Política de Seguridad de la Información

CÓDIGO APS-PLT-SI – Versión 1.0

CONTROL DEL DOCUMENTO

Elaborado por:		
Departamento/Cargo	**Nombre**	**Fecha**
Responsable de Seguridad de la Información (ISO)	Rafael Fernández Garrido	28/04/2025
Revisado por:		
Departamento/Cargo	**Nombre**	**Fecha**
Comité de Seguridad de la Información (CSI)	Enrique Sánchez Bermúdez	09/05/2025
Aprobado por:		
Departamento/Cargo	**Nombre**	**Fecha**
Comité de Seguridad de la Información (CSI)	Enrique Sánchez Bermúdez	09/05/2025

CONTROL DE VERSIONES

VERSIÓN	FECHA VIGOR	CAMBIOS
1.0	09/05/2025	Versión inicial.

FICHA DE DISTRIBUCIÓN DE DOCUMENTO

NOMBRE/ÁREA/COMPAÑÍA	SOPORTE DISTRIBUCIÓN
Aareon Proptech Spain	T:\Corporativo\SGSI_Docs

Índice

Política de Seguridad de la Información

1. Introducción

Como proveedor líder de sistemas y soluciones software para la industria inmobiliaria, administradores de fincas y sectores relacionados, la compañía **AAREON PROPTECH SPAIN, S.L.U** (en adelante **APS**), perteneciente al **Grupo Aareon**, se considera obligada a garantizar la seguridad de la información y la protección de los datos de sus clientes, proveedores, accionistas y empleados. La aplicación de la presente política se basa en la norma **ISO/IEC 27001:2022**, estándar de seguridad reconocido internacionalmente.

La interconexión de empresas en todo el mundo y la continua proliferación de amenazas a la seguridad de la información traen como consecuencia que las exigencias relacionadas con los sistemas de seguridad y de defensa sigan aumentando. La creciente necesidad de proporcionar un acceso cómodo y fiable a nuestros sistemas nos presenta, además, retos adicionales.

La existencia misma de nuestra empresa depende de la capacidad para prestar servicios de tecnologías de la información, que a su vez están sujetos a un proceso de cambio constante y que continúa generando nuevos desafíos, por lo que se requieren nuevos enfoques para nuestras soluciones. El contexto y ambiente de **APS** se caracteriza por una evolución continua en los requisitos de seguridad, rendimiento y flexibilidad.

El creciente despliegue e interacción de los sistemas, aplicaciones y procedimientos de tecnologías de la información nos obliga a redoblar nuestros esfuerzos para proteger los datos confidenciales y la información procesada y almacenada por **APS**. En consecuencia, la disponibilidad de nuestros sistemas y aplicaciones tiene un papel importante que desempeñar, así como la utilización segura de nuestra información y datos corporativos.

Además de la presente Política de Seguridad de la Información, **APS** dispone de un conjunto de documentos adicionales que detallan cómo deben implementarse los diversos aspectos de seguridad de la información cubiertos por la misma.

Esta Política de Seguridad de la Información está aprobada por el Comité de Seguridad de la Información de **APS** y se encuentra publicada y comunicada tanto a los empleados incluidos en el alcance descrito más adelante como al resto de partes interesadas relevantes.

2. Propósito de la Política de Seguridad de la Información

La Política de Seguridad de la Información de **APS** establece el compromiso de la Dirección y la estrategia de la organización para gestionar adecuadamente la seguridad de la información. Este documento define los principios de alto nivel, los objetivos generales y el alcance de la gestión de la seguridad de la información en **APS**. La presente política se complementará con aspectos relacionados con la seguridad de la red, la seguridad de los servidores, la seguridad de los dispositivos móviles y las normas de gestión de sus usuarios, entre otros.

3. Alcance

El alcance de esta política engloba los sistemas de información asociados a la plataforma tecnológica que da soporte a las soluciones **TucoBan y Tucomunidad**, incluyendo los servicios de desarrollo, soporte e implantación de aplicaciones informáticas.

4. Términos y Definiciones

4.1 Información

La información cubierta por esta política abarca toda aquella que se almacena y/o comparte de alguna manera. Se incluye, por tanto, información electrónica, información en papel e información compartida de forma oral o incluso visual (por ejemplo, mediante conferencias telefónicas o videoconferencias).

4.2 Gestión de la seguridad de la información

Gestionar la seguridad de la información implica proteger la información y los sistemas de información asociados frente al acceso, el uso, la divulgación, la interrupción, la modificación, la lectura, la inspección, el registro o la destrucción que no hayan sido autorizados por la organización.

4.3 Protección de datos / Privacidad

La protección de datos se refiere a las medidas de seguridad que garantizan que, al recopilar, procesar y utilizar datos personales, no se vean afectados los intereses legítimos de las personas afectadas.

4.4 Incidencia de seguridad de la información

Una incidencia de seguridad de la información es la consecuencia de uno o varios eventos de seguridad no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio de la organización y de amenazar la seguridad de la información o la protección/privacidad de los datos.

