
	<b>SYSTEM POLICY</b>		Código: VPSIS00009
			Revisión: 1.0
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>			
<i>Sistema de gestión:</i> ISO 27001 Information Security Management	<i>Proceso:</i> P11 - Manage Information Technology	<i>Centro de trabajo:</i> VPS	
<i>Revisado por:</i> Luis Villafranca Rodriguez 10/11/2023	<i>Aprobado por:</i> Juanje Alberdi 10/11/2023	<i>Aprobado por:</i>	

<b>LISTADO DE MODIFICACIONES</b>	
<i>Revisión</i>	<i>Descripción de la modificación</i>
1.0	Creación del documento

## INDICE

1.	INTRODUCCIÓN .....	2
2.	OBJETO .....	2
3.	ALCANCE.....	2
3.1.	EMPLEADOS .....	2
3.2.	SISTEMAS DE INFORMACIÓN .....	3
3.3.	TERCERAS PARTES .....	3
4.	ROLES & RESPONSABILIDADES.....	3
4.1.	USUARIOS.....	3
4.2.	PROPIETARIOS.....	4
4.3.	AMINISTRADORES .....	4
5.	MANTENIMIENTO, APROBACIÓN Y REVISIÓN DE LA POLÍTICA.....	4
6.	DISTRIBUCIÓN DE LA POLÍTICA .....	5
7.	SANCIONES/PROCESO DISCIPLINARIO .....	5
8.	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN .....	5

	<b>SYSTEM POLICY</b>		Código: VPSIS00009
			Revisión: 1.0
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>			
<i>Sistema de gestión:</i> ISO 27001 Information Security Management	<i>Proceso:</i> P11 - Manage Information Technology	<i>Centro de trabajo:</i> VPS	
<i>Revisado por:</i> Luis Villafranca Rodriguez 10/11/2023	<i>Aprobado por:</i> Juanje Alberdi 10/11/2023	<i>Aprobado por:</i>	

## 1. INTRODUCCIÓN

---

Los procesos de negocio de AZKOYEN dependen en gran medida de los Sistemas de Información y la Información que almacenan. La Política de Seguridad tiene como misión establecer las directrices globales de Seguridad para la organización, así como proteger los activos de información.

Estas directrices incluyen la adopción de una serie de medidas organizativas y normas que se presentan en este documento y se desarrollan en sus documentos asociados y cuya finalidad es la de proteger los recursos de información de AZKOYEN y los sistemas de información utilizados para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y legalidad de la información.

Esta Política está basada en las recomendaciones de buenas prácticas para garantizar la Seguridad en la Gestión de Sistemas de Información (Normas internaciones ISO 27001 e ISO 27002), así como en la legislación vigente aplicable a la materia.

## 2. OBJETO

---

El objetivo principal de la creación de esta Política es garantizar a los usuarios el acceso a la información con la cantidad y calidad que se requiera para el desempeño, así como evitar serias pérdidas de información y accesos no autorizados a la misma.


## 3. ALCANCE

---

### 3.1. EMPLEADOS

---

La Seguridad de la Información es un esfuerzo conjunto. Requiere la implicación y participación de todos los miembros de la organización que trabajan con Sistemas de Información. Por ello, cada empleado debe cumplir los requerimientos de la Política de Seguridad y su documentación asociada. Los Empleados que deliberadamente o por negligencia incumplan la Política de Seguridad serán sometidos a las acciones disciplinarias según se contempla en el último capítulo de este documento.

	<b>SYSTEM POLICY</b>		Código: VPSIS00009
			Revisión: 1.0
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>			
Sistema de gestión: ISO 27001 Information Security Management	Proceso: P11 - Manage Information Technology	Centro de trabajo: VPS	
Revisado por: Luis Villafranca Rodriguez 10/11/2023	Aprobado por: Juanje Alberdi 10/11/2023	Aprobado por:	

### **3.2. SISTEMAS DE INFORMACIÓN**

Esta Política afecta a todos los activos de información de AZKOYEN VPS, tanto a la información en soporte digital o papel, de carácter personal o no y albergada en equipos personales o servidores, smartphones, redes, aplicaciones, sistemas operativos, procesos de la empresa que pertenecen y/o son administrados por AZKOYEN. Esta Política cubre los aspectos más directamente relacionados con la responsabilidad y buen uso del personal.

### **3.3. TERCERAS PARTES**


La presente Política de Seguridad es de extensible conocimiento y cumplimiento para cualquier persona externa perteneciente a terceras entidades que realice cualquier tipo de tratamiento sobre la información propiedad de AZKOYEN. Asimismo, esta Política y sus procedimientos asociados serán de obligado cumplimiento para las empresas terceras proveedoras contratadas para la ejecución de servicios profesionales en los ámbitos que se consideren oportunos, en el caso de que realicen cualquier actividad que implique acceso o tratamiento a cualquier sistema o información propiedad de AZKOYEN y así se definirá contractualmente.

## **4. ROLES & RESPONSABILIDADES**

### **4.1. USUARIOS**

Los usuarios deben conocer y aplicar las Políticas de Seguridad, procedimientos, estándares y aplicar la legislación vigente. Deben entenderlos y cumplir con los mismos.

En general, cualquier persona que genera información es responsable de su clasificación de acuerdo con las instrucciones de la Compañía. Asimismo, cualquier persona que utiliza información y los sistemas de información está obligada a gestionarlos con el cuidado necesario, así como de utilizarlos únicamente para realizar las tareas autorizadas y en cumplimiento de la normativa. Esto también es aplicable al personal externo.

