POLÍTICA DE PRIVACIDAD – FREEMINDTRONIC SL

Sitio web y software – Versión y fecha del documento: V2.0 del 28/02/2025

ARTÍCULO 1 – INTRODUCCIÓN

1.1. Identificación del responsable del tratamiento

La presente Política de Privacidad es emitida por **Freemindtronic SL**, sociedad de responsabilidad limitada registrada bajo las leyes del Principado de Andorra, con domicilio social en:

Av. Co-Príncipe de Gaulle, 13, Edificio Valira, Planta baja, AD700 Escaldes – Engordany, Andorra.

Freemindtronic es responsable del procesamiento de los datos recopilados o procesados a través del uso de su sitio web oficial https://freemindtronic.com , así como de su software, aplicaciones, extensiones y sistemas integrados.

1.2. Champ d'Application

Esta Política de Privacidad se aplica a todos los servicios, software, aplicaciones, extensiones y sistemas integrados desarrollados y operados por Freemindtronic.

No se aplica a los sitios web, servicios o plataformas de terceros a los que se puede acceder a través de los servicios de Freemindtronic. Freemindtronic no es responsable de las prácticas de privacidad de estos servicios de terceros.

1.3. Compromiso: Cero Confianza y Cero Conocimiento

Freemindtronic se adhiere a un estricto marco **Zero Trust & Zero Knowledge**, lo que garantiza que no se acceda, almacene ni comparta los datos de los usuarios.

Todo el software, las aplicaciones, las extensiones y los sistemas integrados desarrollados por Freemindtronic funcionan **sin un servidor remoto, una base de datos centralizada, la creación de una cuenta de usuario, la identificación del usuario y la transmisión de datos**.

Todas las funciones de Freemindtronic garantizan que los datos del usuario no se almacenen ni se transmitan a servidores remotos. Todo el procesamiento se lleva a cabo exclusivamente localmente en el dispositivo del usuario, sin interacción con una infraestructura externa.

1.4. Cumplimiento de la normativa

- Freemindtronic cumple con las normativas internacionales más estrictas en materia de protección de datos y ciberseguridad, entre las que se incluyen:
- Reglamento General de Protección de Datos (RGPD – Reglamento (UE) 2016/679)
- Ley de Resiliencia Operativa Digital (DORA – Règlement (UE) 2022/2554)
- Directiva NIS2 (Directiva (UE) 2022/2555) sobre la ciberseguridad de las infraestructuras críticas
- Ley de Privacidad del Consumidor de California (SCCA – EE. UU., Código Civil de California § 1798.100 et seq.)
- Ley General de Protección de Datos (LGPD – Brésil, Ley n.º 13.709/2018)
- Ley 15/2003 de Protección de Datos Personales en Andorra, modificada por la Ley Cualificada 29/2021
- Reglamento (UE) 2021/821, de 20 de mayo de 2021, sobre el control de las exportaciones de productos de doble uso

- Normas ISO/IEC 27001 y mejores prácticas de seguridad del NIST (Instituto Nacional de Normas y Tecnología, EE. UU.)

1.5. DefinicionesEn esta política, los siguientes términos se definen de la siguiente manera:

- **Datos personales** : cualquier información relativa a una persona física identificada o identificable, directa o indirectamente, en particular por referencia a un identificador como un nombre, un número de identificación, datos de localización, un identificador en línea, o a uno o más elementos específicos de su identidad física, fisiológica, genética, mental, económica, cultural o social.
- **Datos** sensibles: cualquier información cuya divulgación no autorizada pueda suponer un alto riesgo para los derechos y libertades de los interesados. Esto incluye, pero no se limita a:
    - Identificadores únicos (nombres de usuario, contraseñas, códigos de autenticación).
    - Claves de cifrado y autenticación.
    - Información de pago y datos bancarios.
    - Datos confidenciales de clientes y socios (estrategias comerciales, patentes, documentos protegidos por secretos comerciales).
    - Cualquier dato personal que entre en las categorías especiales del RGPD (origen étnico, opiniones políticas, creencias religiosas, salud, biometría, vida sexual).
- **Se** entiende por tratamiento cualquier operación o conjunto de operaciones que se realicen con datos personales, ya sea por medios automatizados o no, como la recogida, el registro, la organización, la estructuración, el almacenamiento, la adaptación o la modificación, la extracción, la consulta, el uso, la divulgación por transmisión, la difusión o cualquier otra forma de puesta a disposición, la cotejo o la combinación, limitación, supresión o destrucción.
- **Responsable del tratamiento** : la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de datos personales.
- **Encargado** del tratamiento: la persona física o jurídica, autoridad pública, agencia u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
- **Consentimiento** : cualquier manifestación libre, específica, informada e inequívoca de la voluntad del interesado por la que éste acepta, mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen.
- **Seudonimización** : tratamiento de datos personales de tal manera que ya no puedan atribuirse a una persona física concreta sin información adicional, que debe mantenerse separada y protegida por medidas técnicas y organizativas adecuadas.
- **Anonimización** : transformación irreversible de los datos personales de tal manera que ya no sea posible identificar directa o indirectamente al interesado.
- **Violación de datos personales** : Cualquier violación de la seguridad que accidental o ilegalmente resulte en la destrucción, pérdida, alteración, divulgación no autorizada o acceso a datos personales. Esto incluye el acceso no autorizado a inicios de sesión, contraseñas, claves de cifrado u otros datos confidenciales protegidos.

