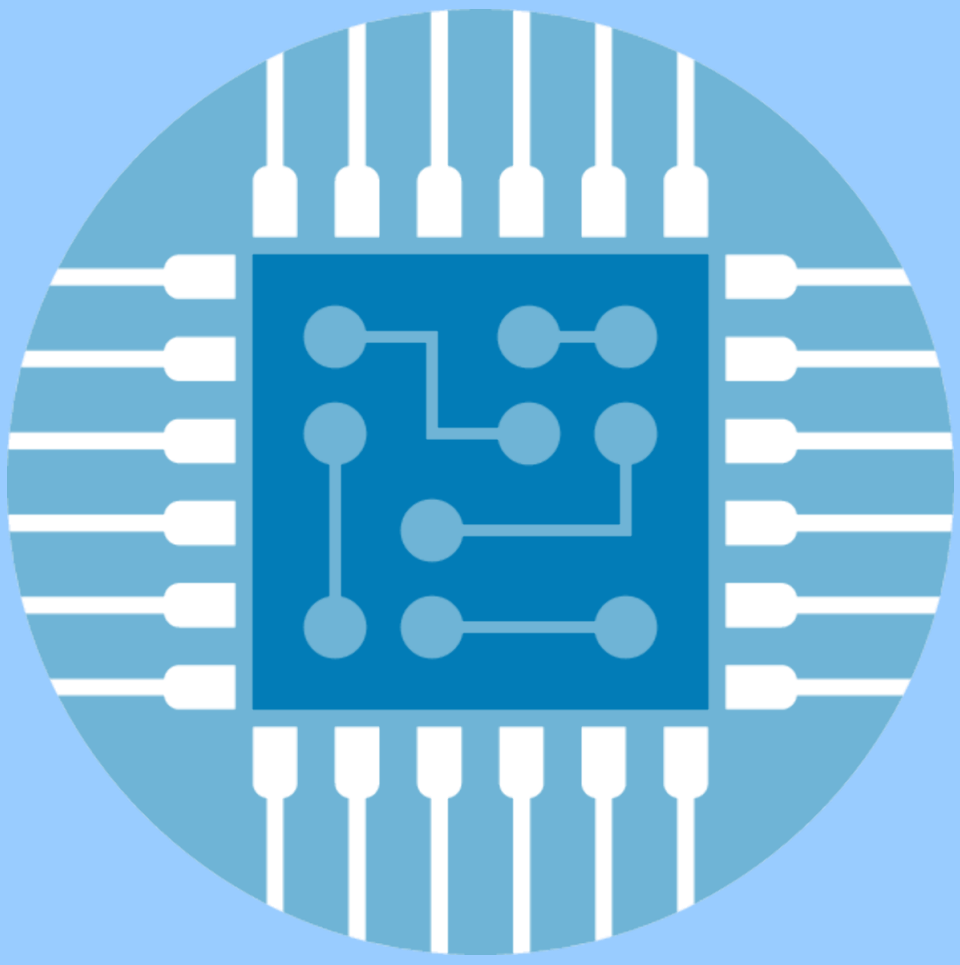


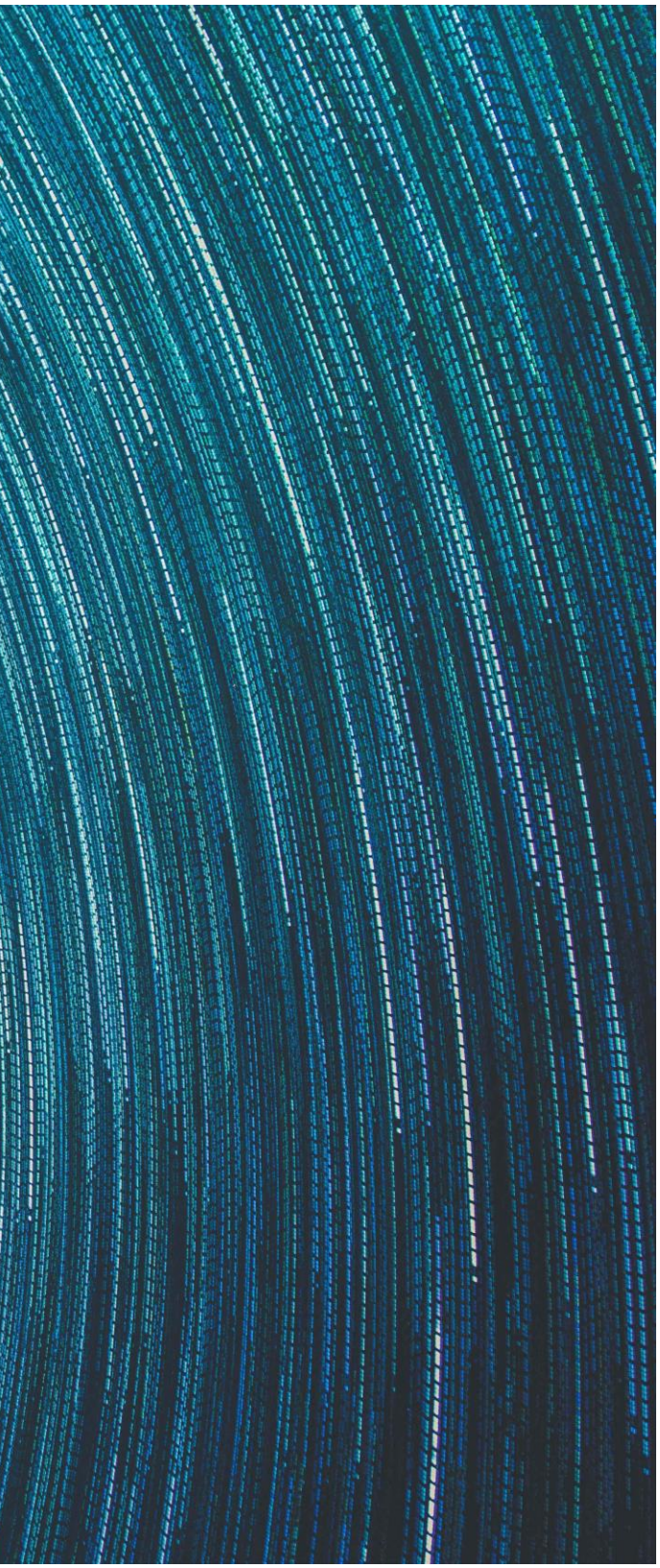
CIBER.gal - Nodo de ciberseguridade en Galicia

Área de Infraestruturas e Telecomunicacións

Axencia para a Modernización Tecnolóxica de Galicia (AMTEGA)

Edita: Xunta de Galicia. Axencia para a Modernización Tecnolóxica de Galicia – AMTEGA

Santiago de Compostela. Ano 2020



Contidos

Capítulo 1
Ciberseguridade: concepto, tendencias e retos

1.1. Unha formulación europea común

1.2. Tendencias e retos

1.3. Marco europeo de referencia

Capítulo 1 | Ciberseguridade: concepto, tendencias e retos

Ciberseguridade
Ferramentas, directrices, accións, formación, boas prácticas, seguros e tecnoloxías que poidan utilizarse para protexer os activos de organizacións e usuarios no ciberespazo, segundo a Unión Internacional de Telecomunicacións.

1.1. Unha formulación europea común

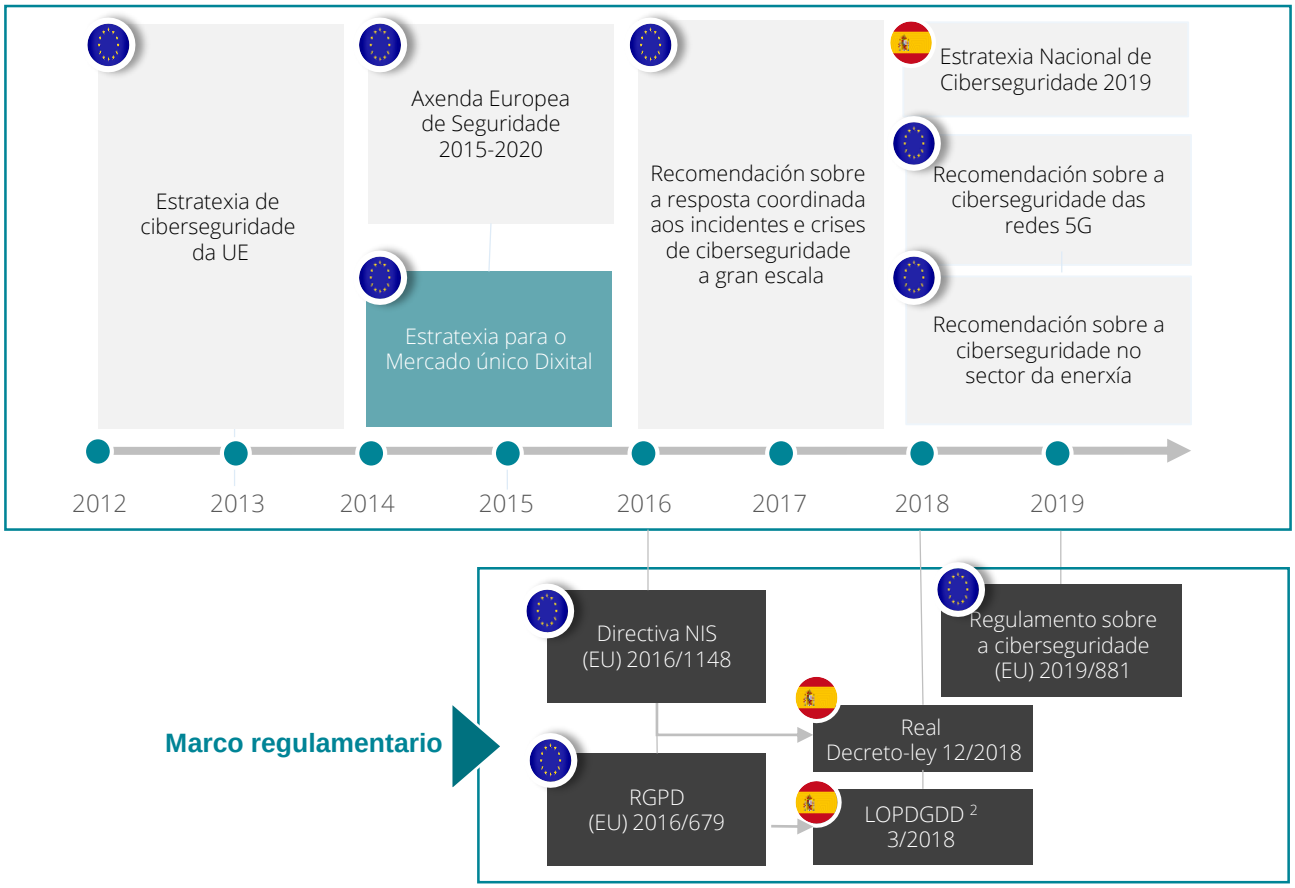
A medida que a vida cotiá e a economía vólvense máis dependentes das tecnoloxías dixitais, os cidadáns europeos están cada vez máis expostos a incidentes cibernéticos graves. A seguridade futura depende da mellora da capacidade de protexer á cidadanía contra as ciberameazas, xa que tanto a infraestrutura civil como as capacidades militares dependen duns sistemas dixitais seguros[1].

Deste xeito, a Comisión Europa traballa desde principios de 2010 na definición das estratexias e regulamentos que permitan avanzar no ámbito da protección dos activos no ciberespazo, tanto das organizacións como das persoas usuarias.

Con todo, as leccións extraídas de políticas públicas exitosas nos sectores da alta tecnoloxía mostraron que, ademais da investigación e a innovación, a actuación pública para apoiar o «insumo ascendente» en ámbitos tecnolóxicos en rápida evolución pode ser decisiva para xerar valor e responder ao mesmo tempo as necesidades do sector público.

Así, a estratexia para o Mercado Único Dixital, publicada no ano 2015, puxo en marcha un marco sólido e apoiado ao máis alto nivel político. En Tallin, os xefes de Estado e de Goberno europeos identificaron a ciberseguridade como un dos principais alicerces dunha economía dixital forte.

Marco Estratéxico



Deste xeito, precisamente en Tallin, sitúase o primeiro xerme do futuro Programa Europa Dixital, elemento central da resposta integral da Comisión Europea ao desafío da transformación dixital, que forma parte da proposta de Marco Financeiro Plurianual (MFP) para 2021-2027.

[1] 2018/0328 (COD)

[2] LOPDGDD: Lei Orgánica 3/2018, do 5 de decembro, de Protección de Datos Persoais e garantía dos dereitos dixitais.

Sen ningunha dúbida, o papel da Administración Pública na promoción da ciberseguridade é crucial. Así o demostra un dos últimos estudos elaborados polo Centro de Investigación da Comisión Europea (Commission´s Joint Research Centre – JRC-) que pon de manifesto que sen a intervención da Administración para coordinar a actual fragmentación de esforzos e capacidades de innovación, a industria da ciberseguridade europea atopará dificultades para explotar o seu potencial e competir con outros actores globais (Estados Unidos, Israel, China e Corea do Sur).

Así, como primeiro paso, e para orientar as reflexións futuras, a Comisión Europea pon en marcha unha fase piloto no marco de Horizonte 2020 co fin de axudar a reunir aos centros nacionais nunha rede e así dar un novo impulso en materia de competencia en ciberseguridade e desenvolvemento tecnolóxico. De forma paralela, e ante as necesidades inminentes de protección, os xefes de Estado e de Goberno solicitan que a Unión se converta nun "líder mundial en ciberseguridade para 2025", a fin de garantir a confianza, a seguridade e a protección dos nosos cidadáns, consumidores e empresas en liña e permitir unha Internet libre e legal".

