La importancia de la seguridad en la protección de datos en la investigación clínica

Agència de **Ciberseguretat** de Catalunya

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

L'Agència de **Ciberseguretat** de Catalunya

Objectiu

Garantir la ciberseguretat
a tot el territori de **Catalunya**

Els nostres pilars

Desplegar

un servei públic de ciberseguretat executant polítiques públiques.

Impulsar

una cultura de ciberseguretat que permeti assolir una ciutadania digital plena en matèria de ciberseguretat.

Garantir

la ciberseguretat de l'Administració de la Generalitat de Catalunya, del seu sector públic i de la resta d'entitats i institucions públiques.

Potenciar

el sector econòmic de la ciberseguretat com a sector estratègic.

Volumetria d'activitat de l'Agència de Ciberseguretat

A la Generalitat de Catalunya **gestionem un incident de seguretat cada**

2,94h

Generalitat de Catalunya

24 Departaments i organismes rellevants

+2.200 Sistemes d'informació

+220m Usuaris

Àmbits

Salut

Universitats

Administració local

Centres de recerca

Infraestructures crítiques

>4.400M
Atacs detectats durant l'últim any

=2.175
incidents de seguretat anuals gestionats

+24
Programes de seguretat / any

OAT
Entitat certificadora de l'ENS

Internet Segura
Conscienciació i sensibilització de la societat

+70
Més de 70 normes i estàndards

Dades memòria Agència Ciberseguretat de Catalunya 2022

Context **actual**

Salut
Àmbit hospitalari

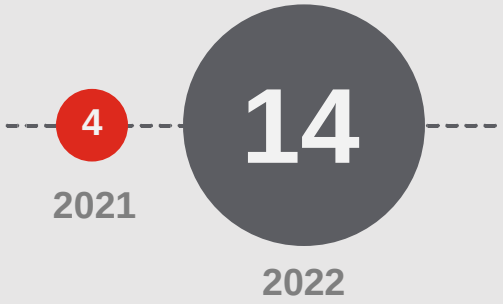
Una enquesta a **649** entitats sanitàries confirma que, l'any 2022, el

53%

van patir atacs de *ramsomware*.

L'Agència de Ciberseguretat de Catalunya ha identificat **3 àmbits** que, pel seu nivell de criticitat i l'increment d'activitat bel·ligerant, requereixen una atenció específica:

El *ransomware* contra hospitals a Espanya s'ha multiplicat per 2,5



Evolució del nombre d'incidents de *ransomware* al sector hospitalari d'Espanya (Double Extortion)

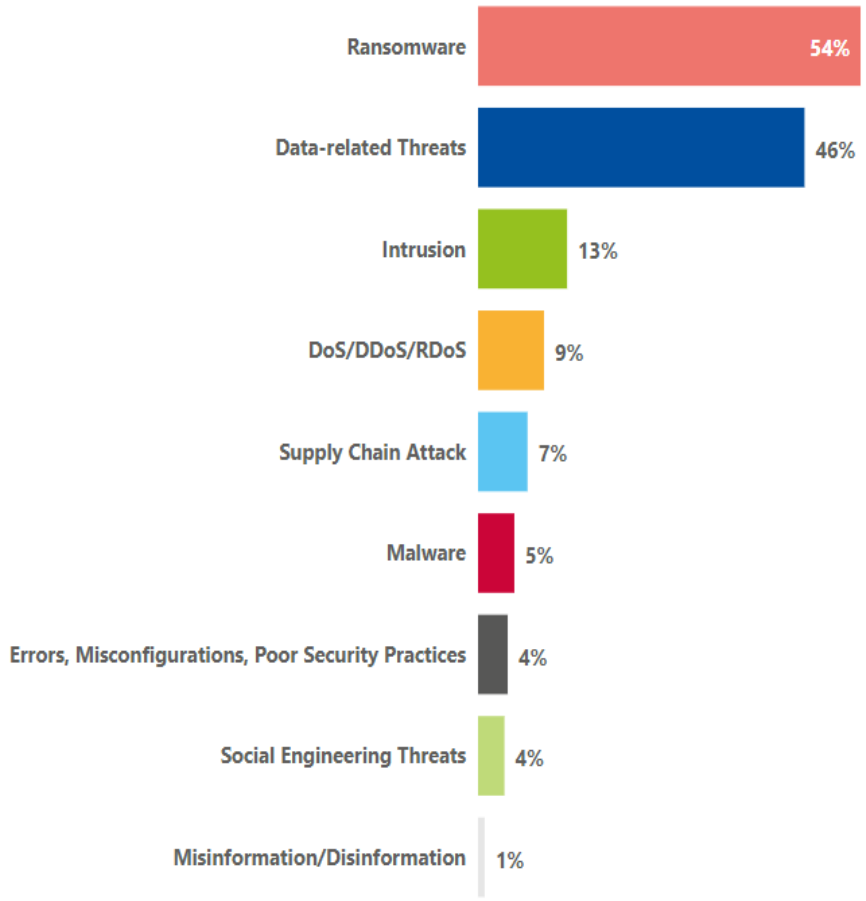
Segons una enquesta a **145** professionals de TI del sector sanitari:

al **86%**

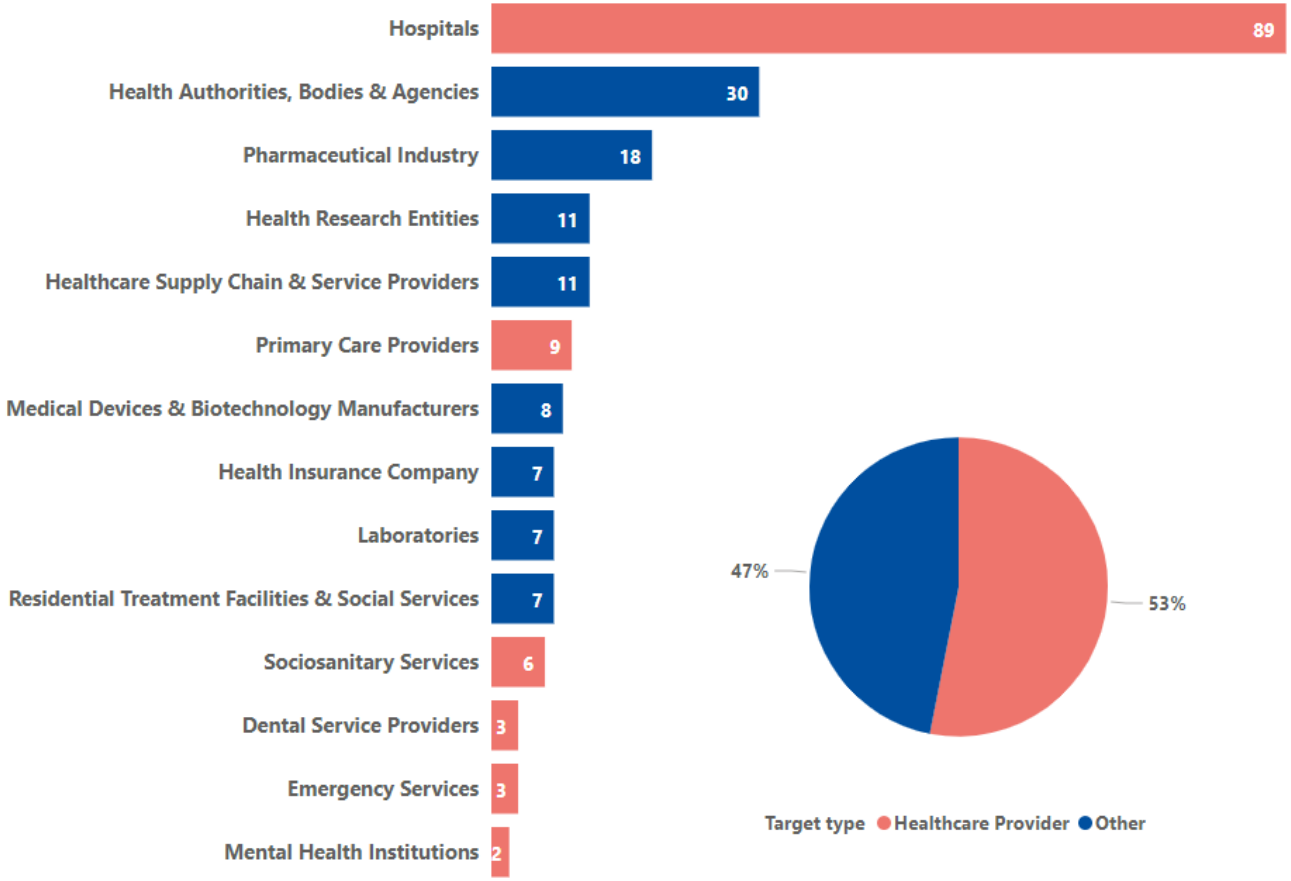
de les organitzacions, el *ransomware* ha provocat l'**aturada de l'activitat operativa**.

Health ENISA Threat Landscape (1/2)

Amenazas en el sector sanitario (2021-2023)

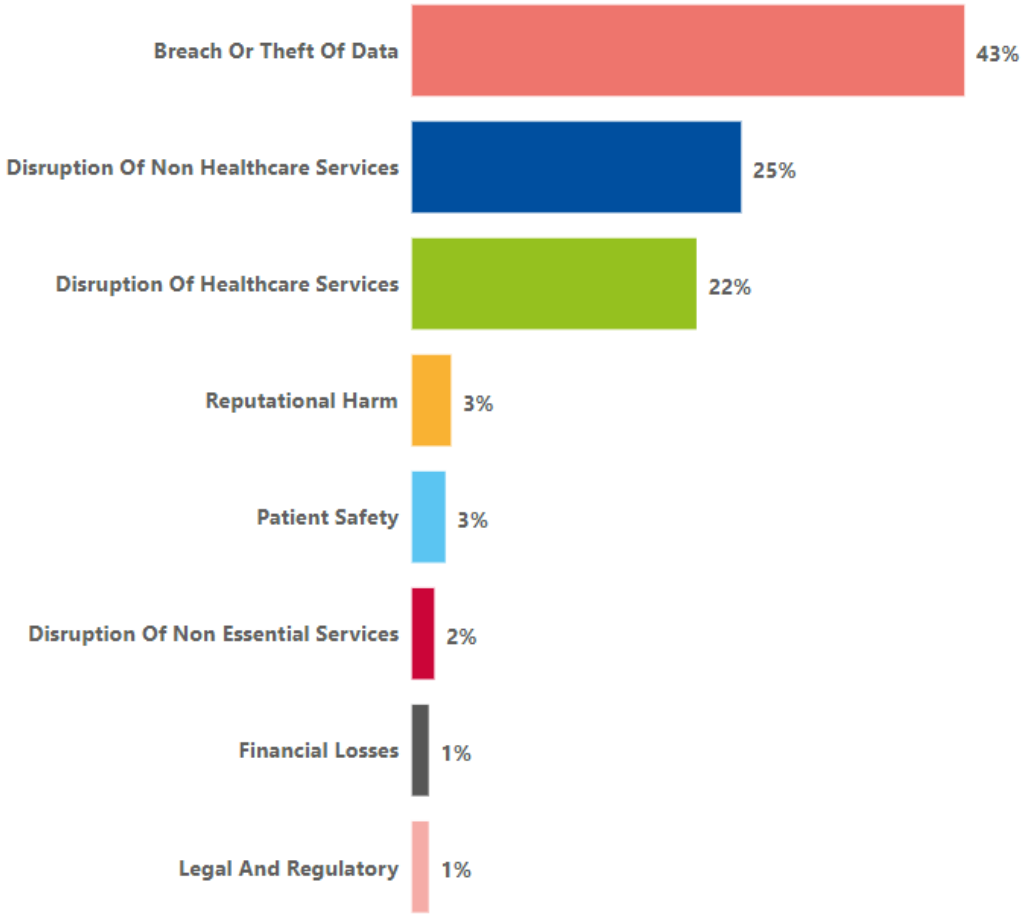


Número de incidentes por tipología de entidad

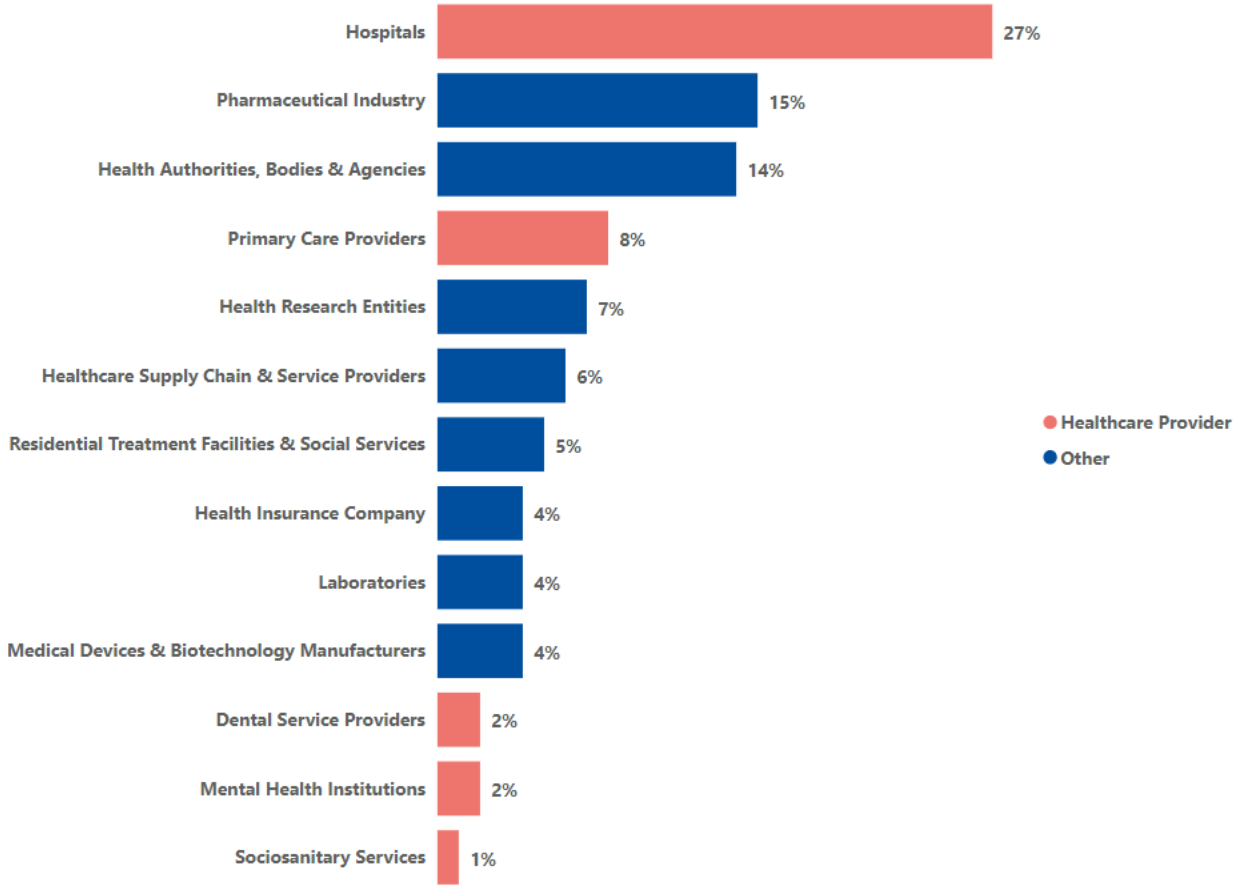


Health ENISA Threat Landscape (2/2)

Consecuencias



Entidades afectadas por robo de datos



Incidentes recientes

German hospital ransomware attack (2020)

[9][10]Nevertheless, the two-month-long investigation concluded the patient was so ill she "likely would have died anyway" [10]; hence the ransomware attack is involved but not to blame despite the delay in provided healthcare.[1]

Swedish DPA: Investigation of 1177-incident finalized

11 June 2021 Sweden

The Swedish Authority for Privacy Protection (IMY) has finalized its investigation of an incident where recorded phone calls to the medical consultation service, 1177, were available unprotected on the Internet.

Further to the contraventions that were established, the IMY has issued an administrative sanction of 12 million SEK (1 193 813 €) towards Medhelp.

Hacked therapy centre's ex-CEO gets 3-month suspended sentence

Publiquen 52 gigues de dades confidencials robades en el ciberatac a 13 centres sanitaris

L'atac informàtic a hospitals i centres d'atenció primària del Barcelonès i el Baix Llobregat va afectar "un volum reduït de dades", segons el Consorci Sanitari Integral

11/10/2022 - 20.23 | Actualitzat 12/10/2022 - 12.05

Health data breach: Dedalus Biologie fined 1.5 million euros

4 May 2022 France

On February 23, 2021, a massive data breach regarding nearly 500,000 people was revealed in the press, involving the company Dedalus Biologie. The name, first name, social security number, name of the prescribing doctor, date of the examination, but also and above all medical information (HIV, cancers, genetic diseases, pregnancies, drug therapy of patients, or genetic data) of these people were thus released on the Internet.

Conti cyber attack on the HSE

Independent Post Incident Review

Commissioned by the HSE Board in conjunction with the CEO and Executive Management Team

03 December 2021

6 març 2023 13:01 *Nota de premsa*

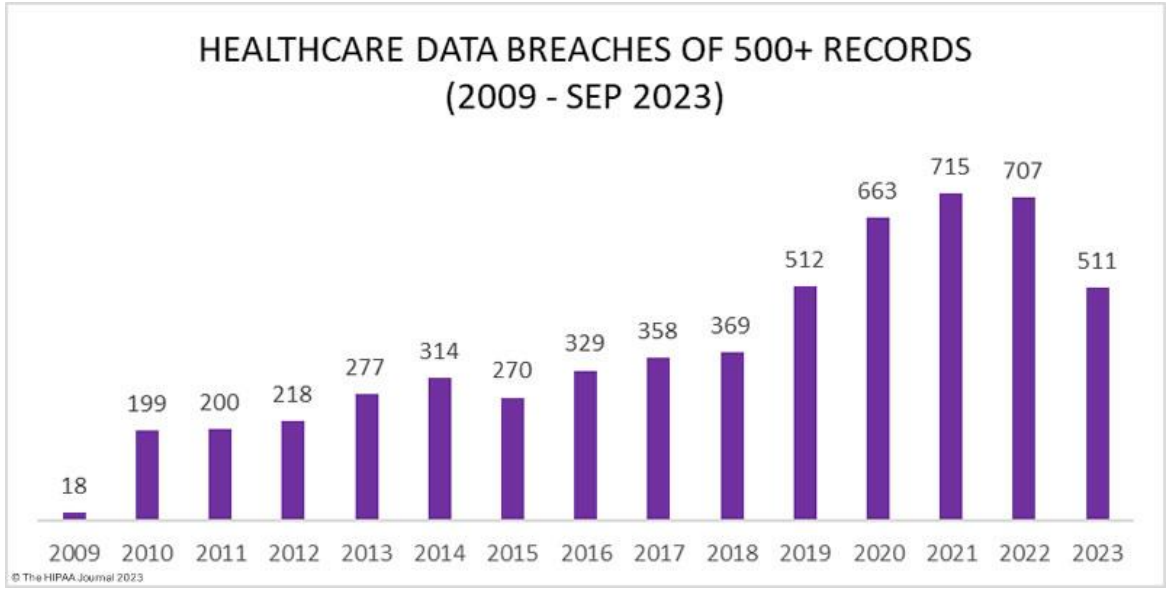
El ciberatac al Clínic afecta la seva activitat assistencial habitual

Segons l'activitat habitual de l'hospital, s'han suspès unes 150 intervencions i entre 2.000 i 3.000 visites a consultes externes. El principal és la seguretat dels pacients i, mentre no tinguem accés a la seva història s'han de demorar aquestes actuacions.

*El **Hospital Centro de Andalucía** ha sido víctima de un incidente de seguridad informática.*

*El equipo de respuesta a ciber incidentes de **AMAVECA SALUD** se encuentra trabajando ininterrumpidamente en la resolución del mismo. A fecha de hoy, se ha podido evidenciar una fuga de datos, cuyo alcance está aún pendiente de concretar.*

Brechas de seguridad



https://www.hipaajournal.com/healthcare-data-breach-statistics/

Entre 2009 y 2022, se han reportado 5,150 vulneraciones de datos de salud que involucran 500 o más registros a la Oficina de Derechos Civiles del HHS. Estas vulneraciones han resultado en la exposición o divulgación no permitida de 382,262,109 registros de atención médica. Esto equivale a más de 1.2 veces la población de los Estados Unidos.

Model de ciberseguretat per a àmbits estratègics

ALINEAMENT I COMPLIMENT DE L'ESQUEMA NACIONAL DE SEGURETAT	▪ Conèixer el nivell de compliment actual respecte el perfil de compliment seleccionat. ▪ Dissenyar i impulsar mesures que permetin garantir el compliment de l'ENS posant atenció a les principals amenaces. ▪ Estructurar i operativitzar un procés de seguiment continu de compliment per a obtenir les acreditacions i certificacions corresponents **Certificació del compliment de l'ENS / Acreditació del perfil de compliment de Salut**
MODEL D'OPERACIÓ DE LA CIBERSEGURETAT	Desplegar **capacitats d'operació de la seguretat amb focus en l'exposició a les principals amenaces,** en **4 fases globals**: ▪ ON SOM? ▪ PLA DE SEGURETAT ▪ POSADA EN SERVEI ▪ PROTECCIÓ
COMUNICACIÓ I COL·LABORACIÓ	▪ Establiment del **model de relació** específic amb l'àmbit. ▪ **Seguiment del desplegament.** ▪ Identificació de **noves necessitats** (millora del model).