ARTÍCULO 2 – RECOGIDA Y TRATAMIENTO DE DATOS

2.1. Falta de recopilación sistemática de datos

Freemindtronic no recopila, almacena, comparte ni vende ningún dato personal o técnico de los usuarios, excepto en el caso de interacción directa, incluso para:

- Un pedido a través de las plataformas oficiales.

- Una solicitud de contacto relacionada con el servicio de atención al cliente o una asociación oficial.

Los datos solo se procesan dentro del estricto alcance de la ejecución del contrato o la relación comercial y nunca se utilizan para ningún otro propósito.

2.2. Datos que se pueden recopilar

Si un usuario proporciona información de forma voluntaria, solo se tratan los datos estrictamente necesarios:

- Identidad (apellidos, nombre)
- Datos de contacto (correo electrónico, teléfono, dirección de facturación y entrega)
- Información profesional
- Contenido enviado voluntariamente

Los datos transaccionales se utilizan exclusivamente para la gestión de los pedidos y su entrega, sin transmisión a terceros salvo por obligaciones legales (fiscales y contables).

2.2.1 – Datos almacenados localmente en la extensión o aplicaciónAlgunas aplicaciones y extensiones de Freemindtronic pueden utilizar localStorage o la API de almacenamiento web para almacenar temporalmente la configuración local en el dispositivo del usuario. Estos datos nunca se transmiten a servidores remotos y solo se puede acceder a ellos dentro del software utilizado.

2.3. Almacenamiento y seguridad de los datos

Freemindtronic aplica los más altos estándares de seguridad, cumpliendo con **las regulaciones GDPR, DORA, NIS2, ISO/IEC 27001 y NIST**.

- **Almacenamiento seguro fuera de línea** : Los datos se guardan en medios cifrados a los que solo se puede acceder a través de unidades flash USB seguras EviKey NFC y/o medios de almacenamiento cifrados y/o datos cifrados.
- **Zero Trust & Zero Knowledge** : Falta de servidores remotos y bases de datos centralizadas para almacenar y/o gestionar datos sensibles para todos los productos de Freemindtronic.
- **Seguridad reforzada para comunicaciones confidenciales**: El intercambio de datos confidenciales se realiza exclusivamente a través de **las herramientas DataShielder** o un protocolo seguro definido por el cliente.
- **Alternativa impuesta si es necesario** : Si el servicio al cliente no garantiza un nivel suficiente de seguridad, Freemindtronic ofrece **DataShielder** como único canal seguro.

2.4. Protección de datos clasificados y entornos sensibles

Las soluciones de Freemindtronic identificadas como un producto civil y militar de doble uso están diseñadas para proteger la información crítica e incluyen:

- **Aislamiento físico y partición** : No se almacenan datos en un servidor remoto.
- **Autenticación sólida** : NFC HSM y cifrado de clave segmentada patentado. El uso del cifrado asimétrico RSA-4096 permite que las claves CBC AES-256 se compartan de forma segura entre dispositivos HSM NFC, incluso de forma remota, sin transmisión a través de

infraestructuras centralizadas. Este mecanismo elimina el riesgo de exfiltración de claves y proporciona protección avanzada para los intercambios cifrados.
- **Cifrado de extremo a extremo** : AES-256 CBC, RSA-4096, PGP - Todos los sistemas de cifrado simétrico seguro se logran a través de claves segmentadas y sistemas de control de acceso patentados y entregados internacionalmente. Esta arquitectura hace que el cifrado sea resistente a los ataques cuánticos, lo que garantiza la protección a largo plazo de los datos confidenciales.
- **Registro descentralizado** : Caja negra local a la que solo puede acceder en NFC un administrador autorizado.
- **Pruebas de estrés y ciberseguridad proactiva** : evaluaciones periódicas contra ataques APT, espionaje industrial y amenazas cibernéticas avanzadas.

Si una extensión o aplicación de Freemindtronic accede a archivos locales en un dispositivo Windows o Mac (por ejemplo, para almacenar claves de cifrado o archivos seguros), estos archivos se procesan exclusivamente localmente y nunca son accesibles por terceros. El usuario conserva el control total sobre sus datos y no se comparten con otros servicios.

2.5. Almacenamiento, eliminación y retención de los datos del cliente

- Los datos proporcionados a través de un **formulario de contacto** se utilizan únicamente para responder a la solicitud y se eliminan inmediatamente después del procesamiento.
- Los datos del cliente resultantes de las transacciones se conservan solo durante el período legal necesario, de acuerdo con las regulaciones aplicables en las siguientes jurisdicciones:
    - **Andorra: Ley Cualificada 29/2021 – conservación de documentos fiscales durante 5 años**
    - **Unión Europea: Artículo 6 de la Directiva de Protección al Consumidor 2011/83/UE: retención de datos de transacciones durante un máximo de 10 años según los requisitos contables locales**
    - **Francia: Artículo L123-22 del Código de Comercio francés: conservación obligatoria de los documentos contables durante 10 años**
    - **EE. UU.: Publicación 583 del IRS - Retención de datos de transacciones de 3 a 7 años**
- **No se almacenan datos bancarios** : las transacciones se procesan a través **de proveedores externos seguros** (por ejemplo, PayPal).

2.6. Transferencias internacionales de datos

Freemindtronic no transfiere ningún dato fuera del EEE a menos que se aplique un marco legal adecuado (**Cláusulas Contractuales Estándar - CCT**).

