POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ÍNDICE

1. Ámbito de aplicación

Esta Política aplica a todo el GRUPO, entendiendo como tal el conjunto de sociedades encabezado por Clínica Baviera S.A. incluyendo no únicamente aquellas en las que Clínica Baviera S.A., tiene una participación accionarial mayoritaria, sino también aquellas en las que sea responsable de su gestión efectiva.

2. Posición del GRUPO

El GRUPO reconoce la importancia de proteger la información y los servicios que presta, y establece para ello un Sistema de Gestión de Seguridad de la Información que implementa, mantiene y mejora de manera continua en base al estándar ISO27001. El Consejo de Administración de Clínica Baviera S.A. declara su compromiso para liderar y fomentar a todos los niveles la seguridad de la información, de acuerdo con esta Política, garantizando la preservación de los pilares confidencialidad, integridad y disponibilidad.

3. Principios de seguridad

El GRUPO define los siguientes principios como directrices fundamentales de seguridad de la información que han estar presentes en cualquier actividad relacionada con el tratamiento de información:

Carácter estratégico:

La seguridad de la información requiere la coordinación e integración con el resto de las iniciativas estratégicas para conformar un marco completamente coherente y eficaz, y debe contar con el compromiso y apoyo de todos los órganos de la dirección del GRUPO.

Seguridad integral:

La seguridad de la información se concibe como un proceso integral constituido de elementos técnicos, humanos, materiales y organizativos adecuadamente coordinados que debe aplicarse de manera sistemática y planificada procurando evitar, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad debe estar presente y aplicarse en el diseño y mantenimiento de los sistemas de información.

Gestión de riesgos:

La gestión de riesgos es un proceso intrínseco a la seguridad de la información. A través de la gestión de riesgos se debe mantener un entorno de control, minimizando los riesgos hasta niveles aceptables. Para mitigar los riesgos se deben aplicar medidas de seguridad, seleccionadas considerando su coste y eficacia, y alineadas con el nivel de protección requerido.

Proporcionalidad:

Las medidas adoptadas para minimizar los riesgos deben estar justificadas y ser proporcionales a los riesgos identificados.

Mejora continua:

Debe existir un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la progresiva evolución de los riesgos.

Seguridad por defecto y desde el diseño:

Los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto, y proporcionar la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.

4. Compromiso y responsabilidades

El Consejo de Administración de Clínica Baviera, S.A., consciente de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos de negocio, se compromete a:

- Asegurar que se definen periódicamente objetivos de seguridad de la información alineados con la estrategia corporativa.
- Facilitar los recursos necesarios para alcanzar los objetivos de seguridad de la información y la aplicación efectiva de esta Política.
- Designar funciones y responsabilidades en el ámbito de la seguridad de la información.
- Recibir formación de forma periódica para detectar riesgos y evaluar las prácticas de gestión de riesgos de seguridad de la información y su repercusión en los servicios proporcionados por la entidad.
- Considerar los resultados arrojados por los análisis de riesgos de seguridad de la información en la toma de decisiones.
- Supervisar la adopción de medidas de seguridad efectivas que den respuesta a los riesgos de seguridad de la información.
- Impulsar y promover una cultura de seguridad entre los empleados del GRUPO.
- Conocer y exigir el cumplimiento de las directrices internas, de la legislación vigente y de los requisitos de los reguladores en materia de la seguridad de la información.
- Revisar periódicamente el Sistema de Gestión de seguridad de la Información y velar por su mejora continua.

5. Supervisión y revisión

La presente Política será objeto de revisión en el momento en el que las circunstancias normativas, sociales, empresariales o de cualquier otra índole así lo requiera.

6. Aprobación

La aprobación de la presente Política corresponde al Consejo de Administración de Clínica Baviera, S.A.

7. Entrada en vigor

Esta Política entrará en vigor el 20 de diciembre de 2025 y será publicada en la web para consulta de todas las partes interesadas.

Madrid, a 19 de diciembre de 2025.

El Secretario del Consejo de Administración