

# XXIII

# REUNIÓN DEL FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS DE SALUD

"Salud inteligente: Datos seguros y retos en la era de la Inteligencia Artificial"

## BILBAO

## 25 y 26 de febrero 2026

Hotel Ercilla  
c/Ercilla 37-39

### Organiza

SOCIEDAD ESPAÑOLA DE



INFORMÁTICA DE LA SALUD

Colaboración Institucional



Síguenos en twitter:  
#SEISforoPD  
@SEISsalud



seisesalud



Osakidetza



EUSKO JAURLARITZA  
GOBIERNO VASCO

OSASUN SAILA  
DEPARTAMENTO DE SALUD

SOCIO TECNOLÓGICO PRINCIPAL

SOCIO TECNOLÓGICO COLABORADOR



DEXCOM



# INTRODUCCIÓN

La Sociedad Española de Informática de la Salud (SEIS) estableció el Foro de Seguridad y Protección de Datos de Salud para generar un lugar de encuentro para todos los profesionales del sector sanitario (médicos, personal de enfermería, farmacéuticos, investigadores, estudiantes y profesionales de las Tecnologías de la Información y la Comunicación (TIC), gestores, directivos, etc.), las autoridades en materia de protección de datos y seguridad de la información, así como los principales líderes del sector tecnológico al objeto de compartir experiencias y conocimiento en aras de promover una utilización segura de las TIC que contribuya a una atención sanitaria de calidad, eficiente y especialmente respetuosa con los derechos de los ciudadanos.

La herramienta más importante con la que cuenta el Foro de Seguridad y Protección de Datos de Salud para cumplir este objetivo es su reunión anual, que en 2026 alcanzará ya su XXIII edición y que se celebrará los días 25 y 26 de febrero en Bilbao.

El Foro es, pues, una iniciativa madura y plenamente consolidada que se ha convertido en una cita anual ineludible para todas aquellas personas y organizaciones públicas y privadas del sector sanitario en cuyas manos descansa la preservación de la privacidad de los pacientes como un elemento de calidad en las prestaciones asistenciales y en las labores de investigación y gestión.

Bajo el lema “Salud inteligente: Datos seguros y retos en la era de la Inteligencia Artificial”, el Foro girará sobre los aspectos más relevantes incluyen la protección de información sensible de pacientes en sistemas de IA, los desafíos éticos y legales del uso de algoritmos predictivos en diagnósticos, la interoperabilidad segura entre plataformas sanitarias digitales, el equilibrio entre innovación tecnológica y privacidad del paciente, y los marcos regulatorios necesarios para garantizar el uso responsable de la IA en medicina personalizada, telemedicina y análisis masivo de datos clínicos.

La inauguración oficial del Foro, será llevada a cabo por el Consejero de Salud del País Vasco, el Presidente la SEIS y el Coordinador del programa de la XXIII edición del Foro de Seguridad y Protección de Datos de Salud.

Tras la sesión inaugural, la primera sesión del Foro estará dedicada a las autoridades de protección de datos motivo por el cual se contará con la representación de las autoridades de la Agencia Española de Protección de Datos, de la Agencia Vasca de Protección de Datos, de la Autoridad Catalana de Protección de Datos y del Consejo de Transparencia y Protección de Datos de Andalucía.

Así, una vez más, las autoridades de protección de datos muestran su apoyo a esta iniciativa de la SEIS que desde aquí queremos agradecer pues resulta fundamental para la consecución de los objetivos del Foro de Seguridad y Protección de Datos de Salud.

A continuación de la sesión de las Autoridades de Protección de Datos el Ministerio de Sanidad realizará la presentación de la Estrategia CiberSeguridad Sistema Nacional de Salud.

Dando continuidad a las conferencias, se llevará a cabo la segunda sesión del Foro, la cual tendrá formato de mesa redonda, y estará dedicada a la presentación de soluciones para la cada vez más compleja gestión de la ciberseguridad en entornos sanitarios. Se tratarán los aspectos clave como la defensa contra ransomware y ataques dirigidos a sistemas hospitalarios críticos, la implementación de arquitecturas de seguridad Zero Trust, la protección de dispositivos IoT médicos conectados, la formación del personal sanitario, etc.

La tarde de la jornada del miércoles comenzará con la tercera sesión del Foro que tendrá como tema principal el referente a los “Seguridad y trazabilidad de los datos sanitarios”, donde se tratará la implementación de registros de auditoría inmutables, el control de accesos basado en roles y privilegios mínimos, la trazabilidad completa, los sistemas de gestión documental seguros para historias clínicas electrónicas, la interoperabilidad entre sistemas manteniendo cadenas de custodia, el cumplimiento del derecho de los pacientes a conocer quién accede a sus datos, y las herramientas forenses para investigar brechas de seguridad.

