

# POLÍTICA DE PRIVACIDAD Y MANEJO DE DATOS PERSONALES (AVISO INTEGRAL)

## SECCIÓN 1: IDENTIDAD, DECLARACIONES Y DOMICILIO DEL RESPONSABLE

### 1.1. Identidad del Responsable

El presente Aviso de Privacidad se emite en cumplimiento con la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)** y su Reglamento. La entidad responsable de la recolección, resguardo y tratamiento de sus datos personales es **Aetherion Systems S.A. de C.V.** (en adelante referida como "EL RESPONSABLE"), una sociedad mercantil debidamente constituida bajo las leyes de los Estados Unidos Mexicanos, con facultades plenas para la gestión tecnológica y operativa de la plataforma denominada **Skantis**.

### 1.2. Declaraciones de "EL RESPONSABLE"

Aetherion Systems, a través de su arquitectura técnica Skantis, declara bajo protesta de decir verdad lo siguiente:

- Legalidad:** Que cuenta con las autorizaciones necesarias para operar sistemas de gestión de incentivos digitales y procesamiento de datos en el estado de Aguascalientes.
- Infraestructura:** Que posee la infraestructura técnica propia y mediante servicios de nube de alta seguridad para garantizar que los datos personales no sean vulnerados, alterados o extraviados.
- Compromiso Ético:** Que el tratamiento de los datos personales de los usuarios de Skantis se rige por los principios de **Licitud, Consentimiento, Información, Calidad, Finalidad, Lealtad, Proporcionalidad y Responsabilidad**, de conformidad con el Artículo 6 de la LFPDPPP.

### 1.3. Domicilio Legal y de Notificaciones

Para todos los efectos legales relacionados con el presente Aviso de Privacidad y el ejercicio de sus derechos ARCO, EL RESPONSABLE señala como su domicilio el ubicado en el complejo corporativo de tecnología en la **Ciudad de Aguascalientes, México**. Este domicilio será el punto receptor de cualquier solicitud física de acceso a la información,

previa cita y validación de identidad, para garantizar la seguridad de nuestra base de datos central.

#### 1.4. Designación del Oficial de Privacidad

Aetherion Systems ha designado un **Departamento de Datos Personales (Oficial de Privacidad)**, el cual está encargado de velar por la protección de su información al interior de la organización y de dar trámite a sus solicitudes. Los datos de contacto para cualquier duda relacionada con el manejo de su información son:

- **Área Responsable:** Departamento de Cumplimiento Legal y Ciberseguridad.
- **Correo Electrónico Directo:** [privacidad@aetherion.systems](mailto:privacidad@aetherion.systems)
- **Horario de Atención:** Lunes a Viernes de 9:00 a 17:00 horas (Hora del Centro de México).

#### 1.5. Ámbito de Aplicación de la Sección

Esta sección rige para toda interacción del usuario con los activos digitales de Skantis, incluyendo:

- La aplicación móvil (iOS y Android).
- Kioscos de acopio inteligentes operados por software de Aetherion.
- Plataformas de soporte técnico y portales de pago de servicios interconectados.

Al aceptar los presentes términos en la pantalla de inicio de Skantis, el USUARIO reconoce la personalidad jurídica de Aetherion Systems y se da por enterado de la ubicación y canales de comunicación para ejercer sus derechos sobre su información privada.

---

## SECCIÓN 2: DATOS PERSONALES SOMETIDOS A TRATAMIENTO

Para la operación eficiente del ecosistema Skantis, EL RESPONSABLE recabará y tratará diversas categorías de datos personales. Estos se clasifican según su naturaleza y la función técnica que desempeñan dentro de la infraestructura de Aetherion Systems.

### 2.1. Datos de Identificación y Contacto (Perfil de Usuario)

Son aquellos datos básicos necesarios para dar de alta al usuario en la base de datos central y permitir la personalización de la experiencia:

- **Nombre completo:** Requerido para la emisión de comprobantes internos de canje.
- **Correo electrónico:** Utilizado como identificador único de cuenta (UID) y canal primordial para el envío de confirmaciones de pago de servicios.

