

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

## ESTADO DE REVISIÓN/MODIFICACIÓN DEL DOCUMENTO

N.º EDICIÓN	Fecha	Naturaleza de la Revisión
00	08/06/2020	Edición inicial
01	05/04/2021	Actualización compromisos de la política
02	13/12/2021	Cambio de versión del SOA
03	01/02/2022	Modificación del alcance
	08/02/2023	Revisión por ampliación del alcance (sin cambios)
	03/03/2023	Revisión por ampliación del alcance (sin cambios)
	20/06/2024	Revisión por ampliación del alcance (sin cambios)
04	07/01/2025	Separación de política de seguridad de la información y adición de los principios particulares y responsabilidades específicas

**ELABORADO**

Responsable de SIG

Graciela Manga

**REVISADO**

Responsable de SIG

Graciela Manga

**APROBADO**

Dirección

Firmado:

Firmado:

Firmado:

## ÍNDICE

<b>ESTADO DE REVISIÓN/MODIFICACIÓN DEL DOCUMENTO .....</b>	<b>1</b>
<b>ÍNDICE .....</b>	<b>2</b>
<b>MISIÓN .....</b>	<b>3</b>
<b>ALCANCE .....</b>	<b>3</b>
<b>VISIÓN DEL SISTEMA INTEGRADO DE GESTIÓN .....</b>	<b>3</b>
<b>VALORES CORPORATIVOS .....</b>	<b>3</b>
<b>POLÍTICA DE GESTIÓN INTEGRADA DE GRUPO ASPASIA.....</b>	<b>4</b>

PÚBLICO

## MISIÓN

Ofrecer una formación adaptada y orientar a las personas hacia un mundo globalizado y digitalizado mediante herramientas y metodologías innovadoras.

## ALCANCE

El alcance del sistema de gestión integrada del grupo Aspasia es el diseño, la planificación y la ejecución de formación privada, formación profesional para el empleo/trabajo y la formación profesional reglada en todas sus modalidades online, presencial y virtual, así como la orientación profesional, la asistencia al autoempleo y la inserción laboral. Asimismo, la tramitación y desarrollo de subvenciones y convocatorias públicas en el ámbito del empleo y la formación tanto a nivel local como autonómico, nacional e internacional.

Todos los procesos relacionados con los sistemas de información son conforme a la declaración de aplicabilidad versión 3.

**Exclusiones** Anexo A 27001:

TIPO 1: 8.4, 8.11, 8.30

TIPO 2: 7.9, 8.4, 8.11, 8.25, 8.27, 8.28, 8.29, 8.30, 8.31, 8.33

TIPO 3: 7.9, 8.4, 8.11, 8.25, 8.27, 8.28, 8.29, 8.30, 8.31, 8.33

Exclusión de aplicabilidad de la norma ISO 9001:2015:

- Requisito 7.1.5.2 de la Norma ISO 9001:2015 “Trazabilidad de las mediciones” por no haber dispositivos de seguimiento y medición para dar conformidad a los cursos

## VISIÓN DEL SISTEMA INTEGRADO DE GESTIÓN

Nuestra visión es brindar a las personas un aprendizaje a lo largo de la vida, siendo el modelo de referencia en excelencia formativa, y constituirnos como líderes en el sector de la formación para empresas, organismos, instituciones, trabajadores y particulares a nivel nacional e internacional

## VALORES CORPORATIVOS

**Motivación** a través de la delegación. Confianza y reconocimiento de los méritos de nuestro equipo.

**Compromiso** con la misión -código ético- y con las necesidades de todas las personas usuarias de nuestros servicios.

**Capacidad de comunicación** clara y directa, favoreciendo el contacto con nuestro entorno a través de una información precisa.

**Proactividad:** Orientada a resultados, con capacidad de aprendizaje y una adecuada gestión del riesgo y las oportunidades.

