



Manual Política de Seguridad

MS-02

Versión 10.0

Información Confidencial

© 2025 Facephi Biometría. Todos los derechos reservados.

El logotipo Facephi y todas las marcas comerciales de "Facephi Biometría S.A."

(A-54659313) están registradas internacionalmente. Los nombres de otros productos y empresas aquí mencionadas pueden ser marcas comerciales de sus respectivos titulares para los que Facephi cuenta con la correspondiente autorización. Debido a que Facephi presenta con frecuencia nuevas versiones y actualizaciones de su software, las imágenes mostradas en este documento pueden ser diferentes de las que vea en pantalla.

Declaración de confidencialidad

Este documento contiene información confidencial y de propiedad exclusiva. Todos los datos presentados son brindados sobre la base del consentimiento a no usar ni divulgar la información aquí contenida, excepto en los tratados comerciales con Facephi Biometría.

El receptor de este documento acepta informar a todos los empleados y socios, actuales y futuros, que consulten o tengan acceso al contenido del documento, acerca de la confidencialidad del mismo. El receptor acepta dar instrucciones precisas a los empleados para que no divulguen información relacionada con este documento, excepto en el caso de que se trate de cuestiones de público conocimiento y que estén disponibles para uso público. El receptor también acepta no reproducir o distribuir o permitir que otros reproduzcan o distribuyan cualquier material aquí contenido sin el consentimiento expreso, por escrito, de Facephi Biometría.

Facephi Biometría retiene todos los derechos de titularidad, posesión y propiedad del material y marcas registradas aquí contenidas, incluida la documentación de respaldo, los archivos, el material de comercialización y multimedia.

La aceptación de este documento implica que el receptor acepta estar legalmente vinculado a la declaración antes mencionada.

Tabla de actualizaciones

	Elaborado por	Aprobado por
Nombre	Raúl López	Jorge Sanz
Cargo	GRC Officer	Director General
Fecha	12/09/2025	24/09/2025

Versión	Fecha	Observaciones
1.0	26/06/2020	Primera versión
2.0	24/09/2021	Adecuación ENS
3.0	13/12/2021	Nueva referencia roles y responsabilidades
4.0	31/01/2022	Se indica el ámbito normativo del SGI
5.0	02/08/2022	Se incorpora la norma ISO 27017 Seguridad de la información en cloud
6.0	22/01/2024	Se crear el punto 5
7.0	22/04/2024	Revisión tras auditoría externa
8.0	07/06/2024	Revisión del documento
9.0	29/08/2024	Se actualiza el apartado 1 y el apartado 4.1, así como el organigrama de Gobierno del SGI
10.0	12/09/2025	Tras auditoría externa, se elimina el organigrama y referencias explícitas a documentación interna. Además, se añade ISO 27701 al apartado 4.1 al tomar como referencia y como guía controles de la misma

Índice de contenidos

1 Alcance y Misión.....	5
2 Desarrollo.....	6
3 Creación, actualización, aprobación y comunicación	7
4 Anexos.....	7
4.1 Marco Legal y Regulatorio.....	7
4.2 Roles y Funciones.....	8
4.2.1 Responsable de Seguridad.....	8
4.2.2 Responsable del Sistema	8
4.2.3 Responsable de la Información.....	9
4.2.4 Responsable del Servicio.....	9
4.2.5 Delegado de Protección de Datos	9
4.3 Comités de seguridad	10
4.3.1 Gobierno Corporativo SGI.....	10
4.3.2 Dirección Ejecutiva SGI.....	10
5 Principios y requisitos de seguridad.....	11
6 Riesgos derivados del tratamiento de Datos de carácter personal.....	12
7 Gestión de riesgos.....	12
8 Información documentada.....	13

1 Alcance y Misión

Esta política aplica a las actividades, servicios, activos, recursos y resto de partes involucradas en la prestación de productos y servicios de Facephi Biometría S.A.

Facephi se adhiere a los mayores estándares internacionales sobre Seguridad de la información y la Continuidad de negocio e incorpora las mejores prácticas implementando controles basados en ISO 27001, ISO 27017, ISO 22301, Esquema Nacional de Seguridad (ENS), además toma como referencia y como guía controles sobre gestión de la privacidad, entre otros. Todo ello compone el Sistema de Gestión Integrado (SGI).

