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

Osakidetza

EUSKO JAURLARITZA GOBIERNO VASCO
OSASUN SAILA
DEPARTAMENTO DE SALUD

Siguenos en twitter:
#SEISforoPD
@SEISeSalud

seisesalud

SOCIO TECNOLÓGICO PRINCIPAL

Abbott · Dedalus · dexcom · FUJITSU · GENOMCORE years · MINSAIT · Roche · T-Systems · NTT DATA

SOCIO TECNOLÓGICO COLABORADOR

FUJIFILM Value from Innovation · Microsoft · PHILIPS · SIEMENS Healthineers

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 2027 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 realizara 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 trataran 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 practica 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 "Trasparencia algorítimica 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 continua 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 riegos de ciberseguriad 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 pseuoanonimización en la Inteligencia Artificial", se revisarna 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 DE PROGRAMA

Coordinador
Juan Díaz García

Miembros
Blanca Álvarez Yaque
Miguel Ángel Benito Tovar
Carlos García Codina
Pedro Alberto González González
Francisco Martínez del Cerro
Joaquín Pérez Catalán
Francesc Xavier Urios Aparisi
Juana Mª Vegas Fernández

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 - 14.15 **Segunda Sesión**
Soluciones para la ciberseguridad en entornos sanitarios

14.15 - 16.00 **Coctel - networking en el hotel**

16.00 - 17.00 **Tercera Sesión Debate - Sala A**
Seguridad y trazabilidad de los datos sanitarios

17.00 - 17.15 **Networking**

16.00 - 17.15 **Sesión Técnica 1 - Sala B**

17.15 - 18.15 **Cuarta Sesión Debate - Sala A**
Transparencia algorítimica en datos de salud

17.15 - 18.30 **Sesión Técnica 2 - Sala B**

18.15 - 18.30 **Networking**

18.30 - 19.30 **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

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 - 13.00 **Septima Sesión**
Soluciones de seguridad ante el tratamiento de datos de salud

13.00 - 14.00 **Octava Sesión Debate**
Anonimización y pseuoanonimización en la Iteligencia Artificial

14.00 - 14.30 **Acto de Clausura**