2.7. Procedimiento de violación de datos

De conformidad con los artículos 33 y 34 del **RGPD** y la **Ley Cualificada 29/2021**, Freemindtronic aplica una **respuesta proactiva** en caso de incidencia:

- **Contención inmediata** y **análisis de impacto**.
- **Notificación en un plazo de 72 horas** a la Agencia Andorrana de Protección de Datos (APDA) si fuera necesario.
- **Informar a los usuarios afectados** si se identifica un alto riesgo.

- **Auditoría post-incidente** para reforzar las medidas de protección.

2.8. Ciberresiliencia y protección frente a catástrofes y ciberataques

Freemindtronic garantiza **la integridad y disponibilidad** de los datos incluso en caso de avería, robo, desastre o ciberataque masivo.

2.8.1. Cifrado y copia de seguridad segura

- **Cifrado avanzado** : AES-256 CBC, AES-256 CBC PGP, BitLocker con claves almacenadas **en NFC HSM PassCypher**.
- **Separación de claves y datos**: Las **claves de descifrado** nunca se almacenan en el mismo medio que los datos. Las claves de cifrado AES-256 CBC son altamente seguras y se pueden compartir a través de NFC HSM DataShielder, funcionan sin contacto, sin servidor y sin bases de datos. Este mecanismo garantiza la transmisión segura de claves, incluso a distancia, eliminando cualquier riesgo de interceptación por parte de terceros.
- **Copias de seguridad cifradas y redundantes**: datos replicados **en múltiples medios, sin conexión** y seguros.

2.8.2. Protección mejorada contra los ciberataques

- **Ransomware y sobrecifrado** : Las copias de seguridad cifradas fuera de línea y las claves físicamente subcontratadas fuera de línea evitan la manipulación o la recuperación fraudulenta.
- **Ciberataques avanzados (APT, Zero-Day, Espionaje):** La arquitectura **Zero Trust & Zero Knowledge** y **la separación de claves físicas** evitan la exfiltración. La arquitectura de seguridad de Freemindtronic, que incorpora sistemas de cifrado segmentados patentados y control de acceso basado en hardware, garantiza que no se puedan filtrar claves privadas ni datos cifrados, incluso bajo restricciones físicas o lógicas. La combinación del cifrado AES-256 CBC y RSA-4096 aumenta la resistencia a los ataques avanzados, incluidos los asistidos por inteligencia artificial.
- **Resiliencia sin nube** : **no depende de servidores remotos**, lo que elimina el riesgo de ataques centralizados.

2.8.3. Resiliencia ante desastres físicos y pérdidas accidentales

Los protocolos de Freemindtronic siempre garantizan el acceso a los datos cifrados con sus claves, incluso en caso de:

- **Robo o pérdida** de medios cifrados: Sin **claves externalizadas**, los datos siguen siendo inutilizables.
- **Destrucción accidental o desastre natural** : Las **copias de seguridad duplicadas** garantizan que se recuperen los datos confidenciales.
- **Aislamiento geográfico de las copias de seguridad**: Los medios cifrados se mantienen en una variedad de ubicaciones seguras, lo que evita un compromiso total.

2.9. Acuerdos de confidencialidad (NDA) y confidencialidad del comercio

Todas las relaciones comerciales con Freemindtronic que impliquen el intercambio de información sensible o confidencial están cubiertas habitualmente por un **Acuerdo de Confidencialidad (NDA).**

- **Aplicación estricta** : Cualquier información intercambiada en el contexto de asociaciones, colaboraciones técnicas o discusiones comerciales está protegida por cláusulas de confidencialidad legalmente vinculantes. Todos los documentos confidenciales, cifrados o no, intercambiados con clientes y socios se firman digitalmente sistemáticamente a través de la función integrada en DataShielder HSM PGP. Esta firma digital garantiza la integridad y autenticidad de los documentos, asegurando que no se hayan producido daños o alteraciones después de su emisión. Además, las comunicaciones por correo electrónico que involucran información confidencial siempre están protegidas a través de PGP, lo que evita la interceptación o manipulación de mensajes.
- **Alcance del NDA** : El NDA cubre **documentos, comunicaciones, intercambios técnicos, innovaciones, datos internos**, así como cualquier información confidencial transmitida por Freemindtronic o recibida de un socio.
- **Sanciones por violaciones** : Cualquier divulgación no autorizada de información confidencial está sujeta a **sanciones contractuales y legales** que pueden incluir acciones legales por violación de confidencialidad y secretos comerciales.
- **Plazo de protección**: Las obligaciones de confidencialidad permanecen vigentes **incluso después de la finalización de la relación contractual, de** acuerdo con el plazo definido en cada acuerdo.

Esta cláusula refuerza el compromiso de Freemindtronic de proteger toda la información crítica intercambiada en el curso de su negocio, garantizando un marco legal estricto contra cualquier fuga o compromiso.

ARTÍCULO 3 – USO DE SENSORES Y ACCESO A LOS DATOS DE LOCALIZACIÓN

Es posible que algunos programas, aplicaciones o extensiones de **Freemindtronic** requieran acceso a los sensores de los dispositivos de los usuarios.

