

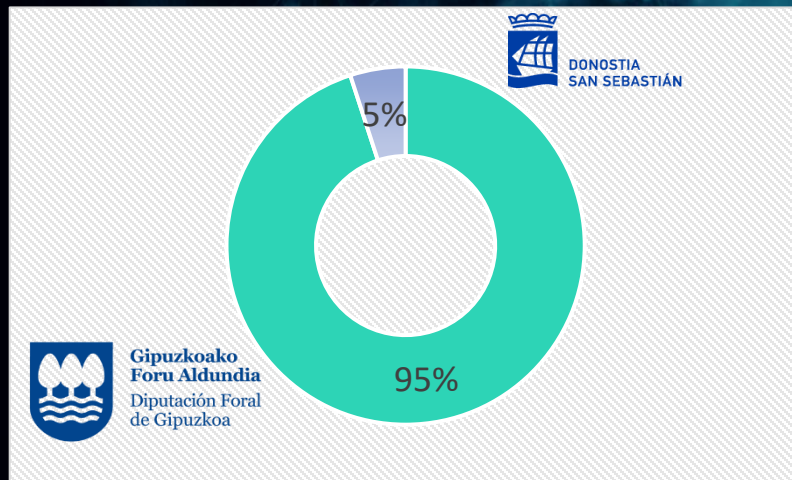
ZIUR

INDUSTRIAL **CYBER SECURITY**
CENTER-GIPUZKOA

ZIUR Fundazioa es el resultado de un proceso de reflexión estratégica y puesta en operación de los siguientes aspectos:

1. Estrategia Etorkizuna Eraikiz
2. Estrategia GFA-DFG en el ámbito de la Ciberseguridad

ZIUR es una Fundación Pública Foral, **cuyo objetivo es reforzar las capacidades de ciberseguridad industrial de las empresas de Gipuzkoa como objeto de competitividad.**



DIFUSION

1

Fomentar el conocimiento en ciberseguridad

FORMACIÓN

2

Capacitar y sensibilizar a las empresas

**INVESTIGACIÓN
Y
EXPERIMENTACIÓN**

3

Vigilancia tecnológica, observatorio de ciberseguridad y laboratorio

PREVENCIÓN

4

Proporcionar herramientas de prevención en ciberseguridad



SITUACION ACTUAL

AMENAZA GLOBAL

1

24% han crecido los ciberincidentes en empresas

2

1 ataque cada 39 segundos

3

22.000 empresas afectadas

4

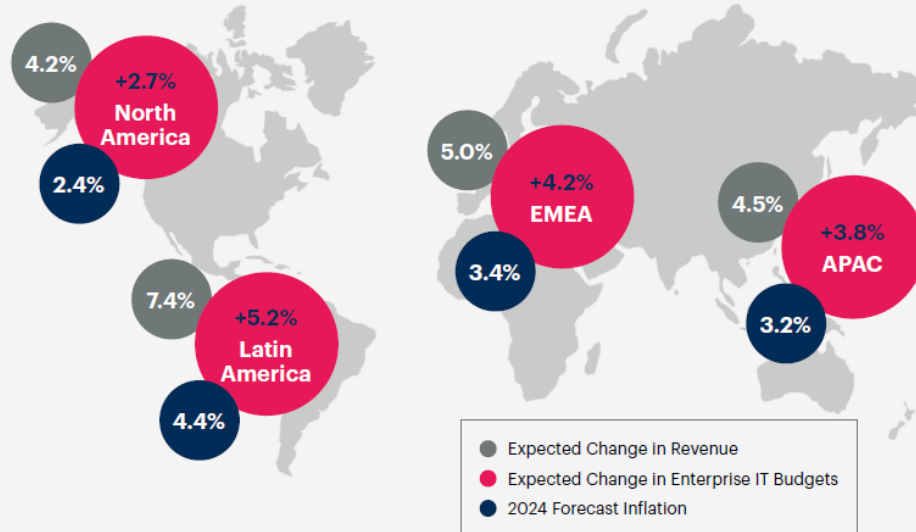
83.517 ciberincidentes

5

GUIPUZCOA 2023 – 6.900 empresas han sufrido ciberincidente

IT Budget Change, Revenue Change Expectations and Inflation

Average Change



n varies by Region: North America (n = 683); Latin America (n = 259); EMEA (n = 797); APAC (n = 412) CIOs and Technology Executives Answering

Q. By what percentage do you expect your enterprise's IT budget to increase or decrease from 2023 to 2024?

Q. By what percentage do you expect your enterprise's revenue to increase or decrease from 2023 to 2024?

Source: 2024 Gartner CIO and Technology Executive Survey

Inflation (CPI) Total Annual Growth Rate (%), August 2023 or Latest Available Organization for Economic Co-operation and Development (OECD)



Operation Cronos What have we learnt?



