos incidentes de ciberseguridade

O 15,5% das empresas sufriu incidentes de ciberseguridade, destas o 38,6% sufriu consecuencias provocadas por eses incidentes. Deste xeito, o 6% do total de empresas galegas víronse afectadas polos incidentes de ciberseguridade.

A incidencia é do 14,4% das empresas de 50 ou máis persoas empregadas e, por sectores, destaca o comercio, co 9,6%. Pero cruzando as dúas variables, a incidencia máis alta está nas empresas de construción de máis de 49 empregados, co 26,5%.

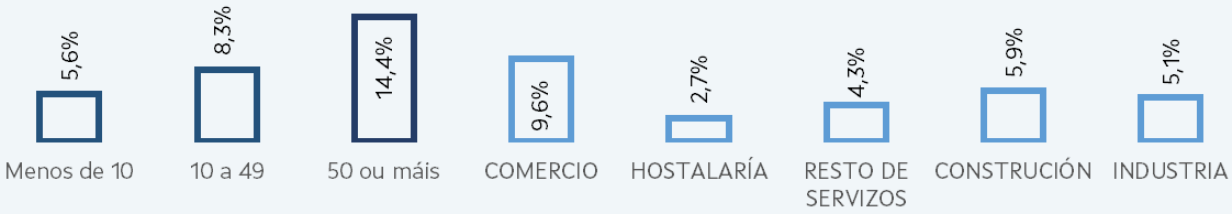
G. 11. Empresas que sufriron consecuencias dos incidentes de ciberseguridade

O 6% das empresas sufriron consecuencias provocadas polos incidentes de ciberseguridade.



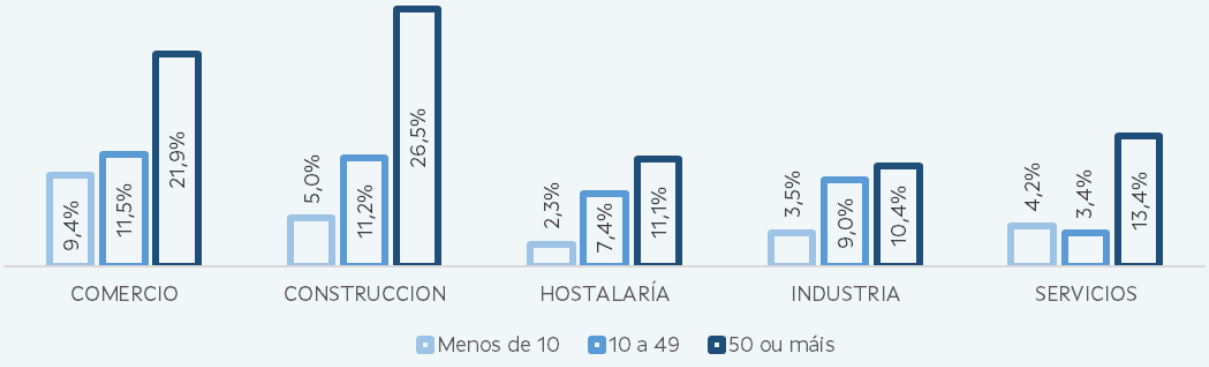
Fonte: OSIMGA-IGE

G. 12. Empresas que sufriron consecuencias dos incidentes por sector e por tamaño



Fonte: OSIMGA-IGE

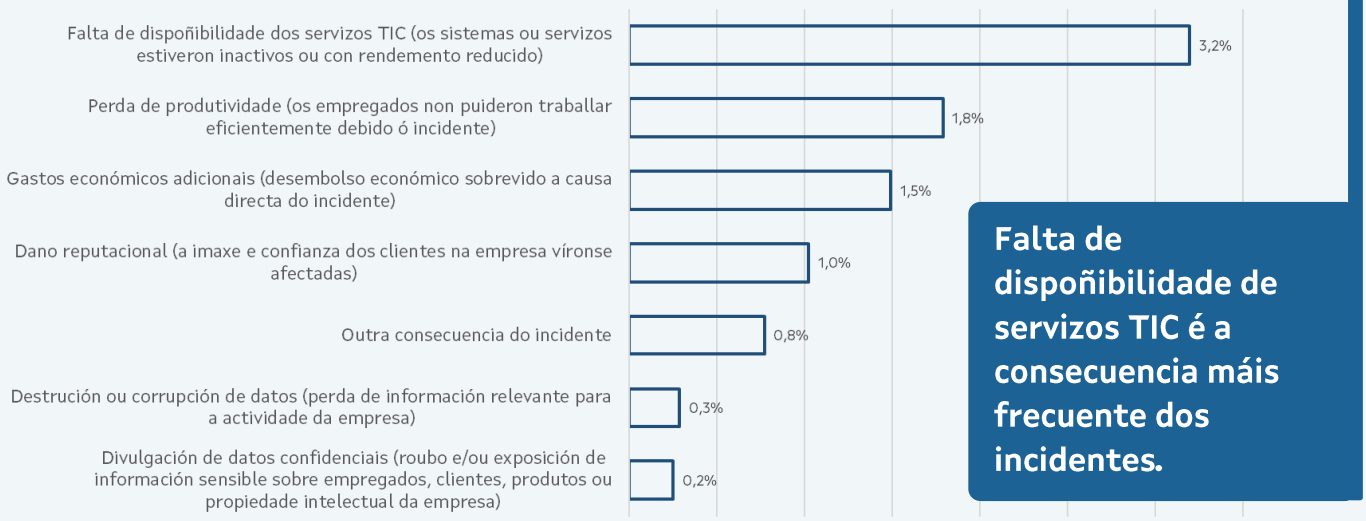
G. 13. Empresas que sufriron consecuencias dos incidentes cruzadas por sector e tamaño



Fonte: OSIMGA-IGE

A consecuencia máis habitual dos incidentes de ciberseguridade é a "falta de dispoñibilidade de servizos TIC". Afecta ao 3,2% do total de empresas, que supón o 53,3% das que sufriron algunha consecuencia dos incidentes de ciberseguridade. A perda de produtividade afectou ao 1,8% das empresas (29,8% das que sofren consecuencias dos incidentes) e gastos económicos adicionais son sinaladas polo 1,5% do total (24,8% das que sufriron algunha consecuencia).

G. 14. Consecuencias dos incidentes de ciberseguridade



Falta de dispoñibilidade de servizos TIC é a consecuencia máis frecuente dos incidentes.

Fonte: OSIMGA-IGE

G. 15. Consecuencias dos incidentes de ciberseguridade por número de empregados/as

Clase de consecuencia do incidente	Menos de 10	10 a 49	50 ou máis
Falta de dispoñibilidade dos servizos TIC (os sistemas ou servizos estiveron inactivos ou con rendemento reducido)	3,3%	2,2%	3,8%
Perda de produtividade (os empregados non puideron traballar eficientemente debido ó incidente)	1,6%	3,2%	5,8%
Gastos económicos adicionais (desembolso económico sobrevido a causa directa do incidente)	1,1%	3,6%	6,6%
Dano reputacional (a imaxe e confianza dos clientes na empresa víronse afectadas)	1,0%	0,9%	1,8%
Outra consecuencia do incidente	1,2%	2,1%	3,2%

Fonte: OSIMGA-IGE

G. 16.Consecuencias dos incidentes de ciberseguridade por sector de actividade

Clase de consecuencia do incidente	COMERCIO	HOSTALARÍA	RESTO DE SERVIZOS	CONSTRUCIÓN	INDUSTRIA
Falta de dispoñibilidade dos servizos TIC (os sistemas ou servizos estiveron inactivos ou con rendemento reducido)	6,1%	0,5%	2,9%	1,9%	1,9%
Perda de produtividade (os empregados non puideron traballar eficientemente debido ó incidente)	1,8%	0,5%	3,0%	1,9%	1,1%
Gastos económicos adicionais (desembolso económico sobrevido a causa directa do incidente)	1,8%	1,4%	0,3%	2,4%	2,4%
Dano reputacional (a imaxe e confianza dos clientes na empresa víronse afectadas)	1,4%	0,4%	0,9%	1,3%	0,7%
Outra consecuencia do incidente	1,8%	1,2%	1,1%	1,5%	0,4%

Fonte: OSIMGA-IGE

2.3. Empresas que recibiron asistencia externa tras o incidente

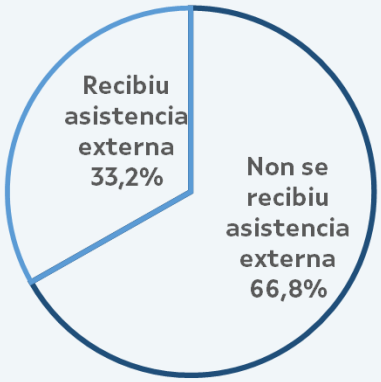
O 33,2% das empresas que sufriron incidentes de ciberseguridade, recibiron asistencia externa, que supón 4,2% do total empresas, tivesen ou non incidentes.

O 17,1% das empresas que sufriron incidentes de ciberseguridade, recibiron asistencia dunha empresa de seguridade TIC, o 7,2% dos corpos de seguridade e o 3,2% do INCIBE.

Por tamaños, as diferenzas son menores que noutras variables, xa que as empresas de menor tamaño acoden tamén a miúdo a asistencia externa (31%). No sector que máis acoden a asistencia externa tras un incidente de ciberseguridade é a industria, co 52,4%.