- Número telefónico móvil: Empleado como factor de autenticación secundaria y para el envío de alertas críticas sobre el estado de sus transacciones.

## **2.2. Datos de Localización y Georreferenciación (Obligatorios)**

Dado que los beneficios de Skantis están limitados geográficamente al estado de Aguascalientes, la aplicación recolecta:

- Coordenadas GPS (Latitud y Longitud): Capturadas en el momento exacto de cada escaneo de residuos y cada solicitud de canje de puntos.
- Datos de Red: Identificación de las torres de telefonía celular y puntos de acceso Wi-Fi cercanos para triangular y validar la posición, evitando el uso de "Fake GPS" o herramientas de emulación.
- Zonas de Interés: Registro de las estaciones de acopio físico de Aetherion visitadas con mayor frecuencia para optimizar las rutas de recolección logística.

## **2.3. Datos Técnicos del Dispositivo y Conectividad**

Para garantizar que la seguridad de los servidores de Aetherion Systems no se vea comprometida, el software recopila metadatos técnicos del terminal:

- Identificador de Dispositivo (IMEI / IDFA): Para vincular la cuenta a un hardware físico específico y prevenir accesos múltiples fraudulentos.
- Modelo de Hardware y Marca: Para optimizar el rendimiento del algoritmo de escaneo de cámara.
- Versión del Sistema Operativo: Vital para asegurar que el dispositivo cuenta con los parches de seguridad mínimos requeridos para manejar transacciones financieras.
- Dirección IP (Internet Protocol): Registrada en cada inicio de sesión para el monitoreo de intentos de intrusión y auditoría de ciberseguridad.

## **2.4. Datos de Comportamiento Ecológico y Transaccionales**

Información generada por el uso activo de la plataforma:

- Historial de Reciclaje: Registro detallado del tipo de material (PET, Aluminio, etc.), peso estimado y frecuencia de entrega.
- Balance de Eco-Tokens: Registro histórico de puntos acumulados, puntos en tránsito (en proceso de validación) y puntos redimidos.
- Datos de Terceros (Proveedores): Números de servicio, números de medidor o referencias de contratos de servicios públicos (ej. CFE,

MIAA) que el usuario registra voluntariamente para aplicar los pagos. Aetherion Systems no almacena datos de tarjetas de crédito o débito, limitándose al manejo de los Eco-Tokens como método de pago.

## **2.5. Datos Sensibles y Biométricos**

Skantis no recolecta de forma directa datos personales sensibles (origen étnico, estado de salud, creencias religiosas). Sin embargo, en caso de que el usuario active la Autenticación Biométrica (FaceID o TouchID), se establece lo siguiente:

- El procesamiento de la huella o rostro se realiza exclusivamente de forma local dentro del enclave seguro (Secure Enclave) del dispositivo del usuario.
- Aetherion Systems solo recibe del sistema operativo un "token de éxito" o "error"; en ningún momento la imagen de la huella o el rostro es transmitida, almacenada o procesada en nuestros servidores centrales.

## **2.6. Veracidad de la Información**

---

# **SECCIÓN 3: FINALIDADES DEL TRATAMIENTO DE LOS DATOS**

Aetherion Systems trata los datos personales recabados a través de Skantis con el objetivo de garantizar una experiencia de usuario segura, eficiente y legalmente válida. El tratamiento se divide en dos categorías, de conformidad con los lineamientos de transparencia vigentes.

## **3.1. Finalidades Primarias (Originarias y Necesarias)**

Estas finalidades son esenciales para la existencia, mantenimiento y cumplimiento de la relación jurídica entre EL USUARIO y EL RESPONSABLE. La negativa a estas finalidades imposibilitará la prestación del servicio:

- Gestión de Identidad y Acceso: Validar que cada cuenta corresponde a un usuario único para evitar la duplicidad de incentivos y asegurar que los Eco-Tokens sean asignados al titular legítimo.
- Validación de la Economía Circular: Utilizar los datos de geolocalización y reconocimiento de imagen para certificar que el proceso de reciclaje se realizó físicamente en las estaciones de acopio de Aguascalientes.