A la misma hora se inicia la Sesión Técnica 1 también este año, incorporando una visión práctica de los retos tecnológicos que afectan a la Seguridad de la Información y las herramientas disponibles para abordarlos.

A continuación se llevará a cabo la cuarta sesión bajo el lema “Transparencia algorítmica en datos de salud”, donde se hablará sobre el desarrollo de IA explicable (XAI) en aplicaciones médicas, el derecho de pacientes y profesionales a comprender las decisiones automatizadas, la detección y mitigación de sesgos algorítmicos que puedan discriminar a ciertos grupos poblacionales, la documentación técnica accesible sobre el funcionamiento de modelos predictivos en salud, la validación clínica y ética de algoritmos antes de su implementación, los mecanismos de supervisión humana en decisiones críticas.

También tendrá lugar en paralelo la Sesión Técnica 2 donde se continúa la revisión tecnológica de soluciones a implementar en los diferentes sistemas de información y organizaciones sanitarias.

Como cierre de la jornada del miércoles, se llevará a cabo la quinta sesión bajo el lema “Gestión de riesgos de ciberseguridad en dispositivos médicos: Una misión compartida”, donde se recogen aspectos como la colaboración entre fabricantes, proveedores sanitarios y autoridades reguladoras, la gestión del ciclo de vida completo de dispositivos, la aplicación de estándares, los procesos de gestión de vulnerabilidades y parches de seguridad sin interrumpir servicios críticos, la segmentación de redes para aislar dispositivos médicos, las evaluaciones de riesgo continuas considerando tanto amenazas cibernéticas como impacto clínico, y los protocolos de respuesta ante incidentes que involucren equipos de soporte vital o diagnóstico.

Como en anteriores ediciones, la segunda jornada del Foro comenzará con la sexta sesión “Casos prácticos: la experiencia de las autoridades de protección de datos” mediante la cual las autoridades de protección de datos presentarán las consultas, los casos reales y las experiencias más interesantes relativas a la protección de datos de salud en las cuales han trabajado durante el año 2025. Los aspectos a tratar incluyen sanciones por brechas de seguridad o tratamientos ilícitos de datos de salud, buenas prácticas identificadas en auditorías a instituciones sanitarias, casos de violaciones de derechos de pacientes, lecciones aprendidas de incidentes notificados, criterios interpretativos del RGPD, etc.

En la séptima sesión del Foro, que tendrá formato de mesa redonda, se presentarán las soluciones y propuestas más novedosas para securizar los entornos sanitarios desde la perspectiva de los tratamientos de datos de salud durante su recopilación, almacenamiento, procesamiento y transferencia, minimizando riesgos de exposición

La octava, y última sesión del Foro, vendrá a dar continuidad al tema principal del Foro como es la “Anonimización y pseudoanonimización en la Inteligencia Artificial”, se revisarán aspectos como la anonimización irreversible mediante agregación o ruido diferencial para datasets grandes, versus la pseudonimización reversible con claves para fines como investigaciones médicas; los desafíos en mantener la utilidad de los datos mientras se cumple con regulaciones como el RGPD, que distingue entre ambas; el uso de herramientas como k-anonymity o federated learning para mitigar redentificación; y las implicaciones éticas en IA, donde un mal manejo podría llevar a discriminación o fugas, enfatizando la necesidad de auditorías para equilibrar innovación y protección de derechos.

La clausura del Foro servirá para poner en común los principales temas y conclusiones del Foro y será llevada a cabo por el Secretario General de Salud Digital del Ministerio de Sanidad, el Gerente del Servicio Vasco de Salud y el Coordinador General de la XXIII edición del Foro de Seguridad y Protección de Datos de Salud.

Asimismo, cabe resaltar que de manera previa a la celebración del Foro tendrán lugar dos sesiones de trabajo del Comité Técnico de Seguridad de la Información Sanitaria (CTSIS) el cual se puso en marcha en el año 2013 a iniciativa de la SEIS. El CTSIS está compuesto por los responsables de seguridad y delegados de protección de datos de todos los servicios de salud autonómicos y tiene como principales objetivos, entre otros, los de compartir experiencias, inquietudes y soluciones así como el de homogenizar criterios en materia de seguridad y protección de datos en el sector sanitario.