3.1 Estos sensores incluyen:

- **GPS** (ubicación precisa)
- **Wi-Fi y redes móviles** (ubicación aproximada)
- **Bluetooth** (detección local sin transmisión externa)
- **Datos biométricos** (huella dactilar, reconocimiento facial)
- **Micrófono y cámara** (solo con consentimiento explícito)
- **Sensores ambientales** (acelerómetro, giroscopio, sensores de proximidad, luminosidad)
- **Módulos de seguridad** (NFC, HSM, HSM, PGP)

3.2 Todos los datos generados por estos sensores:

- **Permanecen exclusivamente en el dispositivo del usuario** y no se transmiten a un servidor remoto o servicio de terceros bajo ninguna circunstancia.
- **No están sujetos a almacenamiento externo o remoto**.
- **Solo son accesibles con el consentimiento explícito del usuario**, especialmente para sensores sensibles como el micrófono y la cámara.

- **Puede ser gestionado por el usuario**, que puede cambiar o revocar los permisos concedidos en cualquier momento a través de la configuración de su dispositivo.

Los sensores de los dispositivos (cámara, micrófono, NFC, GPS, Wi-Fi, Bluetooth) solo se utilizan localmente y nunca transmiten datos a servidores externos, terceros u otros servicios de Freemindtronic. El usuario puede controlar y deshabilitar este acceso a través de la configuración de su dispositivo.

3.4 Garantizar que los datos de los sensores no se utilicen con fines de seguimiento del comportamiento

Freemindtronic garantiza que **los datos recopilados a través de los sensores del dispositivo nunca se utilicen para el seguimiento del comportamiento, la publicidad dirigida o la elaboración de perfiles de usuario**.

El acceso a los sensores está estrictamente limitado a las funciones esenciales del software y solo después de obtener el consentimiento explícito del usuario.

Sobre la base de estos datos no se lleva a cabo ningún análisis de los patrones de uso, que no se almacenan ni se transmiten a terceros.

ARTÍCULO 4 – CUMPLIMIENTO DE LAS PLATAFORMAS DE DISTRIBUCIÓN

El software, las aplicaciones y las extensiones desarrolladas por **Freemindtronic** cumplen con los requisitos de las siguientes plataformas:

- **Google Play Console** (aplicaciones Android)
- **Chrome Web Store** (extensiones de navegador)
- **Complementos de Microsoft Store y Edge** (aplicaciones de Windows y extensiones de navegador)
- **Apple macOS e iOS** (aplicaciones distribuidas en la App Store)

Freemindtronic se compromete a cumplir con las pautas **de seguridad y privacidad** impuestas por estas plataformas.

- **La arquitectura Zero Trust y Zero Knowledge está garantizada** para que no se recopilen, transmitan ni almacenen datos de usuario más allá del dispositivo del usuario.
- **No hay integración con servicios de terceros** para mitigar los riesgos asociados con el seguimiento o la recopilación de datos personales.
- **Los requisitos de cada plataforma se revisan periódicamente** para garantizar el cumplimiento continuo de los cambios en la normativa aplicable.

SECCIÓN 5 – CLÁUSULA DE NO DISCRIMINACIÓN (CUMPLIMIENTO DE LA CCPA)

De acuerdo con las disposiciones de la Ley de **Privacidad del Consumidor de California (CCPA), Freemindtronic garantiza que los usuarios no serán discriminados** en el ejercicio de sus derechos en materia de protección de datos personales.

No se aplicarán restricciones ni limitaciones a los usuarios que deseen ejercer sus derechos, en particular en lo que respecta a:

- Acceso a sus datos personales.
- Rectificación de información inexacta o incompleta.
- Supresión de los datos facilitados voluntariamente.
- Oponerse o limitar el tratamiento de sus datos.

Freemindtronic se compromete a no aplicar tarifas adicionales, ni cambios en el acceso a las funciones, en respuesta a una solicitud de ejercicio de derechos por parte de un usuario.

Cualquier usuario que desee hacer valer sus derechos puede ponerse en contacto directamente con Freemindtronic utilizando los datos de contacto proporcionados en esta Política de Privacidad.

De acuerdo con la CCPA, el ejercicio de los derechos de protección de datos personales (acceso, supresión, oposición) no supondrá ninguna modificación, restricción o degradación de los servicios ofrecidos por Freemindtronic.

ARTÍCULO 6 – PROHIBICIÓN DE ELABORACIÓN DE PERFILES Y TOMA DE IMPRESIONES DACTILARES

6.1. Ausencia de elaboración de perfiles y decisiones automatizadas

Freemindtronic no lleva a cabo ninguna elaboración de perfiles, seguimiento del comportamiento o toma de decisiones automatizada que afecte a los usuarios.

- No se realiza ningún análisis de la actividad del usuario.
- No se utiliza ningún algoritmo de inteligencia artificial para clasificar a los usuarios.
- No se ha establecido ningún mecanismo para personalizar los servicios en función de los datos de los usuarios.

6.2. Ausencia de huellas dactilares

La huella digital es una técnica que consiste en recopilar información específica sobre el hardware o el software de un dispositivo, como la dirección IP, el sistema operativo, la resolución de la pantalla y otros parámetros, con el fin de crear una huella digital única del usuario. A diferencia de las cookies, este método es difícil de detectar y bloquear, lo que plantea importantes problemas de privacidad.

En diciembre de 2024, **Google anunció que, a partir del 16 de febrero de 2025, permitiría a los anunciantes utilizar las huellas dactilares** para el seguimiento de usuarios, revirtiendo su política de 2019 que prohibía la práctica. La medida generó críticas de reguladores como **la Oficina del Comisionado de Información (ICO) del Reino Unido,** que calificó el cambio de "irresponsable" debido a la reducción de la elección y el control que las personas tienen sobre la recopilación de su información.