	<b>SYSTEM POLICY</b>		Código: VPSIS00009
			Revisión: 1.0
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>			
<i>Sistema de gestión:</i> ISO 27001 Information Security Management	<i>Proceso:</i> P11 - Manage Information Technology	<i>Centro de trabajo:</i> VPS	
<i>Revisado por:</i> Luis Villafranca Rodriguez 10/11/2023	<i>Aprobado por:</i> Juanje Alberdi 10/11/2023	<i>Aprobado por:</i>	

#### **4.2. PROPIETARIOS**

Los propietarios de activos de información generalmente se corresponden con la Dirección General, o responsables de Área, quienes deben adquirir, desarrollar y mantener aplicativos de la Compañía como sistemas de soporte a las decisiones y otras actividades de la misma.

Los propietarios deben indicar la clasificación de sus activos que mejor corresponde con su valor crítico, disponibilidad e importancia relativa para la organización. Su clasificación marcará el nivel de riesgo y de protección, así como el nivel de acceso a dicha información o aplicativo.

#### **4.3. ADMINISTRADORES**

Los administradores son Empleados a cargo de salvaguardar la información de la Compañía propia y cedida por terceros.

Cada sistema de información debe disponer de, al menos, un Administrador autorizado según consta en el Documento de Seguridad.

Son los responsables de almacenar la información, implementar controles de acceso (para prevenir accesos no autorizados) y ejecutar copias de seguridad periódicas (para asegurar la disponibilidad de la información crítica).


### **5. MANTENIMIENTO, APROBACIÓN Y REVISIÓN DE LA POLÍTICA**

El Responsable de Seguridad de la Información es el responsable de establecer y mantener la Política de Seguridad, manuales y procedimientos correspondientes de AZKOYEN.

La Dirección General es la responsable de la aprobación y publicación de la Política, de distribuirla a todos los Empleados y terceros afectados, así como revisar y evaluar la Política de Seguridad.

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

Periódicamente, y en todo caso no superando el plazo de un año, se 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.

	SYSTEM POLICY		Código: VPSIS00009
			Revisión: 1.0
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>			
Sistema de gestión: ISO 27001 Information Security Management	Proceso: P11 - Manage Information Technology	Centro de trabajo: VPS	
Revisado por: Luis Villafranca Rodriguez 10/11/2023	Aprobado por: Juanje Alberdi 10/11/2023	Aprobado por:	

## 6. DISTRIBUCIÓN DE LA POLÍTICA

El documento de Política de Seguridad será accesible a todo el personal interno, se entregará en la incorporación de un nuevo empleado y cada 12 meses se distribuirá por correo electrónico a todos los Empleados internos y externos subcontratados por AZKOYEN que manejen datos y recursos pertenecientes a la misma para conocimiento y conciencia de las normas de seguridad dispuestas.

Cualquier cambio sustancial en el documento será distribuido a todos los usuarios a través de una notificación formal, enviada por correo electrónico o por comunicación interna en medios accesibles a los mismos mediante un modelo de comunicación habilitada para tal efecto.

## 7. SANCIONES/PROCESO DISCIPLINARIO

Cualquier violación premeditada o negligente de las políticas y normas de seguridad y que suponga un potencial daño, consumado o no a AZKOYEN, será sancionada de acuerdo a los mecanismos habilitados en el convenio de la Compañía y en la normativa legal, contractual y corporativa vigentes.

Todas las acciones en las que se comprometa la seguridad de AZKOYEN y que no estén previstas en esta Política, deberán ser revisadas por la Dirección General y por el Responsable de Seguridad para dictar una resolución sujetándose al criterio de la Compañía y la legislación prevista.


Las acciones disciplinarias en respuesta a los incumplimientos de la Política de Seguridad son atribución de los Responsables de Departamento en conjunción con Administración y la Dirección General.

## 8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Los procesos de negocio de Azkoyen dependen en gran medida de los Sistemas de Información y de la Información que almacenan. Esta Política de Seguridad persigue establecer las directrices globales de Seguridad para proteger los activos de información corporativos.

Dichas directrices incluyen la adopción de una serie de medidas organizativas y el establecimiento de un conjunto de normas dirigidas a hacer frente a amenazas -internas o externas; deliberadas o accidentales- con el fin de asegurar el cumplimiento de los principios de **confidencialidad, integridad, disponibilidad y legalidad** de la información.

Esta Política está basada un modelo de gestión del sistema de información acorde con la aplicación de la norma internacional ISO/IEC 27001:2022, e integrada con las normas ISO/IEC 9001: 2015 e ISO /IEC

	<b>SYSTEM POLICY</b>		<i>Código:</i> VPSIS00009
			<i>Revisión:</i> 1.0
<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>			
<i>Sistema de gestión:</i> ISO 27001 Information Security Management	<i>Proceso:</i> P11 - Manage Information Technology	<i>Centro de trabajo:</i> VPS	
<i>Revisado por:</i> Luis Villafranca Rodriguez 10/11/2023	<i>Aprobado por:</i> Juanje Alberdi 10/11/2023	<i>Aprobado por:</i>	

45001, así como en el cumplimiento de la legislación vigente; especialmente, en materia de protección de datos personales:

- Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016 RGPD, General de Protección de Datos (RGPD/GDPR).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD).

El equipo de alta Dirección de Azkoyen VPS está firmemente implicado en la labor de promover y liderar un Sistema de Gestión de la Información integrado, en el que todos los usuarios sean conscientes de que cada uno de ellos es un factor clave en la seguridad del mismo y deberá guiarse por los siguientes principios rectores referidos anteriormente (confidencialidad, integridad, disponibilidad y legalidad).