POLÍTICA DE GESTIÓN DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

Redactado por:	Aprobado por:
Oficina de Ciberseguridad	*Javier Zapata Victori (CISO)* *Comité de Dirección*

CONTROL DE CAMBIOS RESPECTO A ÚLTIMA VERSIÓN		
Versión	**Fecha**	**Modificación**
0	25/09/2019	Borrador inicial
1	10/11/2019	Revisión de observaciones
2	09/01/2020	Revisión de acuerdo con la política de Fresenius
3	30/01/2020	Revisión de Flujo de aprobación de Políticas
3.1	11/02/2020	Revisión de Marco Regulatorio
3.2	29/04/2020	Referencia al Grupo Quironsalud
4	12/05/2021	Revisión de ciclo de mejora continua
5	26/04/2023	Adaptación ENS y ampliación roles y responsabilidades
6	15/07/2025	Actualización de la norma ISO 27001:2022 y revisión del alineamiento

INDICE

1. INTRODUCCIÓN Y ALCANCE

Quirónsalud es el grupo líder en la prestación de servicios sanitarios y de prevención de riesgos laborales de España. Para el desempeño de sus actividades, requiere de la utilización de sistemas e información que deben ser controlados para evitar los riesgos asociados a estos en el ámbito de la seguridad de la información y ciberseguridad.

La presente política establece las directrices y principios que regirán la gestión de la Ciberseguridad y Seguridad de la información a fin de garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información gestionada por el Grupo Quirónsalud y todas las organizaciones que pertenecen al mismo.

El documento, además de estar alineado a las normativas españolas y europeas vigentes en materia de Seguridad de la información aplicables al Grupo, se apoya en los principios de la Política de Ciberseguridad de Fresenius, así como en sus diferentes requerimientos de seguridad de la información a fin de garantizar alineamiento con los objetivos estratégicos del Grupo.

La presente política es aplicable a nivel Corporativo, a cada una de las compañías pertenecientes al Grupo Quirónsalud, a los centros y hospitales que pertenecen a la red, así como a los proveedores de servicios que trabajan para cualquiera de las compañías del Grupo.

1.1. Obligaciones del personal

Todos los miembros del Grupo Quirónsalud tienen la obligación de conocer y cumplir esta Política de gestión de Ciberseguridad y Seguridad de la información, así como del cuerpo normativo del Grupo, siendo responsabilidad del Comité de Seguridad Territorial disponer los medios necesarios para que la información llegue a los afectados. Además, deberán realizar las formaciones corporativas obligatorias sobre Seguridad de la Información y protección de datos que se les exija.

1.2. Terceras partes

Cuando el Grupo Quirónsalud preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Gestión de Ciberseguridad y Seguridad de la información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad.

Cuando el Grupo Quirónsalud utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Gestión de Ciberseguridad y Seguridad de la información y del Cuerpo normativo que implique a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa.

2. MISIÓN Y OBJETIVOS

La misión del Grupo Quirónsalud es cuidar la salud y el bienestar de las personas, poniendo a su disposición servicios sanitarios y de prevención de riesgos laborales de máxima calidad con los mejores profesionales, unas modernas estructuras hospitalarias, unos avanzados medios tecnológicos y unos innovadores procesos de atención.

El Grupo Quirónsalud busca asegurar el cumplimiento de los siguientes objetivos:

- Proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los sistemas de información e información asociada.
- Cumplir con las obligaciones legales y los requerimientos regulatorios, mediante el establecimiento de políticas y procedimientos de seguridad corporativos.
- Reducir el riesgo de Ciberseguridad y Seguridad de la información.
- Mejorar la Ciberseguridad y Seguridad de la información en todos los centros pertenecientes a la red del Grupo Quirónsalud.