La SEIS está convencida de que el programa de la XXIII edición del Foro de Seguridad y Protección de Datos de Salud ofrece suficientes atractivos para que resulte de interés a todos los profesionales, gestores y técnicos que desempeñan su labor en el sector sanitario por lo que les invita a reunirse en Bilbao los próximos días 24 y 25 de febrero del 2026 con el fin de participar en el mismo para actualizarse en sus conocimientos, conocer nuevas experiencias y enriquecer con su participación las sesiones y debates que se producirán.

## COMITÉ ORGANIZADOR

### Presidente

Luciano Sáez Ayerra

### Coordinador General

Miguel Ángel Benito Tovar

### Miembros

Juan Díaz García  
Carlos García Codina  
Francisco Martínez del Cerro  
José Quintela Seoane

## COMITÉ LOCAL

### Miembros

Benjamín Juez Fernández  
Carmen Recalde Langarica

## COMITÉ DE PROGRAMA

### Coordinador

Juan Díaz García

### Miembros

Blanca Álvarez Yaque  
Miguel Ángel Benito Tovar  
Carlos García Codina  
Francisco Martínez del Cerro  
Joaquín Pérez Catalán  
Francesc Xavier Urios Aparisi  
Juana M<sup>a</sup> Vegas Fernández

## Programa Preliminar

## Programa Preliminar Miércoles, 25 de febrero

- 09.00 - 10.00 Inscripción y recogida de documentación
- 10.00 - 10.30 Inauguración Oficial
- 10.30 - 11.30 **Primera Sesión**  
Mesa Autoridades Protección de Datos
- 11.30 - 12.00 Pausa - Café
- 12.00 - 12.30 **Presentación Estrategia Ciberseguridad en el Sistema Nacional de Salud**
- 12.30 - 14.00 **Segunda Sesión**  
Soluciones para la ciberseguridad en entornos sanitarios
- 14.00 - 15.30 Tiempo de comida
- 15.30 - 17.15 **Sesión Técnica 1 - Sala B**
- 16.00 - 17.15 **Tercera Sesión Debate - Sala A**  
Seguridad y trazabilidad de los datos sanitarios
- 17.15 - 17.30 **Networking**
- 17.15 - 18.30 **Sesión Técnica 2 - Sala B**
- 17.30 - 18.30 **Cuarta Sesión Debate - Sala A**  
Transparencia algorítmica en datos de salud
- 18.30 - 18.45 **Networking**
- 18.45 - 19.45 **Quinta Sesión Debate - Sala A**  
Gestión de riegos de ciberseguridad en dispositivos médicos: Una misión compartida
- 21.30 - 23.30 **Cena - Cocktail - Guggenheim**

## Jueves, 26 de febrero

### Programa Preliminar

- 09.30 - 11.00 **Sexta Sesión Debate**  
Casos prácticos: la experiencia de las autoridades de protección de datos
- 11.00 - 11.30 Pausa - Café
- 11.30 - 12.45 **Séptima Sesión**  
Soluciones de seguridad ante el tratamiento de datos de salud
- 12.45 - 13.00 **Networking**
- 13.00 - 14.00 **Octava Sesión Debate**  
Anonimización y pseudoanonimización en la Inteligencia Artificial
- 14.00 - 14.30 **Acto de Clausura**

### Programa Preliminar

## Miércoles, 25 de febrero

### Programa Preliminar

09.00 - 10.00 Inscripción y recogida de documentación

10.00 - 10.30 Inauguración Oficial

**Intervienen** **Don Alberto Martínez Ruiz**  
Consejero de Salud del Gobierno Vasco

**Don Juan Fernando Muñoz Montalvo**  
Secretario General de Salud Digital, Información e  
Innovación en el Sistema Nacional de Salud del  
Ministerio de Sanidad

**Don Lorenzo Cotino Hueso**  
Presidente de la Agencia Española de Protección de  
Datos

**Don Luciano Sáez Ayerra**  
Presidente de la Sociedad Española de Informática  
de la Salud

**Don Juan Díaz García**  
Coordinador de Programa  
XXIII Foro de Seguridad y Protección de Datos de Salud

## Miércoles, 25 de febrero

10.30 - 11.30 **Primera Sesión**  
Mesa Autoridades Protección de Datos

**Modera** **Don Javier Ureña Morales**  
Director General del Servei de Salut de les Illes Balears

**Ponentes** **Don Lorenzo Cotino Hueso**  
Presidente de la Agencia Española de Protección de  
Datos

**Doña Meritxell Borràs i Solé**  
Directora. Autoridad Catalana de Protección de Datos

**Don Unai Aberasturi Gorriño**  
Presidente. Autoridad Vasca de Protección de Datos

**Don Jesús Jiménez López**  
Director. Consejo de Transparencia y Protección de  
Datos de Andalucía

11.30 - 12.00 **Pausa Café**

### Programa Preliminar



## Miércoles, 25 de febrero

### Programa Preliminar

12.00 - 12.30 **Presentación Estrategia CiberSeguridad Sistema Nacional de Salud**