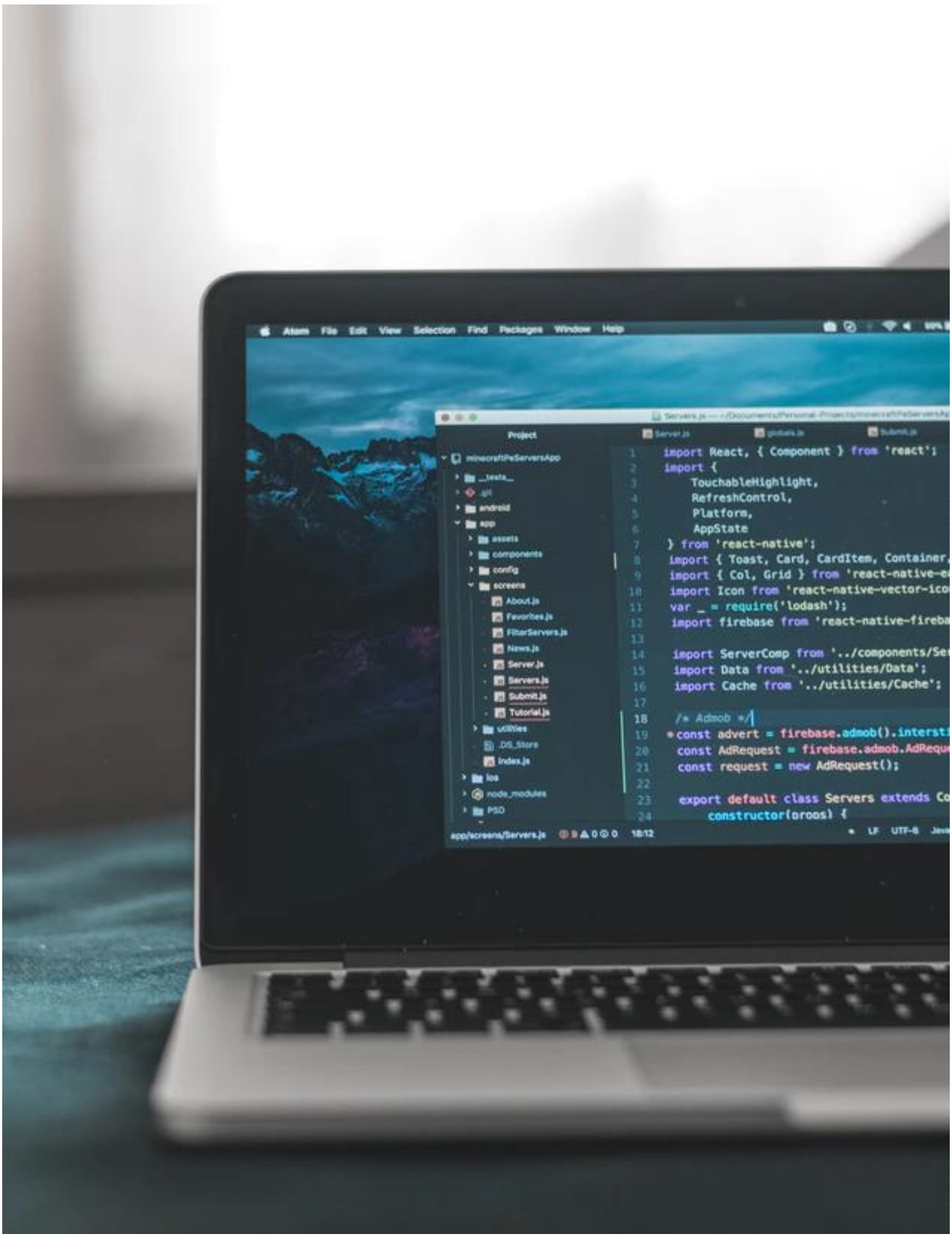
O novo Centro Europeo de Competencia Industrial, Tecnolóxica e de Investigación en Ciberseguridade e a Rede de Centros Nacionais de Coordinación

Así, en setembro 2018, o Parlamento e o Consello Europeo presentan unha proposta para establecer o Centro Europeo de Competencia Industrial, Tecnolóxica e de Investigación en Ciberseguridade e a Rede de Centros Nacionais de Coordinación co obxectivo de facer fronte aos crecentes desafíos en materia de ciberseguridade, baseándose na Estratexia de ciberseguridade de 2013 e nos seus obxectivos e principios para fomentar un ecosistema cibernético fiable, seguro e aberto.

Pendente da súa aprobación definitiva, a iniciativa inclúe a necesidade de incorporar a opinión e asesoramento do sector privado, organizacións de consumidores e outros axentes relevantes, mediante a constitución dun Comité Consultivo que garantise a colaboración público privada no ámbito da ciberseguridade. O modelo de gobernanza consideraba así mesmo, un Comité de Dirección e un Director Executivo. Entre as actuacións para desenvolver polo Centro destacan: apoio á investigación; asesoramento experto, identificación de gaps na disposición e xestión de talento e capacidades, etc. Para iso, o Centro de Competencia executará, en concreto, as partes pertinentes dos programas Europa Dixital e Horizonte Europa.

A rede de European Dixital Innovation Hubs (EDIHs)

Do mesmo xeito, a DG Connect da Comisión Europea prevé organizar o apoio ás pemes e ao sector público no seu proceso de transformación dixital ao redor dos Hubs europeos de innovación dixital: unha organización, ou consorcio de organizacións con coñecemento complementario e sen ánimo de lucro. A ciberseguridade será un elemento crucial neste proceso de transformación.


Atom File Edit View Selection Find Packages Window Help
Project
minecraftPeServersApp
__tests__
.git
android
app
assets
components
config
screens
About.js
Favorites.js
FilterServers.js
News.js
Server.js
Servers.js
Submit.js
Tutorial.js
utilities
.DS_Store
index.js
ios
node_modules
PSD
import React, { Component } from 'react';
import {
TouchableHighlight,
RefreshControl,
Platform,
AppState
} from 'react-native';
import { Toast, Card, CardItem, Container,
import { Col, Grid } from 'react-native-e
import Icon from 'react-native-vector-ico
var _ = require('lodash');
import firebase from 'react-native-fireba
import ServerComp from '../components/Se
import Data from '../utilities/Data';
import Cache from '../utilities/Cache';
/* Admob */
const advert = firebase.admob().interst
const AdRequest = firebase.admob.AdReque
const request = new AdRequest();
export default class Servers extends Co
constructor(props) {
app/screens/Servers.js
18:12
LF
UTF-8

Os organismos e programas de referencia en materia de ciberseguridade en Europa

A Comisión Europea está a reforzar, en colaboración cos estados membro, as súas normas sobre ciberseguridade para facer fronte á crecente ameaza que supoñen os ataques cibernéticos e aproveitar as oportunidades que presenta a nova era dixital. Nese sentido, foron cruciais os organismos que se constituíron nos últimos anos, tanto a nivel internacional como nacional:

Europa

España

De forma adicional, a Comisión Europea ven financiando a investigación, innovación e implementación da ciberseguridade durante os últimos anos a través de distintos instrumentos, especialmente Horizonte 2020:

CONCORDIA	SPARTA	ECHO	Cyber Security for Europe
Rede con liderado en investigación, tecnoloxía e competencias publicas	Nova estrutura da rede de centros, fomentando a investigación e desenvolvemento	Rede de competencia en ciberseguridade cun hub central de competencia	Folla de ruta sobre ciber, certificación, adestramento, educación e *cyberranges*

Coa futura entrada en vigor do novo Marco Financeiro Plurianual 2021-2027, a Comisión Europea reforzará a investigación e innovación en ciberseguridade a través de Horizonte Europa e poñerá en marcha o novo programa Europa Dixital, mencionado anteriormente:

Horizonte Europa
Orzamento total de 100.000 M€

- Especialmente a través do Pilar I –Ciencia Aberta: Consello Europeo de Investigación, infraestruturas de Investigación, accións Marie Sklodowska-Curie - e do Pilar II – Desafíos mundiais e competitividade

Europa Dixital
Orzamento total de 9.200 M€

- Especialmente como unha das tres tecnoloxías –ciberseguridade, intelixencia artificial e computación de alto rendemento-, ademais da interoperabilidade e competencias dixitais.

Con miras a fortalecer a competitividade das empresas europeas, necesitamos os requisitos de seguridade máis esixentes e unha formulación europea común. Temos que compartir os nosos coñecementos sobre os riscos. Necesitamos unha plataforma común, unha Axencia Europea de ciberseguridade reforzada. Só deste xeito poderemos aumentar a confianza na economía interconectada e fortalecer a resiliencia fronte a todo tipo de riscos.

Extracto de discurso
Ursula von der Leyen
Presidenta da Comisión Europa

1.2. Tendencias e retos

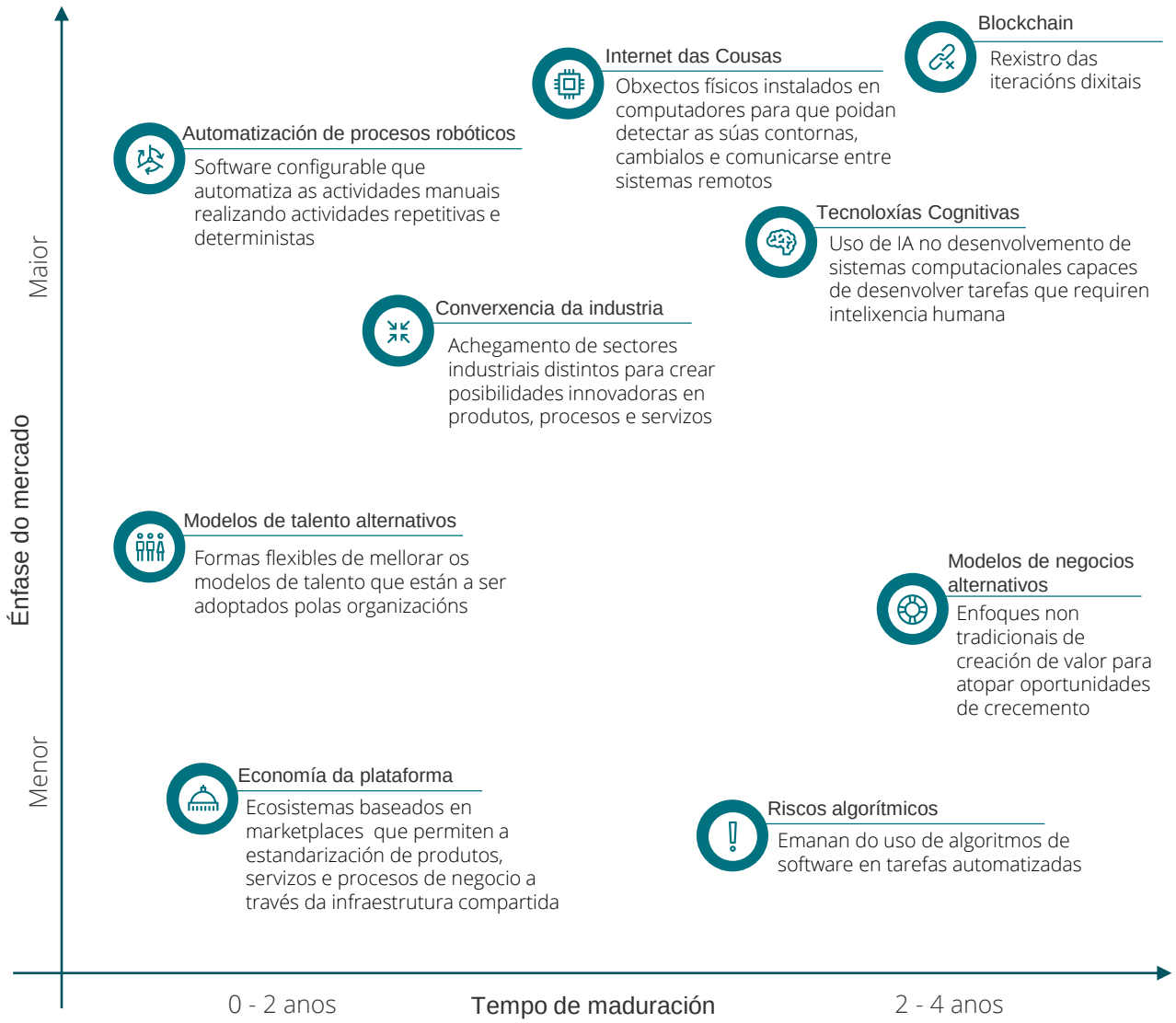
A nosa vida cotiá, os dereitos fundamentais, as interaccións sociais e as economías dependen de tecnoloxías da información e a comunicación que prestan servizos ininterrompidos. Foi este ciberespazo aberto e libre o que promoveu a integración política e social en todo o mundo; o que fixo caer fronteiras entre países, comunidades e cidadáns, potenciando a interacción e o intercambio de información e ideas en todo o planeta[1].

Baixo este contexto, as empresas e administracións téñense que dotar das **capacidades necesarias para responder aos posibles riscos** derivados da operación no **ciberespazo**.