3. MARCO LEGAL Y REGULATORIO

El Grupo cumplirá con la normativa en vigor que encomiendan los órganos competentes (Sistema Nacional de Salud, Agencia Española de Protección de datos u otros) en materia de Seguridad de la información, Ciberseguridad y Riesgos Tecnológicos.

A continuación, se ofrece un listado de las normativas de soporte sobre las que se asienta la Política Corporativa de Ciberseguridad y Seguridad de la información:

Normativa Española:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Normativa Europea:

- Reglamento (EU) 2016/679. Reglamento relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Estándares internacionales:

- ISO/IEC 27001:2022 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- Informática sanitaria. Gestión de la seguridad de la información en sanidad utilizando la Norma ISO/IEC 27002 (ISO 27799:2016) (Ratificada por AENOR en octubre de 2016.)
- ISO/ IEC 27701 ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management.

4. GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN

El Grupo contará con una estructura organizativa sólida y transparente con responsabilidades claramente definidas. Además, los principales responsables de la gestión de la Ciberseguridad y Seguridad de la Información tendrán acceso y contacto directo con los órganos de gobierno de la Organización a fin de garantizar que la información o las cuestiones importantes se comuniquen, se traten y se decidan de manera adecuada.

La estructura de gobierno permitirá dar soporte a la gestión de la Seguridad a través de la toma de decisiones relacionadas con:

- Aprobación de documentos relevantes, tales como políticas o procedimientos, así como las respectivas excepciones.
- Evaluación de las necesidades y expectativas, priorizando y decidiendo en base a los requisitos corporativos de ciber-resiliencia y seguridad de información.
- Análisis y medidas sobre las iniciativas, nuevos proyectos o adquisiciones que impliquen un cambio significativo del perfil de riesgo de ciberseguridad.
- Verificación del cumplimiento de las Políticas y Cuerpo Normativo vigente.
- Supervisión periódica de incidentes relevantes, así como de la definición y activación de los Planes de Respuesta correspondientes.

4.1 Roles y responsabilidades

El Grupo Quirónsalud cuenta con una estructura organizativa para la Gestión de la Ciberseguridad y Seguridad de la información, con funciones y responsabilidades claramente diferenciadas. Cada rol específico, debe conocer y entender sus obligaciones y responsabilidades, las cuales se identifican y detallan en esta sección:

4.1.1. Responsable de Seguridad. CISO.

El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones. Funciones:

- Lidera la gestión de Ciberseguridad y Seguridad de la información, asegurando un nivel adecuado de seguridad para todas las funciones corporativas.
- Informa a la dirección corporativa del Grupo Quirónsalud.
- Aprueba las políticas de ciberseguridad alineadas con las distintas normativas españolas y europeas vigentes aplicables al Grupo. Aprueba además otros documentos relevantes, tales como procedimientos, así como las respectivas excepciones.
- Es propietario de las políticas y procedimientos de seguridad corporativos.
- Lidera la Oficina de Ciberseguridad y al equipo cualificado que la compone.
- Es el punto o persona de contacto (POC) y quien dirige las comunicaciones en el ámbito de la seguridad de la información y gestión de incidentes de ciberseguridad para los servicios prestados.

El Responsable de Seguridad del Grupo, podrá delegar en los responsables de la Oficina de Ciberseguridad o en los diferentes responsables de Seguridad Territoriales y Responsable de Seguridad Locales de cada uno de los centros.

4.1.1.1. Oficina de Ciberseguridad

Entidad responsable de identificar los requerimientos de Seguridad de la información y Ciberseguridad que se deben cumplir para mitigar los riesgos de los sistemas y de la información del Grupo y de definir la política y requisitos mínimos a fin de garantizar la seguridad de la información y sistemas del Grupo. Asimismo, es responsable de promover y difundir el cumplimiento de las directrices definidas en la presente política y brindar soporte a los roles involucrados y otros usuarios del Grupo ante cualquier duda o consulta.