En **Freemindtronic**, estamos firmemente comprometidos con el respeto de la privacidad de nuestros usuarios. Por lo tanto, **no utilizamos ninguna forma de toma de huellas dactilares** en nuestros productos o servicios. **Google anunció en diciembre de 2024 que permitiría la toma de huellas dactilares para los anunciantes a partir del 16 de febrero de 2025** (fuente oficial - https://blog.google/products/ads-commerce/privacy-sandbox-fingerprinting-policy-change).

La medida generó preocupaciones de los reguladores, incluida **la ICO del Reino Unido**. Freemindtronic rechaza estas prácticas y garantiza que **no se implementa** ningún seguimiento, identificación de dispositivos o perfiles de comportamiento.

Todos los sistemas informáticos de Freemindtronic están **completamente aislados e independientes** entre sí. **Ningún dato del usuario se registra, almacena o rastrea** a través de una operación exclusivamente local y fuera de línea. **El uso de soluciones de encriptación de hardware y autenticación NFC HSM** garantiza que no se pueda asociar ninguna huella digital con los usuarios, incluso mediante el uso de la tecnología EviBITB de Freemindtronic.

Freemindtronic implementa una estrategia de **ciberseguridad avanzada** para protegerse contra los ataques asistidos por IA, el fraude del CEO y otros robos de identidad.

- Los **correos electrónicos utilizados para la comunicación externa** son **direcciones de sandbox y correos electrónicos sin respuesta** para **reducir el riesgo de suplantación de identidad y phishing**.
- Cualquier apertura de archivos adjuntos está sujeta a una **estricta política de control** para evitar **cualquier riesgo de archivos maliciosos**.
- Cada **solicitud de un cliente** es verificada sistemáticamente por **un segundo canal de comunicación** para **confirmar su autenticidad** (eliminación proactiva de dudas).

Freemindtronic garantiza **que nunca recogerá, analizará o utilizará las huellas dactilares del dispositivo** a través de métodos de identificación indirecta (por ejemplo, resolución de pantalla, modelo de dispositivo, idioma del navegador).

ARTÍCULO 7 – CUMPLIMIENTO DE LA NORMATIVA SOBRE PRODUCTOS DE DOBLE USO

7.1. Regulaciones y Autorizaciones de Exportación

Freemindtronic hace cumplir estrictamente las regulaciones para la gestión y exportación de tecnologías de ciberseguridad, incluidos los productos de **cifrado clasificados como civiles y militares de doble uso**.

Los productos DataShielder NFC HSM han recibido una **autorización de importación en Francia del Principado de Andorra**, validada el **7 de diciembre de 2024** a través de la empresa **AMG Pro**, de conformidad con el **Decreto n.º 2001-1192 del 13 de diciembre de 2001**, modificado por el **Decreto n.º 2024-95 del 8 de febrero de 2024**.

Esta autorización se obtuvo tras la presentación del expediente a la **ANSSI**, que, de acuerdo con su misión de **verificar el cumplimiento de los requisitos reglamentarios**, no se negó en los plazos previstos por la legislación vigente.

Desde el **7 de febrero de 2025**, los productos **DataShielder NFC HSM** también están autorizados **para su reexportación** desde Francia a los Estados miembros de la Unión Europea, de conformidad con el **Reglamento (UE) 2021/821 de 20 de mayo de 2021** sobre artículos de doble uso.

7.2. Textos de referencia

Esta autorización se expide de conformidad con los siguientes textos:

- **Decreto N° 2001-1192 de 13 de diciembre de 2001**, modificado por **el Decreto de 8 de febrero de 2024**, sobre el control de la exportación y transferencia de bienes y tecnologías de doble uso.
- **Reglamento (UE) 2021/821, de 20 de mayo de 2021,** por el que se establece un régimen de control de las exportaciones de productos de doble uso.

7.3. Compromiso de auditoría

Freemindtronic se compromete a garantizar **auditorías de cumplimiento periódicas** para garantizar **el cumplimiento continuo de los requisitos legales y reglamentarios**. Estas auditorías internas se realizan periódicamente de acuerdo con los requisitos normativos vigentes.

ARTÍCULO 8 – CERTIFICACIONES Y AUDITORÍAS

8.1. Sin requisito de certificación en la nube

Freemindtronic no requiere certificaciones **SOC 2** o **ISO 27001** específicas para infraestructuras en la nube, ya que **no se utilizan servidores remotos** para el procesamiento o almacenamiento de datos.

Los productos están diseñados con un enfoque **100% aislado,** lo que garantiza **el aislamiento total de los datos del usuario** de cualquier infraestructura de red externa. Esta arquitectura justifica **la ausencia de ciertas auditorías** que normalmente se aplican a los sistemas conectados.

8.2. Auditoría de seguridad y control de calidad

Este enfoque **se aplica a lo largo de toda la cadena** de valor, desde el **diseño del producto** hasta la **fabricación**. Todas las auditorías realizadas tienen como objetivo garantizar la **resistencia, la seguridad y la ausencia de fugas de datos de** los sistemas de Freemindtronic.

Además de las auditorías internas para garantizar el cumplimiento de los productos, Freemindtronic aplica **controles mejorados sobre la gestión de pagos** y la **protección de las transacciones financieras**.