Tendencias con impacto na ciberseguridade

Á vez que se adoptan novas iniciativas e solucións no ámbito dixital é necesario traballar por conseguir que as entidades e empresas operen nun **ecosistema ciberseguro**. Será necesario analizar e abordar o impacto destas tendencias nas organizacións desde a perspectiva da ciberseguridade.

Tendencias crave para o futuro dos negocios



Fonte: Deloitte: análise elaboración propia.

[1)] Estratexia de ciberseguridade da Unión Europea. (JOIN(2013) 1 final).

Ciberriscos e ciberdelincuencia

O desafío actual das organizacións é a mellora do súa capacidade competitiva mediante o uso seguro das novas tecnoloxías.

Neste contexto, a **Enquisa sobre Percepción de Riscos Globais de 2019**, do **Foro Económico Mundial** sinala un incremento dos ciberataques, tanto en poder de prevalencia como en poder rupturista. Aínda que a maioría dos ataques están relacionados coa interrupción de operacións e o roubo de datos, cada vez é maior a oferta de servizos dos cibercriminais así como o impacto dos mesmos na privacidade de empresas e administracións.

Do mesmo xeito, segundo datos da Comisión Europea publicados en 2018, os ataques triplicáronse entre 2016 e 2018 o que conduciu ao 87% dos europeos a considerar que a ciberdelincuencia é un desafío importante para a seguridade interior da UE.

Retos en ciberseguridade

A continuación sinálanse algúns dos retos aos que as empresas e organizacións deben facer fronte no ámbito da ciberseguridade:

Un maior número de sistemas e dispositivos conectados tradúcese na expansión da superficie de ataque dunha organización

Incremento das entradas laterais de ciberataques (cadea de subministración, socio comercial e outros axentes de relación)

Patróns de ataque cada vez máis parecidos ao comportamento normal

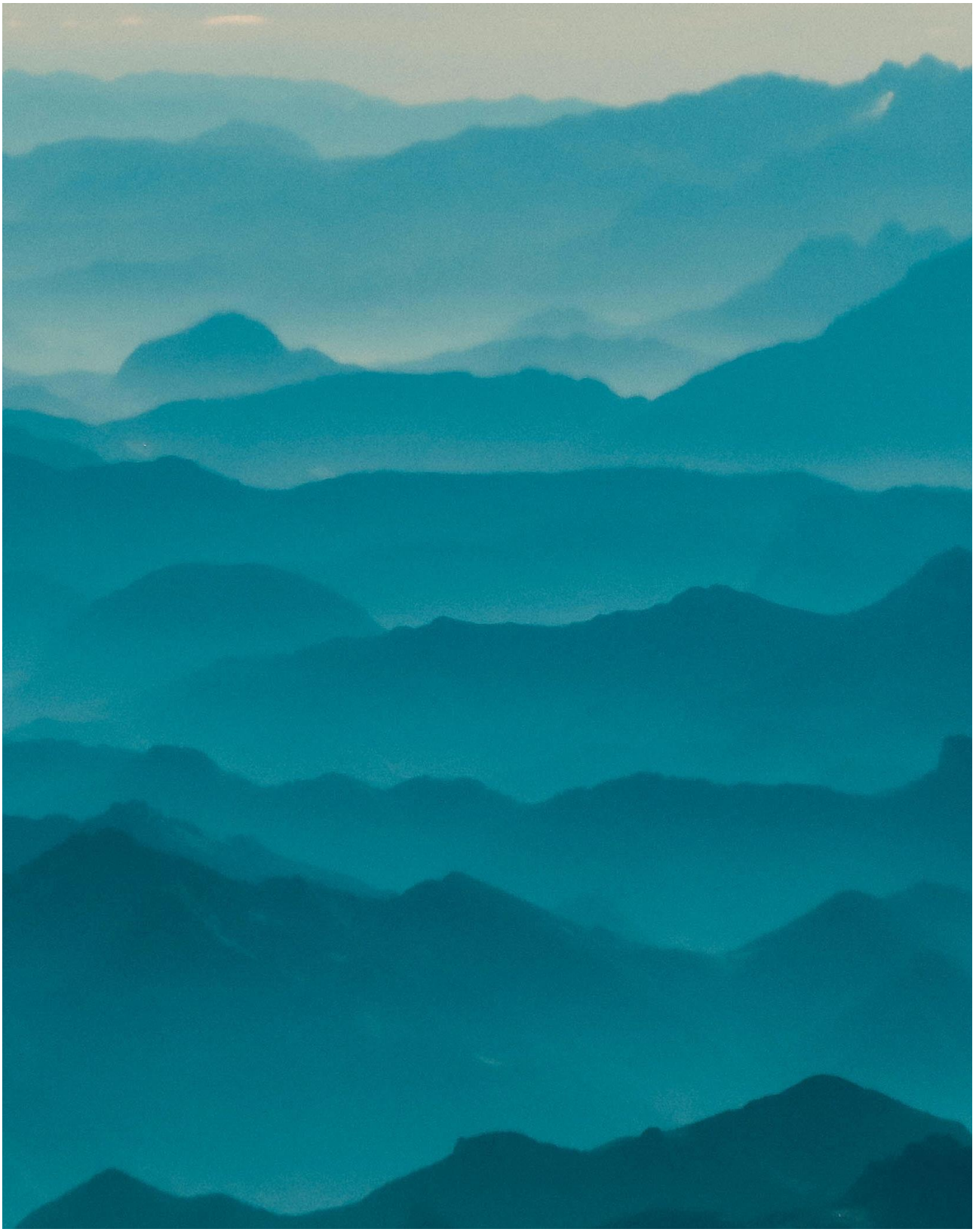
Ransomware e os ataques de integridade de datos aumentan en sofisticación e frecuencia

Escaseza e alto custo do talento cualificado

Capacidades asimétricas de guerra a través do crime como plataforma de servizo

Falta de coñecemento, concienciación e prevención dos riscos derivados da operación no ciberespazo, principalmente en pemes e micropemes.

Aumento dos costes de prevención e remediación



Definición de capacidades en ciberseguridade

Resulta, por tanto, necesario que as organizacións dediquen esforzos a obter un entendemento adecuado das ameazas ás que se enfrontan, a identificar os activos e información en risco, así como as actuacións e iniciativas a acometer para previr estas ameazas.

En definitiva, deben dotarse das capacidades necesarias para facer fronte aos ciberataques.

Proceso de definición de capacidades fronte a ciberataques

Quen podería atacarnos?

- Criminais Cibernéticos (Cyber criminais)
- Hacktivistas (hackers con fins políticos e sociais)
- Colaboradores con fins maliciosos
- Provedores deshonestos
- Competidores
- Hacker habilidoso con fins individuais

Cales son os riscos clave do negocio que necesito mitigar?

- Roubo de información sensible (corporativa, reportes do consello executivo, información financeira, información de investidores, etc.)
- Fraude financeira
- Incumprimento do Sistema de Calidade
- Incumprimento da súa Visión Misión e Valores.
- Incumprimento do regulamento

Que tipo de tácticas e técnicas podería empregar un atacante ou axente ameaza?

- Enxeñería Social
- Vulnerabilidades en software ou hardware
- Ataques a través de infraestrutura de terceiros
- Credenciais de autenticación roubadas

Ciclo de evolución das organizacións

A resposta das organizacións virá condicionada polo nivel de madurez das súas capacidades. O establecemento de estruturas e procedementos para a protección das organizacións ante as ciberameazas resulta esencial. Estes virán condicionados polo nivel de madurez da organización.

Para avaliar o nivel de madurez das **capacidades** da organización en relación á **protección**, **monitoraxe** e **recuperación** ante un incidente téñense que considerar os seguintes ámbitos:

Gobernanza

Aliñación da dirección cos compromisos de ciberseguridade definidos

Nivel de desenvolvemento de plans, capacidades e recursos para cumprir cos obxectivos definidos de ciberseguridade

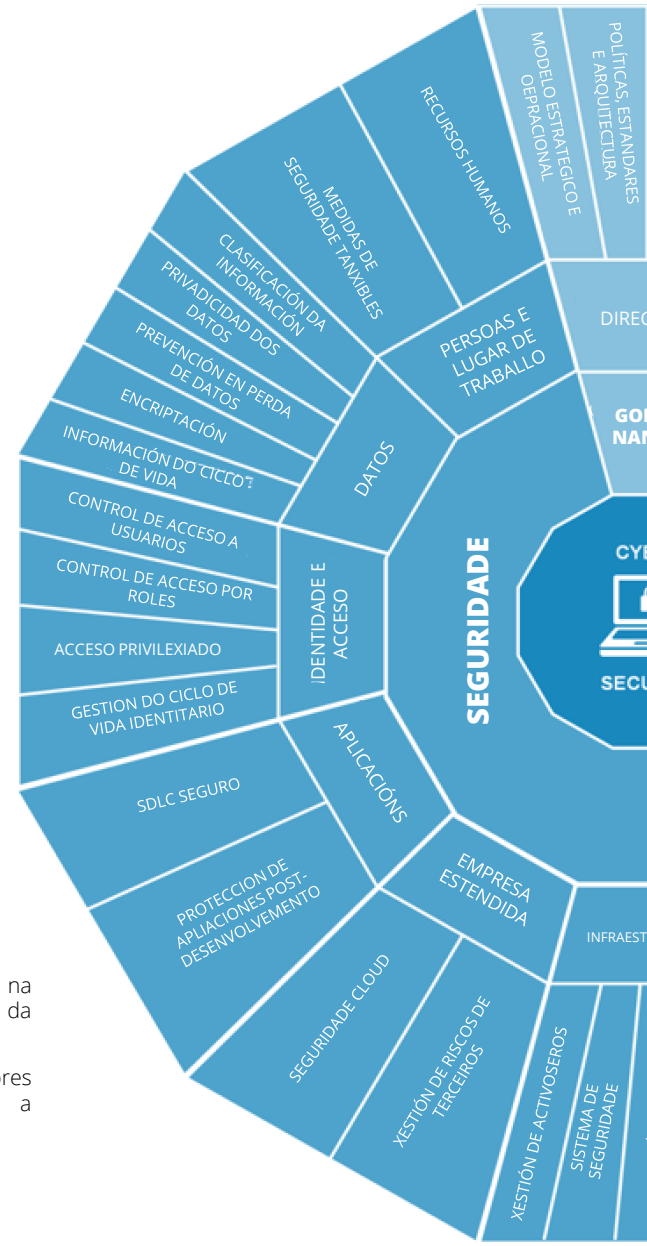
- Coordinación da dirección cos obxectivos de ciberseguridade
- Habilidades orientadas cara ao desenvolvemento de contornas seguras
- Estratexias e estrutura operativa orientados á ciberseguridade
- Políticas e cultura para o desenvolvemento de ecosistemas seguros

Seguridade

Defensas dunha organización e todos os seus compoñentes e capacidades asociadas

Protección de infraestrutura, xestión de vulnerabilidades, protección de aplicacións, xestión de identidade e acceso, e privacidade e protección da información

- Aliñar a estratexia de ciberseguridade coa estratexia de negocios.
- Identificar os teus principais activos.
- Desenvolver un marco de referencia en ciberseguridade.
- Integrar a ciberseguridade na estratexia global da organización.
- Desenvolver as mellores ferramentas para a administración dos datos.

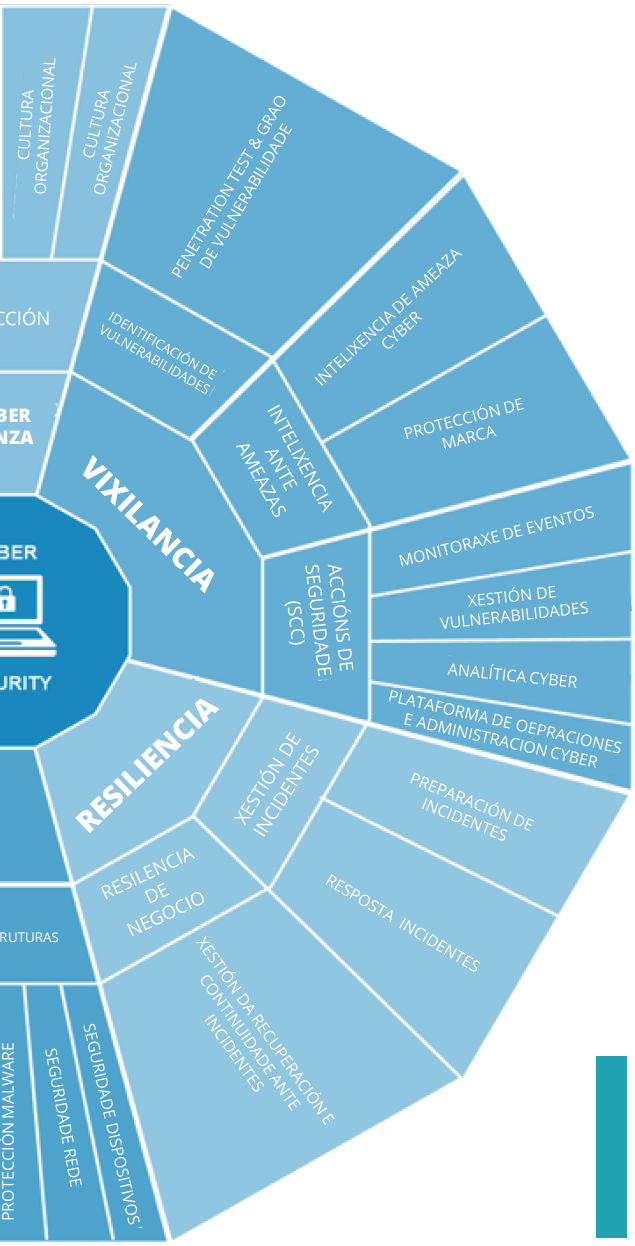


O nivel de madurez das **capacidades** da organización determinará a súa **resposta** ante ameazas

Actuacións de inicio

Actuacións de seguinte nivel

Framework



Vixilancia

A vixilancia é o sistema de alerta temperá dunha organización

As capacidades neste ámbito axudan a detectar e predicir as ameazas antes de que se convertan en ataques e ataques antes de que se convertan en infraccións e/ou en crises.