Además, tendrá delegadas las funciones de revisar y aprobar excepciones que surjan a los requisitos de esta política evaluando los riesgos y posibles repercusiones, además de medidas de control compensatorias si aplicara.

4.1.2. Responsable del servicio

Es la función encargada de determinar los requisitos de los servicios prestados a la Administración Pública. Es responsable de que se incluyan las especificaciones de seguridad en el ciclo de vida de los servicios, acompañadas de los correspondientes procedimientos de control.

4.1.3. Responsable de Seguridad Territorial

Responsable de la gestión de Ciberseguridad y Seguridad de la información para cada Territorio, asegurando un nivel adecuado de seguridad y la alineación con las políticas y requerimientos del Grupo en los centros que forman parte del Territorio bajo su responsabilidad. Además, deberá asegurar que las directrices e iniciativas de seguridad que se despliegan en el Grupo son comunicadas a las áreas correspondientes de cada centro y aplicadas en los centros de su territorio.

4.1.4. Delegado de Protección de datos (DPO) o Responsable de la información

Figura responsable de determinar los requisitos, en materia de Seguridad de la información tratada en el Grupo Quirónsalud. Vela por el cumplimiento de la seguridad de la información en sus diferentes formatos: protección lógica y física.

Adicionalmente, es la función que se crea por el Reglamento General de Protección de datos como un garante del cumplimiento de la normativa de protección de datos personales. Sus principales funciones son las siguientes:

- Informar y asesorar en cuanto al tratamiento de datos de carácter personal por la empresa.
- Supervisar el cumplimiento de la normativa.
- Participar en las Evaluaciones de Impacto.
- Cooperar con AEPD.
- Punto de contacto con AEPD y con los afectados ya que sus datos de contacto deben figurar en la cláusula informa.

4.1.5. Responsable del sistema

Responsable de operar y mantener los sistemas de información durante todo su ciclo de vida y de verificar su correcto funcionamiento, así como de la implementación de la seguridad en el sistema, atendiendo a las medidas de seguridad determinadas por el CISO y la Oficina de Ciberseguridad.

Asimismo, es responsable de definir la topología y sistema de gestión de los sistemas de información del Grupo, estableciendo los criterios de uso y los servicios disponibles en el mismo. Podrá tomar la decisión de rescindir contrataciones de proveedores de servicios TI cuando se encuentren deficiencias graves de seguridad en los servicios prestados.

Puede delegar sus funciones a responsables técnicos de aplicación o sistema según sea necesario.

4.1.5.1. Responsable técnico de la aplicación o sistema

Figura responsable de diseñar e implementar aplicaciones o sistemas y de ejecutar las medidas de seguridad sobre estos que permitan cumplir con la presente Política, así como del cumplimiento de las políticas corporativas aplicables a los activos relacionados con la aplicación o sistema del que es responsable y de identificar y documentar cualquier desviación sobre las mismas. Asimismo, es responsable de la supervisión de la operación diaria de la aplicación o sistema del que es responsable, atendiendo a las medidas de seguridad determinadas por el CISO y la Oficina de Ciberseguridad. Esta figura será siempre personal laboral.

Deberá mantener informado en todo momento al Propietario de la aplicación o sistema en lo que al ciclo de vida del activo se refiere, manteniéndole informado de los cambios sobre el aplicativo, sistema o infraestructura que lo sostiene para que el propietario del aplicativo o sistema pueda reportar adecuadamente estos cambios y actualizaciones sobre el registro del mismo.

4.1.6. Propietario de la aplicación o sistema (o Responsable de negocio del activo)

Responsable, por la parte de negocio, de asegurar que las aplicaciones o sistemas cumplan con la presente política, así como de informar cualquier desviación sobre la misma. Esta figura será siempre personal laboral.
Los propietarios de aplicación o sistema son responsables de la correcta gestión del ciclo de vida de los activos que se les asignan y trabajarán junto con el personal de TI correspondiente y la Oficina de Ciberseguridad para crear, mantener y enriquecer el registro de activos de información con ayuda del responsable técnico de la aplicación.