**Presenta** **Agencia Vasca de Ciberseguridad**

**Imparte** **Doña Noemí Cívicos Villa**  
Directora General de Salud Digital y Sistemas de Información en el SNS del Ministerio de Sanidad

### Programa Preliminar

## Miércoles, 25 de febrero

12.30 - 14.00 **Segunda Sesión**  
Soluciones para la ciberseguridad en entornos sanitarios

**Modera** **Don Benjamin Juez Fernández**  
Subdirector de Informática y Sistemas de Información de OSAKIDETZA - Servicio Vasco de Salud.

**Ponentes** “Firewall for AI: Cómo cerrar las brechas de seguridad que introduce la IA generativa”  
**Don Chistian Scotti**  
Senior Solutions. Akamai

“Fugas de datos, sin mala intención”  
**Don José Luis Suárez Fueyo**  
Ingeniero de Ventas. Proofpoint

“SOC para entornos críticos: del inventario a la gestión del riesgo mediante automatización e inteligencia artificial”  
**Don Ivan Pérez Muñoz**  
Healthcare Cybersecurity Anlyst. Telefónica Tech

“La ciberseguridad no es un coste”  
**Don Jose de la Cruz**  
Director Técnico. TrendIA

Plexus

**Don Carlos Piñera Sánchez**  
SASE & Security Sales & Business Manager HPE

“SOC especializado en Sector Salud integrado con el Cumplimiento y Mejora de la Seguridad”

**Don Xavier Isern Martín**  
Consultor Especialista en Ciberseguridad de Nunsys Group

14.00 - 15.30 **Tiempo de comida**

## Miércoles, 25 de febrero

### Programa Preliminar

15.30 - 17.15 Sesión Técnica 1 - **Sala B**

**Moderador** **Don Benigno Rosón Calvo**  
Subdirector General de Sistemas y Tecnologías de la Información en el Servicio Gallego de Salud

**Ponentes** **KPMG**

**Doña Laura López Granero**  
Head of OT Cybersecurity. Fujitsu

**Don Javier Alonso**  
Palo Alto

Emulación y protección de entorno DICOM en gemelo digital sanitario

**Don Thomas Dupont**  
Ingeniero prevención. Stormshield

**Watchguard**

## Miércoles, 25 de febrero

16.00 - 17.15 **Tercera Sesión Debate - Sala A**  
Seguridad y trazabilidad de los datos sanitarios

**Moderador** **Don Francesc Xavier Urios Aparisi**  
Jefe de la Asesoría Jurídica de la Autoridad Catalana de Protección de Datos

**Ponentes** **Doña Matilde Vera Rodríguez**  
Subdirectora de la Asesoría Jurídica del Servicio Andaluz de Salud

**Don Ángel Blanco Rubio**  
Director Corporativo de Organización, Procesos, TI y Digital de Quironsalud

**Doña Ana Delgado Roy**  
Jefa de Área de Oficina del Dato del Sistema Nacional de Salud. Área de Historia Clínica Digital del SNS

**Don Jordi de la Osa**  
Director de Estrategia y Desarrollo de Negocio .IQVIA

17.15 - 17.30 **Networking**

### Programa Preliminar

## Miércoles, 25 de febrero

### Programa Preliminar 17.15 - 18.30 Sesión Técnica 2 - Sala B

**Modera** **Doña Rocío Montalbán Carrasco**  
Subdirectora General de Transformación Digital de la  
Consejería de Salud de Cantabria

**Ponentes** **Don Raul García Pérez**  
Director Técnico. Xmcyper

“Desarrollos IA para mejorar la operación y seguridad  
de los Network Packet Brokers”

**Don Ferrán Orsola**  
Consulting Sales Engineer. Gigamon

“NDR para entornos hospitalarios: detección temprana  
de amenazas en redes clínicas. Despliegue práctico en  
Ibsalut”

**Don Borja de la Maza**  
CEO. Redborder

Yubico/ingecom

## Miércoles, 25 de febrero

17.30 - 18.30 **Cuarta Sesión Debate - Sala A**  
Transparencia algorítmica en datos de salud

**Modera** **Don Manuel González Seco**  
Jefe de Gabinete de Cumplimiento. Consejo de  
Transparencia y Protección de Datos de Andalucía

