



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Revisión 1.1

Fecha: 18/12/2023

Control de revisiones		
Revisión	Fecha	Descripción modificaciones
Rev 0	12/02/21	Versión inicial
Rev 1	17/03/21	Punto 2: Incorporación punto 5.2.b) norma ISO 27001 Punto 3: Alcance: Ajuste del alcance a lo recogido en el Manual del Sistema Integrado de Gestión Punto 9: Referencia a otra normativa y procedimientos de Seguridad de la Información
Rev 1.1	18/12/23	Referencias acordes a la ISO 27001:2022 y nuevo anexo 18 Gestión de la seguridad de servicios en la nube

ÍNDICE

1	Propósito de la Política de Seguridad de la Información.....	4
2	Fundamentos de la Política de Seguridad de la Información	4
3	Alcance de la Política de Seguridad de la Información.....	4
4	Normativa de referencia.....	4
5	Principios de la Política de Seguridad de la Información	5
6	Organización para la seguridad de la información.....	5
7	Proceso de Gestión de Seguridad de la Información.....	6
	7.1 Análisis y gestión de los riesgos de seguridad de la información.....	6
	7.2 Control de los riesgos de seguridad de la Información.....	6
8	Comunicación.....	6
9	Revisión	6
10	Auditoría.....	7
11	Incumplimientos con la Política de Seguridad de la Información.....	7

Propósito de la Política de Seguridad de la Información

La Política de Seguridad de la Información de Habitat Inmobiliaria se establece como marco de actuación para garantizar la protección de todos los activos de información y la tecnología utilizada para su tratamiento, de las amenazas internas o externas, deliberadas o accidentales, con el propósito de asegurar la:

- ▲ **Integridad** (información correcta y libre de modificaciones y errores)
- ▲ **Disponibilidad** (información accesible cuando es necesaria)
- ▲ **Confidencialidad** (información accesible únicamente para las personas autorizadas)

El enfoque en Seguridad de la Información está alineado con la Misión, Visión y Valores y el Código Ético de Habitat Inmobiliaria.

2 Fundamentos de la Política de Seguridad de la Información

Los fundamentos de la Política de Seguridad de la Información de Habitat Inmobiliaria son los siguientes:

- Cumplir todos los requisitos legales aplicables en Seguridad de la Información.
- Asegurar la integridad, disponibilidad y confidencialidad de la Información.
- Compromiso con el cumplimiento de los requisitos de Seguridad de la Información de nuestros clientes, empleados, proveedores, accionistas y otras partes interesadas que se determinen.
- Concienciar a todas las personas de la organización en el cumplimiento de sus obligaciones en Seguridad de la Información y de la protección de los Activos de Información.
- Mejorar de forma continua y sostenible nuestro Sistema de Gestión de Seguridad de la Información.
- Velar por el cumplimiento por parte de los proveedores y colaboradores con acceso a los Activos de Información de todas las obligaciones y requisitos en Seguridad de la Información.
- Proporcionar un marco de referencia para el establecimiento de los objetivos de Seguridad de la Información.

Alcance de la Política de Seguridad de la Información

El alcance de la Política de Seguridad de la Información engloba los sistemas de información que dan soporte a las actividades de "Promoción Inmobiliaria Residencial: compra de suelo, gestión del desarrollo de proyectos, comercialización, gestión de la construcción y servicio posventa", de acuerdo a la Declaración de Aplicabilidad vigente.

Esta Política de Seguridad de la Información es de aplicación a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de Habitat Inmobiliaria para los procesos descritos.

Las personas sujetas a esta Política incluyen a todos los usuarios con acceso a la información descrita, independientemente del soporte automatizado o no en el que se encuentre esta y de si el usuario es empleado o no de Habitat Inmobiliaria. Por lo tanto, también se aplica a los proveedores, colaboradores, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de Habitat Inmobiliaria.

El contenido de esa Política de Seguridad de la Información, está desarrollado en procedimientos, objetivos, planes y normativas complementarios de seguridad de la información.

La aplicación de esta Política es complementaria a otras Políticas de obligado cumplimiento, como la Política de Protección de Datos de Carácter Personal, y aquellas otras normativas y procedimientos que regulan cuestiones relacionadas con la información de la compañía.

3 Normativa de referencia

Para garantizar que la Política de Seguridad de la Información sea implantada en Habitat Inmobiliaria se ha implantado y se mantiene un Sistema de Gestión de Seguridad de la Información conforme a la norma **ISO 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad**.

