Política de privacidad y protección de datos

1- Política de privacidad y protección de datos personales.
SmartHome Solutions se compromete a respetar y proteger su privacidad. Los datos de los usuarios que ingresen al programa, serán preservados de manera confidencial. No serán divulgados ni compartidos con terceras partes ni serán utilizados para fines distintos a lo indicado en la presente política.

Los datos se recolectarán únicamente para obtener informaciones estadísticas que ayuden en la mejora en versiones siguientes del programa y presentar resúmenes de cambios y/o ayuda a los usuarios correspondientes.

El programa tiene como función ofrecer a los usuarios una mejor gestión y vinculación de los dispositivos inteligentes que se encuentran dentro de una vivienda, con la finalidad de que su experiencia sea grata y beneficiosa, garantizando un sistema seguro, eficiente, confiable, optimizado en costos y sostenible.

Esta política se establece para la protección de la privacidad de las personas visitantes al programa, así como de la seguridad de la información relativa a ellas.

Toda información que se ingrese de sus usuarios al programa, será debidamente resguardada, de maneral tal que no podrá comunicarse, modificarse o divulgarse públicamente, sino bajo las condiciones y en los casos que la ley N° 25.326 de Protección de los Datos Personales lo establezca o lo autorice.

SmartHome Solutions empleará todos los medios técnicos y tomará todos los resguardos legales necesarios para asegurar la protección de los datos personales y la privacidad de los mismos.

2- Definición de los términos de política de privacidad y protección de datos personales.
Para la interpretación de los términos que sean utilizados en la política como así también en la normativa se entenderán, según el Art. 2 de la ley 25.326:

- Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables (tales como: nombre y apellido, DNI, fecha de nacimiento, sexo, domicilio real, número de teléfono celular, una dirección válida de correo electrónico, entre otros.
- Datos sensibles: Datos Personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

- Archivo, registro base o banco de datos: Indistintamente, designan al conjunto
  organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación almacenamiento, organización o acceso.
- Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de Datos Personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.
- Responsable de archivo, registro, base o banco de datos: Persona humana o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.
- Datos informatizados: Son los Datos Personales sometidos al tratamiento o procesamiento electrónico o automatizado.
- Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto de tratamiento de acuerdo con la legislación vigente.
- Usuario de los datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.
- Disociación de Datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.
- Cesión de datos: toda revelación o comunicación de datos realizada en el marco de esta Política y de SmartHome Solutions.
- Derecho de acceso: es el derecho que permite al titular del dato saber si se encuentra o no incluido en un banco de datos; todos los datos relativos a su persona incluidos en ese banco de datos; la finalidad del tratamiento y los eventuales cesionarios de la información.
- Derechos de información: es el derecho que permite a cualquier persona solicitar a la AAIP información sobre la existencia de bases de datos, sus finalidades y la identidad de los responsables conforme se explica en esta Política.
- Derecho de rectificación, actualización y supresión: son los derechos que permiten al titular corregir la información falsa, errónea, incompleta o incorrecta relacionada a sus Datos Personales existente en una base de datos.

3- Procesamiento de recolección, verificación, administración y destrucción de datos personales.
SmartHome Solutions recopila la información personal, tal como nombre y apellido, correo electrónico y vinculación de todos los dispositivos tecnológicos

en el hogar, que tengan la capacidad de asociarse al programa, al momento de realizar el registro y/o creación de la cuenta. SmartHome Solutions no solicitara información que sea incompatible con la finalidad de sus actividades, ni que directa o indirectamente revele datos sensibles, como ser datos que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical, información referente a la salud o a la vida sexual. SmartHome Solutions utilizara la información de los/las usuarios para:

- Datos de contacto para registrar en su usuario, fines estadísticos que puedan ayudar a la mejora del programa, y la interacción entre el usuario y los dispositivos vinculados, con finalidad de reducir costos para el usuario y tener conciencia ambiental, cumpliendo el objetivo y finalidad del programa.
- Notificación por parte del programa hacia el usuario, danto alternativas y mejoras que, mediante la recopilación y el proceso estadísticos con respecto al global de usuarios, pueda brindar cuando los parámetros se encuentren por debajo de lo estimado, con un propósito de “ayuda” y no de “restricción” hacia el usuario.

En caso de cesión o utilización para una finalidad diferente, SmartHome Solutions solicitara a los usuarios su consentimiento libre, expreso e informado. En el supuesto de comprobarse que los datos personales recolectados no resulten útiles o que se cumplió con el fin para el cual fue recabado, los mismos deberán destruirse conforme al procedimiento de eliminación segura de información.

4- Seguridad de los datos personales.
SmartHome Solutions implementara todas las medidas necesarias para mantener la seguridad de la información personal que brindan los/as usuarios/as, contemplado las medidas técnicas y organizativas internas necesarias para garantizar la seguridad y confidencialidad de los datos, tratando por todos los medios de evitar el acceso no autorizados a los mismos.

El acceso a los datos personales está restringido a empleados y proveedores de SmartHome Solutions, y a terceras partes ajenas a SmartHome Solutions.

Sin perjuicio a lo expuesto, considerando que internet es un sistema abierto, de acceso al público. SmartHome Solutions no puede garantizar que terceros no autorizados no puedan eventualmente superar las medidas de seguridad y utilizar la información de los/as usuarios/as en forma indebida. En todo caso, SmartHome Solutions mantiene planes de seguridad y de respuestas a incidentes, para ser controlados con el acceso no autorizado a la información privada que recopila o almacena.

5- Derecho de los usuarios sobre sus datos.

Las personas titulares de los datos cuentan con los siguientes derechos:

- Derecho a la información: Solicitar al organismo de control la información registrada desde el momento de alta de la cuenta, esta información debe ser clara, amplia y completa.
- Derecho de acceso: obtener la información de sus datos personales registrados y dispositivos vinculados al programa, resúmenes estadísticos que impliquen en la mejora de las funcionalidad y recomendaciones que cumplan con la misión de la empresa.

Plan de Gestión de trabajo en equipo

El trabajo fue realizado en conjunto, si bien cada alumno era responsable de un área en particular, la consulta y el abordaje de áreas distintas, ayudaron al enriquecimiento y el mejor desenvolvimiento del trabajo, teniendo como punto valido, abordar el problema desde otro punto de vista y poder desarrollarlo de forma efectiva.

De acuerdo a lo detallado anteriormente, dividimos la gestión del proyecto con los siguientes encargados:

Apellido y Nombre	DNI	Detalles
Aballay Javier Ali	-	Se cambio de grupo
Camolotto Alejo Nicolas	44.606.044	Base de datos
Fiori Debi	-	Abandono
Flores Lopez Giancarlo	95.113.172	Ética y Deontología Profesional
Quevedo Jorge Francisco	31.218.408	Programación I
Quevedo Oscar Alberto	34.839.723	Programación I

Análisis de Impacto

El análisis de impacto es un proceso fundamental que permite identificar y evaluar los riesgos asociados con el tratamiento de datos personales en SmartHome Solutions. Este análisis se va a estructurar en las siguientes etapas:

a) Identificación de Datos Sensibles

Tipos de Datos Recopilados, es crucial identificar qué datos se recopilan, en el caso de SmartHome Solutions, esto incluye:

- Datos de Identificación: Nombre, apellido, número de documento, dirección de correo electrónico.
- Datos de Dispositivos: Información sobre los dispositivos inteligentes vinculados, como tipo, modelo y configuraciones.
- Datos de Uso: Información sobre cómo los usuarios interactúan con el programa, incluyendo patrones de uso y preferencias.
- Clasificación de Datos: Los datos deben clasificarse según su sensibilidad. Por ejemplo, los datos que revelan información sobre la salud o la vida sexual se consideran datos sensibles y requieren un tratamiento especial.

b) Evaluación de Riesgos

Identificación de Amenazas Potenciales, se deben considerar diversas amenazas, como:

- Acceso No Autorizado: Posibilidad de que terceros accedan a datos personales sin autorización.
- Pérdida de Datos: Riesgo de que los datos se pierdan debido a fallos técnicos o errores humanos.
- Violaciones de Seguridad: Ataques cibernéticos que comprometan la integridad de los datos.

Análisis de Impacto: Cada riesgo identificado debe ser evaluado en términos de su probabilidad de ocurrencia y el impacto que tendría sobre los usuarios. Por ejemplo:

- ❖ Un acceso no autorizado a datos sensibles podría tener un impacto grave en la privacidad de los usuarios y su confianza en el servicio.

c) Medidas de Mitigación

Implementación de Controles Técnicos:

- Cifrado de Datos: Utilizar cifrado para proteger los datos personales tanto en tránsito como en reposo.
- Autenticación de Dos Factores: Requerir un segundo método de verificación para acceder a cuentas de usuario.

Controles Organizativos: Establecer políticas y procedimientos claros sobre el manejo de datos, incluyendo:

- Auditorías Regulares: Realizar auditorías de seguridad periódicas para evaluar la efectividad de las medidas de protección.
- Capacitación del Personal: Proporcionar formación regular a los empleados sobre la importancia de la protección de datos y las mejores prácticas.

Plan de actualización

El plan de actualización debe ser un documento dinámico que se ajuste a las necesidades cambiantes de la organización y a la evolución de la legislación sobre protección de datos.

a. Frecuencia de Revisión

- Revisiones Anuales: Se recomienda realizar revisiones anuales de la política de privacidad y el análisis de impacto para asegurarse de que se mantenga actualizado.
- Actualizaciones por Cambios Normativos: Cualquier cambio en la legislación sobre protección de datos debe ser evaluado y reflejado en la política de inmediato.

b. Capacitación Continua

- Programas de Capacitación: Implementar programas de capacitación continua para todos los empleados sobre la importancia de la privacidad y la protección de datos.
- Simulacros de Seguridad: Realizar simulacros de incidentes de seguridad para preparar al personal sobre cómo responder en caso de una violación de datos.

c. Actualización de Documentación

- Mantenimiento de Registros: Asegurarse de que toda la documentación relacionada con la política de privacidad se mantenga actualizada y accesible para los usuarios.
- Comunicación de Cambios: Informar a los usuarios sobre cualquier cambio significativo en la política de privacidad o en el tratamiento de datos.

d. Evaluación de Nuevas Tecnologías

- Análisis de Impacto de Nuevas Tecnologías: Antes de implementar nuevas tecnologías, realizar un análisis de impacto para evaluar cómo afectarán la recolección y el tratamiento de datos personales.
- Pruebas de Seguridad: Realizar pruebas de seguridad antes de la implementación de nuevas funciones o tecnologías que involucren datos personales.

Manual ético para usuarios finales

Introducción

El manual ético tiene como objetivo proporcionar a los usuarios finales de SmartHome Solutions una guía clara sobre el uso responsable y ético del programa. La tecnología debe utilizarse de manera que respete la privacidad y los derechos de todos los usuarios, fomentando un entorno seguro y confiable.

Principios Éticos

1. **Transparencia**
    - **Información Clara**: Los usuarios deben recibir información clara y comprensible sobre qué datos se recopilan, cómo se utilizan y con quién se comparten.
    - **Acceso a la Política**: La política de privacidad debe estar fácilmente accesible dentro del programa y en el sitio web.
2. **Consentimiento**
    - **Consentimiento Informado**: Los usuarios deben proporcionar su consentimiento explícito antes de que se recopilen sus datos. Esto incluye una descripción clara de los propósitos para los cuales se utilizarán los datos.
    - **Opciones de Exclusión**: Los usuarios deben tener la opción de optar por no participar en la recopilación de datos no esenciales.
3. **Responsabilidad**
    - **Manejo de Credenciales**: Los usuarios son responsables de mantener la confidencialidad de sus credenciales de acceso y deben cambiar sus contraseñas regularmente.
    - **Notificación de Incidentes**: Los usuarios deben notificar a SmartHome Solutions sobre cualquier uso no autorizado de su cuenta.
4. **Respeto a la Privacidad**
    - **Uso Responsable de la Tecnología**: Los usuarios deben utilizar la tecnología de manera que no invadan la privacidad de otros, como el uso de dispositivos de grabación sin el consentimiento adecuado.
    - **Compartición de Información**: Los usuarios deben ser cautelosos al compartir información personal en plataformas públicas o en redes sociales.
5. **Cumplimiento Legal**

- **Adherencia a Normativas**: Los usuarios deben cumplir con todas las leyes y regulaciones aplicables en materia de protección de datos y privacidad.
- **Conocimiento de Derechos**: Los usuarios deben estar informados sobre sus derechos en relación con sus datos personales.

Derechos de los Usuarios

1. **Derecho a la Información**
    - Los usuarios tienen derecho a solicitar información sobre qué datos personales se están recopilando y con qué finalidad. SmartHome Solutions debe proporcionar esta información de manera clara y accesible.
2. **Derecho de Acceso y Rectificación**
    - Los usuarios pueden acceder a sus datos personales y solicitar correcciones si la información es incorrecta o incompleta. Este proceso debe ser sencillo y rápido.
3. **Derecho a la Supresión**
    - Los usuarios tienen el derecho de solicitar la eliminación de sus datos personales en cualquier momento, siempre que no existan obligaciones legales que impidan su eliminación. SmartHome Solutions debe tener un procedimiento claro para manejar estas solicitudes.
4. **Derecho a la Portabilidad de Datos**
    - Los usuarios pueden solicitar que sus datos personales sean transferidos a otro proveedor de servicios, en un formato estructurado y de uso común, facilitando la movilidad de los datos.
5. **Derecho a la Oposición**
    - Los usuarios tienen el derecho de oponerse al tratamiento de sus datos personales en ciertos contextos, especialmente cuando se utilizan para fines de marketing.

Conclusión

Este manual ético es una herramienta fundamental para garantizar que todos los usuarios de SmartHome Solutions utilicen el programa de manera responsable y respeten la privacidad de los demás. Se alienta a los usuarios a revisar este manual periódicamente y a estar informados sobre sus derechos y responsabilidades. La colaboración de todos es esencial para crear un entorno digital seguro y de confianza.