Estrategia de ciberseguridad del SNS

# Hacia una administración digital Resiliente

Gobierno de La Rioja | Sector Público Autonómico

# El Imperativo Estratégico

## La Ciberseguridad como Habilitador Crítico

La ciberseguridad ya no es un asunto técnico: es un elemento fundamental para la prestación de servicios públicos y la confianza ciudadana, en un entorno de alta volatilidad.

## Nuestra Respuesta

Una estrategia coordinada con visión de futuro para construir resiliencia digital ante amenazas emergentes.

# ⚠ COYUNTURA ACTUAL DE RIESGOS

## 1 Tensión geopolítica y económica

- Operaciones en el ciberespacio como herramienta de presión estatal
- Riesgo en cadena de suministro tecnológica (tension comercial EE.UU./UE)
- Disponibilidad comprometida de soluciones críticas

## 2 Hiper-digitalización de Servicios Públicos

- Migración cloud masiva y expansión IoT/OT
- Uso intensivo de IA en administración
- Incremento de la superficie de exposición (activos e identidades)
- Mayor valor de activos (datos sanitarios, económicos)

## 3 Sofisticación de Amenazas

- Profesionalización de cibercrimen : CyberCrime-as-a-Service
- APT dirigidos a infraestructuras críticas
- Ransomware, Phishing, DDoS contra servicios esenciales

## 4 Marco normativo y de protección (Riesgo de cumplimiento)

- NIS2: Marco europeo consolidado de protección para sectores esenciales
- Nuevas regulaciones europeas y estatales en: ciberseguridad, infraestructuras críticas, protección de datos, IA y servicios financieros

# Spain

**1 Cyber ↑**

2 Natural catastrophes ↓

3 Fire ↓

*Cyber is the new top risk. AI (#5), and critical infrastructure blackouts (#8) are the only other risers in this year's top 10 corporate risks.*

## Top 10 risks in Spain

*Source: Allianz Commercial.* Figures represent how often a risk was selected as a percentage of all responses for that country.
Respondents: 102. Figures don't add up to 100% as up to three risks could be selected.

| Rank | | Percent | 2025 rank | Trend |
|---|---|---|---|---|
| 1 | Cyber incidents *(e.g., cyber crime, IT network / service disruptions, malware / ransomware, data breaches, fines, and penalties)* | **48%** | *4 (31%)* | ↗ |
| 2 | Natural catastrophes *(e.g., storm, flood, earthquake, wildfire)* | **31%** | *1 (48%)* | ↘ |
| 3 | Fire, explosion | **27%** | *1 (48%)* | ↘ |
| 4 | Business interruption *(incl. supply chain disruption)* | **25%** | *3 (36%)* | ↘ |
| 5 | Artificial intelligence *(e.g., implementation challenges, liability exposures, misinformation / disinformation)* | **22%** | **NEW** | ↗ |
| 5 | Changes in legislation and regulation *(e.g., tariffs, new directives, sustainability requirements)* | **22%** | *5 (18%)* | → |
| 7 | Climate change *(e.g., physical, operational and financial risks as a result of extreme weather)* | **16%** | *6 (16%)* | ↘ |
| 8 | Critical infrastructure blackouts *(e.g., power disruption)* or failures *(e.g., aging dams, bridges, rail tracks)* | **15%** | **NEW** | ↗ |
| 9 | Political risks and violence *(e.g., war, political instability, terrorism, polarization, coup d'état, civil unrest, strikes, riots, looting)* | **14%** | *8 (11%)* | ↘ |
| 10 | Energy crisis *(e.g., supply shortage / outage, price fluctuations)* | **10%** | *9 (9%)* | ↘ |

Fuente: Allianz Risk Barometer 2026.
(https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/allianz-risk-barometer-2026.pdf)

# Global Risks 2026: A Briefing for Information Security Leaders

## IMMEDIATE THREATS: THE NEXT 2 YEARS

### #1 Risk: Geoeconomic Confrontation

Nations now use cyberattacks on supply chains and critical infrastructure as strategic weapons.

### #2 Risk: Misinformation & Disinformation

AI-driven deepfakes and manipulated content are eroding trust and fueling sophisticated social engineering.

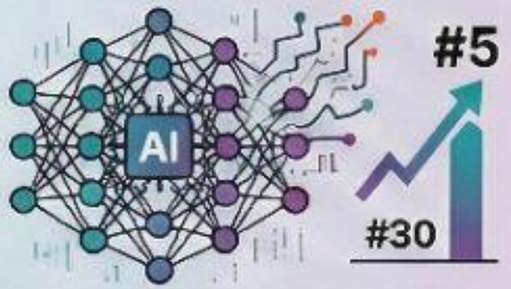

### #6 Risk: Cyber Insecurity

Attacks on businesses and critical infrastructure are growing in frequency and sophistication.