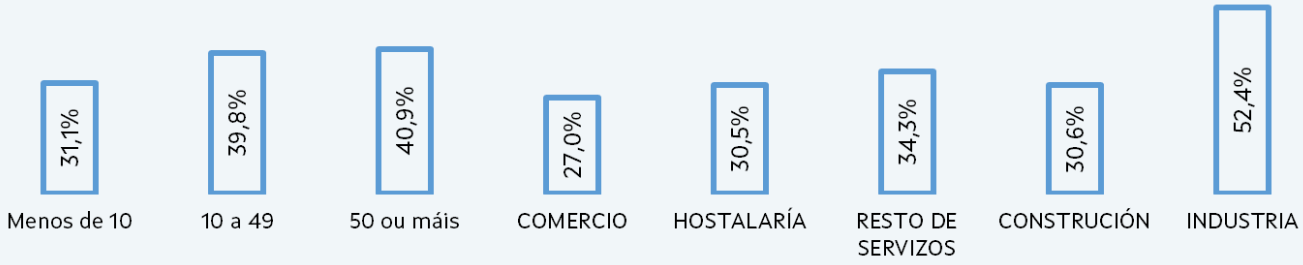
O 33,2% das empresas recibe asistencia externa tras o incidente de ciberseguridade sufrido

G. 17. Recibiron asistencia externa tras incidentes de ciberseguridade



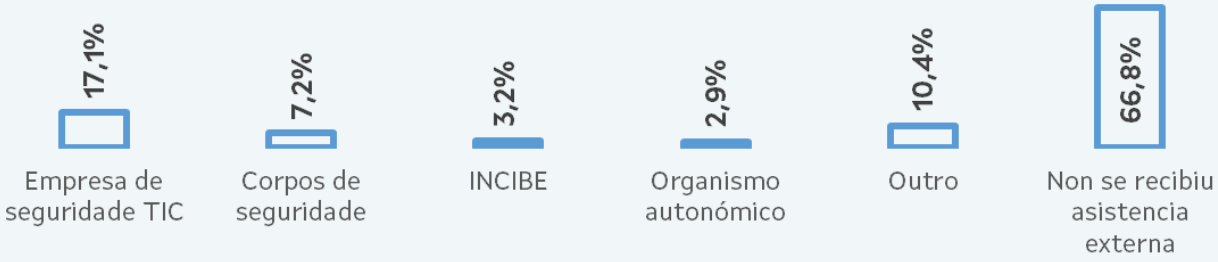
Fonte: OSIMGA-IGE

G. 18. Asistencia externa tras incidentes de ciberseguridade por sector e tamaño



Fonte: OSIMGA-IGE

G. 19. Organismo do que recibe asistencia externa tras incidentes de ciberseguridade



Fonte: OSIMGA-IGE

Dese 33,2% de empresas que reciben asistencia externa tras o incidente de ciberseguridade, o recurso máis común é unha "empresa de seguridade TIC" xa que, co 17,1% dos casos, supón máis da metade das veces que se acode a algún organismo.

As empresas de seguridade TIC son o principal recurso externo, especialmente nas empresas máis grandes e nas de Industria e resto de Servizos.

G. 20. Organismo externo ao que acoden tras incidente: tamaño da empresa

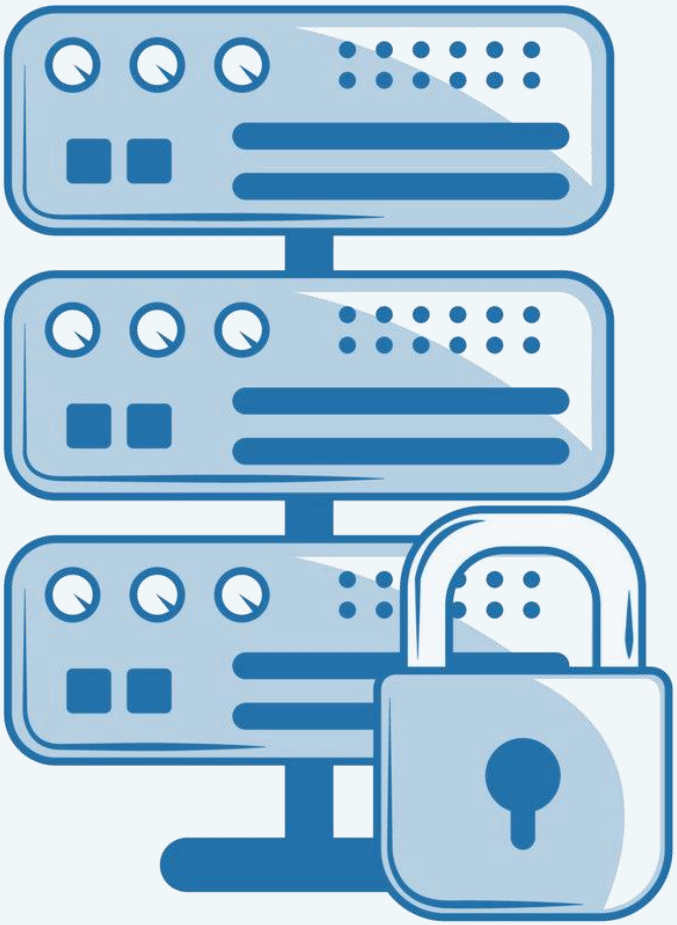
Organismo externo ao que acudiu	Menos de 10	10 a 49	50 ou máis
Empresa de seguridade TIC	14,8%	23,0%	30,7%
Corpos de seguridade	8,5%	1,9%	7,5%
INCIBE	3,8%	1,1%	2,7%
Organismo autonómico	3,8%	0,0%	0,8%
Outro	9,0%	17,1%	6,0%
Non se recibiu asistencia externa	68,9%	60,2%	59,1%

Fonte: OSIMGA-IGE

G. 21. Organismo externo ao que acoden tras incidente: sectores

Organismo externo ao que acudiu	COMERCIO	HOSTALARÍA	RESTO DE SERVIZOS	CONSTRUCIÓN	INDUSTRIA
Empresa de seguridade TIC	9,8%	7,0%	21,8%	11,9%	39,7%
Corpos de seguridade	7,8%	9,5%	5,9%	4,2%	9,6%
INCIBE	7,7%	0,1%	0,1%	0,1%	2,1%
Organismo autonómico	7,7%	0,1%	0,0%	0,0%	0,1%
Outro	9,5%	14,0%	6,8%	14,9%	13,7%
Non se recibiu asistencia externa	73,0%	69,5%	65,7%	69,4%	47,6%

Fonte: OSIMGA-IGE



3. RECURSOS DE CIBERSEGURIDADE

3. RECURSOS DE CIBERSEGURIDADE

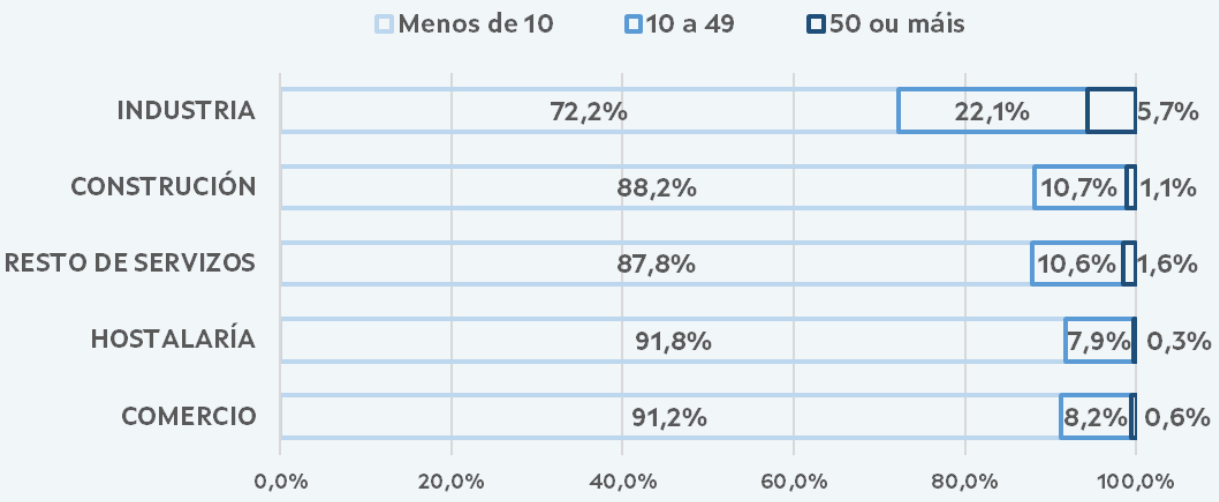
Mentres no capítulo anterior deuse conta das incidencias e consecuencias dos ataques á seguridade TIC, neste capítulo descríbense en detalle os recursos que utiliza a empresa para previr e impedir os incidentes de ciberseguridade.

Para isto enténdese recursos dende un punto de vista xeral, incluíndo medidas de prevención concretas, formación, gasto ou persoal especialista.

Debe terse en conta o tamaño das empresas, que fai que as necesidades e a capacidade de cada unha poida ser moi diferente. Tamén o sector é relevante, xa que a natureza de cada un pode facer que moitos dos traballadores desempeñen as súas labores conectados e que as actividades de máis valor engadido da empresa se fagan en dispositivos electrónicos.

Así, por exemplo, as empresas de máis de 10 empregados supoñen arredor do 8 a 12% en todos en todos os sectores de actividade, excepto no caso da industria, polo que cabe esperar que o comportamento da industria se pareza máis ao das empresas grandes que o doutros sectores.

G. 22. Distribución das empresas por tamaño e sector de actividade.



Fonte: OSIMGA-IGE

Por tanto, na maior parte dos casos arredor o 90% das empresas son de menos de 10 empregados, o que fai que o dato global de cada sector de actividade tenda a parecerse moito ao das empresas pequenas.