4.2 Comités

4.2.1. Comité Estratégico

Tiene como objetivo tratar a alto nivel el estado de la seguridad de la organización y los riesgos relacionados, revisión de la estrategia y objetivos junto el estado del presupuesto. En este comité participa el Director General de Organización, Procesos, TIC y Digital y todos los directores del área de la dirección general TyS, el CISO, y el DPO.

4.2.2. Comité Táctico Corporativo de Seguridad

Tiene como objetivo revisar las necesidades de seguridad del Grupo, evaluar indicadores de seguridad y elevar los riesgos competentes. En este comité participa el Director General de Organización, Procesos, TIC y Digital, el CISO, DPO, el Responsable de Sistemas de Territorios y el Responsable de Infraestructura.

4.2.3. Comité Táctico de Seguridad Territorial

Tiene como objetivo exponer el estado de la estrategia y niveles de seguridad en los centros, comunicar/revisar novedades normativas y evaluar indicadores asociados a los territorios/centros. En este comité participa el CISO, los Responsables de Seguridad Territoriales y el Responsable de Seguridad de Quirónprevención.

4.2.4. Comité Operativo de Seguridad

Tiene como objetivo revisar las actividades de seguridad según su estado y relación con el equipo de TI (infraestructura). Participa el CISO, la Oficina de Ciberseguridad y el Responsable de infraestructura.

4.2.5. Comité de Seguimiento de Seguridad

Tiene como objetivo tratar los indicadores y resultados operativos de seguridad en el día a día, informar del estado de las actividades y escalado de aspectos relevantes. Asiste el CISO, los Responsables de la Oficina de Ciberseguridad y el Responsable de Seguridad LATAM.

4.2.6. Comité de seguridad de la información y protección de datos de los centros

Es el órgano colegiado para la gestión y supervisión de la Seguridad de la Información y Continuidad de Negocio, que coordinará las actividades y controles de seguridad establecidos en los distintos Sistemas de Gestión de la Seguridad de la Información que se implanten en cada centro y que velará por el cumplimiento de la normativa vigente, interna y externa, en materia de seguridad de la información y continuidad de negocio que les sea de aplicación. Es el encargado de impulsar la implementación y desarrollo de las Políticas Corporativas y locales de Seguridad de la Información y protección de datos. Este comité deberá existir únicamente en aquellos casos que por requerimientos regulatorios los Centros estén obligados a crearlo. En el resto de los casos, es opcional y puede crearse a nivel territorial.

4.3 Proceso de designación y renovación de roles o funciones de seguridad

El proceso de designación y renovación de los roles de seguridad definidos en esta Política se realizará de la siguiente forma:

- El nombramiento del Responsable de seguridad (CISO) y del Delegado de protección de datos (DPO) se realizará por parte de la Dirección general. Únicamente se revisarán cuando el puesto quede vacante.
- El nombramiento de la Oficina de Ciberseguridad se realizará por parte del Responsable de seguridad (CISO). Únicamente se revisará cuando algún puesto quede vacante.
- El nombramiento de los responsables de seguridad territorial será propuesto por los diferentes responsables de TI territoriales con aprobación del CISO. Estos roles serán revisados cada dos años.

4.4 Resolución de conflictos

En caso de producirse conflictos se resolverán en el Comité correspondiente, en función del problema tratado, áreas involucradas y criticidad del conflicto.