Generalitat de Catalunya

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Modelo integral de ciberseguridad para el sector sanitario

01. DÓNDE ESTAMOS (DIAGNÓSTICO)

Identificación del grado actual de protección del ámbito respecto a las principales amenazas aplicables:

- **Análisis externo de debilidades y riesgos** (pentest)
- **Consultoría interna** (arquitectura, ENS, backup, segmentación de red, obsolescencia...)

02. PLAN DE SEGURIDAD (TRATAMIENTO)

Determinación del **plan de seguridad para cada entidad** con el objetivo de ser más **resiliente ante las amenazas:**

- **Plan de Seguridad:** Conjunto de proyectos para reducir las debilidades(1)

(1) Despliegue de soluciones y proyectos no incluidos.

03. PUESTA EN SERVICIO (REHABILITACIÓN)

Despliegue de los procesos y servicios asociados a la integración con la ACC:

- **Integración con el SOC – Salut**
- Definición del **modelo de relación**
- Despliegue del **protocolo de respuesta ante incidentes**

04. PROTECCIÓN

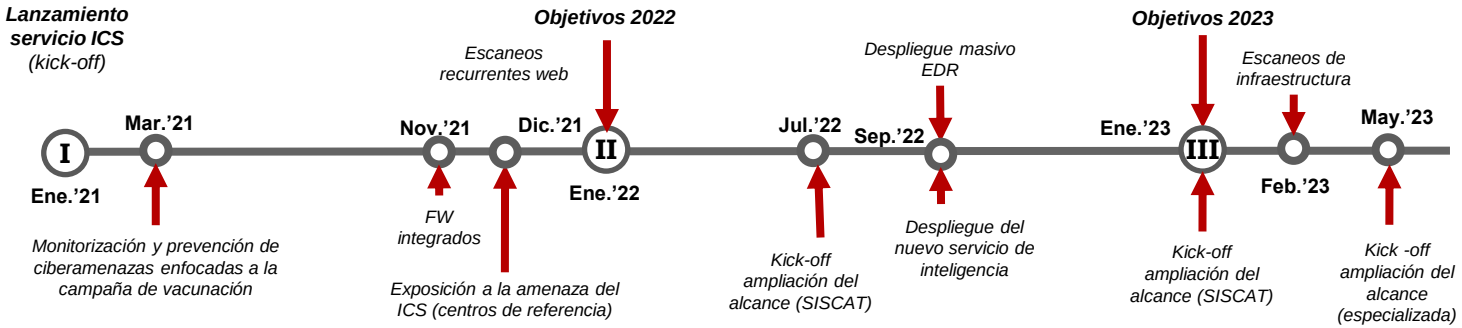
Despliegue del modelo integral de ciberseguridad para el ámbito:

- **SOC – Salut (Monitorización y Respuesta 24x7)**
- **Programa de Formación y Capacitación**
- **Oficina de Cumplimiento del ENS**
- **Servicio de Gobierno y Comunicación**
- **Oficina de Evolución en Ciberseguridad**
- **Capacidades de Recuperación *(Cyber Recovery Backup)***

Generalitat de Catalunya

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Estrategia y cronología del modelo de protección en el sector sanitario



Una estrategia adaptada a los diferentes ámbitos asistenciales

Ante esta situación, el gobierno catalán ve necesario **preparar al sector público de Salud** para poder **hacer frente a los incidentes de seguridad** que puedan impactar en el servicio al ciudadano. Con este fin, el Departamento de Salud y la Agència de Ciberseguretat de Catalunya trabajan conjuntamente en el diseño y despliegue de un **modelo de ciberseguridad común para todo el ámbito sanitario**, teniendo en cuenta el **elevado grado de interconexión entre todas las modalidades asistenciales**, así como la complejidad y heterogeneidad asociadas del ecosistema:

1. **Modelo sistémico**: el alcance del modelo de protección y resiliencia ante incidentes de ciberseguridad abarca la atención primaria, atención especializada y atención intermedia y salut mental.

2. **Atención especializada primero**: se ha iniciado el despliegue del modelo en los hospitales del Sistema de Salut de Catalunya (SISCAT) por su grado de exposición a las principales amenazas y volumetrías asistenciales y de tecnologías médicas involucradas.

3. **Modelo con actualizaciones recurrentes**: en paralelo al despliegue del modelo en hospitales, se actualiza el modelo existente en la atención primaria y se inicia el despliegue progresivo en atención intermedia y salud mental.

Generalitat de Catalunya

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Muchas gracias

Albert Haro
aharo@ciberseguretat.cat

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya