POLÍTICA DE CIBERSEGURIDAD

1. INTRODUCCIÓN

La información y los sistemas asociados son activos estratégicos que deben ser gestionados y estar protegidos frente a distintas fuentes de riesgo. Los riesgos pueden ser naturales, accidentales y/o intencionados, resultando en interrupciones del negocio y en la vulneración de datos empresariales y/o personales de carácter confidencial.

Tal y como queda recogido en nuestro Código de Conducta, Grifols, S.A. y sus filiales ("**Grifols**") disponen de información valiosa tanto no financiera (por ejemplo, científica, técnica, comercial) como financiera. Debemos proteger esta información, así como nuestro negocio y continuidad del suministro. Al actuar así, también protegemos a nuestros pacientes, los cuales confían en nuestros productos y servicios para su salud y bienestar, y a los donantes que hacen que nuestras terapias sean posibles, así como a nuestros clientes y proveedores.

Grifols está firmemente comprometida en proteger sus activos empresariales mediante la implementación de los controles necesarios, incluyendo políticas, procesos y procedimientos, con el fin de proteger su negocio y a las partes interesadas (*stakeholders*), y equilibrar los niveles de riesgo con una asignación eficiente de los recursos, basándose en principios de proporcionalidad.

2. OBJETO

El objetivo de esta política (la "**Política**") es establecer los principios básicos y el marco general para disminuir la exposición de Grifols a amenazas de ciberseguridad internas y externas dentro de los niveles de tolerancia definidos, cumpliendo al mismo tiempo con las leyes y normativas vigentes en materia de ciberseguridad de forma que Grifols pueda alcanzar sus objetivos y cumplir con su misión.

3. ÁMBITO DE APLICACIÓN

Esta Política es de aplicación a todos los empleados de Grifols y comprende toda la información de Grifols y sus sistemas asociados, incluyendo la tecnología de la información, la tecnología operativa, y los dispositivos médicos.

En las sociedades donde Grifols tenga intereses financieros, pero no el control de la gestión, Grifols recomendará la adopción a, y cumplimiento de, los principios y directrices establecidos en esta Política.

Adicionalmente, Grifols aplicará los principios y directrices establecidos en esta Política a sus socios terceros a lo largo de toda la cadena de suministro.

4. PRINCIPIOS

Grifols establece los siguientes principios básicos para gestionar los riesgos de ciberseguridad:

- Mantener sistemas robustos, actualizados y resilientes para el tratamiento de la información personal, apoyados en el cifrado, anonimización y otras medidas oportunas.

- Definir un enfoque sistemático que identifique y evalúe continuamente los riesgos de ciberseguridad, incluidos los riesgos de terceros, así como la reacción ante cualquier incidente en materia de ciberseguridad.

- Implementar medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información y procesos asociados (incluidos los sistemas de información gestionados por terceros), y supervisar constantemente su eficacia para garantizar una mejora continua.

- Implementar procedimientos e invertir en herramientas para facilitar una adaptación ágil a las condiciones cambiantes en el entorno tecnológico.

- Garantizar la existencia de programas efectivos de respuesta y recuperación, que comprendan personas, procedimientos, sistemas de información y tecnologías para: detectar, evaluar, responder en un plazo razonable para, rectificar y, si es necesario de acuerdo con la legislación aplicable, notificar a los inversores cualquier incidencia y amenaza real o potencial de ciberseguridad; recuperarse eficazmente de los incidentes de ciberseguridad; escalar los incidentes de ciberseguridad a la dirección y al equipo de ciberseguridad; y notificar cualquier incidente a las autoridades tal como exige la legislación y la normativa aplicables.

- Mantener un equipo de ciberseguridad altamente cualificado, conformado por personal directivo, informático y legal, concretando unos criterios de contratación apropiados y estableciendo planes de formación rigurosos.

- Garantizar que empleados, ejecutivos y directivos reciban formación en materia de riesgos de ciberseguridad y protección de datos personales y confidenciales. La formación incluiría la protección frente a ataques de phishing y directrices sobre el uso del correo electrónico, internet y redes sociales para garantizar que la información confidencial se gestiona y está protegida de manera adecuada, y el proceso de reporte que deben seguir los empleados en caso de identificar un incidente o amenaza de ciberseguridad.

- Colaborar con empresas similares, asociaciones del sector y agencias gubernamentales para compartir las mejores prácticas y soluciones efectivas contra las amenazas a la ciberseguridad.

Para apoyar la implementación de estos principios, Grifols implementa el "Proceso de Seguridad de la Información y Sistema de Gestión" (el "**SGSI**"). El SGSI se basa en una descripción adecuada de los objetivos, roles y responsabilidades, políticas y procedimientos, y tecnología para: (i) identificar amenazas de ciberseguridad y riesgos asociados; (ii) proteger activos estratégicos; (iii) detectar y dar respuesta a amenazas e incidentes en materia de ciberseguridad; y (iv) recuperar los servicios del negocio debido a un incidente de ciberseguridad.

5. MODELO ORGANIZATIVO Y DE REPORTE

El Consejo de Administración de Grifols, a través del Comité de Auditoría, es responsable de supervisar y evaluar la eficiencia del control y gestión en materia de ciberseguridad. El Departamento de Auditoría Interna y Gestión de Riesgos Empresariales de Grifols da apoyo al Comité de Auditoría en el cumplimiento de esta responsabilidad.

El Responsable de la Oficina de Seguridad de la Información ("**ISEC**") reporta al Director de Información Digital y tiene la autoridad para desarrollar e implementar las políticas, estándares y procedimientos en materia de ciberseguridad de la sociedad, además de supervisar la implementación y eficacia del SGSI.

En este sentido, el Responsable del ISEC recibe el apoyo del Comité Global de Ciberseguridad, que facilita la alineación de iniciativas en materia de ciberseguridad con los objetivos del negocio; garantiza la cobertura global del SGSI; colabora en la priorización y ejecución de iniciativas de seguridad y proyectos; y promueve una cultura de protección frente a las amenazas de ciberseguridad en Grifols. El Comité estará formado por representantes de las unidades de negocio, tecnologías de la información y personal legal, así como de las áreas de operaciones y servicios.

El Responsable de Auditoría Interna reportará al Comité de Auditoría, al menos dos veces al año, sobre el control y gestión en materia de ciberseguridad. Para estas actualizaciones el Comité de Auditoría podrá requerir la asistencia del Director de Información Digital y/o el Responsable del ISEC.

6. ADMINISTRACIÓN E INTERPRETACIÓN

El Consejo de Administración de Grifols delega la supervisión, cumplimiento y gestión de esta Política al Comité de Auditoría.

El Comité de Auditoría está autorizado a interpretar esta Política y tomar todas las decisiones necesarias, oportunas o recomendadas para la aplicación de esta Política y para el cumplimiento por parte de la Sociedad de cualquier ley vigente.

7. MODIFICACIÓN; TERMINACIÓN

El Consejo de la Administración de Grifols, tras la propuesta del Comité de Auditoría, podrá modificar esta Política en cada momento y a su discreción, y modificará esta Política cuando lo considere necesario. Sin perjuicio de cualquier estipulación contraria a esta Sección 8, ninguna enmienda o terminación de esta Política será efectiva si dicha modificación o terminación (tras considerar cualquier acción realizada por Grifols simultáneamente a dicha modificación o terminación) provoque que Grifols infrinja cualquier ley vigente.

8. DEFINICIONES

A los efectos de esta Política:

- "**incidente de ciberseguridad**" significa un evento no autorizado, o una serie de eventos relacionados no autorizados, en o a través de los sistemas de información de Grifols que hacen peligrar la confidencialidad, integridad o

disponibilidad de los sistemas de información de Grifols o de cualquier información en las mismas;

- "**amenaza de ciberseguridad**" significa cualquier evento potencial no autorizado en o a través de los sistemas de información de Grifos que pudiera causar efectos adversos en la confidencialidad, integridad, o disponibilidad de los sistemas de información de Grifols o cualquier información en las mismas; y
- "**sistemas de información**" significa cualquier recurso de información electrónico, propiedad de o usado por Grifols, incluidos la infraestructura física o virtual controlada por dichos recursos de información, o de sus elementos, organizado para la recopilación, tratamiento, mantenimiento, uso, intercambio, difusión, o eliminación de la información de Grifols con el objetivo de mantener o apoyar las operaciones de Grifols.

9. VALIDEZ DE LA POLÍTICA

Esta Política es efectiva a partir del 16 de noviembre de 2023, fecha en la es aprobada por el Consejo de Administración de Grifols.