7,000+ unique 'attack' builds on the panel

At least 2,110 victims began negotiation process to some degree

Numerous examples of decryption keys not working, with no support provided

More than 100 hospitals and healthcare companies and facilities were targeted



Top 10 countries targeted*



Top 10 countries where negotiation started*



Victims 'checked' manually by admin as important*



*Data is poorly structured and many victims still not geolocated to countries - analysis continues

Case study

In one particular case in December 2022, a children's hospital was targeted by the group. After a complaint, LockBit released a statement on their leaks which said "We formally apologise for the attack on ***** and give back the decryptor for free. The partner who attacked this hospital violated our rules, is blocked, and no longer in our affiliate program".

This was a lie. We now know which partner carried out the attack and they remained an active LockBit actor until our operation in February. In fact, we can see they were responsible for 127 unique attack builds, 50 negotiations, and received multiple ransom payments all after apparently being fired by LockBit. The 'free' decryptor provided to the hospital didn't work properly either.



Data relates to June 2022 - Feb 2024

LOCKBIT

COLABORADORES

76,28% construyen ataques

61,3% han negociado con victimas

77,02% han hecho 0€

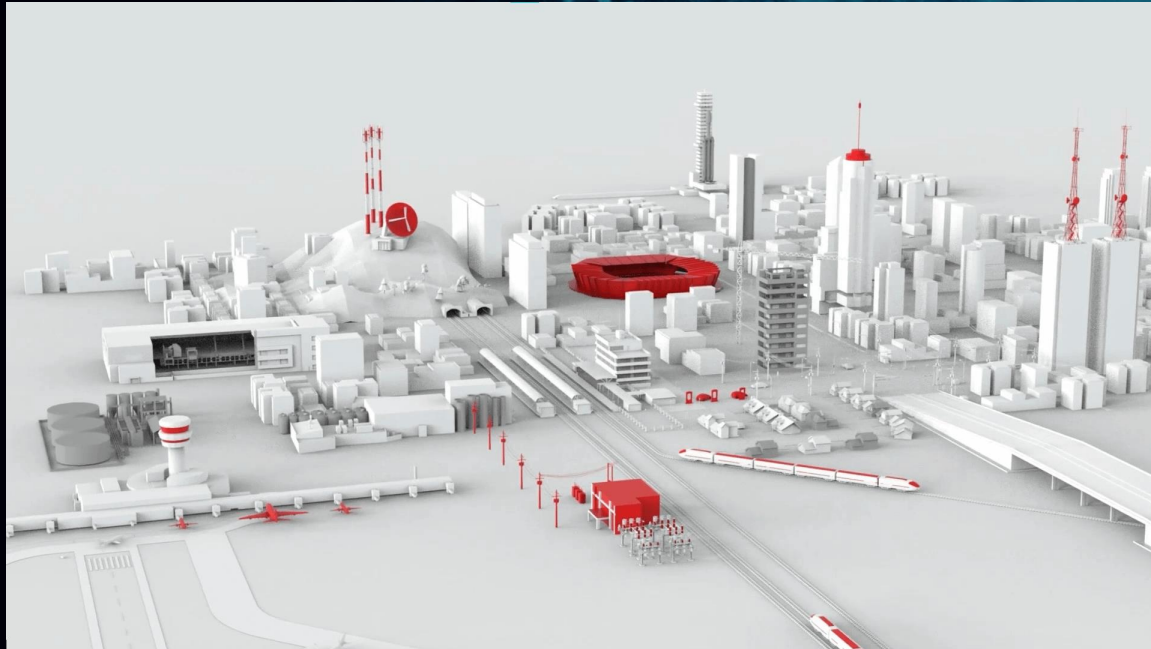


PRINCIPALES RETOS EN CIBERSEGURIDAD

NORMATIVAS

The background of the image is a dark blue gradient. On the right side, there is a complex network of white dots connected by thin white lines, resembling a molecular structure or a data network. The dots are of varying sizes and are scattered across the right half of the image, with some forming distinct geometric shapes like triangles and polygons.

NIS 2



UNECE R155



CRA



MDR



ISO 8102-20:2022



CLC/TS 50701:2021





RESILIENCIA

NORMATIVAS

DEFINICIÓN DE RESILIENCIA

Capacidad de adaptación de un ser vivo frente a un agente perturbador o un estado o situación adversos.

Capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido



CRISIS

Gobierno de una situación compleja decisiva para la supervivencia de una compañía u organización, producida por sorpresa, que afecta al público (interno y externo) y/o al producto y/o al proceso y/o a la distribución y/o a la seguridad y/o a los mercados financieros.

A lo largo de la crisis se acusa una notoria escasez de información y la organización se convierte en centro de atención mediática pudiendo llegar a comprometer su imagen, su credibilidad y/o su producción, y pudiendo interferir en el desarrollo de su actividad, poniendo en duda su viabilidad futura.

La Ciberseguridad es negocio, su materialización puede poner en riesgo la viabilidad de una empresa.

Un incidente debe afrontarse con una visión multidisciplinar y las capacidades necesarias para responder

Deberemos en paralelo contemplar acciones para el futuro, como litigios, lecciones aprendidas, etc.

La respuesta a un incidente se caracteriza por la falta de contexto e información. Estamos en desventaja

Lo que no hayamos preparado y ensayado antes del incidente estará sujeto a decisiones sin contexto y consecuencias desconocidas

La toma de decisiones es esencial, y debe apoyarse en una estrategia clara puesta en el contexto de la crisis

Es posible que la situación nos lleve a tomar decisiones complicadas y dolorosas

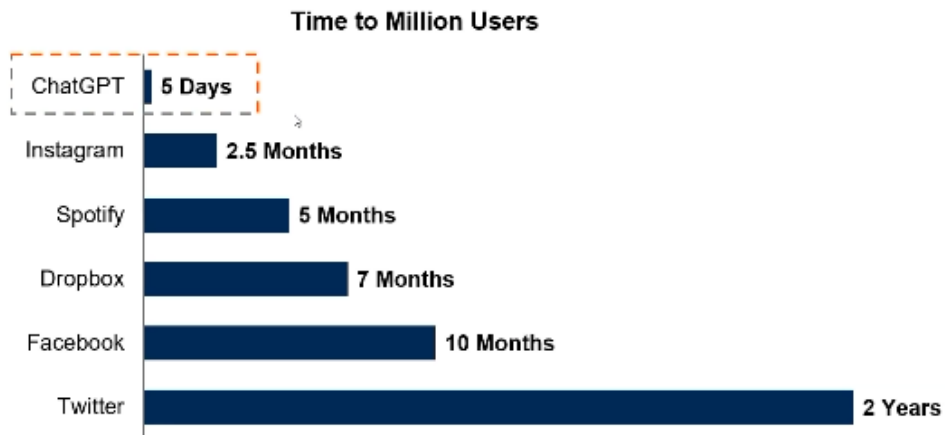


RESILIENCIA

NORMATIVAS

IA

OpenAI ChatGPT's Meteoric Growth



Source: Statista
RESTRICTED DISTRIBUTION
© 2023 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

Hasta 2025, la IA generativa provocará un aumento en los recursos de ciberseguridad necesarios para protegerla, lo que provocará un gasto incremental de más del 15 % en seguridad de aplicaciones y datos.

Top Cybersecurity Trends for 2024

Optimizing for Resilience

- Continuous Threat Exposure Management
- Extending IAM's Cybersecurity Value
- Third-Party Cybersecurity Risk Management
- Privacy-Driven Application and Data Decoupling

Optimizing for Performance

- **Generative AI**
- Security Behavior and Culture Programs
- Cybersecurity Outcome-Driven Metrics
- Evolving Cybersecurity Operating Models
- Cybersecurity Reskilling

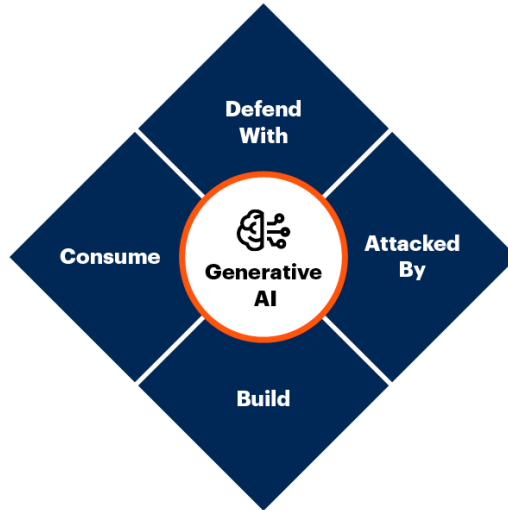
Optimized Cybersecurity Programs

Source: Gartner
802944_C

Key Impacts of Generative AI for CISOs

- Lack of maturity
- Risks due to vendor rush
- Privacy and efficacy challenges

- Multiple consumption options
- Shadow AI
- Data privacy and copyright



- Skill augmentation
- Attack automation
- Content generation

- Data theft/poisoning
- No best practice
- Upcoming regulation

Source: Gartner
793265_C



RESILIENCIA

NORMATIVAS

IA

TALENTO

External Threats That Impacted or Are Impacting Enterprise Growth in 2022-23

Percentage of I&O Leaders



n = 122 I&O Leaders

Q: Which of the following external threats impacted or/Is impacting your enterprise's growth in 2022 and 2023?

Source: 2023 Gartner Cross-Role Navigating Economic Headwinds Survey

802889_C

ZIUR

INDUSTRIAL **CYBER SECURITY**
CENTER-GIPUZKOA



Maria Penilla
mpenilla@ziur.eus



CAMARA DE GIPUZKOA
GIPUZKOAKO BAZKUNDEA