Enquisa de ciberseguridade

METODOLOXÍA

1.Introdución

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. Esta definición reflicte a complexidade do desafío e a necesidade de abordar a ciberseguridade de maneira integral.

Por iso, nunha contorna cada vez máis dixitalizada, a ciberseguridade converteuse nun piar fundamental para as organizacións. A protección dos datos e os sistemas fronte a ameazas cibernéticas 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 o nivel de preocupación que suscita a ciberseguridade nas empresas, e a regulación e normativa que lles afecta nesta materia.
- Coñecer as medidas adoptadas, os incidentes sufridos e as súas consecuencias na actividade da empresa.
- 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 axudarán a proporcionar un panorama máis claro do estado da ciberseguridade na rexión e poderán servir como base para o desenvolvemento de políticas e estratexias que reforcen a resiliencia das empresas fronte a ciberataques.

Necesidade da enquisa:

Actualmente, non se dispón de datos de forma periódica con gran aceptabilidade ou alcance sobre o estado da ciberseguridade do tecido empresarial galego, polo que resulta de gran interese realizar a presente enquisa e posterior estudo, como ferramenta para identificar carencias e avaliar a madurez sobre a importancia da protección en contornos dixitais ante a crecente dixitalización dos procesos empresariais e a dependencia da tecnoloxía.

Ademais, dado que a enquisa servirá de ferramenta para coñecer as carencias das empresas no eido da seguridade da información no entorno dixital, tamén permitirá identificar posibles iniciativas a poñer en marcha que axuden a dar resposta ás carencias detectadas.

2. Obxectivos concretos da investigación

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. 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.

Ámbito temporal: A información recollerase durante o segundo semestre do ano e fará referencia ao ano natural.

Variables a investigar:

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 ameazas 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.

Clasificacións e nomenclaturas: CNAE-2009.

Escalas no tratamento de variables: O número de especialistas encargados de realizar funcións relativas á ciberseguridade e o investimento da empresa en ciberseguridade son variables numéricas que poden tomar valores naturais.

A existencia de revisións periódicas sobre a normativa de ciberseguridade é unha variable dicotómica que pode ser positiva (SI) ou negativa (NON).

As outras variables son categóricas a escoller entre unha lista que, nalgúns casos, inclúe unha opción aberta (OUTRO).

3. Unidades estatísticas

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).

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: Responsable de tecnoloxía da empresa (ou na súa ausencia, o director ou máximo responsable da empresa)

Unidades excluídas ou limiares: Empresas e autónomos sen asalariados, así como todas as empresas correspondentes ás seccións non incluídas anteriormente.

4. Deseño mostral

O marco poboacional empregado foi o Directorio de empresas e unidades locais ao que se accede mediante a seguinte ligazón da web do IGE:

https://www.ige.gal/web/mostrar_actividade_estatistica.jsp?codigo=0307006001&num_pag=1

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 50 traballadores ou máis 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 .

Para o Directorio de empresas e unidades locais do ano 2023 e para un erro relativo do 5%, o número de elementos seleccionados en cada un dos estratos é o seguinte:

	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 total da mostra: 2013 empresas.

Marco: Directorio de empresas e unidades locais. Ano 2023.

5. ESTIMADORES

O estimador do total dunha característica X nun dominio m, ven dado por:

$$\hat{X}_m = \sum_{j \in m} X_j \, F_j$$

onde:

X_j é o valor da característica X do cuestionario j pertencente ao dominio m.

F_j é o factor de elevación do cuestionario j que calculase do seguinte modo:

a) Se a empresa j foi seleccionada nun estrato h e segundo os datos do cuestionario atópase noutro estrato distinto k, entón: $F_j = \frac{N_h}{n_h}$

b) Se a empresa j, aínda pertence ao mesmo estrato h, onde foi seleccionada, entón: $F_j = \frac{\hat{N}_h^*}{n_h^*}$

c) Nos casos concretos nos que se especifique Fj=1.

Variables utilizadas:

N_h = número de empresas no directorio no estrato h.

n_h = número de empresas seleccionadas no estrato h.

n_h^* = número de empresas que contestaron, seleccionadas no estrato h e que non cambiaron de estrato.

$$\hat{N}_h^* = N_h\left(1 - \frac{n_h^{e'}}{n_h}\right) - \Sigma_{k \neq h} \Sigma_{j=1}^{n_h^k} F_j$$

Sendo:

$n_h^{e'}$ = número de empresas seleccionadas no estrato h que teñen incidencia do tipo duplicadas ou inactivas.

n_h^k = número de empresas seleccionadas no estrato h, que segundo o cuestionario están noutro estrato distinto k.

6. Recollida e tratamento de datos

A recollida de datos farase no segundo semestre do ano.

O contacto inicial coa empresa será por correo postal, mediante unha carta dirixida ao enderezo que consta no directorio de empresas na que se incluirá a chave de acceso para cubrir o cuestionario. O texto da carta e o cuestionario inclúense tamén como anexo.

Serán as empresas as que cubran os datos da enquisa mediante un formulario web e unha vez rematada dende o IGE faremos o traballo de depuración chamando ás unidades informantes se fora preciso ou substituíndo as empresas que por cese de actividade ou algún outro problema non poidan cubrila.

7. Difusión

A difusión dos resultados contará polo menos coas seguintes táboas:

CÓDIGO	NOME	DESCRICIÓN
V1	Porcentaxe de empresas que consideran que o seu nivel de preparación fronte a posibles ataques de ciberseguridade é alto	Porcentaxe de empresas que consideran que o seu nivel de preparación fronte a posibles ataques de ciberseguridade é alto
V2	Porcentaxe de empresas que actualmente aplican ao menos dúas medidas distintas de seguridade na empresa	Porcentaxe de empresas que aplican dúas ou máis das seguintes medidas de ciberseguridade: o Autenticación mediante contrasinal seguro o Autenticación mediante métodos biométricos o Autenticación baseada en combinación de ao menos dous mecanismos de autenticación (dobre ou múltiple factor de autenticación) o Encriptado de datos o Copia de seguridade o Control de acceso á rede o VPN o Sistema de monitoreo de seguridade TIC o Manter arquivos de rexistro o Avaliación de riscos das TIC o Probas de seguridade TIC
V3	Porcentaxe de empresas que sufriron incidentes de ciberseguridade no último ano	Porcentaxe de empresas que indican que sufriron un ou varios dos seguintes incidentes de ciberseguridade: o Accesos non autorizados o Instalación de malware o Instalación de Ransomware o Ataques de phishing o Ataque de denegación de servizo o Suplantación de identidade o Perda o roubo de dispositivos o Infiltración en redes internas o Uso indebido de credenciais o Infección por virus informático o Explotación de vulnerabilidades en IoT o Enxeñaría social o Fraude interno o Outro

V4	Porcentaxe de empresas que desenvolveron algunha actividade para mellorar a ciberseguridade no último ano	Porcentaxe de empresas que sinalan que no último ano desenvolveron unha ou varias das seguintes medidas ou actividades para mellorar a ciberseguridade na empresa: o Desenvolvemento de novas medidas de ciberseguridade o Adecuación e actualización de ferramentas de ciberseguridade o Capacitación e concienciación do persoal empregado o Avaliación e xestión de riscos o Actualización de políticas ou plans de ciberseguridade ou resposta a incidentes o Contratación de servizos externos de asistencia en ciberseguridade o Outro