- El sistema de gestión contable y financiera está aislado y no se puede validar ninguna transacción sin una autenticación sólida a través de DataShielder, NFC, HSM Auth y DataShielder MAuth, lo que garantiza una autenticación sólida y elimina el riesgo de fraude.
- El acceso a las cuentas bancarias y a los sistemas de pago está estrictamente limitado a los accionistas autorizados, sin relación de subordinación, para limitar los riesgos internos de fraude.

ARTÍCULO 9 – DELEGADO DE PROTECCIÓN DE DATOS (DPO)

9.1. Nombramiento del DPD

De conformidad con los requisitos del **Reglamento General de Protección de Datos (GDPR – Reglamento (UE) 2016/679)** y otras normativas aplicables, Freemindtronic ha nombrado a un **Delegado de Protección de Datos (DPO)** responsable de garantizar el cumplimiento de la empresa con la protección de datos personales.

El **DPO de Freemindtronic** es:

- **Nombre:** Jacques Gascuel
- **Cargo: Consejero Delegado** y DPO de Freemindtronic SL
- **Contacto :** dpo [arroba] freemindtronic.com

9.2. Misiones del DPD

El DPO de Freemindtronic lleva a cabo varias misiones esenciales, entre ellas:

- Garantizar que **el tratamiento de datos** cumpla con la normativa aplicable (**GDPR, CCPA, LGPD, etc.**).

- Informar y asesorar a Freemindtronic sobre **sus obligaciones en materia de protección de datos**.
- Supervisar la aplicación **de las políticas de seguridad y protección de datos** implantadas.
- Responder a las solicitudes de los usuarios en relación con **sus derechos (acceso, rectificación, supresión, oposición, etc.)**.
- Servir de enlace con **las autoridades de protección de datos**, incluida la **Agencia Andorrana de Protección de Datos** y las autoridades europeas o internacionales pertinentes.

9.3. Contacto y reclamaciones

Cualquier usuario que desee obtener información sobre **la gestión de sus datos personales** o ejercer sus derechos puede ponerse en contacto con **el DPO de Freemindtronic** en la siguiente dirección:

- **Correo electrónico :** dpo [arroba] freemindtronic.com
- **Dirección postal:**
  Freemindtronic SLAv. Co-Príncipe de Gaulle, 13, Edificio Valira, Planta baja, AD700 Escaldes – Engordany, Andorra

Si no se da respuesta en el plazo de **30 días**, el usuario podrá dirigirse directamente **a la Agencia Andorrana de Protección de Datos (APDA)** por **incumplimiento de la obligación legal de responder en el plazo de 30 días**.

ARTÍCULO 10 – REQUISITOS ESPECÍFICOS PARA LAS PLATAFORMAS DE DISTRIBUCIÓN

10.1. Consola Google Play (Android)

Las aplicaciones de Freemindtronic no recopilan, almacenan ni transmiten ningún dato personal. Algunos permisos de Android (por ejemplo, NFC, almacenamiento, cámara) se utilizan solo para habilitar la funcionalidad del producto y no se explotan con fines de terceros. No se comparten datos con terceros, y todas las operaciones se realizan localmente en el dispositivo del usuario, de acuerdo con las políticas de privacidad de Google Play.

10.1.1. Cumplimiento de las políticas de Google Play con respecto a datos confidenciales y permisosLas aplicaciones de Freemindtronic que requieren acceso a funciones confidenciales de Android (NFC, almacenamiento, cámara, micrófono, GPS, SMS, RCS, MMS) cumplen con los siguientes requisitos:

- **Consentimiento expreso** : No hay permisos habilitados de forma predeterminada. El usuario debe habilitarlos manualmente a través de la configuración de su dispositivo.
- **Uso sin problemas** : El acceso a estas funciones está **estrictamente limitado** a las necesidades esenciales de la aplicación, y los datos generados permanecen **exclusivamente en el dispositivo**.
- **Sin abuso de permisos** : Freemindtronic nunca pide acceso a funciones superfluas y respeta la política de transparencia de Google Play.

10.1.2. Protección de datos y almacenamiento localTodos los datos permanecen estrictamente almacenados en el dispositivo del usuario y **solo pueden ser accedidos por la propia aplicación**. Ningún dato del usuario se almacena en **servidores externos** ni se comparte con **terceros**.

10.2 – Chrome Web Store (Extensiones de Chrome)

Las extensiones de Freemindtronic no recopilan ni comparten ningún dato del usuario. Pueden usar localStorage para almacenar temporalmente la información local necesaria para que la extensión

funcione correctamente.

No se realiza ningún seguimiento oculto, ni transmisión de datos a terceros, ni acceso injustificado a las cookies o al historial de navegación.

10.2.1 Uso de Local StorageLas extensiones de Freemindtronic utilizan exclusivamente la API localStorage y Web Storage para almacenar temporalmente los ajustes necesarios para su correcto funcionamiento.
Estos datos:

- **Nunca se transmiten a servidores remotos.**
- **Solo el usuario puede acceder a ellos y en el contexto de la extensión.**
- **La configuración guardada localmente a través de localStorage y Web Storage no contiene ningún dato personal o confidencial.**
- **Los usuarios pueden borrar manualmente los datos locales guardados a través de la opción "Eliminar datos" integrada en la extensión.**

10.3. Complementos de Microsoft Store y Edge (Windows)

Las aplicaciones y extensiones de Freemindtronic cumplen con los estándares de privacidad de Microsoft.