## HORIZON RISKS: THE NEXT 10 YEARS

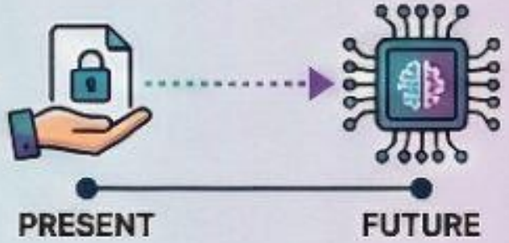
### Fastest-Rising Threat: Adverse Outcomes of AI

This risk skyrockets from #30 in the short-term to #5 in the long-term outlook.




### The Quantum Threat: "Harvest Now, Decrypt Later"

Adversaries are stealing encrypted data today, planning to decrypt it with future quantum computers.





### Only 5% of organizations have implemented quantum-safe encryption.

A significant gap exists between the looming cryptographic threat and enterprise readiness.

# Objetivos Estratégicos de Seguridad (OES)


## Cultura de Ciberseguridad

Fomentar la concienciación y la responsabilidad entre los empleados

## Gobernanza

Establecer políticas y procedimientos claros para la gestión de riesgos

## Protección de Datos

Proteger la información sensible de la organización

## Innovación segura

Innovar y adoptar de manera segura las tecnologías emergentes (IA, Cloud, Automatización...)

## Gestión de Incidentes

Implementar un proceso integral para la respuesta a incidentes

## Resiliencia de Servicios

Garantizar la continuidad de los servicios públicos esenciales

# Alineamiento de los objetivos estratégicos

| | |
|---|---|
| OES1 - Fortalecer gobernanza y modelo organizativo | OB 04: Fomentar cumplimiento<br>OB 05: Establecer indicadores |
| OES2 - Incrementar resiliencia de servicios públicos esenciales | OB 02: Definir medidas para asegurar el dato sanitario<br>OB 07: Garantizar la continuidad asistencial |
| OES3 - Garantizar gestión integral del ciclo de ciberincidentes | OB 01: Establecer red de colaboración (con el fin de mejorar la detección y respuesta) |
| OES4 - Garantizar protección reforzada de información sensible | OB 02: Definir medidas para asegurar el dato sanitario |
| OES5 - Impulsar cultura de ciberseguridad y corresponsabilidad | OB 07: Garantizar la continuidad asistencial (proveedores)<br>OB 08: Promover la capacitación continua |
| OES6 - Fomentar innovación y adopción segura de tecnologías | OB 06: Impulsar la investigación y el análisis de riesgos |
| | OB |

# Fortalezas del plan

Madurez progresiva en la necesidad de cumplimiento.

Estado actual de despliegue de tecnologías de Seguridad en las CC. AA.

Cultura de Innovación Responsable

Coordinación y unidad de acción entre administraciones

Disponibilidad de equipos de Ciberseguridad en las CC.AA.

Nivel de colaboración existente en materia de Ciberseguridad y protección de datos

# Debilidades del plan

# 4.4.11 Búsqueda de líneas financiación

EE 11

## Contexto

La disponibilidad de financiación es crucial para implementar medidas de ciberseguridad efectivas en los Servicios Públicos de Salud. Una búsqueda activa de financiación es esencial para garantizar la sostenibilidad de las iniciativas de ciberseguridad en el sector sanitario.

## Objetivos

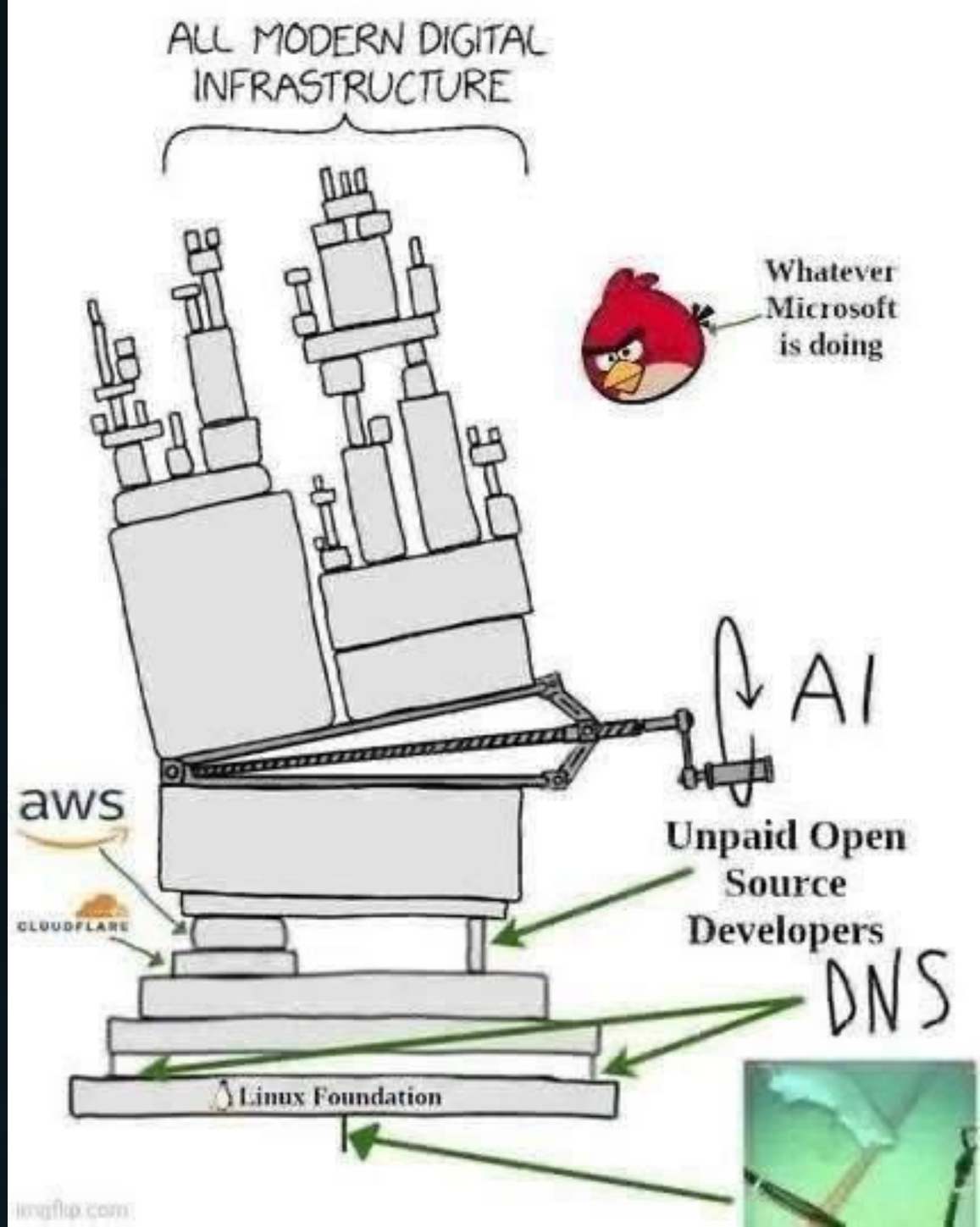
- Establecer un observatorio para monitorizar la disponibilidad de fondos a nivel europeo y nacional.
- Identificar oportunidades de financiación para los Servicios Públicos de Salud.
- Apoyar la implementación de estrategias de ciberseguridad mediante la búsqueda activa de financiación.

PR 11.1

**Establecer un observatorio que monitorice la disponibilidad de fondos tanto a nivel europeo como nacional.**

- Definición del conjunto de fuentes de información y la periodicidad de su monitorización.
- Definición de canales y mecanismos de difusión para la información recogida.

¿Resiliencia?
¿Qué resiliencia?




¿Innovación?
¿Qué innovación?

# Innovación, Tecnologías Emergentes y Cooperación

## Inteligencia Artificial

Evaluación de riesgos, explicabilidad y sesgos en algoritmos avanzados.

## Cloud y Edge Computing

Adopción segura de computación en la nube y procesamiento en el borde.

## Comunicaciones 5G/6G

Tecnologías de comunicaciones críticas de nueva generación.

## Proyectos Piloto

Sandboxes controlados en colaboración con universidades, centros de investigación y empresas del sector.

## Cooperación Institucional

Coordinación con CCN, INCIBE, Ministerio competente, otras CCAA y redes de ciberseguridad sanitaria.

# Soberanía Digital

"La protección de nuestros servicios es la base de nuestra soberanía digital"

> Esta estrategia no es solo un plan de defensa, es un instrumento para anticipar riesgos, gobernar la innovación y preparar a la organización para lo que todavía no ha pasado, pero pasará

> "No gestionamos proveedores, gestionamos dependencias críticas"

La inversión en ciberseguridad es inversión en el futuro

# Gracias