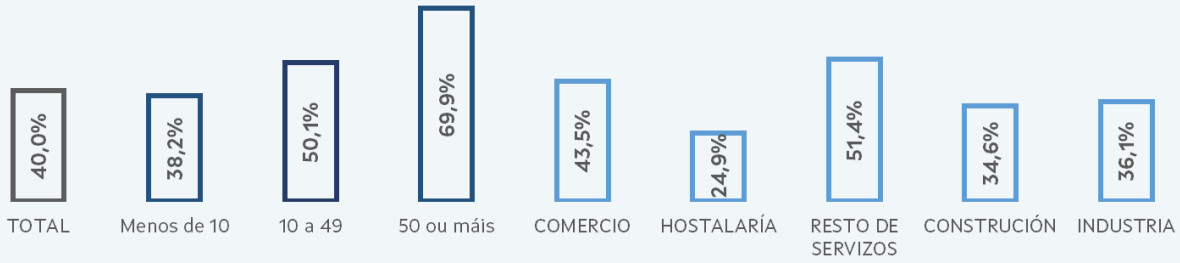
É por isto que se ofrecerá o dobre cruce, por tamaño e sector, e que así poidamos percibir a medida na que certas tendencias pódense explicar máis polo tamaño das empresas do sector que por especificades do mesmo.

3.1. Gasto en ciberseguridade

O gasto que se amose será a media total de todas as empresas, incluíndo as que non gastaron nada en ciberseguridade. Refírese ao gasto estimado para o período de 12 meses antes da enquisa e inclúe todo tipo de recursos. Este gasto pode estar dedicado a formación, adquisición de hardware ou software, contratación de persoal, obtención de certificacións, etc. En xeral, o 40% das empresas galegas realizaron algún gasto en ciberseguridade no último ano. Das que o fixeron, investiron como promedio 3.217 euros anuais.

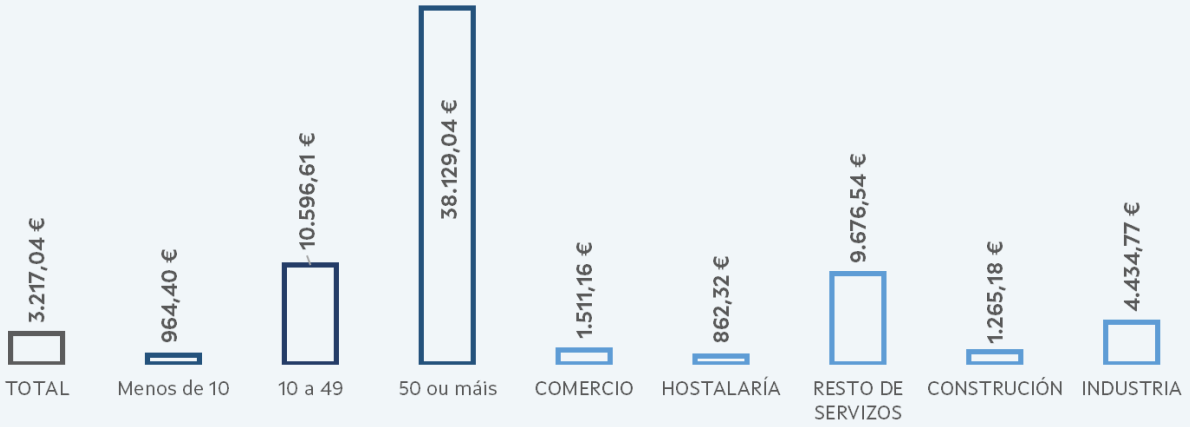
O 69,9% das empresas de 50 ou máis persoas empregadas, gastan en ciberseguridade, destacando o sector de servizos, excluído comercio e hostalaría. O sector de "outros servizos" gasta máis en seguridade en todos os tamaños de empresa, aínda que Industria e Comercio sitúanse moi preto cando son 50 persoas empregadas ou máis, estando nos tres casos arredor dos 30.000 euros de gasto medio anual.

G. 23. Empresas que gastan en ciberseguridade por tamaño e por sector.



Fonte: OSIMGA-IGE

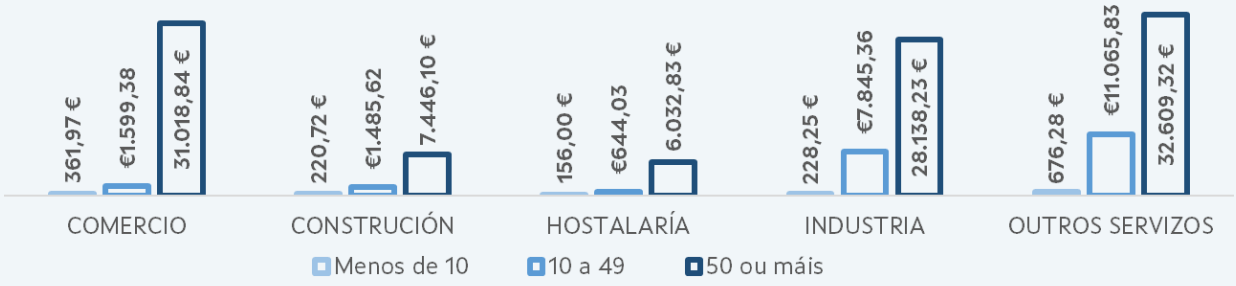
G. 24. Gasto medio en ciberseguridade, por tamaño e por sector.



Fonte: OSIMGA-IGE

Nos datos cruzados por empresa e sector apréciase mellor as diferenzas. Con todo, o gasto do "resto de servizos" é moi superior para calquera tamaño, excepto nas empresas de 50 ou máis persoas empregadas, onde o Comercio e a Industria case o igualan.

G. 25. Gasto medio en ciberseguridade, por tamaño cruzado con sector.



Fonte: OSIMGA-IGE

Das empresas que invisten en ciberseguridade, a principal razón para facelo é "salvagardar a información da empresa". Esa é o principal motivo para investir en ciberseguridade en todos os sectores e tamaños de empresa excepto o "comercio", onde destaca "redución de riscos cibernéticos", co 44,5%.

G. 26. Principal razón pola que invisten en ciberseguridade.

Fonte: OSIMGA-IGE

G. 27. Principal razón para investir en ciberseguridade por sector e tamaño de empresa

Razóns para investir	Menos de 10	10 a 49	50 ou máis	COMERCIO	HOSTALARÍA	RESTO DE SERVIZOS	CONSTRUCIÓN	INDUSTRIA
Cumprimento da normativa	15,5%	9,7%	4,9%	17,1%	25,0%	9,5%	12,6%	11,1%
Redución de riscos cibernéticos	37,0%	30,7%	39,8%	44,5%	36,1%	28,1%	38,1%	32,6%
Salvagardar a información da empresa	44,2%	53,7%	46,4%	38,3%	36,8%	55,5%	43,7%	50,2%
Responsabilidade social corporativa	1,7%	4,9%	3,4%	0,1%	0,7%	5,1%	2,7%	1,1%
Outra	1,6%	1,1%	5,5%	0,0%	1,5%	1,9%	2,9%	5,1%

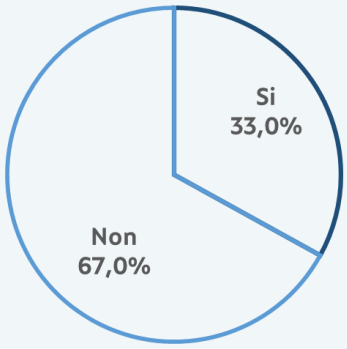
Fonte: OSIMGA-IGE

3.2. Recursos humanos

No último ano, o 33% das empresas consultadas contaban con persoas responsables ou especialistas en tarefas de ciberseguridade. Como era de esperar, a presenza destes especialistas é moito máis numerosa nas máis grandes. Por sectores, as diferenzas son reducidas. Destaca o sector "resto de servizos" (sen hostalaría e comercio), onde o 46,1% emprega persoal especialista de ciberseguridade.

O de "Resto de servizos" supera a media de especialistas en ciberseguridade en todos os tamaños de empresa, ata o máximo de 3,3 nas de 50 ou máis persoas empregadas.

G. 28.Empresas que contaron con especialistas TIC no último ano.



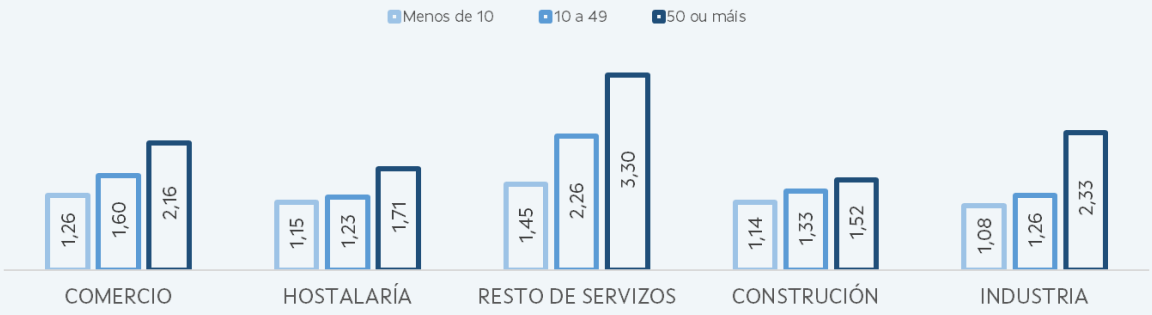
Fonte: OSIMGA-IGE

O 33% de empresas ten especialistas en ciberseguridade, os 71,3% nas de 50 ou máis persoas empregadas.

G. 29. Empresas con especialistas TIC no último ano por sector e por tamaño.

Fonte: OSIMGA-IGE

G. 30. Número medio especialistas en ciberseguridade por sector e tamaño



Fonte: OSIMGA-IGE

3.3. Actividades de mellora desenvolvidas no último ano

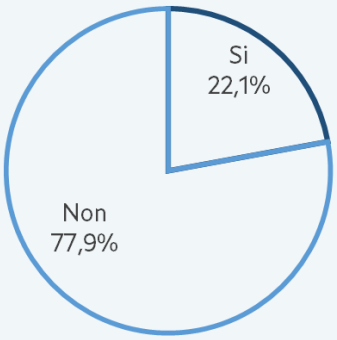
O 22,1% das empresas ofreceu ao seu persoal empregado a posibilidade, no último ano, de cursar actividades formativas sobre seguridade TIC.

Máis da metade das empresas de 50 ou máis empregados ofreceron esta posibilidade. Por sectores, no de "outros servizos" a media é máis de dez puntos superior a calquera outra, co 35,7%.

"Resto de servizos" destaca sobre os demais sectores nas empresas de menos de 50 persoas empregadas, porque nas de maior tamaño, os resultados son moi similares en todos os sectores.

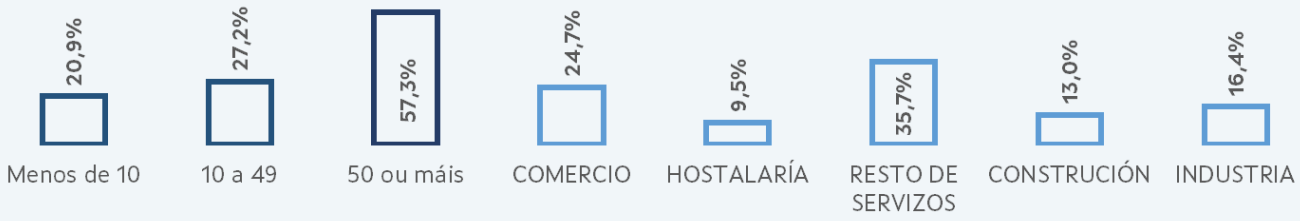
G. 31.Ofreceron actividades formativas aos empregados no último ano.

O 22,1% de empresas ofreceu actividades formativas sobre ciberseguridade ás persoas empregadas.



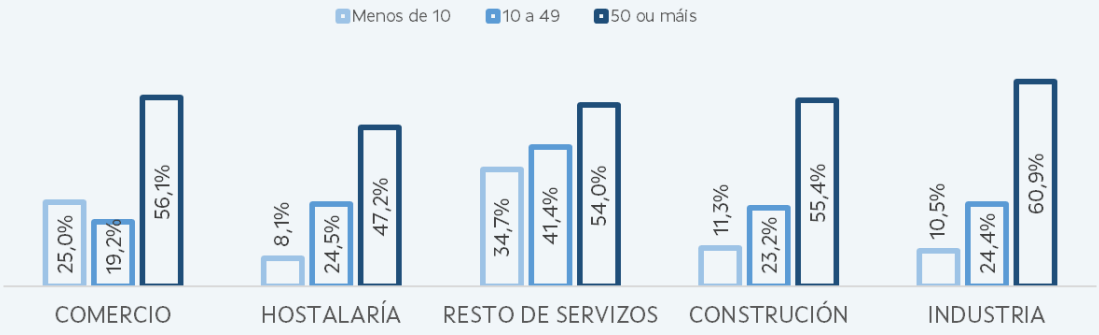
Fonte: OSIMGA-IGE

G. 32.Ofreceron formación aos empregados no último ano por tamaño e por sector



Fonte: OSIMGA-IGE

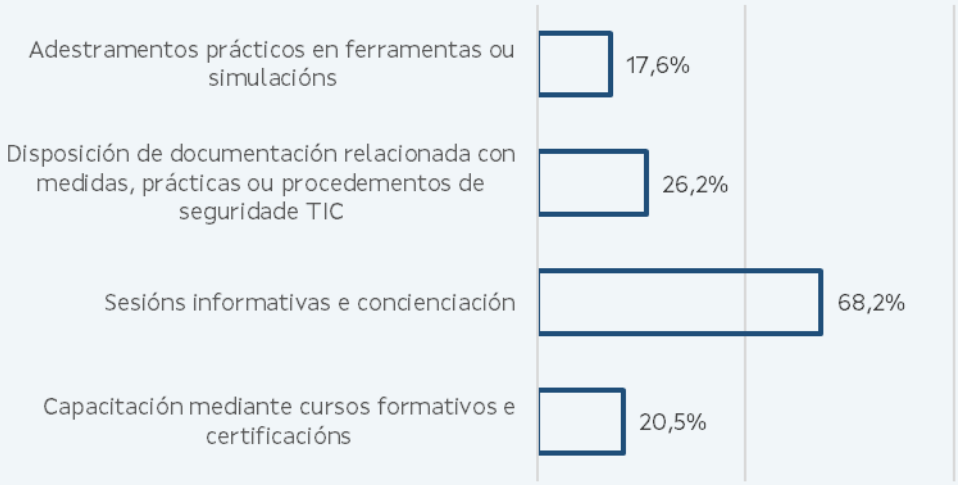
G. 33. Ofreceron formación aos empregados no último ano por tamaño e por sector



Fonte: OSIMGA-IGE

Das accións formativas ofrecidas ao persoal empregado, as máis frecuentes son as "sesións informativas e de concienciación", co 68,2%. Son as máis numerosas tamén para calquera tamaño e sector da empresa.

G. 34. Clases de actividades formativas ofertadas



Fonte: OSIMGA-IGE

G. 35. Recursos formativos ofrecidos por tamaño

Recursos formativos ofrecidos	Menos de 10	10 a 49	50 ou máis
Capacitación mediante cursos formativos e certificacións	4,0%	6,6%	18,2%
Sesións informativas e concienciación	14,0%	19,7%	44,9%
Disposición de documentación relacionada con medidas, prácticas ou procedementos de seguridade TIC	5,1%	8,3%	26,8%
Adestramentos prácticos en ferramentas ou simulacións	3,5%	5,7%	13,9%

Fonte: OSIMGA-IGE

G. 36. Recursos formativos ofrecidos por sector

Recursos formativos ofrecidos	COMERCIO	HOSTALARÍA	RESTO DE SERVIZOS	CONSTRUCIÓN	INDUSTRIA
Capacitación mediante cursos formativos e certificacións	3,2%	2,8%	8,8%	2,8%	3,6%
Sesións informativas e concienciación	17,2%	4,5%	25,0%	9,0%	11,9%
Disposición de documentación relacionada con medidas, prácticas ou procedementos de seguridade TIC	6,5%	0,9%	10,4%	3,6%	4,3%
Adestramentos prácticos en ferramentas ou simulacións	5,0%	1,6%	6,1%	1,2%	2,9%

Fonte: OSIMGA-IGE

3.4. Medidas de seguridade aplicadas na actualidade

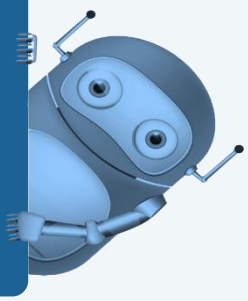
O 81,6% das empresas de Galicia aplican algunha das medidas de seguridade descritas na enquisa nos seus equipos, servizos e comunicacións TIC.

Por sector e tamaño, o uso de medidas de seguridade TIC é case total nas empresas de 50 ou máis persoas empregadas.

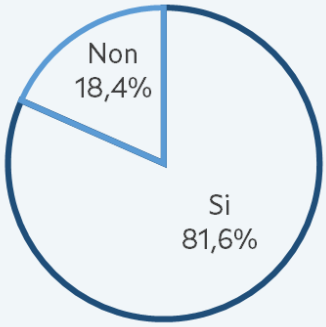
Nas empresas de 10 a 49 persoas empregadas, atopámonos con valores de aplicación de medidas de seguridade que oscilan entre o 86,2% da Hostalaría e o 100% no Comercio.

Descende a valores por debaixo do 75% nas microempresas da Industria e Hostalaría.

O 18,4% das empresas non aplica medidas de seguridade TIC, dato que sobe ata o 34% nas microempresas de hostalaría e 22,5% nas da construción

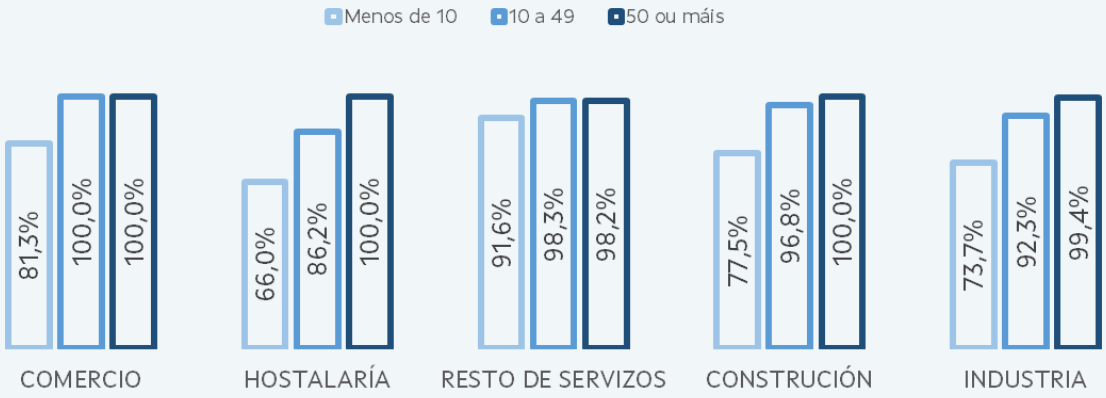


G. 37. Aplica medidas de seguridade TIC na empresa



Fonte: OSIMGA-IGE

G. 38. Aplica medidas de seguridade TIC, por sector e tamaño.



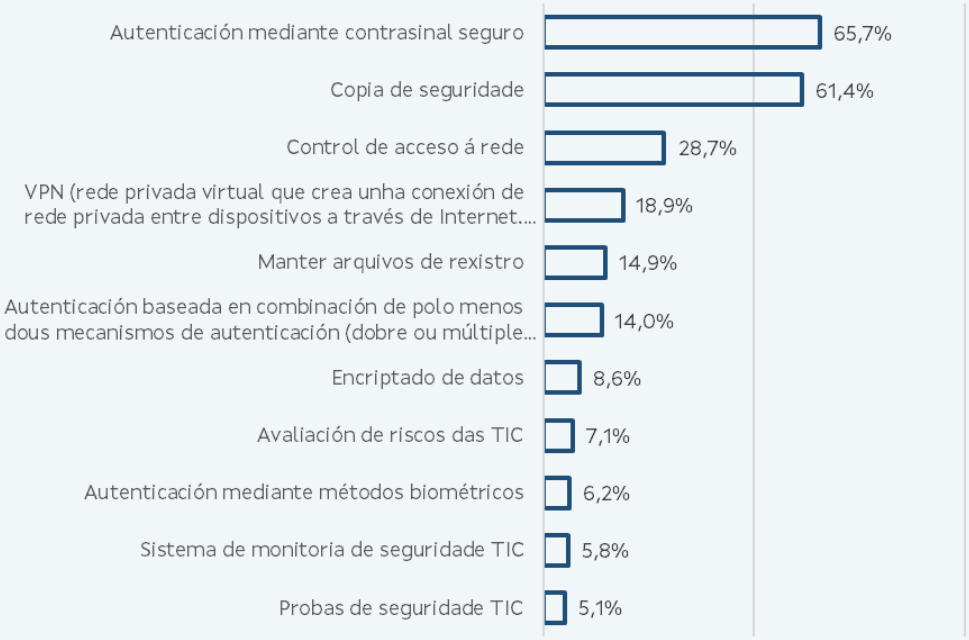
Fonte: OSIMGA-IGE

As medidas de seguridade TIC máis adoptadas polas empresas galegas son o uso de contrasinais seguros para autenticación, e as copias de seguridade, usadas por máis do 60% do total de empresas.

Nas empresas de menos de 10 persoas empregadas, o recurso máis empregado é o do contrasinal seguro, mentres nas de maior tamaño, é maioritario o da copia de seguridade.

Por sectores, só na industria úsase máis a copia de seguridade que o contrasinal seguro aínda que, recordemos que neste sector, a proporción de empresas grandes é maior que no resto.

G. 39. Medidas de seguridade TIC aplicadas.



Fonte: OSIMGA-IGE

G. 40. Medidas de seguridade TIC aplicadas por tamaño da empresa

Medidas de seguridade	Menos de 10	10 a 49	50 ou máis
Autenticación mediante contrasinal seguro	63,7%	78,5%	89,5%
Copia de seguridade	58,1%	84,2%	95,6%
Control de acceso á rede	26,5%	40,9%	71,2%
VPN	15,2%	41,3%	75,8%
Manter arquivos de rexistro	13,7%	20,9%	42,4%
Autenticación baseada en combinación de polo menos dous mecanismos de autenticación	13,0%	17,4%	46,2%
Encriptado de datos	7,4%	14,8%	39,2%
Avaliación de riscos das TIC	6,3%	9,7%	38,1%
Autenticación mediante métodos biométricos	6,2%	5,4%	10,0%
Sistema de monitoria de seguridade TIC	4,8%	10,0%	41,1%
Probas de seguridade TIC	4,1%	9,1%	38,8%

Fonte: OSIMGA-IGE

G. 41. Medidas de seguridade TIC aplicadas por sector de actividade

Medidas de seguridade	COMERCIO	HOSTALARÍA	RESTO DE SERVIZOS	INDUSTRIA	CONSTRUCIÓN
Autenticación mediante contrasinal seguro	66,7%	53,8%	79,1%	55,5%	63,8%
Copia de seguridade	58,8%	44,2%	73,1%	72,1%	60,2%
Control de acceso á rede	31,8%	16,4%	36,4%	30,3%	22,7%
Manter arquivos de rexistro	15,8%	7,5%	20,4%	16,0%	11,5%
VPN	14,6%	6,9%	33,1%	21,0%	17,5%
Autenticación baseada en combinación de polo menos dous mecanismos de autenticación	13,8%	9,5%	19,0%	11,5%	13,6%
Encriptado de datos	7,5%	3,0%	15,8%	7,2%	6,9%
Autenticación mediante métodos biométricos	6,1%	8,3%	5,1%	5,0%	6,7%
Avaliación de riscos das TIC	5,1%	1,8%	15,9%	6,0%	3,8%
Sistema de monitoria de seguridade TIC	4,8%	1,3%	10,6%	8,3%	3,5%
Probas de seguridade TIC	4,0%	0,9%	10,2%	5,8%	3,5%

Fonte: OSIMGA-IGE

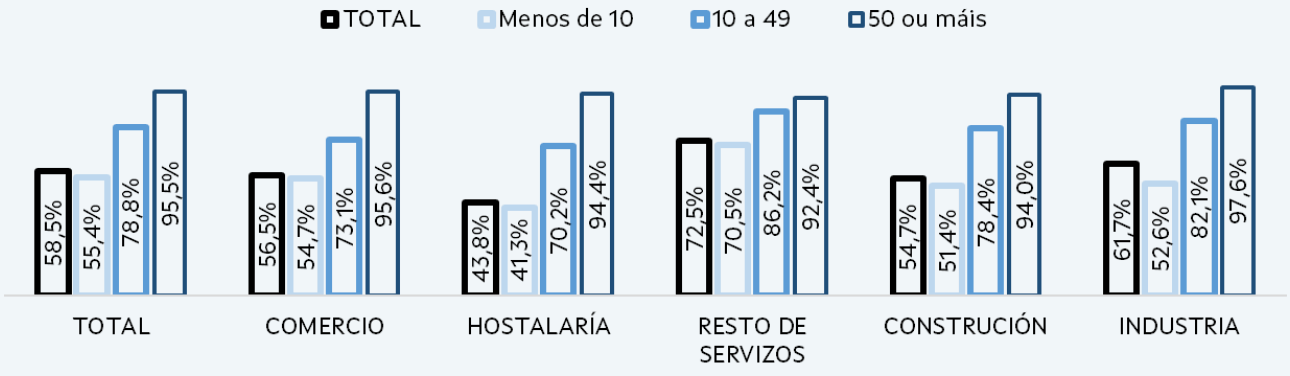
A distribución de empresas que aplican dúas ou máis medidas de seguridade amosa igualmente o maior compromiso coa seguridade das empresas de maior tamaño.

Globalmente, o 58,5% das empresas aplican dúas ou máis medidas de seguridade.

Os valores están entre o 50% e 55% nas microempresas de todos os sectores excepto hostalaría (41,3%) e resto de servizos (70,5%).

As empresas de 10 a 49 persoas empregadas oscilan entre o 70 e o 86%, mentres que nas empresas de 50 ou máis persoas empregadas ningún sector baixa do 92%.

G. 42. Empresas que aplican dúas ou máis medidas de seguridade, por sector e tamaño



Fonte: OSIMGA-IGE

Das 11 clases de medidas de seguridade que se analizaron, as empresas declararon que aplican unha media de 2,36, con resultados moi heteroxéneos por tamaño da empresa e sector.

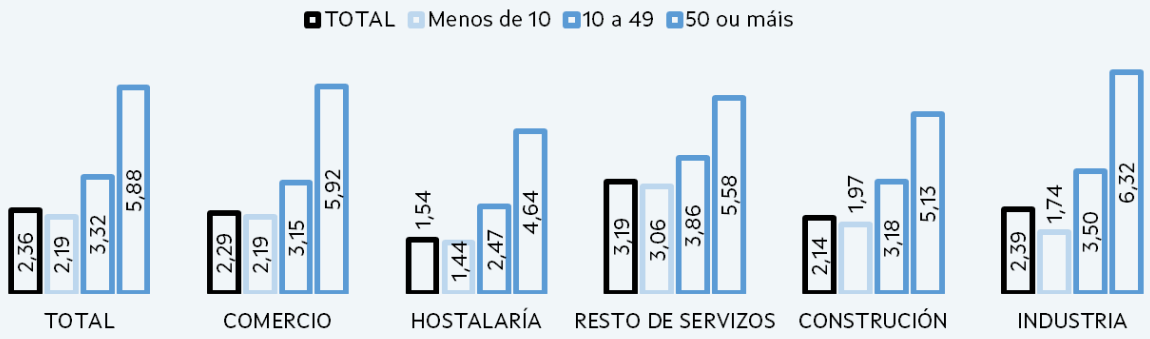
No "resto de servizos" aplícase como promedio 3,19 medidas de seguridade, máis do dobre ca en hostalaría, con 1,54.

As empresas de menos de 10 persoas empregadas, aplican como media 2,19 medidas de seguridade, oscilando entre as 1,44 da hostalaría e 3,06 do resto de servizos.

Nas empresas medianas, todas aplican unha media entre 3 e 3,5 medidas de ciberseguridade, excepto hostalaría, que queda en só 2,47.

Novamente, nas empresas de máis de 49 persoas traballadoras, a hostalaría está á cola, con 4,64 medidas, fronte á industria, que lidera o uso de medidas de seguridade TIC, cun promedio de 6,32.

G. 43. Número medio de medidas de seguridade aplicadas, por sector e por tamaño



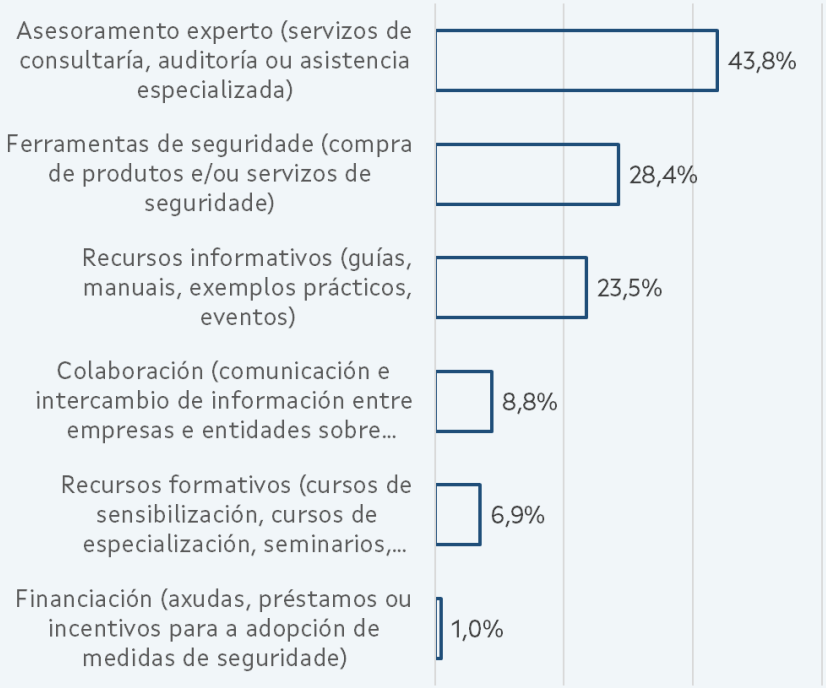
Fonte: OSIMGA-IGE

3.5. Información e recursos utilizados para enfrontarse ás ameazas

Os recursos ou fontes de información aos que acoden as empresas fronte ás ameazas de ciberseguridade veñen encabezados polo asesoramento experto, co 43,8%, e ferramenta específicas de seguridade, co 28,4%. Tamén teñen un uso significativo os recursos informativos, como guías e manuais, co 23,5%. A orde dos tres principais recursos utilizados repítese en todos os tamaños de empresa, destacando que nas de máis de 49 persoas empregadas, utilízanos máis do 50%. Tamén no que se refire aos resultados por sectores temos que se repiten os tres recursos principais en todos eles. Pero neste caso o grao de uso son máis diversos.

- ✓ No sector "outros servizos" e "industria" o uso de ferramentas de seguridade ten case o mesmo nivel que o de asesoramento.
- ✓ No resto, o asesoramento é máis do dobre que as ferramentas de seguridade.
- ✓ O "comercio" lidera o uso do asesoramento, mentres o resto de servizos supera ás demais en "formación", "recursos informativos" e "ferramentas de seguridade.

G. 44. Recursos para facer fronte ás ameazas de ciberseguridade



Fonte: OSIMGA-IGE

G. 45. Recursos fronte ás ameazas de ciberseguridade por tamaño da empresa

Recursos fronte a ameazas de ciberseguridade	Menos de 10	10 a 49	50 ou máis
Asesoramento experto	41,8%	56,0%	70,6%
Ferramentas de seguridade	26,9%	36,3%	64,0%
Recursos informativos	22,7%	26,6%	50,8%
Colaboración	8,6%	8,9%	20,5%
Recursos formativos	6,1%	9,3%	35,6%
Financiación	0,7%	2,8%	6,2%

Fonte: OSIMGA-IGE

G. 46. Recursos fronte ás ameazas de ciberseguridade por sector da empresa

Recursos de ciberseguridade	COMERCIO	HOSTALARÍA	RESTO DE SERVIZOS	CONSTRUCIÓN	INDUSTRIA
Asesoramento experto	52,2%	32,5%	44,8%	45,5%	35,0%
Ferramentas de seguridade	25,7%	14,3%	42,6%	22,4%	34,5%
Recursos informativos	24,2%	14,2%	33,4%	19,4%	20,3%
Colaboración	9,4%	5,6%	10,0%	8,0%	10,6%
Recursos formativos	6,2%	2,1%	13,9%	3,8%	5,2%
Financiación	1,5%	0,5%	0,8%	1,1%	1,0%

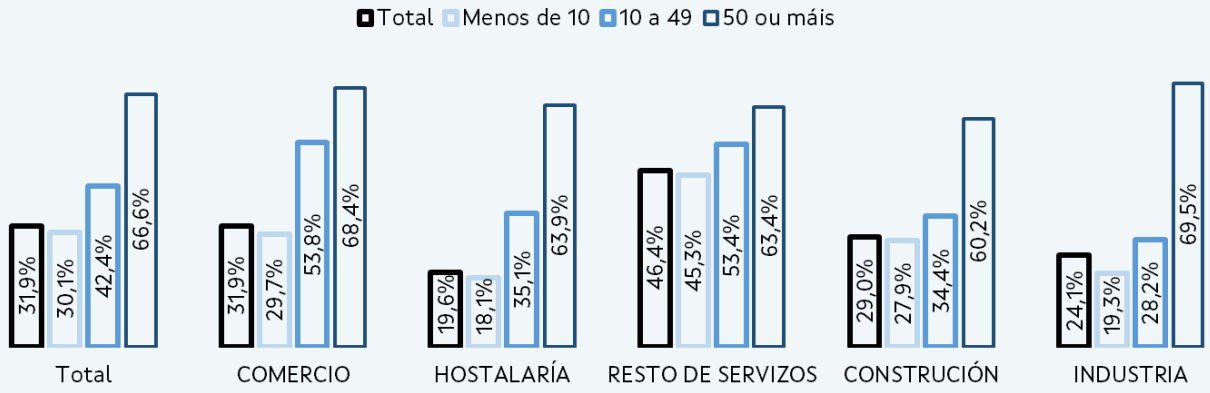
Fonte: OSIMGA-IGE

Seguindo cos recursos de ciberseguridade, tamén se comprobou se as empresas "realizan revisión periódicas sobre a regulación e normativa en materia de ciberseguridade que lle afecta".

Os resultados amósannos que, globalmente o 31,9% de empresas revisa a regulación e normativa de seguridade, superando o 66% nas empresas de máis de 49 persoas empregadas. Neste tamaño de empresa, en todos os sectores supérase o 60%.

Por sectores, a pesares da homoxeneidade entre as empresas grandes, a nivel global a revisión da normativa oscila entre o 46,4% nas empresas de "resto de servizos" e menos da metade, o 19,6% na hostalaría.

G. 47. Empresas que revisan periodicamente a normativa en materia de ciberseguridade que lle afecta



Fonte: OSIMGA-IGE

3.6. Actividades previstas para mellorar a ciberseguridade

Unha vez revisados todos os recursos dos que dispoñen na actualidade as empresas fronte á ciberseguridade, vaise agora a detallar os plans que teñen para melloralos no próximo ano.

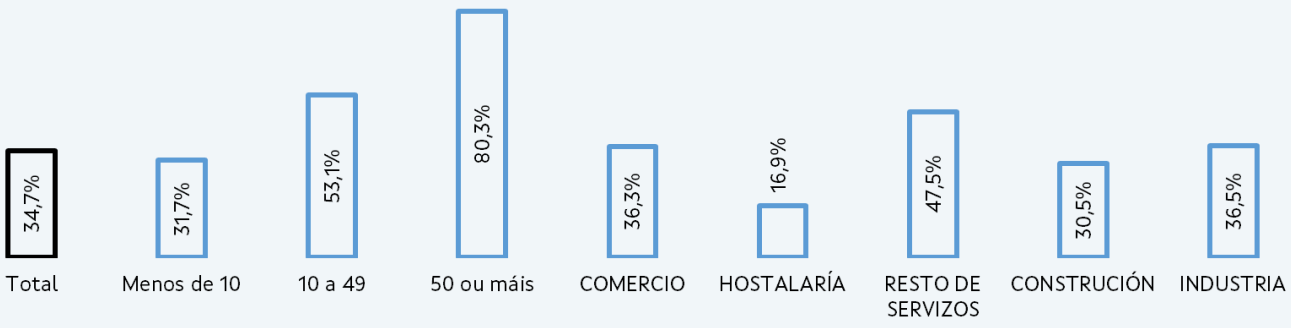
Preguntouse ás empresas respecto aos plans, sobre un listado de 8 posibles accións, para a mellora da ciberseguridade que poderían desenvolver no próximo ano, son as seguintes:

- ✓ Implementación de novas medidas de ciberseguridade: actualización de software, migración a redes seguras, autenticación multifactor, encriptación de datos, etc.
- ✓ Adecuación e actualización de ferramentas de ciberseguridade: antivirus, antimalware, solucións de seguridade na nube.
- ✓ Capacitación e concienciación do persoal empregado: simulación de phishing, cursos de sensibilización ou especialización, campañas de concienciación, etc.
- ✓ Avaliación e xestión de riscos: auditorías de seguridade, avaliación de vulnerabilidades, etc.
- ✓ Actualización de políticas ou plans de ciberseguridade ou resposta a incidentes: elaboración de novos plans, procesos ou políticas.
- ✓ Contratación de servizos externos de asistencia en ciberseguridade: consultaría de ciberseguridade, servizos de seguridade xestionados por terceiros, etc.
- ✓ Outros.

Os resultados indican que o 34,7% de empresas planean aplicar algunha desas medidas nos próximos 12 meses.

Ao igual que no resto de indicadores, hai máis intensidade no uso das ferramentas de seguridade nas empresas máis grandes, e o 80,3% das de 50 ou máis persoas empregadas planean aplicar algunha deses medidas, por só o 31,7% nas de menos de 10 persoas empregadas.