Esto previene el fraude sistémico y asegura la integridad del inventario de residuos de Aetherion Systems.

- Ejecución de Pagos de Servicios: Procesar la transferencia de valor digital desde el balance del usuario hacia los sistemas de facturación de proveedores (CFE, MIAA, etc.). Esto requiere la manipulación técnica de números de contrato y referencias de pago bajo estrictos protocolos de encriptación.
- Seguridad Informática y Auditoría: Monitorear el tráfico en los servidores encriptados de Aetherion para detectar patrones de conducta inusuales, intentos de hacking, o uso de software prohibido, garantizando que la plataforma sea un entorno seguro para todos los ciudadanos.
- Soporte Técnico y Atención al Usuario: Contactar al titular en caso de fallas en el procesamiento de sus puntos, errores en la redención de beneficios o actualizaciones críticas de seguridad en la aplicación.

### **3.2. Finalidades Secundarias (Adicionales)**

Finalidades que, si bien no son indispensables para el servicio básico, permiten a Aetherion Systems mejorar el impacto del proyecto Skantis:

- Análisis Estadístico y Planeación Urbana: Generar informes anónimos y agregados sobre los hábitos de reciclaje en las distintas zonas de Aguascalientes. Estos datos pueden ser compartidos con dependencias municipales para optimizar las rutas de recolección de basura y políticas ambientales.
- Personalización de la Experiencia: Sugerir al usuario los puntos de acopio más cercanos basados en su historial de ubicación y enviarle recordatorios personalizados sobre el impacto ambiental positivo que ha generado.
- Comunicación de Campañas de Incentivos: Notificar sobre temporadas de "Puntos Dobles" o convenios temporales con nuevas marcas o comercios locales que acepten Eco-Tokens.
- Mejora de Algoritmos: Utilizar de forma disasociada las imágenes de los residuos escaneados para entrenar la Inteligencia Artificial de Aetherion, logrando que el reconocimiento de materiales sea cada vez más rápido y preciso.

### **3.3. Mecanismo para Manifestar la Negativa**

EL USUARIO puede, en cualquier momento, manifestar su negativa para el tratamiento de sus datos personales para las Finalidades Secundarias

mediante el envío de un correo electrónico a [soporte@aetherionsystems.com](mailto:soporte@aetherionsystems.com). Es importante señalar que la revocación del consentimiento para las Finalidades Primarias implicará la cancelación automática de la cuenta y la pérdida del balance de puntos acumulados, dado que el sistema no puede operar sin la validación técnica mínima de identidad y ubicación.

### 3.4. Conservación de la Información

Los datos relacionados con las transacciones financieras (pagos de servicios) se conservarán por un periodo de hasta 5 años, conforme a las leyes fiscales mexicanas. Los datos de geolocalización y uso diario se conservarán por un máximo de 24 meses de inactividad, tras los cuales serán eliminados de los servidores activos de Aetherion y movidos a un archivo histórico encriptado o destruidos permanentemente.

---

## SECCIÓN 4: TRANSFERENCIA DE DATOS PERSONALES Y COMUNICACIÓN INTER-SISTEMAS

**Aetherion Systems** se compromete a no vender, alquilar ni comercializar la base de datos de los usuarios de **Skantis** con agencias de marketing o terceros ajenos al programa. No obstante, para la ejecución del modelo de incentivos, se realizan transferencias de datos estrictamente necesarias bajo los términos del Artículo 37 de la LFPDPPP.

### 4.1. Transferencias que no requieren consentimiento

De acuerdo con la legislación mexicana, EL RESPONSABLE podrá transferir sus datos sin necesidad de su consentimiento en los siguientes casos:

1. Cuando la transferencia esté prevista en una Ley o Tratado.
2. Cuando sea necesaria para la prevención o el diagnóstico médico.
3. Cuando sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común de **Aetherion Systems**.
4. Cuando sea necesaria por virtud de un contrato celebrado o por celebrar en interés del USUARIO, por EL RESPONSABLE y un tercero.

