SEGURIDAD DE LA INFORMACIÓN

Política

Abril 2026

SEGURIDAD DE LA INFORMACIÓN

Finanzas · innovación · Tecnología

Autor(es)	**Dirección de Seguridad de la Información**
Fecha Revisión	06 de abril de 2026

HISTORIA DE REVISIONES Y CAMBIOS

Versión / Fecha Modificación	Revisado por	Aprobaciones	Cargo aprobador	Descripción de la modificación/Revisión
V 1.0 01/04/2025	Fabián Díaz	Comité de Seguridad de la Información	Integrantes del Comité	Documento Inicial
V 2.0 06/05/2026	Linda Milena Alvarez	Comité de Seguridad de la Información	Integrantes del Comité	Revisión, cambios menores 2.3

Tabla de contenido

1. Preliminares

1.1. Objetivo del documento

El propósito de este documento es establecer la Política General de Seguridad de la Información para las empresas que hacen parte del ecosistema del FiT Group, reafirmando el compromiso de la organización con la protección de sus activos, el cumplimiento normativo y la salvaguarda de la confidencialidad, integridad y disponibilidad de la información.

Es aplicable a FiT Group, conformado por:

- TODO1 SERVICES INC. DBA iuvity, incluyendo:
  - Integra2 LLC
  - iuvity Colombia LTDA
  - Xperience Customer Management SAS
  - Facturanet Servicios Digitales SAS
  - Unosystems SA
  - iuvity de México S. de RL de CV
- ITC Soluciones Tecnológicas SAS
- Neurona Tecnología Financiera SAS

1.2. Alcance

Esta política es aplicable a todas las empresas que conforman el FiT Group, incluyendo sus activos de información y la totalidad de sus colaboradores; asimismo, se extiende a proveedores de servicios y consultores vinculados a su ecosistema.

Todas las personas naturales o jurídicas que mantengan relaciones contractuales o extracontractuales con las compañías del FiT Group deberán cumplir estrictamente con las políticas, procedimientos y estándares establecidos en materia de seguridad de la información, con el objetivo de garantizar la protección de los datos y la infraestructura tecnológica.

1.3. Documentos de Referencia

Este documento se encuentra alineado a los requerimientos de la norma ISO/IEC 27001:2022 y toma como referencia:

- ISO/IEC 27000:2018 — Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Visión general y vocabulario.
- ISO/IEC 27001:2022 — Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos.
- ISO/IEC 27002:2022 — Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información.

1.4. Vocabulario

- **ACTIVO DE INFORMACIÓN:** Información o elemento relacionado con su tratamiento (sistemas, hardware, software, aplicaciones, infraestructura, servicios) que tenga valor para FiT Group.
- **BASE DE DATOS:** Conjunto organizado de datos personales objeto de tratamiento.
- **BORRADO SEGURO:** Método que sobrescribe la información en un medio de almacenamiento con datos sin significado, haciéndola irrecuperable.
- **CALIFICACIÓN DE LA INFORMACIÓN:** Estatus asignado a la información según riesgo y exposición.
- **CIFRADO**: Proceso que convierte información en ilegible mediante un algoritmo matemático.
- **CLASIFICACIÓN DE LA INFORMACIÓN**: Determinación del nivel de protección que requiere la información según políticas de FiT Group.
- **CONFIDENCIALIDAD**: Propiedad que impide que la información sea revelada a personas o procesos no autorizados.
- **CONTROL DE ACCESO:** Restricción y autorización del acceso a activos según requisitos comerciales y de seguridad.
- **DATOS SENSIBLES:** Información que afecta la intimidad o puede generar discriminación (origen racial, orientación política, religión, salud, vida sexual, datos biométricos).
- **DISPONIBILIDAD**: Propiedad que asegura que la información esté accesible y utilizable por entidades autorizadas.

- **INCIDENTE DE SEGURIDAD:** Evento que indica posible incumplimiento de la política de seguridad o falla de controles.
- **MALWARE**: Programa o código malicioso que daña sistemas.
- **NO REPUDIO:** Capacidad de demostrar la ocurrencia de un evento y su origen.
- **SEGURIDAD DE LA INFORMACIÓN:** Conjunto de procesos para proteger sistemas, medios e instalaciones que gestionan información crítica.
- **SISTEMA DE GESTIÓN:** Estructura para administrar y mejorar políticas, procedimientos y procesos.
- **TIEMPO DE CONSERVACIÓN:** Periodo en que se mantienen registros en papel o medio electrónico según ley u organización.