Analizar e monitorar a situación actual; estar atento.

Prestar atención a todo o ecosistema organizacional.

Desenvolvemento de procedementos, casuísticas e actuacións con simulación de ameazas.

Desenvolver un enfoque de resposta única

Resiliencia

A resiliencia mostra a capacidade regenerativa da organización

A ciber-resiliencia é a capacidade de recuperación dunha organización ante un ataque, respondendo rapidamente para minimizar o dano e facendo que os seus negocios e operacións volvan á normalidade no menor tempo posible.

Comprender e abordar as ameazas potenciais, comezar cun plan de resiliencia inicial.

Realizar test de probas e avaliacións: Wargaming, Rede-teaming, etc.

Desenvolvemento de procedementos, casuísticas e actuacións con simulación de ameazas.

Desenvolver un enfoque de resposta única

1.3. Marco europeo de referencia

Entre as recomendacións expostas pola Comisión Europea, sinaladas en páxinas anteriores, destaca a creación de Comunidades de Competencias en Ciberseguridade , nos distintos Estados Membro, compostas por industria, organizacións de investigación, asociacións e entidades públicas con capacidades nas áreas de investigación, desenvolvemento industrial, formación ou educación.

A continuación, preséntanse as 35 iniciativas identificadas e as 10 seleccionadas como mellores prácticas.

Top35 estruturas de apoio á ciberseguridade

3IF - Industrial Internet In Flanders (Bélgica)	**Algebra LAB** (Croacia)	**CybersecRDI** (Croacia)	**Cybersecurity innovation hub** (República Checa)	**LORCA** (Reino Unido)
Cybersec hub (Polonia)	**NASK -National Research Institute-** (Polonia)	**Piap hub** (Polonia)	**DIH Tartu** (Estonia)	**ZEB Smart House** (Grecia)
Santaka Valley (Lituania)	**DIGIHALL** (Francia)	**TeraLab** (Francia)	**Jessica France - Cap'tronic program** (Francia)	**Mov'eo** (Francia)
ASTER-DIH (Italia)	**Digital Innovation Hub Liguria** (Italia)	**DIH-Confartigianato Ancona** (Italia)	**DIHV - Digital Innovation Hub Virtuale** (Italia)	**Medisdih** (Italia)
Basque Digital Innovation Hub (España)	**Innovalia ZDM Digital Innovation Hub** (España)	**ITI Data Hub** (España)	**Cybersecurity Innovation HUB** (España)	**DaSCII Hub** (España)
DIHBU Industry 4.0 (España)	**I4MSOUTH** (España)	**Boost Smart Industry Hub** (Holanda)	**Novel-T** (Holanda)	**Clúster de ciberseguridad del Norte de Europa** (Finlandia)
Asia Cybersecurity Exchange (Malasia)	**NSW cybersecurity innovation node** (Australia)	**Cyber Security Innovation Node Canberra** (Australia)	**Mid-Atlantic Cyber Center (MACC)** (EEUU)	**Cyber Security Cluster de Bonn** (Alemania)

Top10 estruturas de apoio á ciberseguridade

1. LORCA (Reino Unido) 4,55	**2.** NSW cybersecutiry Innovation node (Australia) 4,55	**3.** Cybersecurity Innovation Hub (España) 4,4	**4.** Clúster de ciberseguridad del Norte de Europa (Finlandia) 4,4	**5.** Cyber Security Cluster de Bonn (Alemania) 4,10
6. Cybersec hub (Polonia) 4,10	**7.** Basque Digital Innovation Hub (España) 3,85	**8.** DIH Tartu (Estonia) 3,85	**9.** Cibersecurity innovation hub (República Checa) 3,8	**10.** CybersecRDI (Croacia) 3,8

Conclusións

Da análise das mellores prácticas nas estruturas de apoio á ciberseguridade extraéronse as seguintes conclusións:

Modelo estrutural

As principais estruturas de apoio á ciberseguridade analizadas, distínguense por conformarse como:

- Entidades públicas adscritas ao departamento competente en materia de ciberseguridade da rexión.
- Colaboración público-privada.
- Consorcios públicos.

Actividades

Identifícanse unha serie de actividades e servizos comúns que se poderían caracterizar da seguinte forma:

- Acceso a Laboratorios e infraestruturas
- Formación e Capacitación.
- Asesoría e *mentoring* a nivel tecnolóxico e económico.
- Interconexión con novos axentes.
- Publicacións e investigacións.

Socios colaboradores

Para crear un ecosistema á vangarda da innovación e áxil, a maior parte de estruturas de apoio á ciberseguridade, levan a cabo colaboracións con:

- Centros nacionais de ciberseguridade.
- Universidades.
- Centros de investigación.
- Asociacións públicas.
- Empresas privadas (sector servizos e industrial).
- Asociacións e agrupación industrial empresariais.

Resulta esencial a aplicación dunha visión **inclusiva** e **participativa,** na que as Administracións Públicas e os sectores económicos, académicos e sociais implicados desempeñen un papel crucial para o desenvolvemento dunha contorna que asegure o **aproveitamento** de sinerxías e a disposición de facilidades para **crear**, **desenvolver** e **soster** no tempo unha estratexia capaz de articular a aposta dun territorio pola **ciberseguridade.**

Capítulo 2
A industria da ciberseguridade en Galicia

2.1. O camiño percorrido

2.2. Exposición a ameazas en Galicia

2.3. Cadea de valor

2.4. Oportunidades e necesidades do sector

2.5. Matriz DAFO

2.1. O camiño percorrido

Ante o propósito da Comisión Europea de crear e instaurar unha contorna segura e proporcionar unha rede europea de centros nacionais de coordinación en ciberseguridade con comunidades de competencias en ciberseguridade, son moitas as rexións que comezaron a potenciar as estratexias e marcos de actuación en ciberseguridade, así como a crear as infraestruturas en favor da mellora da ciberseguridade nos seus territorios.

**DECRETO 252/2011, do 15 de decembro, polo que se crea a Axencia para a Modernización Tecnolóxica de Galicia e apróbanse os seus estatutos. Entre eles:*

- *Definición de estándares, directrices e normas de seguridade e calidade tecnolóxicos aos que deberán axustarse os órganos dependentes da Xunta de Galicia*
- *Dirección das políticas corporativas de seguridade informática da Xunta de Galicia*

A II Estratexia Nacional de Ciberseguridade

A Estratexia Nacional de Ciberseguridade, aprobada en abril 2019, adecúase ás necesidades da Comisión Europea e establece uns obxectivos en favor da unidade, a comunicación e a resposta conxunta dos axentes ante os ataques de ciberseguridade.

Unidade de Acción

Resposta ante un incidente no ámbito da ciberseguridade que poida implicar a distintos axentes do Estado verase reforzada se é coherente, coordinada e resólvese de maneira rápida e eficaz, calidades alcanzables a través da adecuada preparación e articulación da unidade de acción do Estado.

Anticipación

Priman as actuacións preventivas sobre as reactivas. Dispoñer de sistemas eficaces, con información compartida o máis próximo ao tempo real, permite alcanzar un adecuado coñecemento da situación.

Eficiencia

A ciberseguridade precisa do emprego de sistemas multipropósito de gran valor e elevado nivel tecnolóxico, que levan asociadas unhas necesidades moi esixentes e un alto custo derivado do seu desenvolvemento, adquisición e operación.

Resiliencia

Característica fundamental que deben posuír os sistemas e infraestruturas críticas. O Estado está obrigado a asegurar a dispoñibilidade dos elementos que se consideren esenciais para a nación, mellorando a súa protección contra as ciberameazas.

A Ciberseguridade como unha tecnoloxía clave na Estratexia Dixital de Galicia 2030

**Lanzamento do proceso de elaboración.*

Plan de seguridade

Plan director de seguridade TIC 2015 -2021

- Mellorar a seguridade dos sistemas de información da Xunta de Galicia.
- Xestión centralizada desde AMTEGA
- Configuración de servizos e estruturas

Ferramentas de ciberseguridade

CSIRT.gal

- Mitigar o impacto dos incidentes de seguridade da Xunta de Galicia, administrado por Amtega.
- Equipo de persoal técnico especializado
- Desenvolvemento de medidas preventivas e reactivas

A ciberseguridade na Estratexia Dixital de Galicia 2030

A EDG2030, propón iniciativas para incrementar o despregamento de tecnoloxías dixitais a gran escala e promover a súa adopción por parte de cidadanía, tecido empresarial e administracións co fin último de contribuír ao incremento da calidade de vida e o desenvolvemento sustentable nas vertentes económica social e ambiental.

Así mesmo, como acción complementaria aos traballos preparatorios da futura Estratexia Dixital de Galicia, desde a Xunta de Galicia establecéronse convenios de colaboración, en concreto, en materia de ciberseguridade:.

Asina Convenio: Xunta de Galicia - INCIBE.

Colaboración en actividades e iniciativas que permitan progresar na difusión do coñecemento, especialmente no que se refire ás materias propias de ambas entidades, así como no desenvolvemento, en xeral, de calquera outra actividade que ambas as partes consideren oportuna para alcanzar os fins respectivos e os obxectivos de realización de actuacións relativas ao fomento da ciberseguridade

Segundo o último Estudo sobre a Peme 2018 do Ministerio de Industria, Enerxía e Turismo, o 99,93% do tecido empresarial galego está formado por pemes e micropemes que están a abordar procesos de transformación dixital para a mellora da súa competitividade. Estas empresas manteñen, a día de hoxe, unha actitude pasiva fronte ás ciberameazas, polo que gran parte da demanda de servizos de ciberseguridade vén determinada pola xestión de ciberataques.

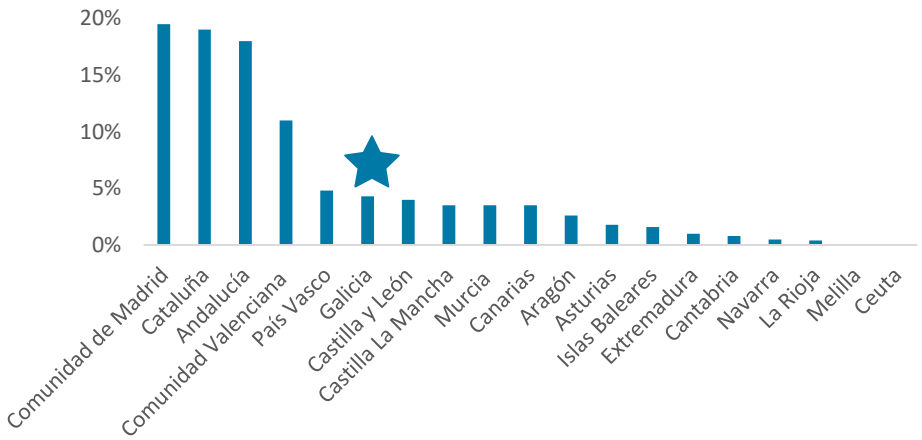
2.2. Exposición a ameazas en Galicia

O Instituto Nacional de Ciberseguridade (INCIBE) detectou durante o ano pasado unha media diaria de máis de 2.800 recursos comprometidos. Os recursos comprometidos inclúen calquera equipo, sistema, servizo, rede ou activo tecnolóxico que fose afectado por un problema de seguridade.

Galicia rexistra un **4,3%** dos casos rexistrados por INCIBE no ámbito nacional.

A clasificación lidérano Madrid, Andalucía e Cataluña, con porcentaxes próximas ao 20%.

A maioría de ataques corresponden ao control remoto de computadores por ciberdelicuentes tras infectalos cun Malware.



Distribución dos recursos comprometidos por Comunidades Autónomas. INCIBE.(2018).

Distribución de recursos afectados por provincias

A Coruña

+30%
Activos tecnolóxicos con problemas de seguridade

Pontevedra

40%
Activos tecnolóxicos con problemas de seguridade

Lugo

20%
Activos tecnolóxicos con problemas de seguridade

Ourense

10%
Activos tecnolóxicos con problemas de seguridade

Distribución dos recursos comprometidos na Comunidade Autónoma Galega. INCIBE.(2018).

2.3. Cadea de Valor

Para levar a cabo a análise dos axentes que configuran o sector da ciberseguridade en Galicia conceptualizouse a cadea de valor na que se agrupan os mesmos en función do rol que ocupan na mesma:

Cadea de valor da ciberseguridade

DRIVERS

Factores, tendencias e retos que motivan o desenvolvemento do sector da ciberseguridade.

Son aqueles xa mencionados nos capítulos anteriores do presente documento.