### 4.2. Interoperabilidad con Proveedores de Servicios (Terceros Receptores)

Para que los Eco-Tokens se conviertan en descuentos reales, los servidores encriptados de Aetherion se comunican con los sistemas de terceros receptores mediante protocolos **API (Application Programming Interface)** de seguridad bancaria.

<b>Tercero Receptor</b>	<b>Finalidad de la Transferencia</b>	<b>Datos Transferidos</b>
<b>Proveedores de Energía (ej. CFE)</b>	Aplicación de abono al recibo de luz.	Número de servicio, monto de redención y token de transacción.
<b>Entidades de Agua (ej. MIAA)</b>	Pago de derechos de suministro y alcantarillado.	Número de contrato, referencia de pago y validación de domicilio.
<b>Empresas de Telecomunicaciones</b>	Recargas de saldo o pago de planes de datos.	Número telefónico a 10 dígitos y código de operador.
<b>Autoridades Municipales</b>	Auditoría de impacto ambiental y bonos verdes.	Datos estadísticos disociados (anónimos).

### 4.3. Protocolo de Seguridad en la Transferencia

Cada transferencia de datos mencionada anteriormente se realiza bajo los siguientes estándares de blindaje:

- **Tokenización de Identidad:** No enviamos su nombre completo al proveedor del servicio; enviamos un **Token Único de Transacción** que el proveedor valida contra el número de servicio para aplicar el pago.
- **Cifrado de Capa de Transporte (TLS):** Los datos viajan por canales privados de comunicación (VPN) que impiden que cualquier nodo intermedio de internet vea la información.
- **Firmas Digitales:** Cada petición enviada desde los servidores de **Aetherion Systems** cuenta con una firma digital única que garantiza que el mensaje no ha sido alterado y que proviene legítimamente de **Skantis**.

### 4.4. Remisión a Encargados de Tratamiento

EL RESPONSABLE utiliza proveedores de infraestructura (como Amazon Web Services o Google Cloud) para el almacenamiento de la información. Estos proveedores actúan como "Encargados" y están obligados contractualmente a mantener los mismos o superiores niveles de seguridad que los descritos en este Aviso de Privacidad, teniendo prohibido

utilizar los datos para cualquier fin distinto al almacenamiento y respaldo solicitado por Aetherion Systems.

#### 4.5. Transferencias Internacionales

Debido a que algunos servidores de respaldo pueden ubicarse fuera del territorio nacional, sus datos pueden ser transferidos a países con leyes de protección de datos similares a las mexicanas (como Estados Unidos o la Unión Europea). **Aetherion Systems** garantiza que estas transferencias se realizan bajo cláusulas contractuales estándar que aseguran que sus datos permanezcan protegidos por el estándar AES-256 en todo momento.

---

## SECCIÓN 5: DERECHOS ARCO (ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN)

De conformidad con la normativa vigente, EL USUARIO posee la facultad de ejercer en todo momento sus derechos de **Acceso, Rectificación, Cancelación y Oposición (Derechos ARCO)** sobre los datos personales que se encuentran bajo el resguardo de **Aetherion Systems**.

### 5.1. Definición de los Derechos

Para efectos de este aviso, se entiende por:

- **Acceso:** El derecho de EL USUARIO a conocer qué datos personales obran en las bases de datos encriptadas de Aetherion, para qué se utilizan y las condiciones del tratamiento que se les da.
- **Rectificación:** El derecho a solicitar la corrección de su información personal en caso de que esté desactualizada, sea inexacta o incompleta.
- **Cancelación:** El derecho a que su información sea eliminada de nuestros registros o bases de datos cuando considere que la misma no está siendo utilizada conforme a los principios de ley o cuando su cuenta de Skantis sea dada de baja.
- **Oposición:** El derecho a oponerse al uso de sus datos personales para fines específicos (por ejemplo, para finalidades secundarias como estadísticas o marketing).

### 5.2. Procedimiento para el Ejercicio de Derechos

Para ejercer cualquiera de los derechos mencionados, EL USUARIO deberá presentar una solicitud formal dirigida al **Oficial de Privacidad de Aetherion Systems** a través del correo electrónico: [privacidad@aetherion.systems](mailto:privacidad@aetherion.systems).

La solicitud deberá contener y acompañarse de lo siguiente (Requisitos de Ley):

1. **Identificación del Titular:** Nombre completo y copia digital de una identificación oficial vigente (INE, Pasaporte o Cédula Profesional) para acreditar la identidad.



2. **Descripción Clara:** La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO.
3. **Indicación de Cambio:** En el caso de solicitudes de rectificación, deberá indicar las modificaciones a realizarse y aportar la documentación que sustente su petición.
4. **Información de Contacto:** Cualquier otro elemento o documento que facilite la localización de los datos personales (ej. el número telefónico asociado a la cuenta Skantis).

### 5.3. Plazos de Respuesta y Ejecución

**Aetherion Systems** se obliga a seguir los siguientes plazos legales:

- **Prevención:** Si la solicitud es insuficiente o falta algún documento de identidad, EL RESPONSABLE contará con 5 (cinco) días hábiles para requerir al usuario la información faltante.
- **Resolución:** Una vez recibida la solicitud completa, se comunicará la determinación adoptada en un plazo máximo de **20 (veinte) días hábiles** contados desde la fecha de recepción.
- **Ejecución:** Si la solicitud resulta procedente, se hará efectiva dentro de los **15 (quince) días hábiles** siguientes a la fecha en que se comunique la respuesta.

### 5.4. Revocación del Consentimiento

Usted puede revocar el consentimiento que, en su caso, nos haya otorgado para el tratamiento de sus datos personales. Sin embargo, es importante que tenga en cuenta que no en todos los casos podremos atender su solicitud o concluir el uso de forma inmediata, ya que es posible que por alguna **obligación legal** (como registros fiscales de pagos de CFE o MIAA realizados anteriormente) requiramos seguir tratando sus datos.

Asimismo, usted deberá considerar que, para ciertos fines, la revocación de su consentimiento implicará que no le podamos seguir prestando el servicio de la plataforma **Skantis**, o la conclusión de su relación con **Aetherion Systems**.

### 5.5. Limitación del Uso o Divulgación de los Datos

Además del ejercicio de los derechos ARCO, EL USUARIO puede limitar el uso de su información personal inscribiéndose en el **Registro Público para Evitar Publicidad (REPEP)** de la Procuraduría Federal del Consumidor (PROFECO), o bien, solicitando su registro en la "Lista de Exclusión de Aetherion", para que sus datos no sean utilizados con fines publicitarios o mercadotécnicos por parte de nuestra empresa.

---

## SECCIÓN 6: ARQUITECTURA DE SEGURIDAD, ENCRIPCIÓN Y RESILIENCIA DE DATOS

### 6.1. Blindaje de la Infraestructura de Aetherion Systems

El ecosistema **Skantis** reside en una infraestructura de servidores privados operada por **Aetherion Systems**, diseñada bajo la premisa de "Seguridad por Diseño" (Security by Design). Los centros de datos donde se aloja la información de los usuarios cumplen con las certificaciones internacionales **ISO/IEC 27001** (Gestión de Seguridad de la Información) y **SOC 2 Tipo II**, garantizando que los controles de seguridad, disponibilidad y confidencialidad sean auditados rigurosamente de forma anual.

## 6.2. Protocolos de Encriptación de Grado Militar

Toda la información que transita entre el dispositivo móvil del USUARIO y los servidores de Aetherion Systems, así como la información almacenada en estado de reposo (Data at Rest), se encuentra protegida mediante los siguientes estándares:

- **Encriptación en Tránsito:** Se utilizan túneles de comunicación cifrados mediante **TLS 1.3 (Transport Layer Security)** con certificados de validación extendida. Esto asegura que ningún tercero, incluyendo proveedores de internet o atacantes "Man-in-the-Middle", pueda interceptar o leer los datos de geolocalización o los números de contrato de servicios.
- **Encriptación en Reposo:** Los discos duros y bases de datos de nuestros servidores emplean el estándar **AES-256 (Advanced Encryption Standard)** de 256 bits. Este nivel de encriptación es el mismo utilizado por instituciones bancarias y agencias gubernamentales a nivel global; se estima que, con la tecnología computacional actual, romper este cifrado tomaría miles de millones de años.

## 6.3. Descentralización y Fragmentación de Datos Sensibles

Para minimizar el impacto de cualquier posible vulnerabilidad, Aetherion Systems implementa un modelo de **Fragmentación de Datos**. Esto significa que el nombre del usuario, sus coordenadas GPS y sus balances de puntos no se almacenan en una única base de datos lineal. La información es segmentada y distribuida en diferentes nodos de servidor; de este modo, incluso en el hipotético caso de un acceso no autorizado a uno de los nodos, la información obtenida sería ilegible e incompleta, al carecer de las "llaves maestras" de reconstrucción que se almacenan en un **Hardware Security Module (HSM)** físicamente aislado.

## 6.4. Gestión de Identidades y Autenticación Multi-Factor (MFA)

La seguridad del acceso a la cuenta de Skantis es responsabilidad compartida. Aetherion Systems ofrece y recomienda la activación de la **Autenticación Multi-Factor**. Al realizar operaciones de canje de puntos para el pago de servicios de alto valor (como recibos de CFE o MIAA), el sistema requiere una segunda capa de verificación, ya sea mediante:

1. Tokens de un solo uso (TOTP) generados por aplicaciones de autenticación.
2. Verificación biométrica (Huella dactilar o FaceID) procesada localmente en el dispositivo del usuario, sin que la biometría cruda salga nunca del terminal.

## 6.5. Resiliencia, Backups y Recuperación ante Desastres

Los servidores de Skantis cuentan con redundancia geográfica. Esto significa que existen espejos de la base de datos en múltiples ubicaciones físicas dentro y fuera del estado de

Aguascalientes para garantizar la continuidad del servicio ante desastres naturales o fallos de infraestructura regional. Los respaldos (backups) se generan cada 15 minutos de forma automatizada y son sometidos a pruebas de integridad para asegurar que el balance de Eco-Tokens de cada ciudadano esté siempre a salvo.

## 6.6. Auditorías de Intrusión y "Ethical Hacking"

Aetherion Systems contrata periódicamente servicios de firmas externas especializadas en ciberseguridad para realizar **Pruebas de Penetración (Pentesting)**. Estas pruebas simulan ataques cibernéticos reales para identificar y parchar vulnerabilidades antes de que puedan ser explotadas. Asimismo, contamos con un sistema de detección de anomalías basado en Inteligencia Artificial que bloquea direcciones IP sospechosas y reporta intentos de fuerza bruta en milisegundos.

## 6.7. Confidencialidad del Personal Técnico

El acceso físico y lógico a los servidores de Aetherion Systems está restringido a un grupo mínimo de ingenieros de alto nivel, quienes han pasado por pruebas de confianza y han firmado acuerdos de confidencialidad (NDA) perpetuos. Cada acceso a la base de datos de producción queda registrado en un log inalterable, auditado por un oficial de cumplimiento externo.

---

# SECCIÓN 7: USO DE COOKIES, WEB BEACONS Y TECNOLOGÍAS DE RASTREO (LOGS)

**Aetherion Systems** informa que en sus plataformas digitales (aplicación móvil **Skantis** y portal web asociado), utilizamos cookies, web beacons y otras tecnologías de monitoreo que permiten mejorar la experiencia del usuario y garantizar la seguridad de los servidores encriptados.

## 7.1. Definición y Alcance Técnico

- **Cookies:** Son archivos de datos que se almacenan en el almacenamiento local de su dispositivo al navegar o utilizar la aplicación. Estos archivos permiten recordar sesiones activas, preferencias de idioma y configuraciones de personalización.
- **Web Beacons:** Imágenes transparentes insertadas en la interfaz o correos electrónicos que permiten a **Aetherion Systems** monitorear el comportamiento del usuario, como la confirmación de lectura de notificaciones de pago o el tiempo de permanencia en una sección de la App.
- **Server Logs:** Registros automáticos que capturan la dirección IP, el tipo de navegador, el ISP (Proveedor de Servicios de Internet), páginas de referencia/salida y sellos de fecha/hora.

## 7.2. Datos Recabados a través de estas Tecnologías

A través de estas herramientas tecnológicas, **EL RESPONSABLE** obtiene la siguiente información:

1. **Hábitos de Navegación:** Secciones de la aplicación Skantis más visitadas y frecuencia de uso del escáner de residuos.
2. **Identificadores de Sesión:** Para mantener la encriptación activa durante el proceso de pago de servicios y evitar que la sesión sea "secuestrada" por terceros.
3. **Estado del Hardware:** Información sobre fallos técnicos (crash reports) que permiten a nuestros ingenieros parchar vulnerabilidades de seguridad en tiempo real.

### 7.3. Deshabilitación de Tecnologías de Rastreo

EL USUARIO puede restringir, bloquear o borrar las cookies y otras tecnologías de rastreo mediante la configuración de los ajustes de su dispositivo móvil o navegador. Sin embargo, **Aetherion Systems** hace notar que, por razones de seguridad sistémica, la deshabilitación de ciertas cookies técnicas impedirá la ejecución de transacciones críticas, como la redención de Eco-Tokens para el pago de agua (MIAA) o luz (CFE), ya que el sistema no podrá garantizar la integridad de la sesión encriptada.

---

## SECCIÓN 8: PROCEDIMIENTO PARA COMUNICAR CAMBIOS AL AVISO DE PRIVACIDAD

El presente Aviso de Privacidad puede sufrir modificaciones, cambios o actualizaciones derivadas de nuevos requerimientos legales, de nuestras propias necesidades por los productos o servicios que ofrecemos, de nuestras prácticas de privacidad, de cambios en nuestro modelo de negocio de economía circular, o por otras causas.

### 8.1. Canales de Notificación

**Aetherion Systems** se compromete a mantenerlo informado sobre los cambios que pueda sufrir el presente aviso a través de:

- **Notificaciones Push:** Enviadas directamente a su dispositivo móvil a través de la App Skantis.
- **Correo Electrónico:** Envío del aviso actualizado a la dirección registrada en su perfil.
- **Sitio Web:** Publicación de la versión vigente en [www.aetherion.systems.com](http://www.aetherion.systems.com).

### 8.2. Vigencia y Aceptación Tácita

Se entenderá que EL USUARIO consiente tácitamente el tratamiento de sus datos conforme a las actualizaciones de este aviso si, una vez publicadas las modificaciones, continúa utilizando los servicios de la plataforma Skantis o no manifiesta su oposición de forma expresa en un plazo de 5 (cinco) días hábiles posteriores a la notificación.

---

# SECCIÓN 9: CONSENTIMIENTO Y FIRMA DIGITAL

EL TITULAR de los datos personales declara haber leído y entendido el presente Aviso de Privacidad Integral de **Aetherion Systems**. Al hacer clic en el botón "**ACEPTO Y CONTINUAR**" dentro de la plataforma **Skantis**, otorga su consentimiento expreso para el tratamiento de sus datos personales, incluyendo las transferencias necesarias a proveedores de servicios públicos, bajo los protocolos de encriptación y seguridad descritos en este documento.

FECHA DE ÚLTIMA ACTUALIZACIÓN: 13 de enero de 2026.

EMISOR: Departamento de Protección de Datos de Aetherion Systems S.A. de C.V.