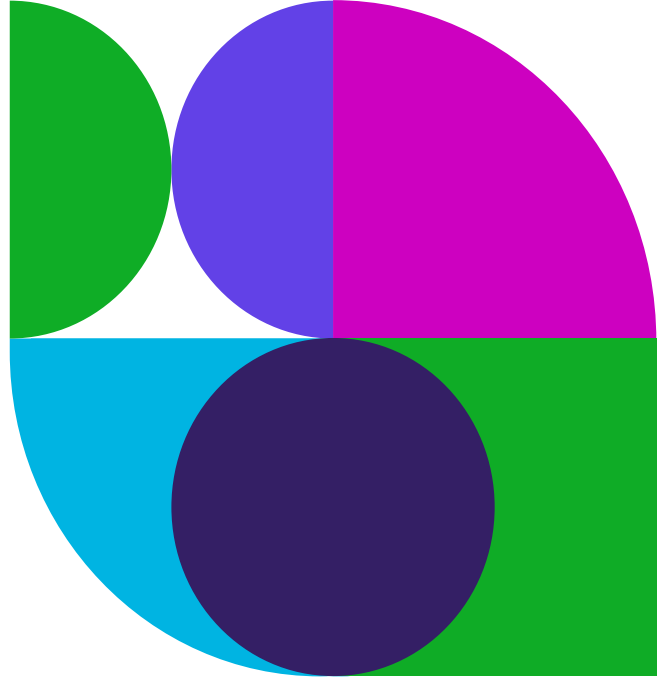




Política de Seguridad de la Información

Teladoc Health International

Versión 1.1

INDICE

1. Objetivo.....	3
2. Alcance.....	3
3. Comunicación y actualización.....	3
4. Cumplimiento	3
5. Principios básicos de la Seguridad de la Información	3
6. El marco de la Seguridad de la Información	4

1. Objetivo

El objetivo de este extracto de la Política de Seguridad de la Información de Teladoc Health International (en adelante "Teladoc Health") es proporcionar directrices y soporte de gestión para la Seguridad de la Información, de acuerdo con los requisitos de negocio y las leyes y regulaciones que afectan a la compañía, así como una afinidad con el marco de políticas de Teladoc Health Inc. El marco normativo de Teladoc Health proporciona las políticas, procesos y procedimientos que, junto con las medidas de carácter legal y las regulaciones vigentes, constituye el Sistema de Gestión de Seguridad de la Información (SGSI) que Teladoc Health International establece y gestiona, basado en la norma ISO/IEC 27001.

2. Alcance

El alcance del contenido en la presente Política cubre a todas las personas, tanto empleados propios como terceras partes implicadas en las actividades de Teladoc Health, incluyendo oficinas, aplicaciones informáticas, centros de datos y cualquier otra ubicación donde haya activos de información de Teladoc Health en cualquier formato.

3. Comunicación y actualización

El presente documento estará al alcance de todas las partes interesadas debidamente publicado y actualizado en la [web](#) de Teladoc Health.

La presente Política se revisará y aprobará, al menos una vez al año, por la Dirección de Teladoc Health o cuando se produzcan cambios significativos en nuestro entorno de riesgo. Se garantizará su actualización con el fin de anticipar y abordar futuros riesgos y amenazas para la Seguridad de la Información.

4. Cumplimiento

El cumplimiento de esta Política, y de las políticas temáticas, los procesos y procedimientos derivados de ésta, es obligatorio. Es voluntad de la Dirección de Teladoc Health que se cumplan o superen los requisitos descritos en los documentos que son parte del SGSI.

5. Principios básicos de la Seguridad de la Información

Proteger la confidencialidad, integridad y disponibilidad de la información es esencial para lograr los objetivos, velar por la reputación de Teladoc Health y obtener la confianza de los pacientes, clientes, y otras partes interesadas.

El compromiso se fundamenta en los siguientes principios básicos de Seguridad de la Información:

- **Garantizar que los requerimientos legales, regulatorios y contractuales** vigentes se cumplen en el tratamiento y gestión de la información.
- **Evaluar los riesgos que puedan afectar a la información** e implementar medidas para su control y mitigación, teniendo en cuenta el impacto que tendrían en la organización.
- **Asegurar la adecuada clasificación de la información**, en función de su criticidad, aplicando los controles necesarios para su correcta gestión.

- **Aplicar medidas de Seguridad** alineadas con las necesidades y objetivos de negocio durante todo el ciclo de vida de la información, independientemente del sistema y forma de tratamiento.
- **Asegurar la disponibilidad de los Sistemas de Información** implementando Planes de Recuperación de Desastres y de Continuidad de Negocio, con el objetivo de restablecer los Sistemas de Información y procesos críticos de negocio en el tiempo acordado.
- **Fomentar la concienciación y formación** con actividades relacionadas con las buenas prácticas en Seguridad de la Información.
- **Garantizar la adecuada gestión de incidentes** que puedan afectar a la información de Teladoc Health en su conjunto.
- **Actuar con diligencia respecto a proveedores de servicios**, en especial aquellos que vayan a realizar tratamientos de datos de carácter personal y/o información confidencial de la organización.
- **Orientar hacia la mejora continua la gestión de la Seguridad de la Información** para que sea adecuada y eficaz, reevaluando periódicamente las medidas para adaptarlas a la constante evolución de los riesgos y sistemas de protección.

6. El marco de la Seguridad de la Información

Sobre la base de esta Política y el marco de políticas de Seguridad de la Información, la ISO/IEC 27001 define los requisitos detallados para los sistemas de información que cubren, en particular, en lo que respecta a los siguientes controles:

Controles organizacionales abarcan diferentes temas como:

- La Seguridad de la Información y la gestión de activos de la organización;
- La gestión, el tratamiento y todos los procesos que se deben seguir para evitar brechas de Seguridad;
- Las personas implicadas en cada proceso;
- Los contactos de las partes interesadas en cada proceso, por ejemplo, pacientes, clientes, proveedores, autoridades, empleados u otros que puedan ser necesarios;
- La respuesta ante cualquier posible incidente intencionado o no intencionado;
- Los requisitos legales y el cumplimiento de las políticas, procesos y procedimientos de Seguridad de la Información.

Controles orientados a las personas definen cómo los empleados y terceros interactúan con los datos. Este conjunto de controles incluye:

- La Seguridad del personal, la gestión del capital humano y la formación y concienciación;
- La gestión de procesos disciplinarios en caso de incumplimiento;
- El teletrabajo y la gestión remota de la información.

Controles físicos garantizan la Seguridad de los activos tangibles, tales como:

- Los sistemas de entrada, los procesos de disposición de activos y puesto de trabajo despejado;
- Las áreas de trabajo seguras y protegidas;
- El mantenimiento de los equipos y el impacto medioambiental;
- La seguridad y el mantenimiento del hardware, las instalaciones y los equipos de la organización.

Controles tecnológicos regulan el control y acceso a la información almacenada, procesada y accesible desde cualquier dispositivo, incluyendo:

- La gestión de accesos, de las redes y la transferencia segura de información;
- La protección ante cualquier ataque, fuga de datos, brechas de seguridad y gestión de vulnerabilidades en los sistemas de información;
- La recuperación de toda la información interna en caso de incidente;
- La protección de la configuración de los dispositivos;
- El desarrollo seguro de las aplicaciones.

Todos los controles definidos para el SGSI de Teladoc Health están comprendidos en el marco normativo de las políticas, procesos y procedimientos junto con las medidas de carácter legal, técnico y organizativo y las regulaciones vigentes.

Presidente de Teladoc Health International

Política de seguridad de la información v1.1 (20/07/2026)