ENTIDADES DE APOIO

Estruturas que promoven a coordinación de actividades, asesoramento experto e procura de recursos para o desenvolvemento de actividades de interese para o sector. Identifícanse como entidades de apoio os nodos de especialización tecnolóxica (5G), clústeres sectoriais e Digital Innovation Hubs creados ata o momento en Galicia: Datalife, Hub Industrial de Galicia, Galactica e Artificial Intelligente

FACILITADORES

Aqueles representantes da órbita institucional que marcan as pautas estratéxicas que ordenan o desenvolvemento do sector da ciberseguridade.

Estes eríxense como os "facilitadores" do ecosistema na medida que sintan unhas bases ou obxectivos comúns e poñen ao disposición do resto de axentes uns medios que contribúan a alcanzalos.

OPERADORES

Actores que ofertan e demandan as solucións de ciberseguridade, así como todos aqueles que contribúen á xeración do valor.

- Ideación - Diferenciación
- Demanda Usos e aplicacións
- Oferta - Desenvolvemento de solucións.

MARCO ESTRATÉXICO – FACILITADORES

	Estratexia
Unión Europea	Estratexia de Ciberseguridade da Unión Europea.
España	Estratexia Nacional de Ciberseguridade 2019
Galicia	Estratexia Dixital de Galicia 2030

OPERADORES

Cadea de valor da ciberseguridade

Ideación - Diferenciación

Universidades

Investigación e formación

Centros tecnolóxicos

Investigación e Transferencia

Propón

Transfire

Oferta – Desenvolvemento de solucións

Servizos

Auditoría Técnica	Certificación de Normativa	Seguridad e na Nube	Cumprimento Legal	Xestión de incidentes
Formación e concienciación	Continxencia e Continuidade	Implantación de Solucións	Soporte e Mantemento	

Produtos

Anti - Fraude	Anti - Malware	Auditoría Técnica	Certificación Normativa
Continxencia e Continuidade	Control de Acceso e Autenticación	Cumprimento Legal	
Prevención de fuga de información	Protección das comunicacións	Seguridade en Dispositivos Móbiles	Intelixencia de Seguridade

Táctica

Plan director. Resposta a incidentes de ciberseguridade transfronteirizos 2017

Plan Director de Ciberseguridade 2019 *(Pendente de aprobación)*

Plan Director de Seguridade TIC 2015-2021

Operativa

enisa · incibe_ · CNPIC · CCN-CERT · amtega

Integrador Consultor · Provedor/ Distribuidor · Fabricante · Fabricante/ Provedor/ Integrador

Solicita

Responde

Demanda – Usos e aplicacións*

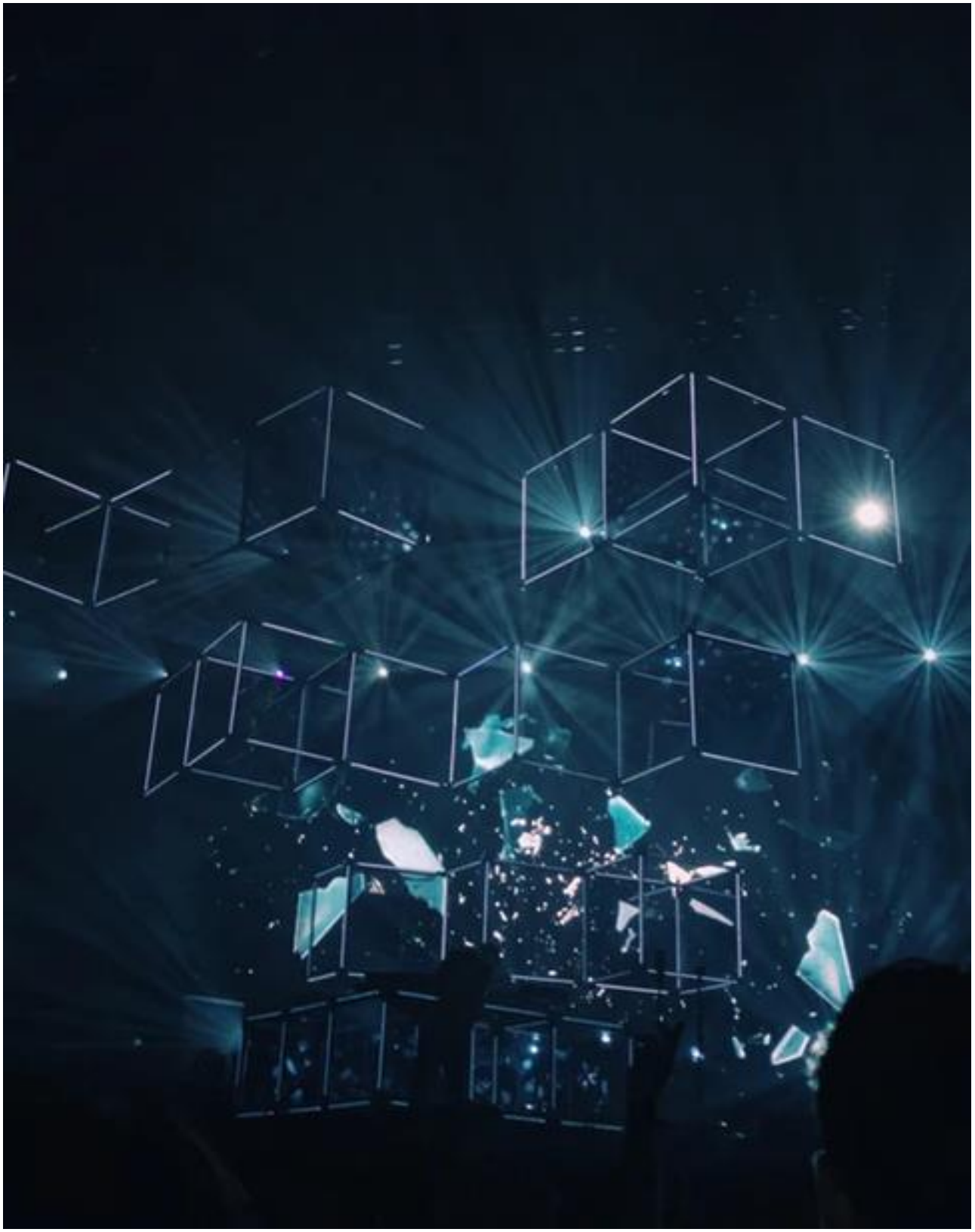
Sector Público

Deputación DA CORUÑA · DEPUTACIÓN DE LUGO · XUNTA DE GALICIA · fegamp · DEPUTACIÓN PONTEVEDRA · DEPUTACIÓN PROVINCIAL DE OURENSE

Sector Privado

//ABANCA · FINSA · COREN · CLUSTER TIC GALICIA

(*) Entidades que colaboraron na análise inicial.



Facilitadores

O sector da ciberseguridade en Galicia deberá atender ás directrices, recomendacións e requirimentos establecidos no seguinte marco estratéxico:

	Unión Europea	España	Galicia
Estratexia	**Estratexia de ciberseguridade da Unión Europea** *(setembro de 2017)* Establece os obxectivos e alicerces para a Unión Europea e os estados membros en base a catro obxectivos: • Mercado único de ciberseguridade. • Marco de certificación común. • Seguridade no deseño e principio de vixilancia. • Cooperación público-privada.	**Estratexia Nacional de Ciberseguridade 2019** *(2019)* Realízase unha actualización da estratexia nacional de 2013, en base á estratexia de ciberseguridade europea, establécense catro alicerces fundamentais: • Unidade de Acción. • Anticipación. • Eficiencia. • Resiliencia.	**Estratexia Dixital de Galicia 2030** *(en elaboración)* O seu obxectivo é establecer, de forma participativa unha estratexia dixital única para Galicia a través de 4 vectores de cambio: • Garantir a igualdade dixital. • Poñer o foco nas persoas. • Potenciar un ecosistema dixital forte. • Promover o liderado dixital.
Plans de Acción	**Plan director. Resposta a incidentes de ciberseguridade transfronteirizos 2017** *(novembro de 2018)* A cooperación como vector principal da ciberseguridade, séguese uns obxectivos centrais: (i) Permitir unha resposta eficaz, compartir o coñecemento da situación e poñerse de acordo sobre mensaxes clave de comunicación.	**Plan Director de ciberseguridade 2019** *(Pendente de aprobación)* *Está pendente de aprobación o Plan Director de Ciberseguridade que de resposta ás necesidades da Estratexia Nacional de Ciberseguridade tanto europea como nacional.*	**Plan Director de Seguridade TIC 2015-2021** Aliñación coa Estratexia Nacional de Ciberseguridade. Os obxectivos principais: • Xestión transversal. • Consolidación e madurez. • Análise e riscos . • Sistemas de información resistentes. • Adecuación a requisitos legais. • Concienciación e formación.
Outras Ferramentas	**ENISA (Axencia de Ciberseguridade Europea)** ENISA, contribúe activamente á política europea de ciberseguridade, apoiando aos Estados membros para apoiar a resposta a incidentes cibernéticos a gran escala.	**INCIBE (Instituto Nacional de Ciberseguridade)** Dependente do Ministerio de Enerxía, Turismo e Axenda Dixital. Protección do ciberespazo utilizado por pemes e cidadáns. **CCN-CERT** Adscrito ao CNI, detén e dá resposta a ameazas nos sistemas de TI e as comunicacións das AAPP e empresas estratéxicas. **CNPIC** Dependente do Ministerio do Interior, protexe as infraestruturas críticas de España.	**Axencia para a Modernización Tecnolóxica de Galicia (AMTEGA)** A Axencia para a Modernización Tecnolóxica de Galicia (Amtega), adscrita á Presidencia da Xunta de Galicia, ten como obxectivos básicos a definición, o desenvolvemento e a execución dos instrumentos da política da Xunta de Galicia no campo das tecnoloxías da información e a comunicación e a innovación e o desenvolvemento tecnolóxico.

Operadores

Dentro do grupo de "operadores" encargados de xerar valor na cadea produtiva de ciberseguridade identifícanse tres tipos de axentes:

Ideación:

Os axentes de ideación cobran unha especial importancia debido ao auxe de novos programas de formación e a creación de novas entidades que fomentan o desenvolvemento e evolución da ciberseguridade. Encargados da formación, a investigación e a transferencia do coñecemento.

En relación coa formación, destaca o Máster Inter-Universitario en ciberseguridade (MUNICS) das Universidades de Vigo e A Coruña. Celébranse ademais diferentes xornadas e eventos relacionados coa ciberseguridade, e recentemente creáronse capítulos autonómicos de asociacións como ISMS que potenciarán esta área.

Respecto á investigación destacan os grupos de investigación da Universidade de Vigo. Así como, os Centros Tecnolóxicos CITIC e en especial Gradiant, quen conta con grupos e diversas liñas de traballo vinculadas á ciberseguridade.

No ámbito da transferencia de coñecemento, cabe mencionar o Tegra Cybersecurity Center iniciativa impulsada por Telefónica e Gradiant e co apoio da Xunta de Galicia e a Rede de Excelencia en Tecnoloxías de Seguridade e Privacidade ÉGIDA financiada polo Ministerio de Ciencia, Innovación e Universidades no marco das axudas CERVERA que liderará Gradiant.

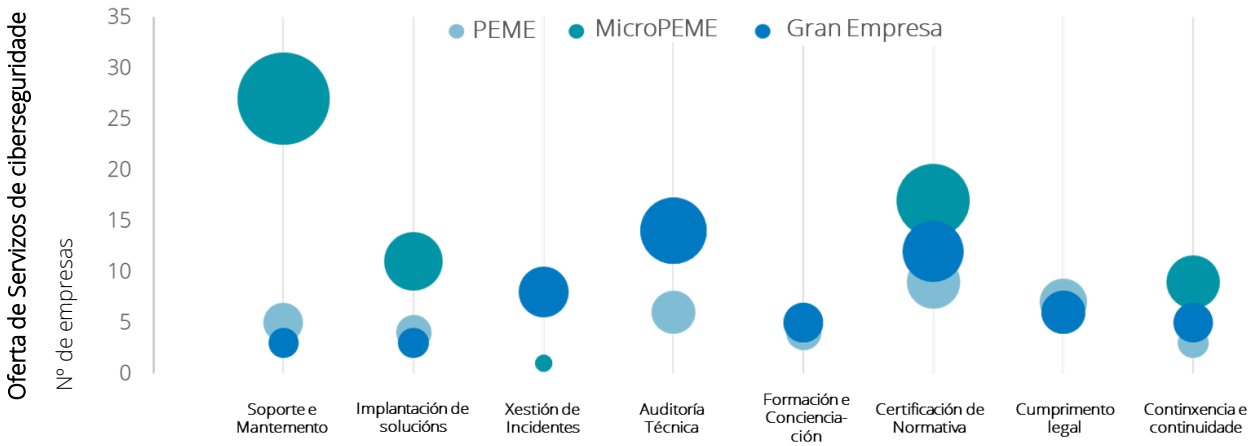
Oferta:

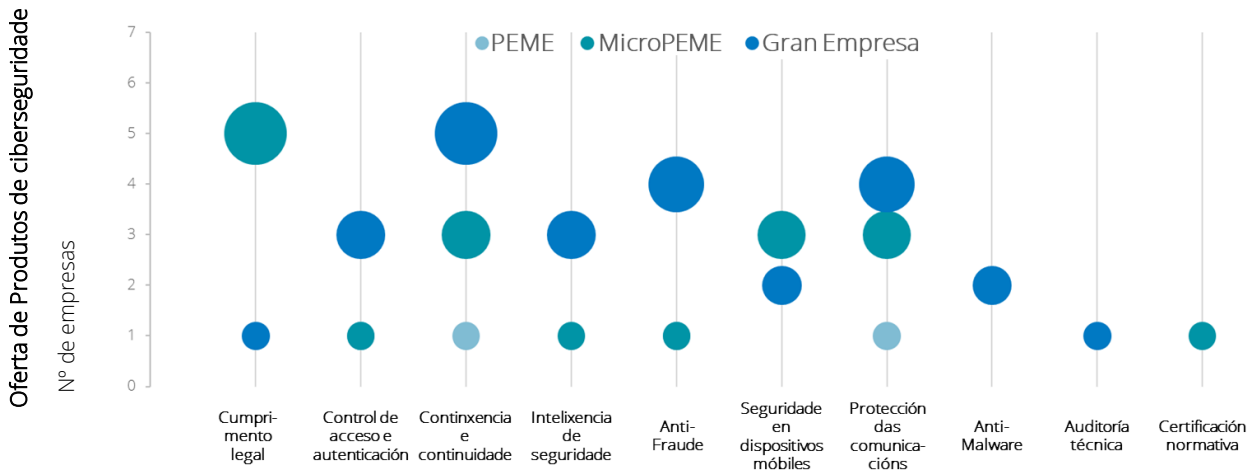
Empresas que desenvolven actividades de prestación de servizos ou desenvolvemento e implantación de solucións de ciberseguridade, en Galicia.

Identificáronse un total de 103 empresas que realizan este tipo de actividades no territorio galego, das cales:

4%	53%	21%	22%
Startups	Micropemes	Pemes	Grandes Empresas

Procedeuse a clasificar as empresas identificadas segundo a clasificación de servizos e produtos que ofrecen, en función á taxonomía de INCIBE:





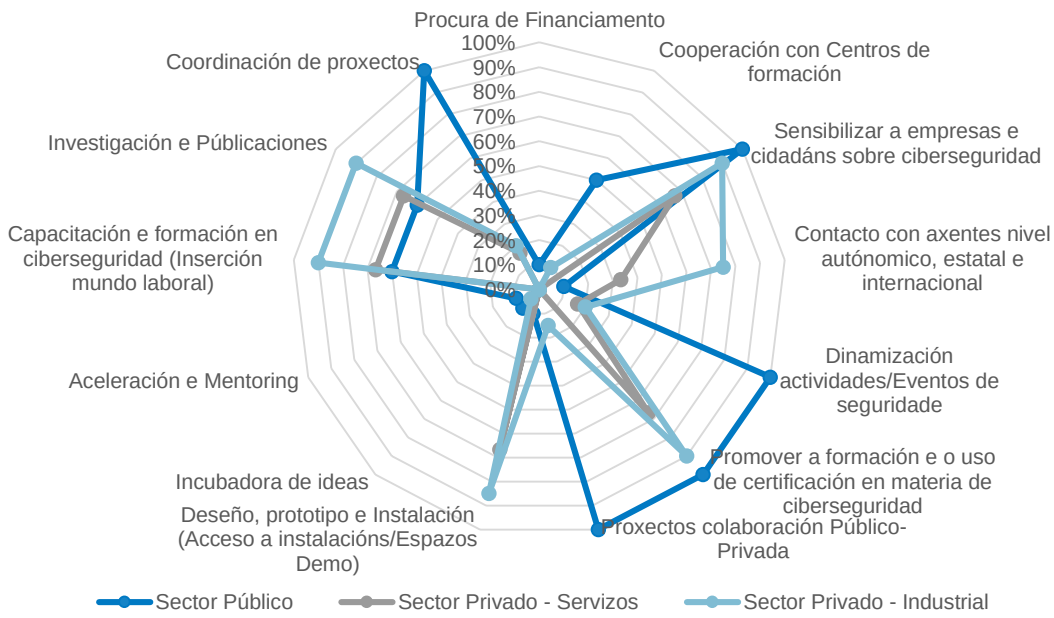
Fonte: elaboración propia a partir de catálogo empresas e solucións de ciberseguridade de INCIBE

Demanda:

Entendidos como os axentes onde a ciberseguridade vai atopar o seu uso e aplicación e clasificados en función da orixe destes demandantes e a súa área de actuación (Sector Público, Sector Privado Industrial e Sector Privado Servizos).

Unha vez identificadas as principais entidades demandantes de produtos e servizos de ciberseguridade en Galicia, en base ás entrevistas levadas a cabo con algúns destes axentes, extráense as seguintes conclusións acerca dos posibles requirimentos ou servizos que debería ofertar unha estrutura de apoio á ciberseguridade en Galicia:

- Destaca o interese as entidades na **capacitación e formación** en materia de ciberseguridade ademais da identificación da necesidade de sensibilizar **a empresas e cidadáns** sobre a importancia da mesma.
- Desde as entidades do **Sector Público** identifícase o interese no impulso de proxectos de colaboración público-privada e a promoción de eventos, formación e certificacións.
- Por último, desde **o Sector Privado** demándase o acceso a instalacións e infraestruturas comúns así como a posibilidade de facilitar o contacto entre os diferentes axentes.



Fonte: elaboración propia a partir das enquisas realizadas aos axentes Demanda.

Interacción e diálogo

Identificáronse 167 entidades que poderían ter relación directa coa estrutura de ciberseguridade en Galicia. Entre elas 103 axentes ofertantes de produtos e servizos de ciberseguridade. Os datos mostrados nestas conclusións baséanse no feedback recibido por 48 destes axentes.

2.4 Oportunidades e necesidades do sector

Recóllense a continuación algunhas das principais conclusións obtidas da realización das enquisas e entrevistas que permiten obter unha imaxe fiel das oportunidades e necesidades do sector e en máis detalle, a posible necesidade dunha estrutura de apoio á ciberseguridade en Galicia. Estes foron os ámbitos analizados:

BLOQUE A

Perfilado e importancia da ciberseguridade nas organizacións

Identificar a entidade, perfil e tipoloxía de servizos acorde coa taxonomía definida por INCIBE, así como a realidade da ciberseguridade na organización.

BLOQUE B

Visión ecosistema ciberseguridade Galicia.

Valorar o coñecemento e percepción do ecosistema da ciberseguridade en Galicia

BLOQUE C

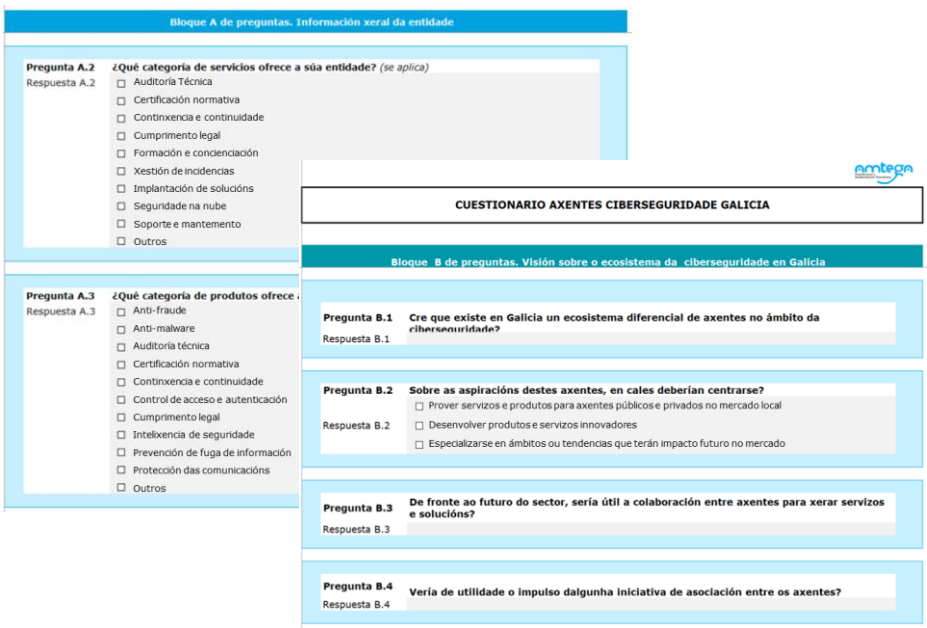
Opinión creación estrutura de colaboración

Coñecer a opinión sobre a posible creación dunha estrutura de coordinación, e caracterización acorde á súa orientación estratéxica.

BLOQUE D

Participación na hipotética estrutura de apoio de ciberseguridade.

Detectar interese na participación e expectativas acerca da estrutura de coordinación.



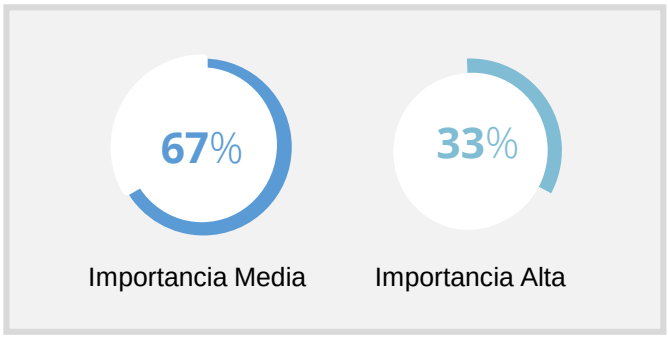
Cuestionarios empregados para as entrevistas e enquisas

No primeiro bloque, destácase a perspectiva das organizacións sobre a importancia da ciberseguridade e as necesidades actuais das organizacións

A B C C

Importancia da ciberseguridade nas organizacións

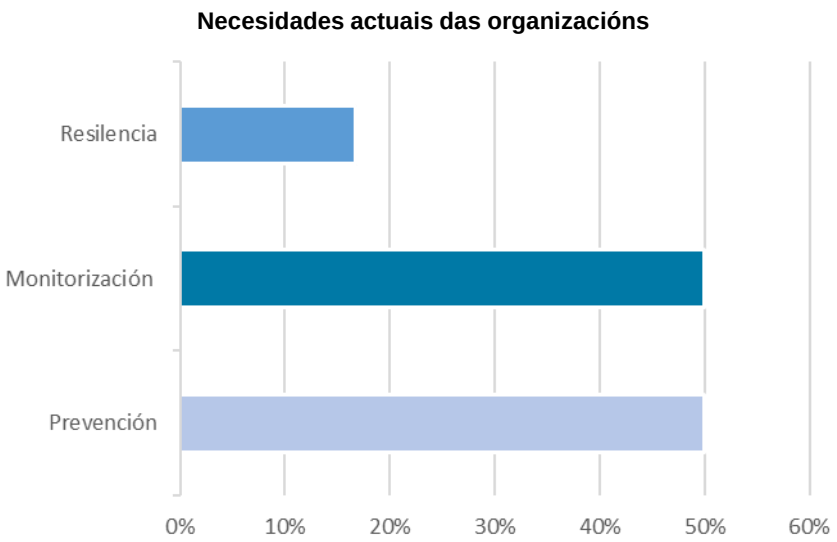
Saliéntase a crecente importancia da ciberseguridade e a aparición das novas necesidades. Afirmando a recente inclusión de estratexias de ciberseguridade, medidas concretas e desenvolvemento de accións de concienciación interna.



Fonte: Resultados de enquisas e entrevistas con axentes da cadea de valor da ciberseguridade en Galicia

Necesidades actuais das organizacións

Os axentes entrevistados e enquisados establecen unha maior necesidade de mecanismos e ferramentas de prevención e seguimento que de resiliencia fronte a ameazas de ciberseguridade.



Fonte: Resultados de enquisas e entrevistas con axentes da cadea de valor da ciberseguridade en Galicia

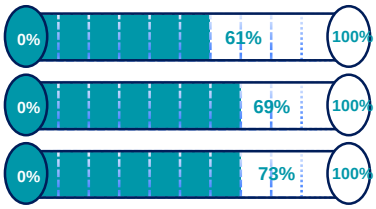
No segundo bloque, destácase a perspectiva das organizacións sobre o ecosistema de ciberseguridade en Galicia, as tendencias e o futuro do sector na súa organización.

A B C C

Aspiración dos axentes

Necesidades e estratexias a seguir polas entidades para lograr un maior desenvolvemento en ciberseguridade en Galicia.

- Prover servizos e produtos para axentes públicos e privados no ámbito local
- Especialización en ámbitos ou tendencias que terán impacto futuro
- Desenvolver produtos e servizos innovadores

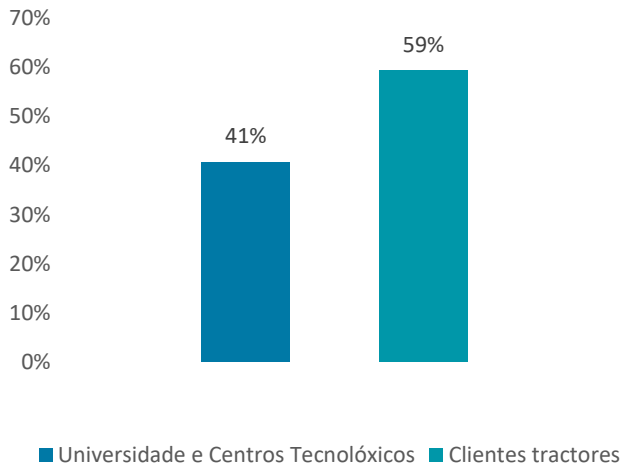


Fonte: Resultados de enquisas e entrevistas con axentes da cadea de valor da ciberseguridade en Galicia

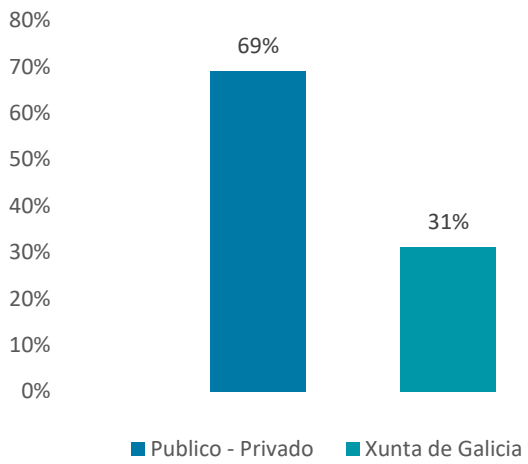
As entidades consideran que ofrecer servizos de valor, ben sexa a través da especialización ou a innovación é relevante para lograr un ecosistema diferencial que poida competir tanto en Galicia como noutras rexións.

Colaboración entre axentes

O 100% dos entrevistados e enquisados, cren que a colaboración entre axentes é necesaria para o desenvolvemento do ecosistema, manifestándose diferenzas en canto aos axentes considerados como prioritarios para esta colaboración:



Sobre a tipoloxía de axentes que deberían de participar nesta iniciativa de colaboración, a visión dos enquisados decántase por unha combinación público-privada:



Fonte: Resultados de enquisas e entrevistas con axentes da cadea de valor da ciberseguridade en Galicia

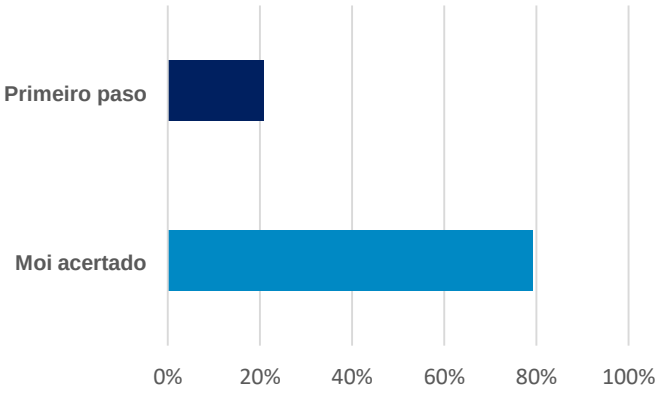
Neste terceiro bloque, recóllese a opinión dos axentes en relación á necesidade dunha estrutura de coordinación e quen debe de asumir o rol de liderado.

Necesidade dunha estrutura de apoio

Case o 80% dos axentes entrevistados e enquisados afirman que esta iniciativa é unha necesidade e unha proposta moi acertada da Xunta de Galicia.

Entre as conclusións achegadas polos axentes destacan dúas conclusións:

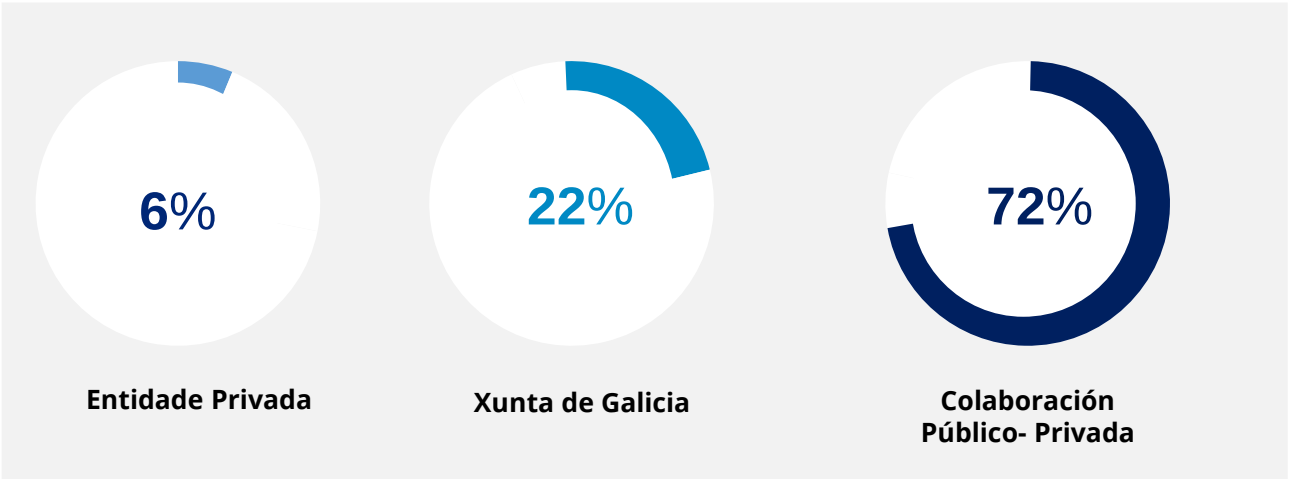
- Necesidade de inclusión de todos os axentes involucrados no sector tanto de grandes, empresas, como pemes, usuarios e universidades. Especial mención aos colexios profesionais e entidades especializadas en materia de ciberseguridade.
- Necesidade de especialización nalgún ámbito concreto da ciberseguridade.



Fonte: Resultados de enquisas e entrevistas con axentes da cadea de valor da ciberseguridade en Galicia

Entidade líder da estrutura de apoio

Sobre o liderado e a xestión do nodo os axentes entrevistados e enquisados sinalan a importancia dunha colaboración Público- Privada.



Fonte: Resultados de enquisas e entrevistas con axentes da cadea de valor da ciberseguridade en Galicia

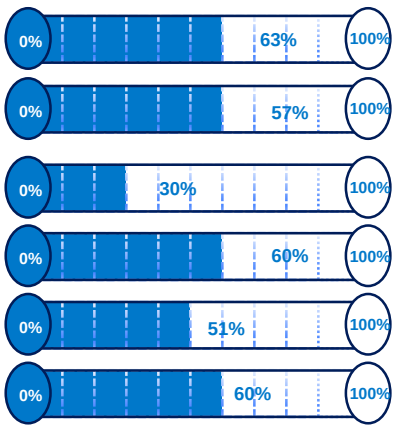
Neste cuarto bloque, recóllese a opinión dos axentes en relación a cal sería o beneficio para a súa entidade e para o conxunto de Galicia.

A B C D

Beneficios para a entidade

En relación a cales son os beneficios que espera o axente que obteña a súa entidade sobre a creación dunha estrutura de colaboración para a súa entidade, concluíronse:

- Facilitar relacións con partners para abordar proxectos
- Facilitar o acceso a novos clientes e mercados
- Acceder a financiamento para proxectos de investigación
- Dispoñer información sobre novas tendencias, certificacións, normativas ou eventos
- Atopar asesoramento experto
- Coñecer proxectos e capacidades innovadoras na rexión

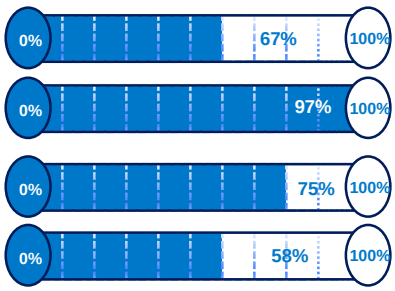


Fonte: Resultados de enquisas e entrevistas con axentes da cadea de valor da ciberseguridade en Galicia

Beneficios para Galicia

Por último, os axentes valoraron cal sería o impacto dunha estrutura de apoio á ciberseguridade para as diferentes estruturas e ferramentas, en consecuencia cales son os beneficios para o sector da ciberseguridade en Galicia:

- Crecemento do sector da ciberseguridade en Galicia
- Incremento de concienciación en empresas e cidadáns
- Xeración dunha rede de colaboración
- Incremento do investimento e capacidades na I+D+i en ciberseguridade



Fonte: Resultados de enquisas e entrevistas con axentes da cadea de valor da ciberseguridade en Galicia

2.5 Matriz DAFO

A continuación, preséntanse en formato DAFO, as conclusións extraídas tras a análise e diálogo cos principais axentes sobre a posibilidade de creación dunha estrutura de apoio á ciberseguridade en Galicia. Estas conclusións agrupáronse nos seguintes ámbitos:

Ámbito estratéxico e regulamentario

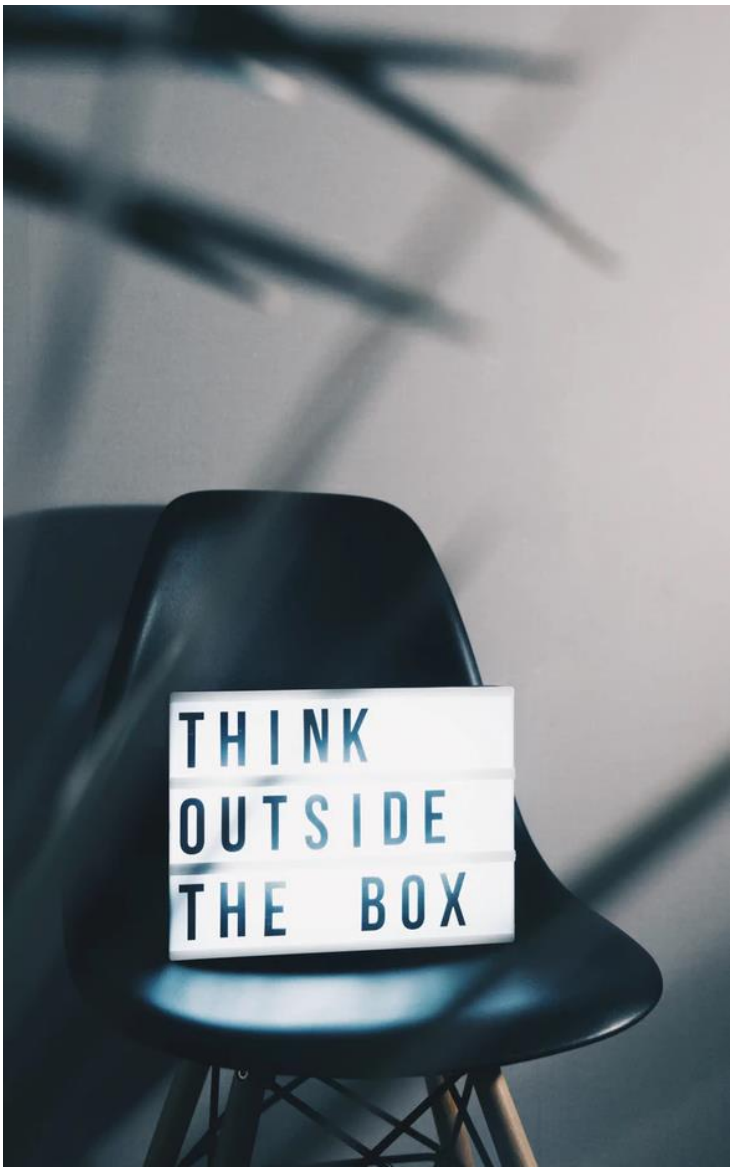
- Marco estratéxico vixente a nivel internacional, nacional e/ou rexional.
- Marco normativo ou regulamentario que podería afectar o ámbito de actividade da ciberseguridade.
- Necesidade de xerar estruturas rexionais de coordinación para a ciberseguridade indicadas pola Comisión Europea.

Ámbito organizativo e de actividade

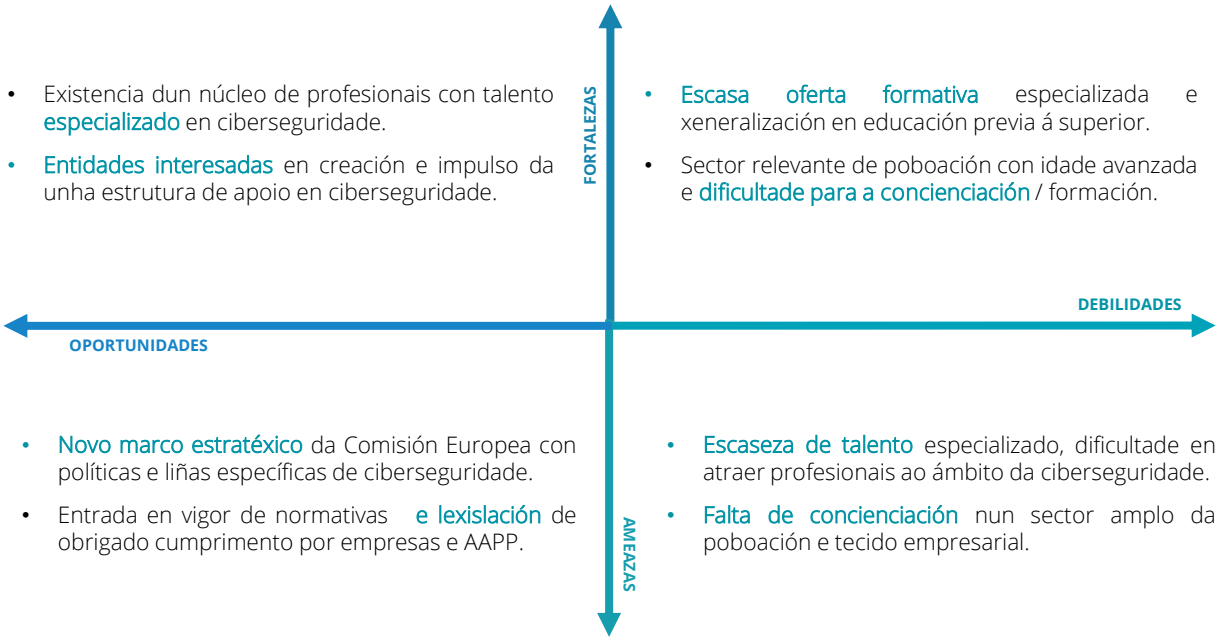
- Composición do ecosistema de ciberseguridade en Galicia.
- Clasificación e necesidades identificadas nos elos da cadea de valor do ecosistema.
- Coordinación cos axentes do tecido socioeconómico e sociedade galega.