G. 48. Planea accións de mellora da ciberseguridade nos próximos 12 meses.



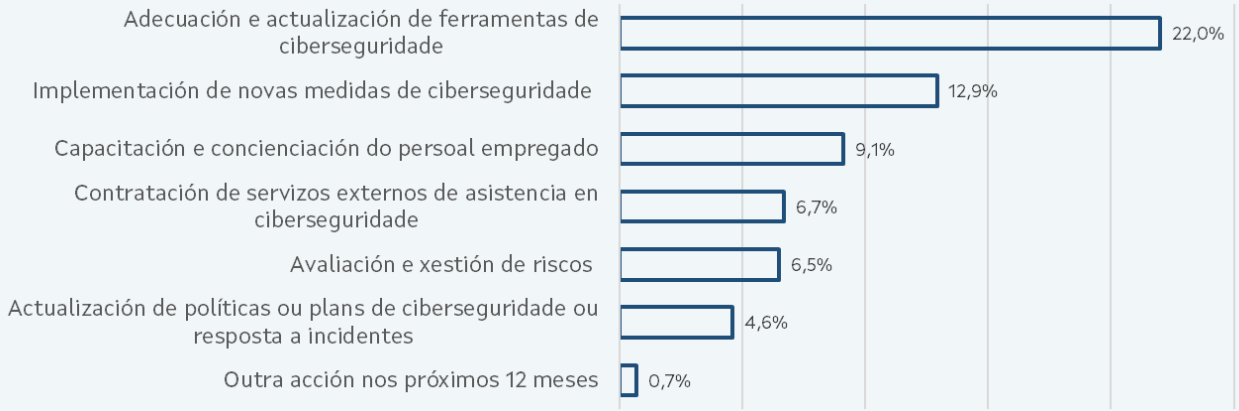
Fonte: OSIMGA-IGE

En canto ás medidas concretas que se planea aplicar nos próximos 12 meses, os resultados máis destacados son a adecuación e actualización das ferramentas de ciberseguridade (22%) e a incorporación de novas medidas (12,9%).

Por tamaño da empresa, as máis grandes lideran todas as accións de mellora a aplicar, sendo máis do 50% en aplicación de novas medidas, actualización de ferramentas e capacitación do persoal.

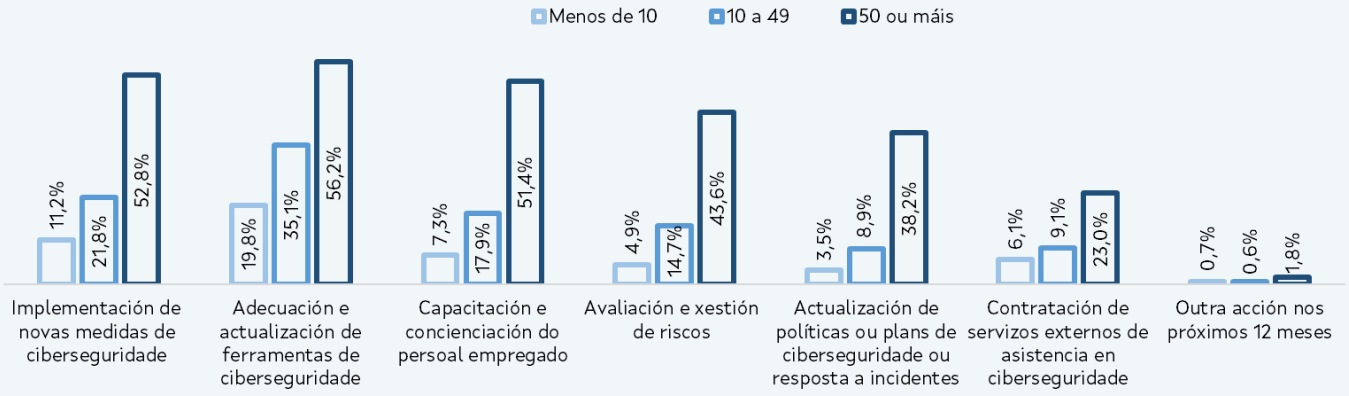
Por sectores de actividade, saliéntase que ningunha das medidas está previsto ser aplicada por máis do 9% nas empresas de Hostalaría. Todos os plans de mellora están liderados polo sector "resto de servizos", a excepción da "contratación de servizos externos", planeados para o próximo ano polo 11,1% de empresas do sector Comercio.

G. 49. Accións de mellora da ciberseguridade nos próximos 12 meses.



Fonte: OSIMGA-IGE

G. 50. Accións de mellora da ciberseguridade nos próximos 12 meses por tamaño da empresa

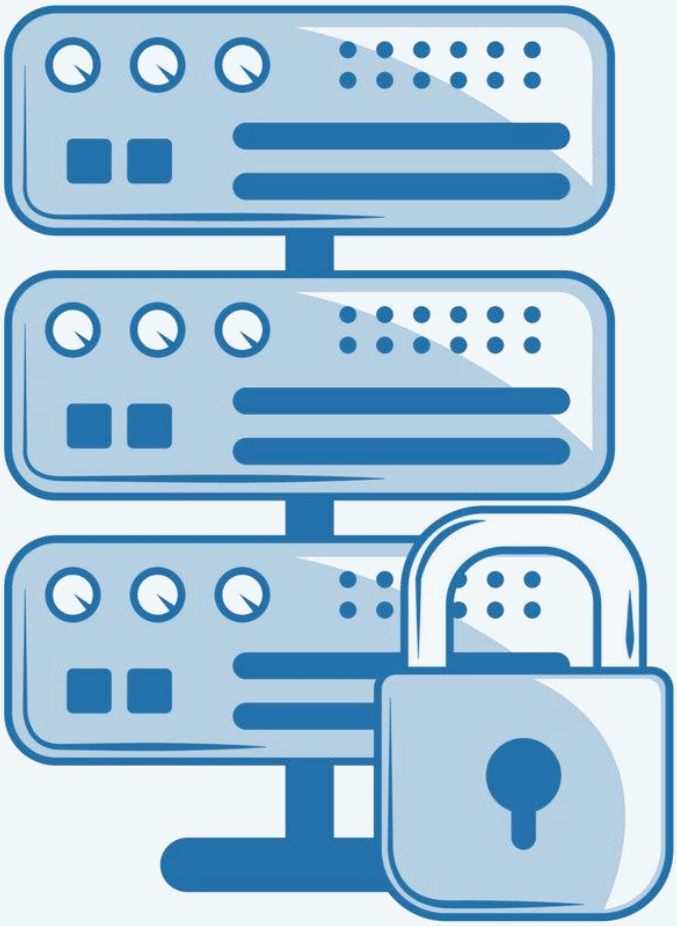


Fonte: OSIMGA-IGE

G. 51. Accións de mellora da ciberseguridade os próximos 12 meses por sector

Accións de mellora	COMERCIO	HOSTALARÍA	RESTO DE SERVIZOS	CONSTRUCIÓN	INDUSTRIA
Implementación de novas medidas de ciberseguridade	11,9%	8,6%	17,3%	10,4%	16,1%
Adecuación e actualización de ferramentas de ciberseguridade	21,4%	8,5%	32,3%	19,7%	25,4%
Capacitación e concienciación do persoal empregado	7,9%	2,5%	16,7%	6,6%	9,5%
Avaliación e xestión de riscos	3,0%	2,6%	13,0%	4,4%	10,7%
Actualización de políticas ou plans de ciberseguridade ou resposta a incidentes	4,8%	2,6%	6,9%	3,3%	3,8%
Contratación de servizos externos de asistencia en ciberseguridade	11,1%	2,3%	5,3%	6,3%	5,3%
Outra acción nos próximos 12 meses	0,0%	0,4%	1,9%	0,5%	0,4%

Fonte: OSIMGA-IGE



4. AUTOAVALIACIÓN DA CIBERSEGURIDADE NA EMPRESA

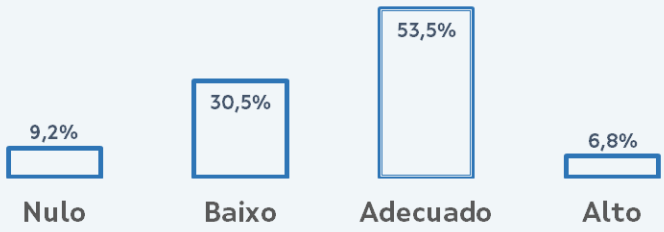
4. AUTOAVALIZACIÓN DA CIBERSEGURIDADE NA EMPRESA

Vense expoñendo ao longo de todo o informe como as grandes empresas teñen unha dedicación de recursos moi superiores á autoprotección e ás políticas de ciberseguridade. Tamén destacamos por enriba da media o sector servizos (excluído hostalaría e comercio) e a industria, mentres que os valores máis baixos tenden a atoparse na hostalaría e a construción. Aínda que os resultados da industria tenden a ser relativamente altos en recursos de ciberseguridade, é un resultado algo sesgado a causa do maior tamaño medio das empresas deste sector.

Neste apartado final vaise comprobar se a autoavaliación da "preparación da súa empresas fronte a posibles ataques ou incidentes de ciberseguridade" conta unhas tendencias acordes á dispoñibilidade de recursos.

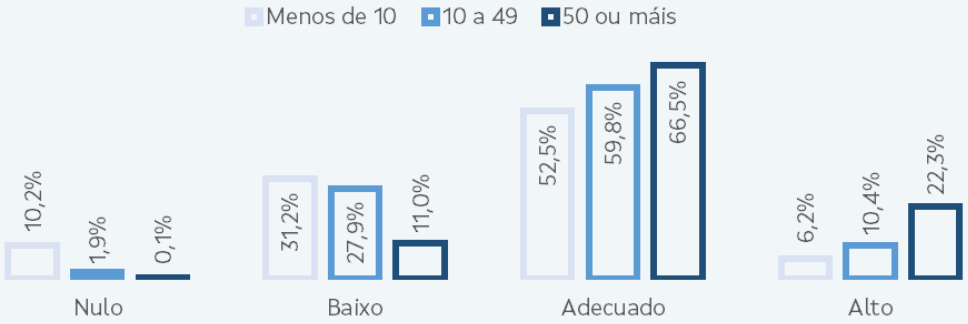
O 60,3% das empresas declaran estar preparadas de xeito adecuado ou alto na seguridade TIC. Este valor oscila entre o 88,8% nas empresas máis grandes e o 58,7% nas pequenas.

