Política de Seguridad de la Información
ISO/IEC 27001:2022, Esquema Nacional de Seguridad

1. Introducción

GRUPO VÍTALY es la compañía que tiene su origen en la fusión entre dos grandes del sector, Grupo Preving y Grupo Cualtis.

GRUPO VÍTALY es el resultado de un trabajo minucioso y cuidado durante meses en los que la Presidencia, los CEOs, Personal Directivo y Asesores Externos de ambas compañías han trabajado mano a mano a través de una Comisión creada a exprofeso.

La seriedad y el compromiso con nuestros clientes ha definido siempre nuestra actuación desde los inicios de ambos Grupos. La confianza que nos otorgan año tras año nos ha convertido en una de las empresas con más alto índice de renovación de nuestro sector.

En ***GRUPO VÍTALY*** creemos que la Calidad consiste en conocer las necesidades de nuestro sector y nuestros clientes brindando servicios y soluciones que satisfagan plenamente sus expectativas y al mismo tiempo dotar de nuestro s servicios tecnológicos de una plataforma de servicios integrales para la prevención, puntera en cuento al propio producto desde su desarrollo hasta su puesta en producción.

De igual forma creemos que la información interna y la de nuestros clientes es un activo de vital importancia para nuestro negocio, por ello la alta disponibilidad, la protección de la información y por tanto la seguridad, forma parte del valor principal que la organización inculca en sus procesos de producción y gestión.

Es por ello por lo que, en GRUPO VÍTALY, ofrecemos servicios de alta disponibilidad y protegemos toda nuestra información y la de nuestros clientes cumpliendo con controles de protección ante pérdidas, manipulaciones o divulgaciones no autorizadas.

Estos niveles de seguridad y calidad de servicios TI están basados en los controles y objetivos establecidos en la norma ISO/IEC 27001:2022 y Esquema Nacional de Seguridad, las legislaciones aplicables a la seguridad de la información en general y en el sector de la prevención de riesgos laborales, el comercio electrónico, y en especial el marco jurídico relacionado con protección de datos de carácter personal.

2. Alcance

Esta Política de Seguridad de la Información es de obligado cumplimiento para todas las empresas del grupo, que son:

- Vitaly Health Services S.L.U.
- Preving Investment Group S.L.
- Infobits S.L.
- Formalia Salud S.L.U.
- Adplusconsultores S.L.U.
- Gabinete de Medicina Preventiva y Salud Laboral S.L.

El alcance cubre todos los servicios indicados en este documento, en particular los relacionados con la prestación de servicios como Servicio de Prevención Ajeno, vigilancia de la salud, actividades técnicas, formación y consultoría.

3. Marco Normativo y Legal

La presente Política se establece siguiendo el compromiso de Vítaly con la ética, el cumplimiento legal y la seguridad de la información, y se desarrolla conforme a los principios y requisitos del Esquema Nacional de Seguridad sobre el RD 311/2022 y de la ISO 27001:2022. Este documento se alinea con las disposiciones legales vigentes en materia de protección de datos personales, servicios digitales y de la sociedad de la información, prevención de riesgos laborales, salud laboral, así como aquellas normativas sectoriales y específicas aplicables a la actividad de cada entidad integrante del grupo. Este marco normativo se complementa con el listado actualizado de legislación aplicable, que se mantiene disponible para su consulta por las partes interesadas autorizadas.

4. Misión

Nuestro Sistema de Gestión establece como principal objetivo de Seguridad de la Información las siguientes bases sobre las aplicaciones externas y aquellas internas necesarias para su funcionamiento:

- **Disponibilidad**: Para asegurar que todas las personas autorizados y procesos tengan acceso a la información cuando lo requieran.
- **Integridad**: Para preservar la veracidad, completitud de la información y los métodos de procesamiento.
- **Confidencialidad**: Para asegurar que a la información solo pueda ser accesible a las personas y procesos que cuenten con la autorización o con los permisos respectivos.
- **Trazabilidad.** Para asegurar que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad
- **Autenticidad.** Necesario para asegurar que la entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Para ello, la Dirección adquiere el compromiso de:

- Desarrollar controles y objetivos de control que permitan identificar y evaluar los riesgos de los activos de información.
- Cumplir con los requisitos de negocio, disposiciones legales, reglamentarias y obligaciones contractuales de seguridad.
- Dotar de los recursos y responsabilidades para implantar y mantener el proceso de mejora continua de la Gestión de la Seguridad de la Información y la Calidad de los servicios de la plataforma tecnológica.

Al igual que las políticas de seguridad y protección de datos, la evolución del producto y servicio Acércate también es de vital importancia para **GRUPO VÍTALY**, por ello y con el afán de ofrecer a nuestros Clientes la mejor solución para la gestión de su negocio, **GRUPO VÍTALY** evoluciona los servicios basándose en tres pilares fundamentales:

- **Cambios legales**: Estamos muy pendientes de los cambios legales que se puedan producir en los países donde tenemos presencia para actualizar el producto y que éste se adecue a les normativas y leyes vigentes de cada país.
- **Nuestros Clientes**: Valoramos y estudiamos los requerimientos solicitados por nuestros clientes y si estos aportan una mejora para el producto o para el servicio, se desarrollan i se incluyen en el estándar, de esta forma la aplicación crece para todos nuestros clientes.
- **Nuevas funcionalidades**: Comprometidos con la constante Investigación el diseño y la implementación (I+D+i) de nuevas tecnologías para brindar nuevas funcionalidades que puedan aportar un valor añadido a nuestro producto.

5. Principios Básicos

Los principios básicos que debe seguir GRUPO VÍTALY para proteger la información y la Infraestructura se basan en el framework NIST y en las buenas prácticas de ISO 27001:2022:

5.1. Prevención

GRUPO VÍTALY 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 implementará las medidas mínimas de seguridad determinadas por los requisitos legales y normativos, así como cualquier control adicional identificado a través de una evolución de amenazas y riesgos.

5.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación y actuar en consecuencia.

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.

5.3. Respuesta

Establecemos mecanismos para responder eficazmente a los incidentes de seguridad.

Designamos puntos de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

Establecemos protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones con las entidades que por Ley o normativas sean necesario informar

5.4. Conservación

El sistema de información de **GRUPO VÍTALY** se compromete a asegurar la integridad y resguardo de los datos e información almacenados en formato electrónico en los servicios de Prevención de Riesgos Laborales. Este compromiso se traduce en la implementación de medidas efectivas que no comprometan la calidad ni la esencia de los demás principios y requisitos fundamentales.

De manera simultánea, se garantizará la continuidad de los servicios a lo largo de todo el ciclo de vida de la información digital, mediante la adopción de una visión estratégica y la implementación de procedimientos sólidos que constituyan los cimientos para la preservación duradera del patrimonio digital.

6. Organización de la Seguridad

La implantación de la Política de Seguridad en **GRUPO VÍTALY** requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol específico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

a) Responsables del Servicio

b) Responsables de la Información

c) Responsable de Seguridad de la Información

d) Responsable del Sistema

e) Delegado de protección de datos

f) El Comité de Seguridad de la Información

6.1. Responsables de la Información y del Servicio

Tiene la potestad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos

Como **product owner**, determina los niveles de seguridad de la información en los roles de los usuarios que acceden a los sistemas de información.

Deriva requisitos de seguridad específicos de los clientes en función de necesidades y aspectos legales.

6.2. Responsable de Seguridad de la Información

Responsable de la definición, coordinación, implantación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo con los objetivos estratégicos de la dirección.
Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de **GRUPO VÍTALY**.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
  - La estrategia de seguridad de la información definida por el Comité de Seguridad.
  - Las normas y procedimientos contenidos en la Política de Seguridad de la Información de **GRUPO VÍTALY** y normativa de desarrollo.
- Supervisar (como responsable último) los incidentes de seguridad informática producidas en **GRUPO VÍTALY**.
- Difundir en **GRUPO VÍTALY** las normas y procedimientos contenidos en la Política de Seguridad de la Información de **GRUPO VÍTALY** y normativa de desarrollo, así como las funciones y obligaciones de todo **GRUPO VÍTALY** en materia de seguridad de la información.
- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables tales como el RGPD.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de **GRUPO VÍTALY**.

6.3. Responsable del Sistema de Información

Tiene las siguientes funciones:

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

El Responsable del Sistema puede proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por la dirección de la entidad, debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de la Seguridad.

6.4. Delegado de Protección de Datos

El Delegado de Protección de Datos, en adelante DPD, tendrá como mínimo las siguientes funciones:

- **Informar y asesorar** a los empleados que se ocupen de las operaciones de tratamientos de datos sobre las obligaciones que tienen según el reglamento vigente y de las políticas internas.
- Ofrecer el asesoramiento que se le solicite acerca **de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.**
- **Atender posibles reclamaciones de los afectados**, tal como se informar en las declaraciones de privacidad
- **Ser un puente de comunicación entre la autoridad de control y la empresa**. Ante cualquier reclamación o incidente que pueda producirse de cara a la protección de la información, el DPD será el encargado de comunicarlo a la AEPD junto con el departamento Jurídico. Además de informar de los problemas, incidencias o amenazas, también será el responsable de informar sobre las medidas de control que se tomen si sucede cualquier filtración o intrusión en el sistema que haya podido afectar a la privacidad de los datos.

Supervisar el cumplimiento de la normativa y de las políticas en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

6.5. Comité de Seguridad de la Información

La seguridad de la Información es una responsabilidad organizativa que es compartida con la Dirección. En consecuencia, la Dirección promueve la composición de un Comité de Seguridad de la Información, en aras de establecer una vida definida y el palpable apoyo a las iniciativas de seguridad.
Dicho Comité está compuesto por las figuras anteriormente mencionadas.
Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión y aprobación de la Política de Seguridad de la Información y de las responsabilidades principales;
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinados a garantizar la Seguridad de dichos activos;
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de tareas, plan director, documentación, riesgos.