Ámbito económico

- Posibilidades de concorrencia a convocatorias europeas para financiamento de actividades e programas de innovación.
- Instrumentos de financiamento vinculados a iniciativas tecnolóxicas en AAPP a nivel autonómico e estatal.
- Viabilidade para mobilizar investimento de iniciativas privadas.



Ámbito estratéxico e regulamentario



- Existencia dun núcleo de profesionais con talento especializado en ciberseguridade.
- Entidades interesadas en creación e impulso da unha estrutura de apoio en ciberseguridade.

- Escasa oferta formativa especializada e xeneralización en educación previa á superior.
- Sector relevante de poboación con idade avanzada e dificultade para a concienciación / formación.

- Novo marco estratéxico da Comisión Europea con políticas e liñas específicas de ciberseguridade.
- Entrada en vigor de normativas e lexislación de obrigado cumprimento por empresas e AAPP.

- Escaseza de talento especializado, dificultade en atraer profesionais ao ámbito da ciberseguridade.
- Falta de concienciación nun sector amplo da poboación e tecido empresarial.

Ámbito organizativo e de actividade

- Acordos con entidades de coordinación estatais (INCIBE, CCN-CERT).
- Sector TIC en Galicia con certa relevancia e con iniciativas e entidades de cooperación xa creadas.

- Tecido empresarial configurado en gran medida por micropemes e pemes.
- Impulso iniciativas público-privadas e coordinación entre múltiples administracións públicas.

- Inicio de actividade en Galicia de asociacións (ISMS Forum / ISACA) con implicación activa.
- Existencia de empresas tractoras con interese en potenciar a cultura de ciberseguridade.

- Necesidade de promover prazos de execución máis curtos nas administracións públicas en canto á xestión e impulso de iniciativas.

Ámbito económico

FORTALEZAS

- Existencia de recursos de partida relevantes (coñecemento, estruturas e ferramentas) en Amtega.
- Entidades nacionais para poñer en marcha iniciativas con custo limitado (INCIBE – CCN).

- Concepción en certas organizacións (pemes e AAPP) da ciberseguridade como un gasto e non como un investimento con capacidade de achegar valor á organización.

DEBILIDADES

OPORTUNIDADES

- Dotación orzamentaria da Comisión Europea en programas de desenvolvemento ciberseguridade.
- Interese de empresas en potenciar tecido empresarial e lanzamento de startups no ámbito ciberseguridade.
- Programas xenéricos de impulso empresarial no ámbito autonómico con posibilidades de orientar cara á ciberseguridade. A inclusión da ciberseguridade no programa Reacciona TIC do IGAPE constitúe unha exemplo.

- Implicación pasiva de actores (provedores oferta, ideación, demanda) se non se definen roles e obxectivos claros nunha estrutura de coordinación.
- Determinar mecanismos que non obstrúan a libre concorrencia entre provedores que poidan prestar servizos vinculados á estrutura de coordinación (tanto internos como externos).

AMEAZAS

Capítulo 3
Una aproximación ao nodo CIBER.gal

Capítulo 3 | Unha aproximación ao nodo CIBER.gal

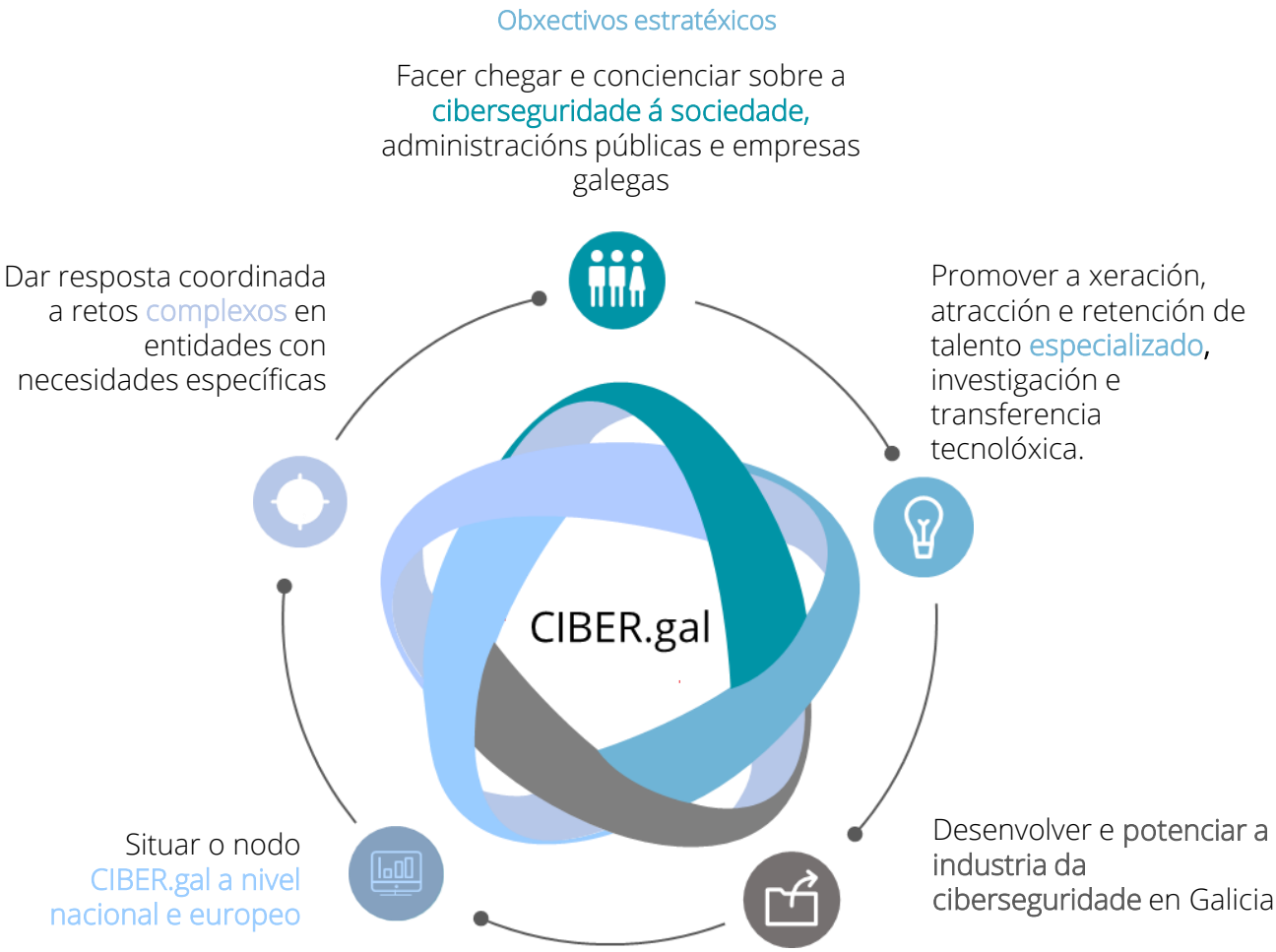
3.1 Visión estratéxica do nodo

A análise realizada ao longo deste documento pon de manifesto a necesidade de favorecer unha contorna dixital segura e afrontar, de forma colaborativa, os retos aos que se deben enfrontar empresas e administracións para protexer os seus activos no ciberespazo.

Para iso, a Xunta de Galicia debe liderar, de forma conxunta con outros axentes públicos e privados, a posta en marcha dunha iniciativa que permita, no medio e longo prazo, dispoñer dunha estrutura de apoio e fomento do sector da ciberseguridade en Galicia (en diante nodo CIBER.gal)

Misión[1]
Impulsar a ciberseguridade en Galicia desde a creación de talento ata a concienciación da sociedade, a través da xeración de iniciativas e o aliñamento de oferta e demanda.

Obxectivos estratéxicos



[1] Definida de acordo á metodoloxía **Balance Score Card** que permite deseñar a estratexia desde un punto de vista global e facela operativa en obxectivos estratéxicos, liñas de actuación e medidas.

Obxectivos

Para cada un dos obxectivos estratéxicos presentados extráense, a continuación, os obxectivos operativos que permiten materializar devanditos obxectivos en servizos ou liñas operativos de actividade do nodo

Obxectivos estratéxicos	Obxectivos Operativos	Axentes involucrados
Ciberseguridade para a sociedade	**Concienciar, Capacitar e Prover Servizos Básicos** • Formación e concienciación a pemes, administracións locais e cidadáns. • Provisión de servizos básicos de seguimento de resposta ante incidentes e cumprimento de normativa. • Certificación de empresas e entidades locais en base a servizos e ferramentas de INCIBE e CCN CERT.	*Administracións locais*, *Xunta de Galicia*, *Pemes*, *Cidadáns*
Talento Especializado	**Ideación e xeración de talento** • Identificación, captación, xeración e retención de profesionais en ciberseguridade a nivel nacional. • Posta en marcha e execución coordinada de proxectos de I+D+i en ciberseguridade de carácter nacional e internacional, en particular no ámbito europeo. • Fomento da formación en todos os niveis educativos e potenciación da Formación Profesional (FP) en ciberseguridade. • Mellora da conexión do sector académico-investigador coa industria de ciberseguridade, potenciando a transferencia de tecnoloxía e coñecemento.	*Asociacións*, *Universidades*, *Colexios / FP*, *Centros tecnolóxicos*
Retos Complexos	**Solucións disruptivas para sectores estratéxicos** • Resposta a necesidades específicas de sectores tractores en Galicia (agroalimentación, automoción, banca, etc.). • Apoio a necesidades estratéxicas da Xunta de Galicia (educación, sector primario, envellecemento, turismo, etc.). • Promoción de iniciativas vinculadas a tendencias tecnolóxicas de impacto sectorial en ciberseguridade (aeronáutica e automoción, entre outros). • Xeración de proxectos tractores de transformación da administración orientados á xeración de produtos innovadores.	*Sector Público*, *Automoción*, *Alimentario*, *Aeronáutica*, *Turismo*
Industria da Ciberseguridade	**Contribución ao desenvolvemento do sector** • Impulso á creación e aceleración de empresas con produtos específicos no ámbito da ciberseguridade. • Axuda no acceso das empresas ao mercado exterior. • Demostración e proba de tecnoloxías en administracións públicas e grandes empresas. • Procura de financiamento para proxectos de I+D+i. • Promoción na cooperación e colaboración (tanto a nivel colectivo como de socios individuais) con outras posibles redes de excelencia ou plataformas tecnolóxicas nacionais, europeas ou internacionais.	*SpinOffs*, *Pemes Grandes Empresas*, *StartUps Micropemes*
Relacións Institucionais	**Contribución ao desenvolvemento do sector** • Participación en foros e reunións nacionais e internacionais en materia de ciberseguridade. • Establecemento de convenios de colaboración con outras axencias a nivel estatal e internacional en materia de ciberseguridade.	*CIBER.gal*

3.2 Carteira de servizos

Co fin de materializar os seus obxectivos estratéxicos e operativos, o nodo poñerá ao dispor de empresas, cidadáns e administracións públicas de Galicia unha oferta harmonizada de servizos que aspire a cumprir as expectativas de todos os actores implicados no mesmo.

A continuación, realízase unha proposta dos ámbitos nos que se poderían chegar a prestar estes servizos:

	Categoría de servizos	Descrición da categoría
	Relacións institucionais (*networking*)	Xestión das relacións a nivel rexional, nacional e internacional con entidades públicas e privadas con intereses comúns en relación ao nodo.
	Observatorio e coñecemento	Seguimento, análise e avaliación do sector da ciberseguridade en Galicia e outros territorios de referencia e xeración de información e coñecemento de interese para o sector.
	Espazos para a investigación e transferencia de coñecemento	Posta ao dispor de espazos para a investigación e transferencia de coñecemento entre os membros do nodo e outras entidades, así como para o desenvolvemento de calquera outra iniciativa considerada na oferta de servizos.
	Asesoramento experto e provisión de servizos	Asistencia técnica e prestación de servizos de detección, prevención e xestión da ciberseguridade en administracións, empresas e outras entidades de interese en Galicia.
	Concienciación e capacitación	Formación para a adquisición do coñecemento necesario e concienciación para o adecuado uso e xestión da ciberseguridade por parte dos cidadáns, empresas e administracións públicas.
	Comunicación e difusión	Xeración de iniciativas e elaboración de contidos formativos e informativos e a súa difusión por canles de comunicación tradicionais e online.

O nodo CIBER.gal agrupará as inquietudes de todos os axentes involucrados no ámbito da ciberseguridade

3.3 Caracterización do nodo

Mapa de axentes

Co obxectivo principal de contribuír ao desenvolvemento do sector e o fomento do traballo coordinado entre todos os axentes do mesmo, o nodo deberá contemplar, na súa configuración final, a participación coordinada de todos os axentes.

De modo ilustrativo agrúpanse a continuación: