

Política de Seguridad de la Información

01. Introducción

En este documento se describen los principios donde se sostiene la **Política de Seguridad de la Información** de **Health in Code, S.L.** La Organización depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos.

Esta Política de Seguridad sigue las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional (CCN), centro adscrito al Centro Nacional de Inteligencia (CNI) y se elabora cumpliendo con la exigencia del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), en el ámbito de la Administración Electrónica, que en su artículo 12 establece la obligación a las Administraciones Públicas y a los proveedores de servicios de las Administraciones públicas de disponer de una Política de Seguridad e indica los requisitos mínimos que debe cumplir.

Además, con esta política se pretende dar cumplimiento a los requerimientos de la norma *ISO/IEC 27001*.

02. Alcance

La presente Política de Seguridad es aplicable a los siguientes los Sistemas de información de la organización y que están definidos en la categorización de los servicios e información.

03. La seguridad como proceso integral

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes. Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que toda la organización debe aplicar las medidas mínimas de seguridad exigidas por el **Esquema Nacional de Seguridad** (en adelante, **ENS**) y el estándar de seguridad internacional *ISO/IEC 27001*, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículos 7 del ENS y los apartados del 5.24 al 5.30 de la norma *ISO/IEC 27001*.

03.1. Prevención

Health in Code, S.L. debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, la organización debe:

- ↳ Autorizar los sistemas antes de entrar en operación.
- ↳ Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- ↳ Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

03.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y

actuar en consecuencia según lo establecido en el ENS y en la norma estándar de la seguridad de la información.

La monitorización es especialmente relevante cuando se establecen líneas de defensa. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

03.3. Respuesta

Health in Code, S.L. debe:

- ↳ Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- ↳ Designar puntos de contacto para las comunicaciones con respecto a incidentes detectados en la entidad o en otros organismos relacionados con Health in Code S.L.

03.4. Recuperación

Para restaurar la disponibilidad de los servicios, se deberán desarrollar planes de contingencia de los sistemas TIC que actividades de recuperación de la información que contribuyan a la continuidad del servicio.

04. Misión

Como respuesta a un nuevo entorno tecnológico donde la convergencia entre la informática y las comunicaciones está facilitando un nuevo paradigma de productividad para las empresas y trazabilidad, Health in Code, S.L. está altamente comprometida en mantener un servicio competitivo siguiendo un modelo de negocio responsable basado en la búsqueda permanente del equilibrio económico, social y ambiental, donde el desarrollo de buenas prácticas en Seguridad de la Información es fundamental para conseguir los objetivos de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y legalidad de toda la información gestionada.

Se ha diseñado una Política de Seguridad de la Información cuyos objetivos principales son:

- **Proteger**, mediante controles/medidas, los **activos** frente a amenazas que puedan derivar en incidentes de seguridad.
- **Paliar** los efectos de los **incidentes de seguridad**.
- Establecer un sistema de **clasificación de la información** y los datos con el fin de proteger los **activos críticos** de información.
- **Definir las responsabilidades** en materia de seguridad de la información generando la estructura organizativa correspondiente.
- **Elaborar un conjunto de reglas**, estándares y procedimientos aplicables a los órganos de dirección, empleados, socios, proveedores de servicios externos, etc.
- **Especificar** los efectos **que conlleva el incumplimiento** de la Política de Seguridad en el ámbito laboral.
- **Evaluar los riesgos** que afectan a los activos con el objeto de adoptar las medidas/controles de seguridad oportunos.
- Verificar el funcionamiento de las medidas/controles de seguridad mediante **auditorías** de seguridad internas realizadas por auditores independientes.
- **Formar a los usuarios** en la gestión de la seguridad y en tecnologías de la información y las comunicaciones.
- **Controlar el tráfico de información** y de datos a través de infraestructuras de comunicaciones o mediante el envío de soportes de datos ópticos, magnéticos, en papel, etc.
- **Observar y cumplir la legislación** en materia de protección de datos, propiedad intelectual, laboral, de servicios de la sociedad de la información, penal, etc., que afecte a los activos de Health in Code S.L.
- **Proteger el capital intelectual** de la organización para que no se divulgue ni se utilice ilícitamente.
- **Reducir** las posibilidades de **indisponibilidad** a través del uso adecuado de los activos de la organización.
- **Defender los activos** ante ataques internos o externos para que no se transformen en incidentes de seguridad.
- **Controlar** el funcionamiento de las **medidas de seguridad** averiguando el número de incidencias, su naturaleza y efectos.

05. Marco normativo complementario

La base normativa que afecta el desarrollo de las actividades y competencias de **Health in Code, S.L.** que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está constituida por toda la legislación y normativa sobre la materia que se encuentre vigente en cada momento.

El mantenimiento del marco normativo será responsabilidad de **Health in Code, S.L.** conforme a lo establecido en el procedimiento **HIC-PG-09 Legal requirements identification**. El registro de la legislación aplicable quedará reflejado en el documento **HIC-PG-09-F-01 Legal requirements**, y la normativa de referencia se incluirá en la pestaña "Documentación externa" del **HIC-PG-00-F-01 List of current documentation**. Dicho mantenimiento incluye las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN).

Así mismo, la **Health in Code, S.L.** también será responsable de identificar las guías de seguridad del CCN, que serán de aplicación para mejorar el cumplimiento de lo establecido en el ENS.

06. Cumplimiento de los requisitos mínimos de seguridad

Health in Code, S.L., para lograr el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), que recoge los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

06.1. La seguridad como un proceso integral y mínimo privilegio

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad en **Health in Code, S.L.**, estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y coordinación, o de instrucciones inadecuadas, constituyan fuentes de riesgo para la seguridad.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

- A. El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
- B. Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
- C. En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
- D. Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

06.2. Vigilancia continua, reevaluación periódica e integridad, actualización del sistema y mejora continua del proceso de seguridad

La vigilancia continua por parte de **Health in Code, S.L.** permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

06.3. Gestión de personal y profesionalidad

Todo el personal, propio o ajeno relacionado con los sistemas de información de **Health in Code, S.L.**, dentro del ámbito del ENS, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente. De igual modo, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados.

06.4. Gestión de la seguridad basada en los riesgos, análisis y gestión de riesgos

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II del ENS, se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Todos los sistemas sujetos a esta Política de Seguridad realizarán un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

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

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

06.5. Incidentes de seguridad, prevención, detección, reacción y recuperación

Health in Code, S.L., dispone de procedimientos de gestión de incidentes de seguridad de la información de acuerdo con lo previsto en el artículo 33 del ENS, la Instrucción Técnica de Seguridad correspondiente, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los

servicios que presta. Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse. Las medidas de detección irán dirigidas a descubrir la presencia de un incidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico. De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

06.6. Líneas de defensa y prevención ante otros sistemas de información interconectados

Health in Code, S.L., ha implementado una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, integradas por medidas organizativas, físicas y lógicas, de tal forma que cuando una capa ha sido comprometida permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema de **Health in Code, S.L.** se conecte a redes públicas, tal y como se definen en la legislación vigente en materia de telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

06.7. Responsabilidades, organización e implantación del proceso de seguridad

Health in Code, S.L., ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "*Organización y Gestión de la Seguridad de la Información*" del presente documento.

06.8. Autorización y control de los accesos

Health in Code, S.L., ha implementado mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

06.9. Protección de las instalaciones

Health in Code, S.L., ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

06.10. Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos o la contratación de servicios de seguridad **Health in Code, S.L.**, se tendrá en cuenta, de forma proporcionada a la categoría del sistema y al nivel de seguridad establecido, la adquisición de aquellos que cuenten con la funcionalidad de seguridad certificada relacionada con el objeto de la adquisición. Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

06.11. Protección de la información almacenada y en tránsito y continuidad de la actividad

Health in Code S.L., prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el RD 311/2022, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

06.12. Registro de actividad y detección de código dañino

Health in Code S.L., con el propósito de satisfacer el objeto del real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos (RGPD) y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, Health in Code S.L. podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

07. Organización de la seguridad

En el marco de cumplimiento la Norma *ISO/IEC 27001* y del ENS, y a fin de conformar la estructura de responsables en materia de seguridad, se han determinado los siguientes roles principales:

- **Responsable de la Información**, responsable del uso que se haga de una cierta información y, por tanto, de su protección.
- **Responsable de Servicio**, responsable por establecer los requisitos del servicio en materia de seguridad.
- **Responsable de Seguridad de la Información**, es el responsable de establecer y mantener las Políticas de Seguridad de la Información, estándares, directivas y procedimientos de la Organización.
- **Responsable del Sistema**, responsable de la infraestructura de sistemas y comunicaciones.

Adicionalmente, la atención, revisión y auditoría de la seguridad de los sistemas será realizada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida:

- **Empleados/usuarios/personal externo**: conocimiento de las políticas y procedimientos de Health in Code, S.L. y las directrices definidas en los mismos.

07.1. Comité de seguridad

El **Comité de seguridad de la información**, (en adelante Comité de seguridad) coordina la seguridad de la información a nivel de organización.

De acuerdo con el ENS las funciones indicadas que corresponden al Comité de seguridad son:

- ① Elaborar (y revisar periódicamente) la Política de Seguridad de la información para que sea aprobada por el CEO de Health in Code S.L.
- ① Aprobar y divulgar los procedimientos de seguridad de Health in Code S.L.
- ① Promover la mejora continua de la gestión de la seguridad de la información de Health in Code S.L.
- ① Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- ① Evaluar los principales riesgos residuales asumidos por Health in Code S.L. y recomendar posibles actuaciones respecto de ellos.
- ① Evaluar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de los empleados en la gestión de incidentes de seguridad de la información.
- ① Promover la realización de las auditorías periódicas y evaluar el cumplimiento de las obligaciones de la organización en materia de seguridad.
- ① Priorizar las actuaciones en materia de seguridad de acuerdo con los recursos disponibles.
- ① Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- ① Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de Health in Code S.L. elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- ① Evaluar las necesidades de recursos requeridos para el cumplimiento de los planes de actuación derivados de la aplicación de la Política de Seguridad.
- ① Elaborar un informe anual que elevará a la Dirección (CEO) de Health in Code S.L.

El Comité de Seguridad estará formado por:

- **Representante de Dirección (CEO)**, que presidirá el comité.
- **Responsable de Seguridad de la Información**, que actuará como secretario del comité.
- **Responsable del servicio**, que actuará como vocal.
- **Responsable de la información**, que actuará como vocal.
- **Responsable del sistema**, que actuará como asesor.

El Comité de Seguridad no es un comité técnico, pero requerirá regularmente del personal técnico propio o externo la información pertinente para tomar decisiones. El Comité de Seguridad se asesorará en los temas sobre los que tenga que decidir o emitir una opinión.

El detalle de las responsabilidades se encuentra recogido en el documento **HIC-PG-02-F-05 DPT**, disponiendo de un registro específico para cada puesto.

07.2. Procedimientos de designación

El desempeño de las responsabilidades definidas en esta Política de Seguridad vendrá determinado por el acceso a los diferentes cargos que se han vinculado a ellas. En el caso de que desapareciese o cambiase de denominación alguno de estos cargos será competencia de la dirección de la organización asignar el nuevo puesto al que quedará vinculada la figura.

07.3. Protección de la información almacenada y en tránsito y continuidad de la actividad

Periódicamente, y en todo caso no superando el plazo de un año, el Comité revisará la vigencia y razonabilidad de la presente política y se llevarán a cabo las mejoras, adaptaciones o modificaciones requeridas en función de los cambios organizativos, técnicos o regulatorios aplicables.

El Responsable de Seguridad de la Información ayudará a construir, mantener y publicar la Política de Seguridad de la Información, si bien, es la Dirección (CEO) de **Health in Code, S.L.** el responsable de la aprobación de dicha Política.

Cualquier cambio o evolución que afecte o pudiera afectar al contenido de la Política de Seguridad de la Información quedará registrado en una nueva firma del documento de aprobación. De esta forma se concreta y confirma el compromiso de estas entidades por la seguridad de la información.

08. Datos de carácter personal

Health in Code, S.L. realiza tratamientos en los que hace uso de datos de carácter personal sometidos a lo dispuesto por el Reglamento 679/2016, del Parlamento Europeo y del Consejo, de 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 (Reglamento General de Protección de Datos-RGPD-) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, respetando, en todo caso, el derecho fundamental a la protección de datos personales, la intimidad y el resto de los derechos fundamentales reconocidos tanto en la legislación y tratados internacionales como en la Constitución vigente.

Las políticas de seguridad aplicables a los tratamientos se rigen por las medidas de seguridad implantadas de acuerdo con el Anexo II (Medidas de seguridad) del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Además, se dispone de un RAT (Registro de Actividades del Tratamiento) donde se indexan los distintos tratamientos de datos afectados por la normativa.

Todos los sistemas de información de **Health in Code, S.L.** se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal. El Delegado de protección de Datos de **Health in Code, S.L.** velará por el cumplimiento del RGPD y de la LOPDGDD.

De acuerdo con lo anterior, **Health in Code, S.L.** dispone de una Política de Protección de Datos establecida en el Manual de Políticas Corporativas.

09. Desarrollo de la Política de Seguridad

Esta Política se desarrolla por medio de una Normativa de Seguridad que afronta los aspectos específicos. La Normativa de Seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. La normativa de seguridad estará disponible para el personal de **Health in Code, S.L.** a través de la herramienta de gestión de documentación.

10. Directrices para la estructuración de la documentación de seguridad del sistema, gestión y acceso

Todos los documentos que forman el sistema de gestión tendrán una reseña con quién ha revisado el documento y quién lo ha aprobado. Preferentemente, los documentos del sistema de gestión de la seguridad de la información tendrán que ser revisados por el Responsable de Seguridad y aprobado por la Dirección.

Toda la documentación del sistema de gestión de la seguridad de la información estará ubicada en una unidad compartida del sistema de **Health in Code, S.L.** Esta unidad será de edición para los miembros del Comité de seguridad. El resto del personal tendrá acceso de lectura a los documentos, ubicados en esta unidad, que deban conocer o que el Comité de seguridad estime oportuno.

La unidad donde se ubique toda la documentación de seguridad del sistema deberá permitir gestionar versionado de los documentos, así como la revisión de la actividad realizada en dicha documentación.

11. Obligaciones del personal

Todos los miembros de **Health in Code, S.L.** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad desarrollada a partir de ella, siendo responsabilidad del Comité de seguridad disponer los medios necesarios para que la información llegue a los implicados.

Todos los trabajadores del **Health in Code, S.L.** bajo el alcance del ENS e *ISO/IEC 27001*, atenderán a una acción de concienciación en materia de seguridad TIC, al menos, una vez cada dos años. Se establecerá un programa de acciones en concienciación continua para atender a todos los miembros de **Health in Code, S.L.**, en particular a los de nueva incorporación, teniendo en cuenta siempre las disponibilidades presupuestarias de Health in Code S.L.

En su caso, si se requiere formación específica para el manejo seguro de los sistemas, las personas con responsabilidad en la operación o administración de sistemas TIC la recibirán en la medida en que la necesiten para realizar su trabajo.

12. Terceras partes

Cuando [Health in Code, S.L.](#) preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Para ello, se establecerán canales para información y coordinación de los respectivos Comités de seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando [Health in Code, S.L.](#) utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que implique a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, con ello, el proveedor deberá garantizar que su personal está adecuadamente formado en materia de seguridad de acuerdo con los requerimientos de [Health in Code, S.L.](#)

13. Entrada en vigor

La presente **Política de Seguridad de la Información** es efectiva desde el día siguiente al de su fecha de aprobación por la Dirección de [Health in Code, S.L.](#) y hasta que sea reemplazada por una nueva Política.

Se dispondrá de los medios para publicar, dar a conocer y facilitar el cumplimiento de esta política y de los documentos que la desarrollan, así como para verificar su aplicación y efectividad. Asimismo, habilitará canales de participación que permitan, a los destinatarios de esta política y de los documentos complementarios, participar en su revisión y mejora.

21 de enero de 2026

José María Fernández Ortega

CEO — Health in Code, S.L.