Si una aplicación accede a archivos locales (por ejemplo, almacenamiento seguro de claves de cifrado), estos archivos permanecen aislados y nunca se comparten con servicios de terceros.

Freemindtronic garantiza que no habrá huellas dactilares o seguimiento oculto, de acuerdo con las políticas de Microsoft Store.

10.3.1. Protección de acceso a archivos locales (Windows)
Algunas aplicaciones de Freemindtronic pueden requerir acceso a archivos locales para **cifrar, proteger o autenticar datos confidenciales**.
Estos archivos:

- **Nunca se reenvían a un servidor remoto.**
- **Permanecen exclusivamente almacenados y procesados en el dispositivo del usuario.**
- **Solo son accesibles para las aplicaciones instaladas localmente con el consentimiento del usuario.**

10.4. Tienda de aplicaciones de Apple (macOS e iOS)

Las aplicaciones de Freemindtronic no rastrean a los usuarios, no recopilan ningún dato para la elaboración de perfiles publicitarios ni transmiten ninguna información fuera del dispositivo.

Si una aplicación accede a sensores iOS/macOS (por ejemplo, NFC, micrófono, GPS), este uso se limita estrictamente a las funciones esenciales y controlables por el usuario.

Si se utilizan API de terceros (por ejemplo, pago a través de Apple Pay), su impacto en los datos del usuario cumple con los requisitos de Apple y es totalmente transparente para el usuario.

10.4.1. Cumplimiento de la Política de Transparencia de Seguimiento de Aplicaciones (ATT)Freemindtronic

garantiza **que no utiliza ID de publicidad** ni **herramientas de seguimiento de usuarios** con fines de marketing o publicidad.
De acuerdo con las directrices de Apple:

- **No se recopilan datos de usuario para la elaboración de perfiles o la orientación publicitaria.**
- **No hay integración con servicios de publicidad o análisis de terceros.**
- **No se permite el uso del ID de Apple (IDFA) para rastrear la actividad del usuario en otras aplicaciones.**
- **Freemindtronic no recopila ni comparte ningún dato de ubicación en segundo plano o sin el consentimiento explícito del usuario.**
- **Las aplicaciones no transmiten ningún dato fuera del dispositivo a menos que el usuario realice voluntariamente una acción que requiera el intercambio de datos.**

ARTÍCULO 11 – CUMPLIMIENTO DE LA LEGISLACIÓN ANDORRANA EN MATERIA DE PROTECCIÓN DE DATOS

11.1. Aplicación de la legislación andorrana

Freemindtronic, como empresa registrada en **el Principado de Andorra**, está sujeta a las normativas locales de **protección de datos**, entre las que se incluyen:

- **Calificado Ley Orgánica 15/2003, de 18 de diciembre,** de Protección de Datos de Carácter Personal
- **Calificado Ley 29/2021, de 28 de octubre de 2021**, que alinea Andorra con los principios del **Reglamento General de Protección de Datos (GDPR – Reglamento (UE) 2016/679)**

Estas leyes garantizan un marco de **protección de datos** equivalente a los estándares europeos, reconocidos **como adecuados** por la Unión Europea de acuerdo con el **artículo 45 del RGPD**.

Además de la normativa vigente, **Freemindtronic implementa medidas físicas y de software avanzadas para garantizar una protección absoluta de los datos**. Esto incluye **el cifrado completo de medios digitales, la autenticación multifactor NFC HSM y el aislamiento físico de las infraestructuras de TI**. Estas medidas aseguran **el pleno cumplimiento de los artículos 10 y 45 del RGPD**, garantizando una protección de datos equivalente a los estándares europeos más estrictos.

ARTÍCULO 12 – PRINCIPIOS DE CUMPLIMIENTO Y SEGURIDAD DE LOS DATOS

12.1. Privacidad desde el diseño

Freemindtronic integra la **protección de datos** en **el diseño de su software y servicios**, de acuerdo con los principios de **privacidad por diseño y privacidad por defecto**.

12.2. Ausencia de almacenamiento de datos

De acuerdo con **el enfoque Zero Trust & Zero Knowledge**, **Freemindtronic no almacena ni procesa ningún dato personal**, excepto en el caso de que el usuario lo proporcione voluntariamente (por ejemplo, formulario de contacto, soporte técnico).

12.3. Adopción de medidas de seguridad reforzadas

Freemindtronic implementa medidas **de seguridad avanzadas** para garantizar **la protección de los datos** y prevenir infracciones, entre las que se incluyen:

- **Cifre sistemáticamente** las comunicaciones y transacciones de los usuarios a través de sus sistemas patentados de cifrado de clave segmentada
- **Falta de** identificadores únicos que se puedan utilizar para rastrear la actividad del usuario
- **Auditabilidad interna periódica** para asegurar el cumplimiento de la normativa vigente

Estas medidas están en consonancia con **el artículo 10 de la Ley Cualificada 29/2021** de Protección de Datos Personales en Andorra.

Freemindtronic aplica una estrategia integral de ciberseguridad que garantiza la protección de los datos incluso en caso de intrusión física en las instalaciones:

Todos los sistemas informáticos (fijos, móviles, servidores y dispositivos de almacenamiento) están totalmente encriptados con claves de ≥256 bits.

Todos los sitios conectados en línea o en una red local utilizan PassCypher NFC HSM y PassCypher HSM PGP con TOTP/HOTP y/o DataShielder NFC HSM y DataShielder HSM PGP Cyber Defense.

No se almacenan claves de cifrado ni se ven en las herramientas de producción.