5. PRINCIPIOS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Gestión de la Ciberseguridad y Seguridad de la información en el Grupo Quirónsalud se basa principalmente en los siguientes pilares:

- **Cultura y formación continua en Ciberseguridad y Seguridad de la información:** La gestión del Grupo Quirónsalud busca crear una cultura corporativa desde el más alto nivel organizacional a los empleados administrativos y personal de salud. Para ello, se contará con un programa continuo de capacitación y concienciación alineado a los objetivos organizacionales.
- **Seguridad como un proceso integral:** el Grupo Quirónsalud entenderá la seguridad como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con los sistemas de información.
- **Gestión basada en dominios de riesgo:** el análisis y gestión de riesgos será parte esencial del proceso de seguridad del Grupo, siendo una actividad continua y permanentemente actualizada. La gestión de riesgos se centrará para cada uno de los dominios de riesgo aplicables, estableciendo estrategias, políticas, procedimientos y controles adecuados para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información para todos los entornos en toda la cadena de suministro.
- **Gestión de incidentes de seguridad (prevención, detección, respuesta y recuperación):** se deberá contemplar acciones relativas a la prevención de incidentes de seguridad, con el objetivo de reducir la posibilidad de que se materialicen amenazas de seguridad o, en caso de materializarse, reducir el impacto. Asimismo, el Grupo Quirónsalud contará con procesos de detección y respuesta que permitan identificar incidentes de seguridad y gestionarlos de forma oportuna y eficaz. Estos procesos deberán estar orientados a la conservación y recuperación de la información y los servicios afectados.
- **Existencia de líneas de defensa:** se establecerá una estrategia basada en múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de modo que cuando una de las capas sea comprometida, se reduzca la posibilidad de que el sistema sea comprometido en su conjunto y a su vez se minimice el impacto.
- **Monitorización continua y reevaluación periódica:** los activos críticos se mantendrán monitorizados con el fin de detectar vulnerabilidades. Además, las medidas de seguridad se reevaluarán periódicamente y actualizarán en los casos necesarios, para adecuar su eficacia a la evolución de los riesgos.
- **Diferenciación de responsabilidades:** en los sistemas de información de Quirónsalud se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema. Las atribuciones de cada responsable se definen en la sección 4. FUNCIONES Y RESPONSABILIDADES del presente documento. El responsable de la seguridad será distinto del responsable del sistema, no existiendo dependencia jerárquica entre ambos o, se aplicarán medidas compensatorias para aquellas situaciones excepcionales en las que resulte necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica.
- **Ciberseguridad y Seguridad de la información integrada en la infraestructura tecnológica, procesos de negocio y gestión de proveedores:** Quirónsalud tomará las medidas necesarias a fin de que la Ciberseguridad y la Seguridad de la Información sea una parte integral en el diseño y/o adquisición de dispositivos, servicios, hospitales, procesos y operaciones para asegurar y proteger la información del paciente y el cliente. Adicionalmente, se asegurará de que aquellos proveedores que tienen acceso o son responsables de los activos de información de Quirónsalud estén sujetos a disposiciones contractuales a fin de garantizar un nivel adecuado de seguridad.
- **Comunicación y transparencia en temas relacionados a la gestión de la Ciberseguridad y Seguridad de la información:** La gestión de Quirónsalud facilitará la colaboración de todo el Grupo y proporcionará transparencia sobre el estado de la Ciberseguridad y Seguridad de la información.

6. REQUERIMIENTOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

El Grupo Quirónsalud, para lograr el cumplimiento de las regulaciones vigentes y asegurar la protección de la información y la continuidad del negocio, deberá cumplir, al menos, los siguientes requisitos mínimos de Seguridad de la información y Ciberseguridad, en función a la naturaleza y los riesgos asociados a la información, sistemas y servicios a proteger:

- **Organización e implantación del proceso de seguridad.** La política de seguridad es conocida por todas las personas que forman parte de la organización.
- **Análisis y gestión de los riesgos.** El Grupo Quirónsalud realiza una gestión de riesgos con el objetivo de mitigar aquellos a los que están expuestos los sistemas e información del Grupo,

evaluando las posibles amenazas y escenarios de riesgo y justificando las medidas mitigadoras adoptadas.

- **Gestión de personal y profesionalidad:** El Grupo Quirónsalud asegura que el personal, interno o externo, tiene a su disposición las normas y procedimientos operativos necesarios para que todos estén formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Asimismo, imparte formación en materia de seguridad a las nuevas incorporaciones y a todos los empleados, al menos, una vez al año.
  Adicionalmente, el Grupo Quirónsalud determina los requisitos de formación y experiencia necesaria del personal para el desarrollo de sus funciones. Por otro lado, se asegura de que las organizaciones que le presten servicios de seguridad dispongan de profesionales cualificados y con un nivel adecuado de gestión y madurez en los servicios prestados.
- **Autorización y control de accesos.** El Grupo Quirónsalud implementa mecanismos de control de acceso a los sistemas de información, limitándolos a los usuarios, sistemas, procesos o dispositivos estrictamente necesarios y debidamente autorizados.
- **Protección de las instalaciones.** La Organización implementa mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados a los sistemas de información y su infraestructura de comunicaciones, en función al riesgo.
- **Adquisición de productos de seguridad y contratación de servicios de seguridad.** La adquisición de productos y servicios de seguridad se realiza bajo el nivel de categorización del sistema, siendo los requisitos de seguridad proporcionales a dicha categorización y a la clasificación de la información que maneje. En caso de subcontrataciones en este tipo de servicios o productos, se deberán mantener los mismos requisitos de seguridad que con el proveedor contratado inicialmente.
- **Mínimo privilegio.** Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, proporcionando únicamente las funciones imprescindibles para su funcionamiento y eliminando o desactivando aquellas que sean innecesarias o inadecuadas.
- **Integridad y actualización del sistema.** Se gestiona la inclusión de cualquier elemento físico o lógico en el catálogo de sistemas y se monitoriza de forma permanente el estado de seguridad de los mismos.
- **Protección de la información almacenada y en tránsito.** El Grupo Quirónsalud aplica medidas de protección de la información almacenada o en tránsito. Se implementan mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentran los documentos, para garantizar que toda información relacionada en soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.
- **Prevención ante otros sistemas de información interconectados.** Se protege el perímetro del sistema de información, en función al riesgo existente en la interconexión del sistema con otros sistemas.
- **Registro de la actividad y detección de código dañino.** Se registra la actividad de los usuarios para detectar e investigar actividades no autorizadas o indebidas, identificando en cada momento a la persona que accede al sistema y que realiza cada actividad. Este registro contiene únicamente la información estrictamente necesaria para su fin. Adicionalmente, se establece un sistema de detección y reacción frente a código dañino.
- **Incidentes de seguridad.** El Grupo Quirónsalud dispone de procedimientos de gestión de incidentes de seguridad y dispone además de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, flujos de comunicación a las partes interesadas y registro de las actuaciones.
  El Grupo Quirónsalud tiene la responsabilidad de notificar los incidentes de ciberseguridad a la autoridad competente según las regulaciones aplicables.
- **Continuidad de la actividad.** Los sistemas de información disponen de copias de seguridad y se establecen los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de situaciones que impidan el uso de los medios habituales de trabajo. Se han desarrollado procedimientos que aseguran la recuperación y conservación de la información.
- **Mejora continua del proceso de seguridad.** El proceso de seguridad de la información implantado en el Grupo Quirónsalud es actualizado y mejorado de forma continua.

7. GESTIÓN DOCUMENTAL Y CICLO DE APROBACIÓN DE POLÍTICAS Y PROCEDIMIENTOS

7.1. Estructura documental

La gestión de la Ciberseguridad y Seguridad de la información en el Grupo Quirónsalud se basa en un Cuerpo normativo de seguridad de negocio y usuarios y de servicios TI e infraestructura, estructurado de la siguiente forma:

- **Nivel 1:** Políticas, procedimientos, guías de seguridad de la información y protección de datos, e instrucciones técnicas corporativas. (A nivel de grupo)
- **Nivel 2:** Políticas, procedimientos, guías de seguridad de la información y protección de datos, e instrucciones técnicas locales. (A nivel de centro, teniendo en cuenta el nivel 1).

7.2. Ciclo de aprobación Nivel 1

A fin de gestionar y controlar el Cuerpo Normativo de Ciberseguridad y Seguridad de la información, se ha definido el siguiente ciclo de aprobación en la Organización:

Fase	Descripción
Elaboración	La **Oficina de Ciberseguridad** se encarga de elaborar las diferentes políticas o procedimientos, identificando los requisitos, definiendo medidas y realizando las correcciones necesarias a fin de que el documento se ajuste a las necesidades del Grupo Quirónsalud.
Aprobación inicial	La Oficina de Ciberseguridad enviará la versión del documento al **responsable de Políticas y Cumplimiento**, quien será responsable de revisar y aprobar la política, procedimiento, guía o instrucción técnica de seguridad, coordinando los cambios o ajustes que crea convenientes.
Aprobación final	El responsable de Políticas y Cumplimiento enviará la última versión del documento al **CISO** para su aprobación, coordinando los cambios o ajustes que crea convenientes. La Política de Ciberseguridad y Seguridad de la Información deberá ser aprobada adicionalmente por el Comité de Dirección cuando se produzcan cambios significativos en la misma que afecten a las directrices contenidas en esta.
Publicación	Finalmente, la **Oficina de Ciberseguridad** gestionará la publicación formal del documento en el Portal de Seguridad de la Intranet Corporativa a fin de que sea de conocimiento de todos los miembros del Grupo Quirónsalud.
Comunicación Territorial	A continuación, el responsable de Políticas y Cumplimiento enviará el documento a los **Responsables Territoriales de Seguridad**. Se les indicará los cambios o las nuevas políticas, se les instará a compartir las políticas con los centros y usuarios o áreas específicas y se les indicará que es de obligado cumplimiento.
Comunicación a Comité	Posteriormente, el documento se presenta en los diferentes **Comités de seguridad de la información y protección de datos de los centros**, por parte de los responsables territoriales, a fin de dar a conocer los detalles de la Política o Procedimiento, así como absolver posibles dudas y/o comentarios.

7.3. Ciclo de aprobación Nivel 2

La Dirección de sistemas de cada centro podrá elaborar políticas locales en caso de ser necesario, por ejemplo, por motivo de certificación de algún sistema de gestión de seguridad de la información. Estas políticas sólo podrán crearse siguiendo los principios mínimos de las políticas de nivel 1, pasando por la revisión del Responsable de Políticas y Cumplimiento de la Entidad en caso de ser necesario, y deberá ser aprobada por el Comité de seguridad de la información y protección de datos de dicho centro.

8. RIESGOS DERIVADOS DE TRATAMIENTO DE DATOS PERSONALES

Cualquier sistema que trate datos personales tendrá en cuenta lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), así como el resto de normativa de aplicación. Se tendrá en consideración al menos los siguientes puntos:

- Registro de actividades de tratamiento.
- Evaluaciones de impacto y análisis de riesgos a la privacidad.
- Ejercicios de derechos.
- Procedimiento de gestión de posibles brechas de seguridad.

9. CICLO DE MEJORA CONTINUA

La presente política y el correspondiente cuerpo normativo deberán ser objeto de revisión y actualización periódica, debiéndose examinar y actualizar al menos una vez cada dos años o cuando se identifiquen nuevos elementos significativos para la gestión de la ciberseguridad, tales como:

- Cambios en la estrategia de Negocio y TI
- Cambios en la estructura organizacional
- Implementación de nuevas tecnologías, tácticas, técnicas o procedimientos que afecten al Grupo
- Cambios regulatorios
- Resultados de auditorías

Las modificaciones que se deban realizar sobre la Política deben ser definidas, implementadas y comunicadas siguiendo el proceso de Ciclo de aprobación de políticas y procedimientos descrito.