1.5. Documentos Relacionados

POLÍTICAS
FIT SIG_POL_002_Política Uso Aceptable de Activos de Información FIT SIG_POL_004_Política Clasificación de la Información
PROCESOS
N/A
PROCEDIMIENTOS
N/A
INSTRUCTIVOS
N/A
FORMATO
FIT SIG_FOR_014_Conocimiento Políticas de Seguridad

2. Desarrollo

2.1. Principios Rectores

FiT Group ha establecido políticas generales de seguridad que definen las reglas y lineamientos para determinar los niveles de protección requeridos por cada activo de información, según su calificación. Estas políticas también establecen las responsabilidades derivadas del incumplimiento de dichas reglas.

La información constituye uno de los activos más valiosos para FiT Group y es esencial para su desarrollo, crecimiento y sostenibilidad. Por ello, se requiere la adopción de medidas integrales que garanticen su protección y salvaguarda.

La gestión de la seguridad de la información busca identificar vulnerabilidades y mitigar amenazas, asegurando la confidencialidad, integridad, disponibilidad y no repudio. Su objetivo es minimizar riesgos y maximizar el valor, la continuidad del negocio y las oportunidades estratégicas dentro del ecosistema FiT Group. A continuación, se presentan los principios que rigen la seguridad de la información en la organización:

1. **Confidencialidad:** Propiedad que garantiza que la información es accesible sólo por el personal autorizado.
2. **Integridad:** Propiedad que garantiza la exactitud y completitud de la información y sus procesos de tratamiento, comunicación y almacenamiento.
3. **No repudio:** Propiedad que permite probar la participación de las diferentes partes en una comunicación.
4. **Disponibilidad:** Propiedad que permite utilizar la información en la forma y tiempo requeridos.

2.2. Lineamientos de Seguridad

La Política de Seguridad de la Información constituye una herramienta estratégica que promueve la conciencia sobre la importancia y sensibilidad de la información dentro de FiT Group. Este documento define las políticas basadas en el estándar ISO 27001, orientadas a mitigar los riesgos asociados a los activos de información y su infraestructura.
Su propósito es garantizar que todas las empresas del ecosistema FiT Group cumplan con las leyes, regulaciones y estándares aplicables, de modo que sus operaciones se desarrollen de forma segura y en conformidad con la normativa vigente, así como con los requisitos y expectativas de las partes interesadas del Sistema de Gestión.

Para ello, FiT Group implementa un Sistema de Gestión de Seguridad de la Información (SGSI) que permite gestionar adecuadamente los riesgos, alineado con la planeación estratégica y el propósito superior de la organización. Este sistema asegura la preservación de la confidencialidad, integridad, disponibilidad y no repudio de la información, reafirmando el compromiso corporativo con la protección de los activos y la continuidad del negocio.

1. La protección de la información y sus instalaciones de procesamiento como parte de una estrategia orientada a la gestión de riesgos, la continuidad del negocio y la consolidación de una cultura de seguridad de la información.

2. Identificación y gestión adecuada de los riesgos asociados con la pérdida de confidencialidad, integridad, no repudio y disponibilidad de la información, a los cuales se exponen los activos de información, con el fin de garantizar el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.
3. La alineación de los objetivos de seguridad de la información con los objetivos estratégicos y las necesidades de negocio de la organización.
4. La integración de la seguridad de la información en todas las fases del ciclo de vida de la información, sistemas tecnológicos y procesos de la organización.
5. Designar y mantener la disponibilidad de los recursos necesarios para el SGSI, los cuales deben ser adecuados para el desarrollo de este.
6. Promover la importancia de la gestión de seguridad de la información eficaz y conforme con los requisitos del SGSI.
7. El seguimiento del SGSI en busca de la mejora continua y asegurando que consigue los resultados previstos.
8. Regirse por un cuerpo normativo de cumplimiento obligatorio que responde a las necesidades de la organización.
9. El cumplimiento con los requerimientos legales y normativos aplicables y la alineación con los estándares y buenas prácticas internacionalmente reconocidos.
10. Garantizar la gobernabilidad y gestión de la seguridad de la información, mediante la definición de una estructura organizacional de seguridad adecuada.
11. Establecer los lineamientos para el uso autorizado de grabaciones de reuniones virtuales realizadas mediante plataformas colaborativa, así como el procesamiento de dicha información mediante herramientas de inteligencia artificial como Copilot, garantizando la protección de los datos, la trazabilidad y el cumplimiento de los principios de confidencialidad, integridad, no repudio y disponibilidad.
12. Asegurar la difusión y el conocimiento de la Política de Seguridad para el SGSI.