**Empatía** para favorecer el compañerismo y la relación fluida entre el personal directivo y la plantilla. A través de la delegación, confianza y reconocimiento de los méritos de nuestro equipo.

**Igualdad:** Integrar la igualdad de oportunidades entre mujeres y hombres como principio básico y transversal

## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Dirección de GRUPO ASPASIA, determina como fundamental la gestión segura de la información a lo largo de todo el proceso formativo, y mejorar el sistema de gestión de seguridad de la información de forma continua y sistemática.

Por ello, y con el objetivo de garantizar la seguridad de la información, la organización tiene implantado un sistema de gestión basado en la norma:

- ISO 27001:2022

Para ello, GRUPO ASPASIA establece los siguientes compromisos:

En **general**:

- Mejora continua del desempeño tanto de los sistemas de gestión como del resultado a obtener.
- Mejora de la eficacia de los sistemas.
- Actualización y cumplimiento del marco legal y de los requisitos propios y específicos que nos puedan poner tanto las personas usuarias de nuestros servicios, las personas proveedoras y las personas implicadas.
- Mantener un alto nivel de cualificación y talento para poder ser eficaces y eficientes en los procesos.
- Mantenimiento de los adecuados canales de comunicación con todas las partes interesadas, con objeto de asegurar su satisfacción con respecto al cumplimiento de sus necesidades, requisitos y expectativas.
- Se adoptarán las medidas necesarias para que todo el personal de GRUPO ASPASIA sea conocedor de esta política. Difundiéndose también ésta al equipo proveedor y colaborador, estando además a disposición del público a través de la página web.

En **seguridad de la información**:

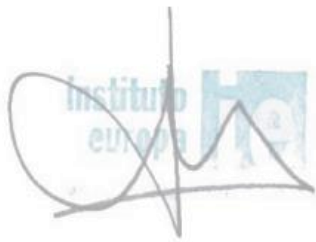
- Política de Disminución del riesgo potencial grave. Se priorizarán las actuaciones sobre riesgos potenciales graves.
- Política de Tolerancia 0 con las incidencias. Se investigará y sancionará aquellas actuaciones dolosas o imprudentes.
- Política de impacto reputacional mínimo. La incidencia reputacional en materia de seguridad debe tender a 0.
- Controlar operacionalmente de forma eficaz las amenazas y riesgos sobre el activo y las instalaciones.
- Gestionar eficientemente las incidencias que afecten a la integridad, disponibilidad y confidencialidad de la información de la empresa.
- Garantizar que nuestras operaciones y procesos actuales y futuros cumplan con la legislación vigente en materia de seguridad de la Información
- Implantar planes de continuidad del negocio que garanticen la permanencia de las actividades de la sociedad en caso de incidencias graves o contingencias.

#### **Principios particulares y responsabilidades específicas:**

- Gestionar eficientemente las incidencias que afecten a la integridad, disponibilidad y confidencialidad de la información de la empresa.
- Implantar planes de continuidad del negocio que garanticen la continuidad de las actividades de la sociedad en caso de incidencias graves o contingencias.
- Política de gestión de personas como activo de información que incluya medidas de sensibilización y/ o formación en materia de seguridad
- Gestionar los roles de los profesionales responsables del sistema de seguridad de la información para asegurar el nivel de profesionalidad necesario.
- Política de control y autorización de accesos se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.
- Política de seguridad física de las instalaciones. Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
- Política de criterios de seguridad de la información aplicados a la gestión de proveedores y en la Adquisición de productos (sistemas y servicios)
- Protección de datos (inactivos y en tránsito/medios) se adoptarán las medidas técnicas y organizativas destinadas a garantizar una adecuada protección de los datos.
- Prevención contra la conexión a través de sistemas interconectados
- Registro de actividad

- Protección de los sistemas y de la comunicación: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

Y como compromiso con el cumplimiento de esta política firma la Dirección a 07 de enero de 2025.



Instituto Europa



La Dirección

PÚBLICO