**Ponentes** **Don Joaquín Cañada González**  
Delegado de Protección de Datos de la Generalitat  
Valenciana

**Don Antonio Martínez Millana**  
Profesor titular en Universitat Politècnica de  
Valencia (DEXCOM)

**Don Gary Robertson**  
Miembro del Comité Operativo del GIA de ISMS FORUM

18.30 - 18.45 **Networking**

Programa Preliminar



## Miércoles, 25 de febrero

### Programa Preliminar

18.45 - 19.45 **Quinta Sesión Debate**  
Gestión de riesgos de ciberseguridad en dispositivos médicos: Una misión compartida

#### Modera

Ponentes **Don Manuel Jimber del Río**  
Responsable de la Unidad de Seguridad TIC del Servicio Andaluz de Salud

**Don Javier Zapata Victori**  
CISO del Grupo Quirónsalud

**Don Manuel del CCN**

**Don Rubén Ortega Güell**  
Manager de ciberseguridad 360° - Healthcare sector  
IndraMind

**Don Juan Díez González**  
Responsable de Ciberseguridad para sector Salud  
INCIBE-CERT

21.30 - 23.30 **Cena - Cocktail - Guggenheim**

## Jueves, 26 de febrero

09.30 - 11.00 **Sexta Sesión Debate**  
Casos prácticos: la experiencia de las autoridades de protección de datos

#### Modera

**Don Pedro Alberto González González**  
Anterior Secretario General y DPD de la Autoridad Vasca de Protección de Datos

Ponentes **Doña María Esperanza Zambrano Gómez**  
Subdirección de Inspección de la Agencia Española de Protección de Datos

**Don Emilio Sánchez García**  
Responsable del Gabinete de Investigación y Correctivo del Consejo de Transparencia y Protección de Datos de Andalucía

**Doña Fina Valls Vila**  
Jefa de Área de Inspección de la Autoridad Catalana de Protección de Datos

**Doña Juana Vegas Fernández**  
Letrada Instructora de la Asesoría Jurídica de la Autoridad Vasca de Protección de Datos

11.00 - 11.30 **Pausa Café**

### Programa Preliminar

## Jueves, 26 de febrero

### Programa Preliminar

11.30 - 12.45 **Séptima Sesión**  
Soluciones de seguridad ante el tratamiento de datos de salud

#### Modera

Ponentes “Acceso Zero Trust para reducir el Riesgo en el Tratamiento de Datos de Salud”

**Don Darragh Kelly**  
Product Marketing Manager  
Cipherbit - Grupo Oesia

“Gestión de proveedores en la infraestructura hospitalaria”

**Don Agustín Valencia**  
OT Security BDM.Fortinet

**Don José Ramón Fernández Alarcón**  
Country Manager.Tenable

S2

Cyberark

**Don Álvaro Fraile Hernández**  
Global Cybersecurity Services Director  
Ayesa

Checkpoint

12.45 - 13.00 **Networking**

## Jueves, 26 de febrero

13.00 - 14.00 **Octava Sesión Debate**  
Anonimización y pseudoanonimización en la Inteligencia Artificial **Programa Preliminar**

#### Modera

**Don Joaquín Pérez Catalán**  
Vocal Asesor de la Agencia Española de Protección de Datos

Ponentes Sergas

**Don Álvaro Alonso Zorita**  
Vocal Asesor del Gabinete Técnico en la Dirección de Salud Digital y Sistemas de Información para el SNS

**Don Ricardo Iglesias Rodríguez**  
Delegado de Protección de Datos del Servicio Madrileño de Salud

**Don David de Falguera Llobet**  
Socio. EY ABOGADOS, SLP

### Programa Preliminar

Jueves, 26 de febrero

## Programa Preliminar

14.00 - 14.30 Acto de Clausura

### Intervienen

**Doña Miren Lorea Bilbao Artetxe**

Directora General de OSAKIDETZA - Servicio Vasco de Salud

**Doña Noemí Cívicos Villa**

Directora General de Salud Digital y Sistemas de Información en el SNS del Ministerio de Sanidad

**Don Miguel Ángel Benito Tovar**

Coordinador General del XXIII Foro de Seguridad y Protección de Datos de Salud

## Programa Preliminar

Con la colaboración de:



## Programa

## Programa Preliminar

Xmcyber  
Proofpoint  
Trendmicro  
Cipherbit  
Cyberak  
Akamai  
watchguard Technologies  
IQVIA  
Dexcom  
Fortinet  
Fujitsu  
Gigamon  
Ayesa  
KPMG  
Nunsys  
Palo Alto  
Plexus  
S2 Grupo  
Minsait  
Stormshield  
Telefonica  
Tenable  
HPE  
EY  
Checkpoint  
Redborder  
Ingecom

## Programa Preliminar