4.5 Sistema de gestión de seguridad de la información

El Sistema de Gestión de Seguridad de la Información de **APS** abarca todos los procesos, estructuras organizativas y de comunicación y acuerdos necesarios para garantizar la seguridad de la información dentro de la organización. El diseño y los principios de la gestión de la seguridad de la información en **APS** se basan en la norma de seguridad ISO/IEC 27001:2022, reconocida internacionalmente.

5. Política de Seguridad de la Información

5.1 Estrategia de seguridad

La estrategia de negocio actual de **APS**, la estrategia de tecnologías de la información y la gestión de los riesgos, definen el marco para identificar, evaluar, tratar y controlar los riesgos relacionados con la seguridad de la información mediante el establecimiento y mantenimiento del Sistema de Gestión de la Seguridad de la Información.

La seguridad de la información está garantizada por esta Política de Seguridad de la Información y un conjunto de documentos subyacentes y complementarios disponibles en los repositorios documentales de **APS**. Con el fin de asegurar las operaciones ante la ocurrencia de incidencias graves, las unidades organizativas de **APS** deben garantizar la disponibilidad de planes de continuidad, de copias de seguridad, de procedimientos para la defensa contra código dañino y actividades maliciosas, para el control de acceso

a los sistemas y a la información, así como para la gestión de eventos, de las incidencias y de los informes relacionados con la seguridad de la información.

5.2 Principios de la política de seguridad de la información

Los principios en los que se sustenta la presente política de seguridad de la información son los siguientes:

- **Disponibilidad:**

  Nuestros sistemas, aplicaciones, procesos y datos tienen asegurado un alto nivel de disponibilidad que está continuamente garantizado y es considerado un factor clave que contribuye al éxito de nuestra empresa.

- **Integridad:**

  Nuestros datos corporativos y los de nuestros clientes, así como los sistemas que soportan la información, están completamente protegidos frente a posibles pérdidas y alteraciones no autorizadas.

- **Confidencialidad:**

  La organización impide el acceso no autorizado o el uso indebido de nuestros datos e información. Consideramos que la observancia y cumplimiento de las normas legales es un requisito esencial, al cual se otorga una alta prioridad en **APS**.

- **Autenticidad:**

  Nuestros datos e información, aplicaciones, sistemas y procedimientos están protegidos contra la manipulación no autorizada mediante una serie de medidas organizativas y técnicas. Las interfaces externas se supervisan continuamente y están protegidas contra el uso no autorizado.

- **Transparencia:**

  Nuestro tratamiento de la información es transparente y fácilmente rastreable.

APS, además, garantiza la seguridad operativa, es decir, el funcionamiento correcto y previsto de sus sistemas y aplicaciones. La seguridad operativa es la condición previa para asegurar la disponibilidad, integridad, confidencialidad, autenticidad y transparencia.

5.3 Objetivos de seguridad

APS se compromete a salvaguardar la confidencialidad, integridad y disponibilidad de todos los activos de información de la organización para garantizar que se cumple con los requisitos legales, operativos y contractuales formalmente establecidos.

Los objetivos generales de la gestión de la seguridad de la información son los siguientes:

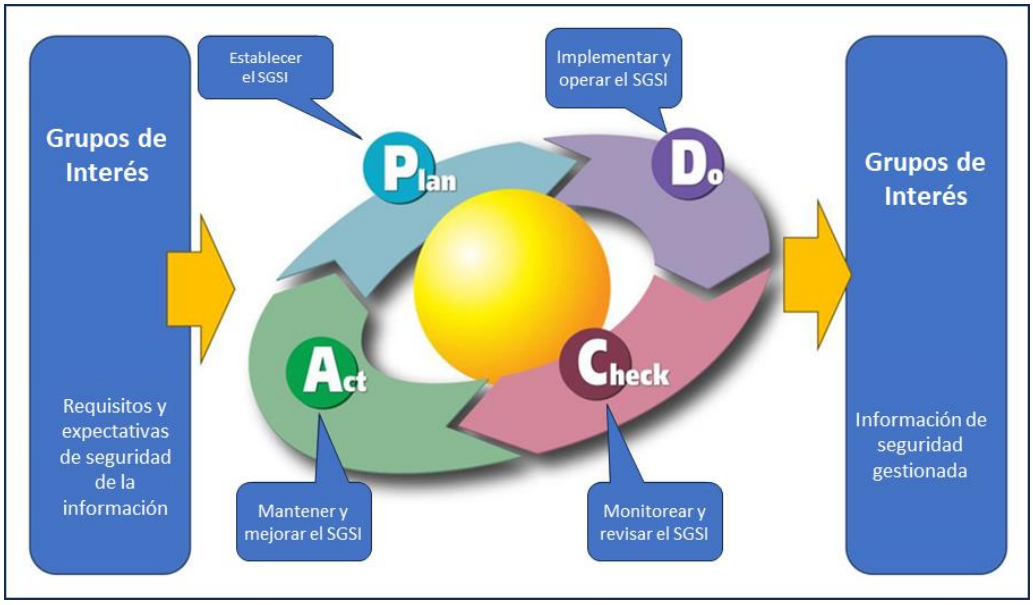
- Garantizar el cumplimiento de las leyes, reglamentos, directrices y contratos vigentes.
- Cumplir con los requisitos de disponibilidad, integridad, confidencialidad, autenticidad y transparencia establecidos, así como garantizar la seguridad operativa.
- Establecer controles para proteger la información y los sistemas de información de **APS** contra el robo, el abuso y otras posibles formas de daño y pérdida.

