***GRUPO “JUNTOS 2025” ÉTICA Y DEONTOLOGÍA***

**Integrantes y usuario de GitHub:**

* Dana Karina Valverde - GitHub: DanaValverde
* Maria Luciana Ferreyra - GitHub: marlufer
* Fernando Agustin Perez - GitHub: bobony97
* Juan Cruz Avila - GitHub: juancruz-dev
* Giuliano Batistela - GitHub: gbatistela
* Axel Bonaldi - GitHub: axelbonaldi

***Política de privacidad y protección de datos***

Esta política de privacidad describe cómo el sistema **SmartHome Solutions**, recolecta, utiliza, almacena y protege los datos personales de sus usuarios. Este documento garantiza asegurar la privacidad de los mismo en un entorno tan sensible como su hogar.

**I. Tipos de datos personales que se recolectarán**

* **Datos de identificación:** Nombre, apellido, correo electrónico.
* **Datos de dispositivos:** Información sobre los dispositivos que se encuentran vinculados a la aplicación de SmartHome con identificadores únicos de usuario y dispositivo, información sobre errores del sistema y bloqueos.
* **Datos de uso:** Historial de encendido/apagado de dispositivos, horarios configurados, modo de utilización y franjas horarias.
* **Datos de ubicación:** dirección de la vivienda.
* **Datos de sensores:** temperatura, movimiento, consumo energético de dispositivos, entre otros.

**II. Finalidad del procesamiento de datos**

En **SmartHome Solutions**, procesamos los datos personales con los siguientes fines:

* Permitir el registro y autenticación del usuario.
* Gestionar y personalizar los dispositivos inteligentes del hogar.
* Ejecutar automatizaciones programadas por el usuario.
* Brindar notificaciones relevantes (por ejemplo, alertas de seguridad).
* Mejorar la eficiencia y el rendimiento del sistema mediante el análisis del uso.
* Garantizar la seguridad y fiabilidad del servicio.
* Cumplir con obligaciones legales, si alguna ley nos lo pide o si lo requiere alguna autoridad.

**III. Medidas de seguridad implementadas**

Para garantizar que el uso de los dispositivos asociados a la aplicación **SmartHome Solutions** sea seguro, ético y confiable se adoptarán una serie de medidas específicas. Estas medidas reflejan tanto los principios fundamentales de la seguridad informática (confidencialidad, integridad, disponibilidad, autenticación y autorización) como los marcos regulatorios y éticos vigentes.

**1. Control de acceso basado en roles y perfiles**

La aplicación implementará control de acceso mediante roles predefinidos, donde el “Administrador” pueda asignar los mismos. A su vez dentro de cada rol exitiran tipos de perfiles que podrán realizar diferentes acciones/usos asignadas por el “Administrador”.

**Queda bajo la responsabilidad del “Administrador” las consecuencias que la asignación de permisos/creación de perfiles pueda ocasionar.**

Los roles predefinidos son los siguientes:

* Rol ***Administrador***: puede configurar dispositivos, perfiles y permisos.
* Rol ***Usuario estándar***: puede operar dispositivos pero no cambiar configuraciones.
* Rol ***Invitado***: acceso limitado a funciones básicas (como encender luces entre otras).

**2. Autenticación y Autorización Seguras**

* Se utilizará un sistema de **inicio de sesión con credenciales cifradas** (hashing con algoritmos seguros)
* Se implementará **autenticación multifactor (MFA)** para todos los usuarios.
* La autorización se gestionará desde un servidor con validación de token por sesión, evitando exposición del mismo.

**3**. **Cifrado de trafico de datos**

* La comunicación entre el cliente (interfaz) y el servidor se realizará mediante **HTTPS** asegurando confidencialidad e integridad del trafico de datos.
* El sistema recopilara y almacenará información sensible (por ejemplo, ubicaciones, configuraciones de cámaras) en una base de datos con las medidas de seguridad correspondientes, como el cifrado de claves.

**4**. **Auditoría y monitoreo de actividades**

* Se implementarán **logs de auditoría** que registren eventos como por ejemplo intentos de acceso, cambios de configuración y errores del sistema. Solicitando la **autenticación multifactor (MFA).**
* Se establecerá un sistema de alertas automáticas ante detección de actividades irregulares, como múltiples intentos de inicio de sesión fallidos.

Estas medidas permitirán detectar posibles incidentes de seguridad a tiempo.

**5. Gestión de contraseñas y datos personales**

* Se aplicará una **política de contraseñas robusta**: mínimo de caracteres, combinación de mayúsculas, minúsculas, y números
* Los usuarios podrán cambiar o recuperar sus contraseñas mediante procesos verificados por correo electrónico (con token de un solo uso) y con fecha limite de expiración.
* El sistema almacenara los tokens y registros de fechas en el momento de creación de una cuenta y cambio de contraseña

**IV. Derechos de los usuarios sobre sus datos**

Para SmartHome Solutions, la privacidad del usuario y la gestión responsable de sus datos constituyen pilares fundamentales de nuestro desarrollo tecnológico. Reconociendo la profundidad de la información que nuestros hogares inteligentes procesan, nos comprometemos a garantizar que los usuarios mantengan un control efectivo sobre sus datos a través del reconocimiento y la aplicación de sus derechos. Estos derechos esenciales dentro del sistema se detallan a continuación.

**1. Derecho de acceso**

Este derecho permite al usuario saber si sus datos están siendo recolectados, conocer con precisión qué información se ha almacenado sobre él, con qué finalidad se está utilizando y quiénes tienen acceso a esos datos. También puede solicitar una copia completa de sus datos personales en posesión del sistema.

**2. Derecho de rectificación**

El usuario puede corregir datos incorrectos o modificar información desactualizada almacenada por el sistema. Esto es fundamental para mantener la integridad y exactitud de los datos, especialmente cuando estos son utilizados para ofrecer servicios personalizados o ejecutar acciones automáticas.

**3. Derecho de supresión (derecho al olvido)**

Este derecho permite al usuario solicitar que sus datos personales sean eliminados de forma parcial o total cuando ya no sean necesarios para los fines originales, cuando haya retirado su consentimiento, o cuando considere que se están usando de forma indebida.

**4.Derecho a presentar reclamaciones**

El usuario tiene el derecho a presentar una queja si considera que sus derechos han sido vulnerados o que sus datos se han usado de forma indebida. Esta reclamación puede hacerse directamente a SmartHome Solutions o a una autoridad pública de protección de datos.

SmartHome Solutions está obligada a responder dentro de un plazo máximo de 30 días hábiles desde la recepción de la solicitud. Si el caso es complejo, se puede ampliar este plazo, pero siempre informando al usuario sobre el motivo de la demora.

**Responsabilidades del Usuario**

Así como SmartHome Solutions se compromete a respetar los derechos de privacidad de los usuarios y proteger sus datos personales, también es fundamental que los propios usuarios actúen con responsabilidad al utilizar el sistema de hogar inteligente.

El buen funcionamiento, la seguridad y la protección de los datos personales no dependen únicamente del diseño técnico del sistema, sino también de la conducta ética y consciente de quienes lo utilizan. A continuación, se detallan las principales responsabilidades del usuario en relación con el uso de la aplicación y la gestión de sus datos:

**1. Veracidad y actualización de los datos**

El usuario es responsable de proporcionar información precisa, completa y actualizada al registrarse o configurar su perfil.  
Si los datos cambian, el usuario deberá modificarlos oportunamente para evitar errores en el sistema o riesgos de seguridad.

**2. Protección del acceso**

El usuario debe mantener segura su cuenta de acceso, usando contraseñas robustas, evitando compartirlas con otras personas y cerrando sesión en dispositivos públicos.  
Asimismo, debe vigilar qué personas del hogar tienen acceso a los dispositivos y asegurarse de que los permisos y roles asignados sean adecuados.

**3. Uso responsable del sistema**

El sistema está diseñado para mejorar la calidad de vida, no para ser utilizado de manera abusiva, invasiva o ilegal. El usuario se compromete a:

* No manipular datos para fines indebidos.
* No usar dispositivos conectados para espiar o invadir la privacidad de otros.
* No desactivar funciones de seguridad o protección de forma intencional sin justificación.

**4. Gestión de dispositivos en caso de transferencia**

En caso de venta, devolución o cesión de un producto conectado, el usuario debe asegurarse de:

* Restablecer el dispositivo a su configuración de fábrica.
* Eliminar cualquier vínculo con su cuenta personal.
* Borrar todos los datos personales almacenados en el equipo o en la aplicación.
* Esto garantiza que la información anterior no quede expuesta al nuevo usuario del sistema