Facephi ha logrado conseguir la confianza por parte de numerosas entidades a nivel global, involucradas en el manejo de información altamente confidencial, y esto ha sido posible gracias al convencimiento y esfuerzo por asegurar la integridad, confidencialidad, autenticidad, trazabilidad y disponibilidad de la información y sistemas que la soportan, de ahí que los objetivos del SGI de Facephi se basen en la preservación de:

- a) La disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.
- b) La confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información. La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. La confidencialidad hace referencia a proteger todos esos datos y recursos contra accesos no autorizados.
- c) La integridad, asegurando que la información se mantiene invariable, es decir, manteniendo la exactitud y completitud de la información y sus métodos en el proceso, es decir, garantiza que los datos sean confiables y correctos, protegiéndolos contra cambios no autorizados. La integridad es decisiva para mantener la calidad de la información.
- d) La trazabilidad, asegurando el rastreo de quién ha accedido y/o modificado una cierta información asociada al servicio.
- e) La autenticidad, asegurando que quien accede al servicio es realmente quien debe ser, y se pueda conocer quién ha accedido.

Desde el inicio, se estableció como propuesta de valor la Seguridad de la Información y la Resiliencia, garantizando además de la disponibilidad, el correcto funcionamiento de los sistemas y servicios, y el cumplimiento de cualquier requisito legal, normativo o contractual.

La misión primordial de Facephi siempre ha sido desarrollar tecnologías para la verificación de la identidad y la autenticación buscando su mejora y excelencia, con el fin de contar con algoritmos de última generación, y para ello realiza una fuerte inversión en I+D, con el fin de contribuir a la evolución del concepto de identidad digital cada vez más segura y resiliente en todos sus procesos.

Algunas cuestiones clave son:

- a) Preservar y asegurar la integridad de los algoritmos analizando las amenazas que puedan afectar a la biometría y por tanto suponer un riesgo para la privacidad de estos.
- b) Gestionar y preservar la identidad y privacidad de los datos.
- c) Asegurar la integridad y la calidad del método, así como la integridad del código.

El principal valor de la compañía es el valor humano ya que cuenta con un equipo comprometido, proactivo, comprometidos con el proyecto y con altas dosis de motivación.

2 Desarrollo

La Dirección de Facephi quiere dar a conocer la Política de Seguridad, ya que su conocimiento y comprensión son esenciales para sus trabajadores, clientes, proveedores y otras partes interesadas, puesto que la Seguridad de la Información, la Continuidad de Negocio y la privacidad son factores clave para el correcto desarrollo de la organización.

Esta Política muestra el compromiso de la Dirección, y tiene como objetivos de alto nivel:

- a) Velar por la satisfacción de los clientes cumpliendo con las necesidades y expectativas de los mismos y preservando la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información.
- b) Demostrar liderazgo asegurando que la Política y los objetivos se establecen y son compatibles con la dirección estratégica de la organización.
- c) Establecer objetivos y metas enfocados a la evaluación del desempeño en materia de Seguridad de la Información y Continuidad de Negocio, y a mejorar las actividades realizadas.
- d) Asegurar el cumplimiento de la legislación y reglamentación aplicables a nuestra actividad, los compromisos adquiridos con los clientes y todas aquellas normas tanto internas como externas a las que está adherida la organización, con el fin de conseguir una mejora continua.
- e) Asignar las funciones y responsabilidades necesarias en el ámbito de la Seguridad de la Información y la Continuidad de Negocio y proporcionar el soporte necesario.
- f) Implementar medidas preventivas eficaces y eficientes en todas las actividades realizadas.
- g) Establecer y revisar periódicamente el apetito del riesgo de la compañía, así como los riesgos identificados, su resolución y/o tratamiento.
- h) Desarrollar, implementar y verificar periódicamente los planes de continuidad y contingencia y las pruebas asociadas a los mismos.
- i) Formar, concienciar y motivar al personal sobre la importancia de cumplir los requisitos establecidos en el SGI tanto en el ámbito de la Seguridad de la Información como de Continuidad de Negocio.
- j) Mantener una comunicación fluida tanto a nivel interno, entre los diferentes estamentos de la empresa, como con los clientes o partes interesadas.
- k) Establecer la correcta estructuración de la documentación además de la adecuada gestión y actualización de normativas.
- l) Tener en cuenta la Seguridad de la Información y la Continuidad de Negocio establecida por sus proveedores para velar ante posibles riesgos provenientes de los mismos.

3 Creación, actualización, aprobación y comunicación

Este documento lo elabora el equipo de GRC, con el soporte y aprobación de la Alta Dirección.

El Responsable de la Información es el encargado de velar por la idoneidad y actualización de este documento. Además, es responsabilidad de todo el personal tanto interno como externo relacionado con Facephi darle cumplimiento a esta Política y velar porque así sea.

Esta Política será notificada a todos los empleados, y podrá ser compartida con terceros y partes interesadas que lo requieran y que estén presentes en la ejecución de actividades relacionadas con la prestación de productos y servicios de Facephi Biometría S.A. En la medida en que sea aplicable, será incluida dentro de los planes de formación del personal y terceros vinculados.

4 Anexos

4.1 Marco Legal y Regulatorio

El marco legal y regulatorio de Facephi se mantiene actualizado y disponible en el **Listado de legislación y normativa**. En el ámbito de seguridad se destacan las siguientes:

- a) Ley 11 /2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (y sucesivas modificaciones).
- b) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (y sucesivas modificaciones).
- c) Real Decreto 203/2021 de 30 marzo. Reglamento de actuación y funcionamiento del sector público por medios electrónicos (y sucesivas modificaciones).
- d) Ley 34/2002 11 julio de servicios de la sociedad de la información y de comercio electrónico (y sucesivas modificaciones).
- e) Reglamento (UE) 2016/679 del Parlamento europeo y del consejo del 27 de abril de 2016, relativo a la protección 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 (RGPD) (y sucesivas modificaciones).
- f) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial).
- g) Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales 3/2018 de 5 de diciembre. (LOPDGDD) (y sucesivas modificaciones).
- h) Ley 10/2021, de 9 de julio, de trabajo a distancia (y sucesivas modificaciones).
- i) Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (y sucesivas modificaciones).
- j) Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

- k) ISO 27001:2022 Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- l) ISO 27002:2022 Marco de controles de Seguridad de la Información.
- m) ISO 22301:2019 Seguridad y resiliencia. Sistema de Gestión de la Continuidad de Negocio.
- n) ISO 27017:2015 Técnicas de Seguridad. Código de buenas prácticas para los controles de seguridad de la información basados en la norma ISO/IEC 27002 para servicios en la nube.
- o) ISO 27701:2019 Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la información sobre privacidad – Requisitos y orientación

4.2 Roles y Funciones

Para demostrar el compromiso y liderazgo de seguridad de la información de la organización, así como su mantenimiento y mejora continua, con la aprobación de la Dirección se nombran los siguientes responsables para el Sistema de Gestión Integrado y para el Esquema Nacional de Seguridad.

La ampliación de funciones de cada rol se describe en PGS.02 Roles, responsabilidades y autoridades.

4.2.1 Responsable de Seguridad

El Responsable de Seguridad es nombrado por la Dirección y determina las decisiones para satisfacer los requisitos de Seguridad de la información y de los servicios. Las dos funciones esenciales que tiene asignadas son:

- a) Mantener la Seguridad de la información manejada y de los servicios prestados por los sistemas de información de acuerdo con lo establecido en la presente política.
- b) Promover la formación y concienciación en materia de seguridad dentro de su ámbito de responsabilidad, monitorizando y analizando las alertas e información de seguridad y distribuirla entre el personal, al igual que los procedimientos de respuesta y escalada de los incidentes de seguridad.

4.2.2 Responsable del Sistema

El Responsable del Sistema es designado por la Dirección Ejecutiva y tiene las siguientes funciones asignadas:

- a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- b) Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- c) Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

4.2.3 Responsable de la Información

El Responsable de la Información es designado por la Dirección Ejecutiva y tiene siguientes funciones asignadas:

- a) El Responsable de la Información tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- b) Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS.
- c) La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.
- d) Gestiona los riesgos de la seguridad de la información y la aceptación del riesgo residual, junto con la Dirección, siendo el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- e) Garantiza el apropiado establecimiento del SGI.

4.2.4 Responsable del Servicio

El Responsable del Servicio es designado por la Dirección Ejecutiva y tiene siguientes funciones asignadas:

- a) El Responsable del Servicio tiene la potestad de determinar los niveles de seguridad de los servicios.
- b) Incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas.
- c) Valorar las consecuencias de un impacto negativo sobre la seguridad de los servicios

4.2.5 Delegado de Protección de Datos

El Delegado de Protección de datos es el responsable de las siguientes funciones:

- a) Privacidad y protección de datos.
- b) Revisión y actualización del aviso legal de la página web.
- c) Control, revisión y actualización de las políticas de privacidad (web y demo) y política de cookies.
- d) Asistencia legal al equipo técnico en el desarrollo de nuevas soluciones (protección de datos).

- e) Soporte al equipo comercial en la investigación de legislación internacional y elaboración de informes.
- f) Elaboración y revisión de acuerdos de encargo de tratamiento.
- g) Apoyo legal en el proceso de homologación de proveedores.
- h) Responsable de acordar y supervisar la ejecución de las evaluaciones de impacto de tratamiento de datos especialmente protegidos cuando proceda. En esos casos, y juntamente con el área técnica, se adoptarán las medidas de seguridad que sean necesarias para eliminar o minimizar los riesgos identificados y analizados.
- i) Informar y asesorar al responsable o encargado del tratamiento, parar tratar datos personales bajo su autoridad directa.
- j) Actuar como punto de contacto de la autoridad de control.

4.3 Comités de seguridad

4.3.1 Gobierno Corporativo SGI

Con el fin de garantizar un alto peso específico en Facephi del Gobierno Corporativo, se le ha dotado de la siguiente composición.

- CEO
- Director General
- CTO
- Director Legal
- Directora People & Culture

Aparte de los miembros fijos que lo forman, podrá convocarse a las reuniones de este a aquellos, internos y externos, cuya presencia se considere de importancia estratégica.

Este comité se utilizará para resolver conflictos de responsabilidad que puedan aparecer entre los responsables y/o diferentes áreas de la organización, elevando aquellos casos en los que no tenga autoridad suficiente para decidir.

4.3.2 Dirección Ejecutiva SGI

Por su carácter práctico, está formada por los miembros de Facephi más inmediatamente responsables de la puesta en práctica de las directrices dadas por el Gobierno Corporativo:

- Responsable de la Información
- Responsable de Sistemas

- Responsable de Seguridad
- Responsable de GRC

Tal como en el Gobierno Corporativo, se podrá convocar presencia de aquellos miembros, exclusivamente de la organización, cuya presencia sea trascendente para la definición y ejecución de alguno de los planes que se pretendan establecer.

Para más detalle de las responsabilidades de los órganos que forman parte del Comité de Seguridad se puede consultar el procedimiento de **Roles, responsabilidades y atribuciones**.

5 Principios y requisitos de seguridad

Facephi, en conformidad con el artículo 12 del Esquema Nacional de Seguridad, ha establecido los siguientes principios básicos y requisitos mínimos de seguridad:

- La seguridad en Facephi se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de información.
- La seguridad de los sistemas de información contemplará los aspectos de prevención, detección y corrección de amenazas para conseguir que estas no se materialicen o afecten a la información y servicios que presta Facephi.
- Se dará gran importancia a la concienciación de quienes intervienen en el proceso y a sus responsables, para prevenir riesgos de seguridad.
- Los accesos a los sistemas de información serán controlados y serán otorgados siguiendo el principio de "mínimo privilegio" y a los usuarios estrictamente necesarios.
- La seguridad de los sistemas de información será atendida, revisada y auditada por personal cualificado durante todo su ciclo de vida.
- Las zonas e instalaciones donde se ubiquen los sistemas de información deberán permanecer en áreas controladas y disponer de mecanismos adecuados y proporcionales.
- La adquisición de productos de seguridad y la contratación de servicios de seguridad deberán proporcionarse al nivel de seguridad requerido.
- El personal de Facephi, ya sea propio o ajeno, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad.
- Se deberá aplicar la debida atención a la información almacenada o en tránsito a través de los equipo o dispositivos portátiles.
- Se deberá registrar las actividades de los usuarios, reteniendo la información estrictamente necesaria, para monitorizar actividades indebidas o no autorizadas.
- Los incidentes de seguridad se deberán tratar conforme al procedimiento de gestión de incidentes. Cualquier empleado debe comunicar dichos incidentes a security@facephi.com.
- Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad del servicio.

- El sistema deberá disponer de una estrategia de protección constituida por múltiples capas de seguridad distribuidas de forma que cuando una se vea comprometida, se pueda:
 - Ganar tiempo para una reacción adecuada frente a los incidentes
 - Reducir la posibilidad de que los sistemas se vean comprometidos en su conjunto
 - Minimizar el impacto final sobre los sistemas
- Estas líneas de defensa deberán estar constituidas por medidas de naturaleza organizativa, física y lógica.
- Las medidas de seguridad se reevaluarán y actualizarán de forma periódica para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

6 Riesgos derivados del tratamiento de Datos de carácter personal

A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en las normas de referencia, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

Para la consecución del fin pretendido, la protección de la Información de Identificación Personal (IIP) datos personales, la ISO 27701 especifica los requisitos y proporciona una guía para implementar, mantener y mejorar un Sistema de Gestión de la Privacidad de la Información (SGPI) como extensión de la ISO 27001 para la gestión de la privacidad en el contexto de organización.

7 Gestión de riesgos

El análisis y gestión de riesgos es parte esencial del proceso de seguridad en Facephi. Todos los sistemas sujetos a esta Política deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis deberá realizarse:

- Regularmente, al menos una vez al año
- Cuando cambie la información o los servicios manejados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Los resultados del análisis de riesgos deberán ser trasladados al Comité de Gobierno Corporativo.

8 Información documentada

Este apartado de “Información documentada” tiene por objeto establecer un control de toda la documentación aplicable dentro del SGI.

Es el Responsable de la Información, o persona que este delegue, el encargado de gestionar cualquier labor relativa a la elaboración, control y gestión de la información documentada.

Para más detalle de este apartado se puede consultar el documento **de control y gestión de la información documental**, en este se desarrollan los puntos más importantes que son:

- Documentación de origen interno
- Codificación de documentos
- Elaboración y aprobación de los documentos
- Revisión de la documentación
- Archivo y distribución de la documentación
- Control de la documentación obsoleta
- Control de los registros
- Documentación externa