- Motivar a los empleados para que mantengan la responsabilidad, la implicación y el conocimiento adecuados en el ámbito de la seguridad de la información, con el fin de minimizar los riesgos y las incidencias de seguridad.
- Asegurar que **APS** sea capaz de continuar con la prestación de sus servicios, incluso si ocurren incidencias de seguridad críticas.
- Garantizar la protección de los datos de carácter personal (privacidad).
- Garantizar la disponibilidad y fiabilidad de la infraestructura de red y de los servicios suministrados y gestionados por **APS**.
- Cumplir con los estándares internacionales de seguridad de la información (ISO/IEC 27001).
- Asegurar que los proveedores de servicios externos cumplan con los requisitos y controles de seguridad de la información de **APS**.

5.4 Proceso de gestión de seguridad (modelo PDCA)

APS entiende la gestión de la seguridad como un proceso continuo, que involucra a las actividades de los participantes en todos los niveles y en todos los aspectos de sus operaciones.

El modelo PDCA (Planificar-Hacer-Verificar-Actuar/Ajustar) es un método de gestión iterativo de cuatro pasos utilizado en la gestión de la seguridad de **APS** para el control y la mejora continua de los procesos y de sus indicadores.



Fuente: ISO/IEC 27001

Las amenazas y las vulnerabilidades deben descubrirse y gestionarse de manera continua. Para ello, los participantes deben revisar, reevaluar y modificar todos los aspectos de la seguridad de la información con el fin de hacer frente a estos riesgos en constante evolución.

Las principales acciones necesarias para hacer frente a los riesgos de seguridad de la información son las siguientes:

1. Evaluación de los riesgos de seguridad.
2. Toma de decisiones sobre el tratamiento de los riesgos, definiendo objetivos, medidas y controles.
3. Aplicación de medidas y controles establecidos.
4. Verificación y auditoría de las medidas y controles aplicados.

6. Organización de la Seguridad

6.1 Funciones y responsabilidades

La Alta Dirección y el Comité de Seguridad de la Información de **APS** son responsables de garantizar el cumplimiento de las normativas internas de seguridad de la información. El personal directivo está obligado a aplicar la Política de Seguridad de la Información y a garantizar su existencia a largo plazo.

Dentro de sus áreas de responsabilidad, los responsables de área y/o departamento deben garantizar la aplicación de las medidas y procedimientos de seguridad, así como su cumplimiento, su observancia y su supervisión en el contexto de la gestión de los riesgos de seguridad.

Todos los empleados son responsables de la información, de los datos y de los equipos que se les facilitan. Esta responsabilidad dimana de los requisitos legales, de los compromisos contractuales y comerciales adquiridos por **APS** frente a sus clientes y socios y de las obligaciones de los empleados.

Cuando sea necesario, **APS** involucrará a sus clientes, proveedores y otros grupos de interés en sus procesos de seguridad de la información con el fin de garantizar un enfoque integral de la gestión de la seguridad.

6.2 Personal con funciones de seguridad

El Comité de Seguridad de la Información y el Responsable de Seguridad de la Información serán designados por la Alta Dirección y son los responsables de seguridad de la información encargados de coordinar las actividades necesarias para implantar la seguridad de la información como un proceso gestionado, según se ha explicado en el apartado 5.4. de esta política.

Cuando resulte necesario, la Alta Dirección designará un Delegado de Protección de Datos.

Se realizan auditorías regulares, así como actividades de formación y concienciación exhaustivas, para garantizar la seguridad de la información de forma integral. En estas actividades, se dará prioridad a la capacidad de las partes interesadas para proporcionar retroalimentación y al principio de mejora continua, como instrumento para mejorar la seguridad de la información.

Todos los empleados de **APS** comparten por igual la responsabilidad de garantizar que la empresa alcance sus objetivos de seguridad de la información y de velar por el cumplimiento de las políticas y estrategias de seguridad. Por tanto, se les pide que aporten su contribución, como parte de un trabajo en equipo, de manera creativa y constructiva, con el fin de garantizar también la consecución de los objetivos estratégicos de alto nivel.

Las infracciones de esta política se documentan y, los casos graves, se comunican a la Alta Dirección de la empresa.

6.3 Gestión de riesgos

Nuestros riesgos de seguridad se registran y revisan a intervalos regulares. Las conclusiones que resultan de este proceso constituyen la base para la definición y adopción de controles y medidas de seguridad y son parte integral del proceso de gestión de riesgos en APS.

Cuando se produce una violación de la seguridad de la información, se adoptarán las medidas apropiadas para resolver el problema y evitar su repetición en el futuro.

Adicionalmente, tenemos en cuenta los principios de viabilidad económica a la hora de implementar la seguridad de la información.

6.4 Revisión

Esta Política de Seguridad de la Información será revisada y actualizada al menos anualmente, o cuando se considere necesario.