4 Principios de la Política de Seguridad de la Información

La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, comunicación, transporte, almacenamiento, difusión y hasta su eventual borrado o destrucción. Por ello, se establecen los siguientes principios mínimos:

- **Principio de confidencialidad:** los sistemas de información deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.
- **Principio de integridad y calidad:** se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.
- **Principio de disponibilidad y continuidad:** se garantizará un nivel de disponibilidad en los sistemas de información y se dotarán los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.
- **Principio de gestión del riesgo:** se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los sistemas de información.
- **Principio de proporcionalidad en coste:** la implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos, sin perjuicio de que se asegurará que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.
- **Principio de concienciación y formación:** se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De igual forma, se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.
- **Principio de prevención:** se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.
- **Principio de detección y respuesta:** los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia respondiendo eficazmente, a través de los mecanismos establecidos al efecto, a los incidentes de seguridad.
- **Principio de mejora continua:** se revisará el grado de cumplimiento de los objetivos de mejora de la seguridad planificados anualmente y el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de la Administración Pública.
- **Principio de seguridad TIC en el ciclo de vida de los sistemas de información:** las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

5 Objetivos de Seguridad de la Información

Los objetivos de Seguridad de la Información se planificarán anualmente a partir de la revisión del alcance y el contexto, y de la planificación de la demanda de capacidad necesaria. Serán aprobados por el Comité de Seguridad de la Información.

6 Organización para la seguridad de la información

La Organización para la Seguridad de la Información en Habitat Inmobiliaria está constituida por las siguientes funciones:

- ❖ Comité de Seguridad de la Información (CSI)
- ❖ Responsable del Sistema de Seguridad de la Información (RSSI)
- ❖ Administradores de Seguridad de la Información (ASI)
- ❖ Usuarios (empleados de Habitat Inmobiliaria y terceros)

Las funciones y responsabilidades que se han establecido en Habitat Inmobiliaria para la seguridad de la información se describen en el [Anexo 1](#) del [P41 Procedimiento de Seguridad de la Información](#).

7 Proceso de Gestión de Seguridad de la Información

Para garantizar el cumplimiento de esta Política, en Habitat Inmobiliaria se han implantado los procesos siguientes:

7.1 Análisis y gestión de los riesgos de seguridad de la información

El análisis y la gestión de riesgos de seguridad de la información se realiza siguiendo la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información).

Se realiza un análisis detallado de los riesgos que afecten a los Activos de Información que quedará documentado en el Análisis de Riesgos de Seguridad de la Información.

7.2 Control de los riesgos de seguridad de la Información

Para asegurar el control de los riesgos de seguridad de la información se han establecido las medidas de control y normativas siguientes:

- Clasificación e intercambio de la Información.
- Gestión de Usuarios y Accesos a Sistemas, Aplicaciones y Servicios
- Seguridad Física y Gestión de Soportes
- Gestión del Trabajo en Remoto
- Configuración y Mantenimiento de Sistemas
- Gestión de Autorizaciones
- Seguridad en dispositivos móviles y portátiles
- Gestión de Capacidad
- Copias de Seguridad
- Gestión de Incidencias de Seguridad de la Información
- Gestión de la Continuidad de Negocio
- Gestión de la Seguridad con Terceros
- **Gestión de la Seguridad en los servicios en la Nube**
- Seguridad en el desarrollo de Software
- Uso de Controles Criptográficos
- Gestión de Cambios en TIC
- Gestión de Recursos Humanos
- Obligaciones del Personal en Seguridad y Protección de Datos
- Revisiones Periódicas

8 Comunicación

La Política de Seguridad de la Información es comunicada a todos los empleados de Habitat Inmobiliaria y está disponible para todas las Partes Interesadas de la compañía.

9 Revisión

Esta Política de Seguridad de la Información, así como otras normativas y procedimientos derivadas de esta Política, serán revisadas anualmente y actualizadas siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

10 Auditoría

El sistema de Gestión de Seguridad de la Información se auditará periódicamente de forma interna y externa, para evaluar la efectiva implantación de esta Política.

11 Incumplimientos

Cualquier incumplimiento con la Política, procedimientos y normativa de Habitat Inmobiliaria en Seguridad de la Información podrá dar lugar al inicio de acciones disciplinarias.

Lo anterior se entenderá sin perjuicio de la responsabilidad administrativa, civil o en su caso penal que pueda ser exigida al infractor (sea o no empleado de Habitat Inmobiliaria) de conforme a la legislación vigente.