2.3. Roles y Responsabilidades

En concordancia con el compromiso adquirido por la alta dirección con la adecuada gestión de la seguridad de la información, se definen los roles y responsabilidades asociados al Sistema de Gestión de Seguridad de la Información en el siguiente documento: **Manual del Sistema de Gestión de Seguridad de la Información.**

Los colaboradores, clientes, terceros (y sus delegatarios) que tengan interacción con los negocios y uso de la red, la información y/o la tecnología de la compañía, tienen a su disposición dos canales de comunicación:

- **Security Operations <secope@fitgroup.tech>** (eventos, incidentes o vulnerabilidades que puedan comprometer confidencialidad, integridad, no repudio y disponibilidad de la

información, los sistemas o los activos tecnológicos de la organización. Esto incluye, pero no se limita a: accesos no autorizados, pérdida o robo de dispositivos, fallos de seguridad en aplicaciones o infraestructura, intentos de phishing, malware detectado, fuga de información, errores de configuración que expongan datos sensibles, uso indebido de credenciales, interrupciones del servicio, y cualquier comportamiento sospechoso que pueda representar una amenaza para la seguridad digital o física de la entidad.

- **Línea Ética FiT <lineaetica@fitgroup.tech>** (irregularidades, casos de fraude, corrupción, conflictos de interés, acoso laboral o sexual, discriminación, mal uso de recursos, violaciones a la privacidad, o cualquier comportamiento que atente contra la integridad, la transparencia o el respeto en el entorno laboral.

3. Cumplimiento y Sanciones

Esta política es parte integral del Sistema de Gestión de Seguridad de la Información y del conjunto de políticas de seguridad de FiT Group. Su cumplimiento es obligatorio para todos los colaboradores de las empresas del ecosistema FiT Group, así como para terceros y sus delegatarios que interactúen con los negocios, la red, la información y/o la tecnología de dichas compañías.

El incumplimiento de esta política puede estar sujeta a acciones disciplinarias, incluyendo la terminación del contrato laboral. En caso de que la infracción sea cometida por contratistas o proveedores, el contrato o servicio correspondiente podrá ser cancelado.

Estos lineamientos se encuentran publicados en el repositorio oficial y son accesibles para todos los colaboradores y terceros vinculados. Asimismo, como condición para mantener la relación contractual, todos los colaboradores, contratistas y proveedores deberán aceptar y firmar una Carta de Reconocimiento.

4. Cronograma de Revisión

El Comité de Seguridad de la Información de FiT Group revisará estas políticas al menos una vez al año y tras cualquier cambio significativo que impacte la gestión de la seguridad de la información, garantizando su actualización y alineación con los objetivos del negocio.

Las revisiones extraordinarias seguirán los procedimientos internos establecidos para la aprobación y modificación de políticas.

5. Control de Registro

Formato Utilizado	Política Seguridad de la Información
Código	FIT_SIG_POL_001
Registro que Origina	FIT_SIG_POL_001 Política Seguridad de la Información
Nivel de Clasificación	Uso Público
Tipo de Registro	Digital
Responsable de Elaboración/ Diligenciamiento	Dirección de Seguridad de la Información
Almacenamiento	FiT Group Home - FiT Group - Confluence
Acceso	Todos los funcionarios de FiT Group, proveedores y terceros
Tiempo de Conservación	Permanente
Responsable de Conservación	Comité de Seguridad de la Información
Disposición Final	De acuerdo con lo definido para documentos de Uso Público

6. Aprobación de la Política

Esta política ha sido revisada y aprobada por la Alta Dirección, demostrado el compromiso con la seguridad de la información y el cumplimiento de los requisitos aplicables.

Cargo en Alta Dirección	Nombre	Firma	Fecha
Representante Legal de FiT Group	Juan Felipe Gómez	Signed by: 1C7EBBF6B6D54CD...	23 de junio del 2026

Inicial FDV