6.6. Designaciones

1. Responsable de Seguridad de la Información:	1. Dirección TI GRUPO VÍTALY, S.L.U.
2. Responsable del Sistema:	2. Dirección GRUPO VÍTALY, S.L.U.
3. DPD:	3. ADEPLUS Consultores, S.L.
4. Comité de Seguridad de la Información:	4. Dirección TI GRUPO VÍTALY, S.L.U., Dirección GRUPO VÍTALY, S.L.U., Coordinador SGSI, ADEPLUS Consultores, S.L. y personal técnico según necesidades.

Servicio **VIGILANCIA DE LA SALUD**	
1. Responsable SERVICIO: 2. Responsable INFORMACIÓN:	1. Dirección Médica 2. Dirección Médica
Servicio **ACTIVIDADES TÉCNICAS**	
1. Responsable SERVICIO: 2. Responsable INFORMACIÓN:	1. Dirección Técnica 2. Dirección Técnica
Servicio **FORMACIÓN**	
1. Responsable SERVICIO: 2. Responsable INFORMACIÓN:	1. Dirección de Formación 2. Dirección de Formación
Servicio **CONSULTORÍA**	
1. Responsable SERVICIO: 2. Responsable INFORMACIÓN:	1. Dirección de Consultoría 2. Dirección de Consultoría
Servicio **GESTIÓN DE ABSENTISMO**	
1. Responsable SERVICIO: 2. Responsable INFORMACIÓN:	1. Dirección de Gabinete y Medicina Preventiva 2. Dirección de Gabinete y Medicina Preventiva
Servicio **TECNOLOGÍAS DE LA INFORMACIÓN**	
3. Responsable SERVICIO: 4. Responsable INFORMACIÓN:	1. Dirección TI GRUPO VÍTALY 2. Dirección TI GRUPO VÍTALY

7. Revisión de la política de seguridad de la información

Será misión del **Comité de Seguridad** la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta.

La Política será aprobada por la Dirección TI y difundida para que la conozcan todas las partes afectadas.

8. Privacidad y Protección de Datos Personales

GRUPO VÍTALY, en la prestación de sus servicios trata datos de carácter personal, tanto como Responsable de Tratamiento como encargado, siendo esta una de las obligaciones principales en materia de seguridad de la información.

Para tal fin se deberá desarrollar y mantener una Política de Tratamiento de Datos Personales y los procedimientos, medidas de seguridad y mecanismos que obliga la Normativa.

9. Gestión de riesgos

Para todos los sistemas sujetos a esta Política de Seguridad de la Información debe realizarse periódicamente una evaluación de los a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información gestionados y los diferentes servicios prestados. El

- Cuando cambie la información gestionada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad

Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

10. Marco Documental

- El cuerpo documental sobre seguridad de la información se desarrollará en cinco niveles por ámbito de aplicación, nivel de detalle técnico y de obligado cumplimiento, de manera que cada documento de un determinado nivel de desarrollo se fundamente en los documentos de nivel superior. Dichos niveles de desarrollo documental son los siguientes:
- **a) Primer nivel. Política de seguridad de la información.**
- Está constituido por la presente política, considerada de alto nivel y es de obligado cumplimiento, al amparo de lo establecido por el Real Decreto 311/2022, los requisitos de ISO 27001:2022
- **b) Segundo nivel. Políticas públicas de seguridad de la información**
- Estas políticas se documentan en el microsite privacidad.vitaly.com y comprenden los aspectos fundamentales de la política de seguridad que se consideran es necesario comunicar a las partes interesadas
- **c) Tercer nivel. Políticas, directrices y requerimientos.** Conjunto de políticas de seguridad de la información y requerimientos documentados en el SGSI y que desarrollan con más detalle los principios establecidos en esta política de alto nivel.

.d) Cuarto nivel. Procedimientos e instrucciones técnicas.

Está constituido por el conjunto de procedimientos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información. Son recomendaciones o informaciones relativas a temas concretos de seguridad basadas en instrucciones previas, que establecen las configuraciones mínimas de seguridad de los diferentes elementos de un sistema de información, recomendaciones de uso o de otro tipo.

La responsabilidad de aprobación de estos procedimientos técnicos dependerá de su ámbito de aplicación, que podrá ser en un ámbito específico o en un sistema de información determinado. Se consideran incluidas en este nivel las guías CCN-STIC

e) Quinto nivel. Normas y buenas prácticas. Conjunto de normas y buenas prácticas dirigidas a usuarios internos de GRUPO VÍTALY, empleados y colaboradores internos.

11. Obligaciones del Personal

- Todos y cada uno de los usuarios de los sistemas de información de **GRUPO VÍTALY** son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.
- Todos los miembros de **GRUPO VÍTALY** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de

Se establecerá un programa de concienciación continua para atender a todos los miembros de **GRUPO VÍTALY**, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las

Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

- Los miembros de **GRUPO VÍTALY** recibirán formación en materia de seguridad de la información al menos una vez al año.

medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

12. Terceras partes

Cuando **GRUPO VÍTALY** 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 ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Dirección Nacional de Tecnología,
Fecha de aprobación: 20-01-2026