G. 52.Autoavaliación da preparación da empresa en ciberseguridade



Fonte: OSIMGA-IGE

G. 53. Autoavaliación da preparación da empresa en ciberseguridade por tamaño

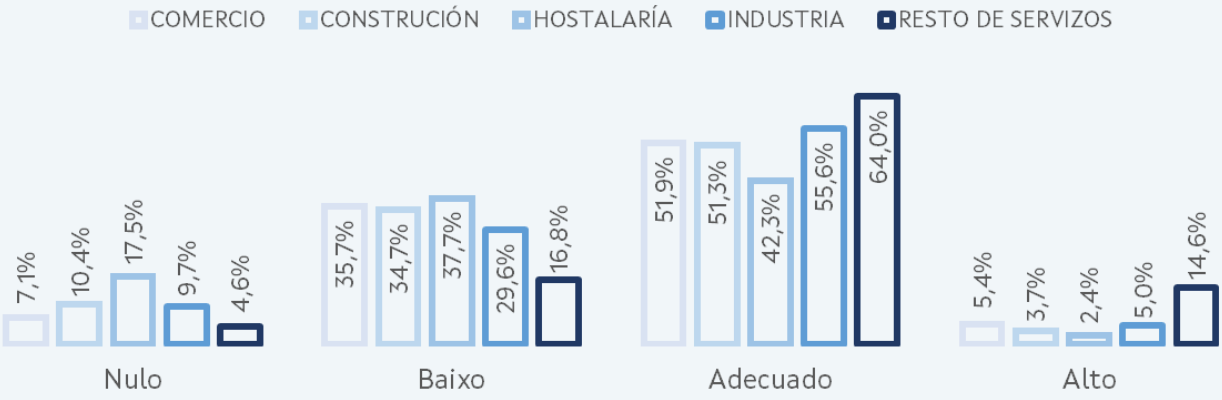


Fonte: OSIMGA-IGE

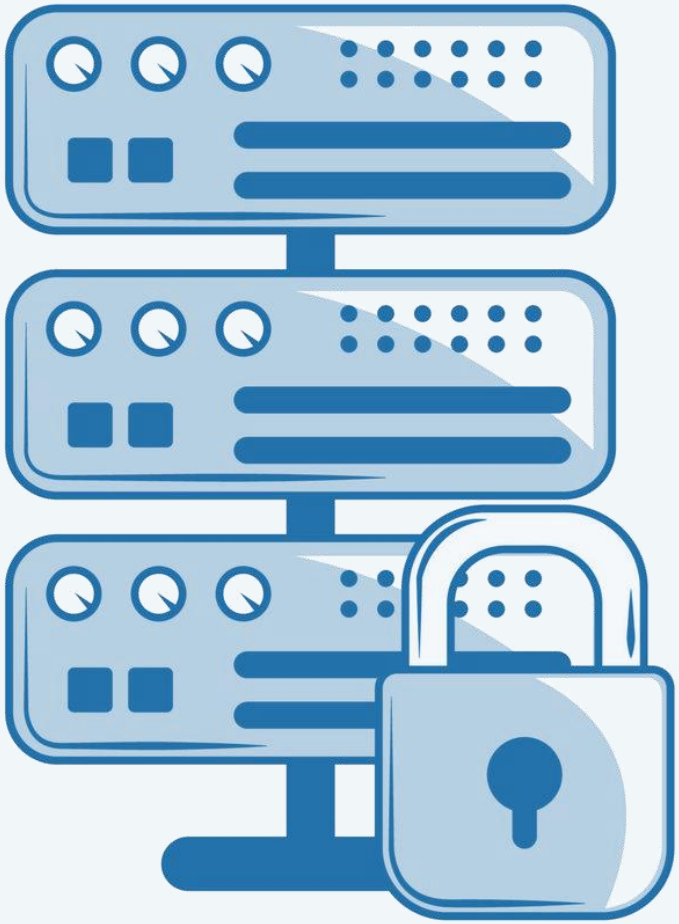
En canto a sectores de actividade, novamente atopamos como o "resto de servizos" e "industria" defínense como máis preparados. No punto máis baixo está con diferenza

a hostalaría, onde só o 44,7% das empresas decláranse preparadas de forma adecuada ou alta fronte á ciberseguridade.

G. 54. Autoavaliación da preparación da empresa en ciberseguridade por sector



Fonte: OSIMGA-IGE



5. RESUMO E CONCLUSIÓNS

5. RESUMO E CONCLUSIÓNS

INCIDENTES DE CIBERSEGURIDADE

O 15,5% das empresas galegas sinalan que sufriron algún incidente de ciberseguridade no último ano.

Nas empresas de máis de 49 traballadores, sufriu incidentes case a metade, o 47,8%.

Por sectores, todos superan o 14% de empresas con incidentes a excepción da hostalaría, que só se veu afectada no 7,6% dos casos.

Do 15,5% que sufriu incidentes de ciberseguridade, o 38,6% sufriu algún tipo de consecuencia deses incidentes. Deste xeito, **o 6% do total de empresas galegas sufriu consecuencias provocadas polos incidentes de ciberseguridade**.

Sufriron consecuencias o 14,4% das empresas de 50 ou máis traballadores e, por sectores, destaca o comercio, co 9,6%. Pero cruzando as dúas variables, a incidencia máis alta está nas empresas de construción de máis de 49 empregados, co 26,5%.

A clase de incidente de seguridade que máis afecta ás empresas galegas é o phising, ou intentos de obter información suplantando unha identidade de alguén externo á empresa. Cabe subliñar que o segundo caso por incidencia ten semellanzas, ao tratarse de suplantación de identidade dentro da empresas, co 2,6%.

Os ataques por virus informáticos e de denegación de servizos afectaron a máis do 2% das empresas no último ano.

As intrusión en sistemas mediante accesos non autorizados afectaron ao 1,9% de empresas galegas.

A instalación de software malicioso para danar sistemas ou datos tamén supera o 1% de afectación a empresas.

A consecuencia máis habitual dos incidentes de ciberseguridade é a **"falta de dispoñibilidade de servizos TIC". Afecta ao 3,2% do total de empresas, que supón o 53,3% das que sufriron algunha consecuencia dos incidentes de ciberseguridade**. A perda de produtividade afectou ao 1,8% das empresas (29,8% das que sofren consecuencias dos incidentes) e gastos económicos adicionais son sinaladas polo 1,5% do total (24,8% das que sufriron algunha consecuencia).

RECURSOS PARA A SEGURIDADE TIC

O 81,6% das empresas de Galicia aplican algunha das medidas de seguridade descritas na enquisa nos seus equipos e comunicacións TIC.

Por sector e tamaño, o uso de medidas de seguridade TIC é case total nas empresas de 50 ou máis persoas empregadas.

Nas empresas de 10 a 49 persoas empregadas, atopámonos con valores de protección que oscilan entre o 86,2% da Hostalaría e o 100% no Comercio.

Descende a valores por debaixo do 75% nas microempresas da Industria e Hostalaría.

En xeral, o **40% das empresas galegas gastaron en ciberseguridade no último ano. Das que o fixeron, investiron como promedio 3.217 euros anuais**.

O 69,9% das empresas de 50 ou máis persoas empregadas, gastan en ciberseguridade, destacando o sector de servizos, excluído comercio e hostalaría. O sector de "outros servizos" gasta máis en seguridade en todos os tamaños de empresa, aínda que "Industria" e "Comercio" sitúanse moi preto cando son 50 persoas empregadas ou máis, estando nos tres casos arredor dos 30.000 euros de gasto medio anual.

O 22,1% das empresas ofreceu ao seu persoal empregado a posibilidade, no último ano, de cursar actividades formativas sobre seguridade TIC. Máis da metade das empresas de 50 ou máis empregados ofreceron esta posibilidade. Por sectores, no de "outros servizos" a media é máis de dez puntos superior a calquera outra, co 35,7%.

AUTOAVALIACIÓN DAS EMPRESAS FRONTE Á AMEAZAS DE CIBERSEGURIDADE

O 60,3% das empresas declaran estar preparadas de xeito adecuado ou alto na seguridade TIC. Este valor oscila entre o 88,8% nas empresas máis grandes e o 58,7% nas pequenas.

En canto a sectores de actividade, novamente atopamos como o "resto de servizos" e "industria" defínense como máis preparados. No punto máis baixo está con diferenza a hostalaría, onde só o 44,7% das empresas decláranse preparadas de forma adecuada ou alta fronte á ciberseguridade.

6. ANEXOS

6. ANEXO

6.1. Descrición dos códigos de actividade empresarial incluídos na enquisa.

- ✓ Industria: Sectores de Industrias extractivas (B), Industrias manufactureiras (C), Subministración de enerxía eléctrica, gas, vapor e aire acondicionado(D) e Subministración de auga, saneamentos, xestión de residuos e descontaminación (E)
- ✓ Construción (F)
- ✓ Comercio (G)
- ✓ Hostalaría (I)
- ✓ Resto de servizos: sectores de Transporte e almacenamento (H), Información e comunicacións (J), Actividades Inmobiliarias (L), Actividades profesionais, científicas e técnicas (M) e Actividades administrativas e servizos auxiliares (N) que non estean incluídas dentro do sector TIC.

Exclúense aquelas empresas que realizan actividade TIC recollidas nos epígrafes:

26.1 Fabricación de compoñentes electrónicos e circuítos impresos ensamblados.

26.2 Fabricación de ordenadores e equipamentos periféricos.

26.3 Fabricación de equipamentos de telecomunicacións.

26.4 Fabricación de produtos electrónicos de consumo.

26.8 Fabricación de soportes magnéticos e ópticos.

46.5 Comercio por xunto de equipamentos para as tecnoloxías da información e as comunicacións.

58.2 Edición de programas informáticos.

61.1 Telecomunicacións por cable.

61.3 Telecomunicacións sen fíos.

62.0 Telecomunicacións por satélite.

63.1 Proceso de datos, hospedaxe e actividades relacionadas; portais web.

95.1 Reparación de ordenadores e equipamentos de comunicación.