Los medios sensibles (memorias USB, discos duros) se almacenan en una caja fuerte resistente al fuego y a las intrusiones.

Cualquier extracción de datos confidenciales es imposible, incluso en caso de robo físico de servidores o exfiltración ilícita de archivos.

Estas medidas garantizan que, incluso en el caso de una intrusión en las instalaciones de Freemindtronic, no se pueda explotar ningún dato, incluso en el caso de una intrusión ilegal exitosa.

12.4. Compromiso con la seguridad continua

Freemindtronic sitúa la **protección de datos** en el centro de sus actividades y se compromete a:

- **Mejore continuamente sus medidas de seguridad** manteniéndose al día con las amenazas y regulaciones en evolución.
- **Adaptar sus protocolos** de protección para garantizar un nivel de seguridad acorde con los nuevos avances tecnológicos y las mejores prácticas de ciberseguridad.
- **Monitoree constantemente** las amenazas cibernéticas, incluidas las asistidas por inteligencia artificial (IA), para anticiparse a posibles intentos de intrusión y fortalecer las defensas en consecuencia.

12.4.1 Protección estratégica: Freemindtronic no divulga públicamente todos los detalles técnicos de sus mecanismos de seguridad para no facilitar un análisis por parte de un atacante o inteligencia artificial que busque identificar una posible vulnerabilidad. Sin embargo, todas las medidas puestas en marcha cumplen con los estándares **más estrictos** en materia de ciberseguridad y protección de datos.

12.5. Seguridad operativa y protección de datos sensibles

Freemindtronic aplica un estricto modelo de seguridad que garantiza **la máxima protección frente a los riesgos de espionaje interno y externo**.

12.5.1 Aislamiento de sistemas informáticos

- No se permiten conexiones de red entre sistemas internos ni se permite el uso compartido de archivos o impresoras.

- Cada sistema es completamente independiente, evitando vulnerabilidades relacionadas con conexiones externas.

12.5.2 Transferencias seguras de datos confidenciales

- Todas las transferencias de archivos confidenciales se realizan **exclusivamente a través de** las unidades flash USB seguras **EviKey NFC** de Freemindtronic.
- Estas llaves tienen **autobloqueo automático** cuando no están en uso, lo que evita el acceso no autorizado.
- Un **registro de trazabilidad** está integrado en la caja negra de las llaves EviKey NFC, lo que permite verificar cada desbloqueo y su geolocalización**.**

12.5.3 Aislamiento físico y seguridad de las herramientas de producción

- Los equipos y herramientas de producción sensibles **nunca se conectan a Internet** y se aíslan estrictamente después de su uso.
- Después de su uso, estas herramientas se guardan **en una caja fuerte especial que** es resistente al fuego y a la intrusión física.

12.5.4 Generación y protección de claves de autenticación

- Las herramientas de producción **generan aleatoriamente las claves de autenticación contra la falsificación que también sirven como** claves segmentadas.
- Estas claves **no se muestran ni se guardan** en las herramientas de producción, lo que garantiza la ausencia de cualquier rastro utilizable.

12.5.5 Estricto control de acceso y mitigación de riesgos internos

- Solo **dos personas autorizadas**, que también son **accionistas de la empresa**, están autorizadas a utilizar las herramientas de producción.
- Esta restricción tiene como objetivo **minimizar los riesgos asociados con las relaciones subordinadas** y garantizar el control total sobre el acceso a las infraestructuras sensibles.

12.6. Estricto control de acceso y mitigación de riesgos internos

12.6.1 Seguridad de acceso y cifrado sistemático

Freemindtronic aplica protocolos avanzados de autenticación y encriptación para garantizar que todos los accesos y medios digitales estén protegidos contra cualquier intento de intrusión o robo.

12.6.1.1 Protección del acceso a sitios y redesTodos los sistemas de red en línea y locales utilizan únicamente las siguientes tecnologías de autenticación sólida:

- PassCypher NFC HSM et/ou PassCypher HSM PGP, intégrant des protocoles TOTP (Time-Based One-Time Password) et HOTP (HMAC-Based One-Time Password).
- DataShielder NFC HSM y/o DataShielder HSM PGP en la versión Cyber Defense, que combinan autenticación sólida y cifrado de acceso avanzado.
- Emuladores de teclado USB Bluetooth para proteger la entrada de datos confidenciales eliminando cualquier riesgo de registro de teclas.

12.6.1.2 Cifrado de datos y medios de almacenamientoTodos los sistemas informáticos (fijos, móviles) y dispositivos de almacenamiento que contienen datos sensibles están cifrados con claves de cifrado iguales o superiores a 256 bits.

- Discos duros internos y externos totalmente encriptados.
- Dispositivos móviles de almacenamiento y copia de seguridad protegidos por encriptación de hardware y/o software.

12.6.1.3 Resistencia a las intrusiones físicas y digitalesTodo está diseñado para garantizar que, en caso de intrusión en las instalaciones de Freemindtronic, robo de medios digitales o extracción ilícita de datos sensibles, ningún dato sea utilizable o físicamente accesible.

- Claves de cifrado seguras en dispositivos NFC HSM, evitando el acceso no autorizado.
- Bloqueo automático de llaves o bloqueo en caso de intento de compromiso con trazabilidad de caja negra.

12.6.1.4 Integración de productos que utilizan la tecnología EviKey NFC

Los productos de Freemindtronic que incorporan la tecnología **EviKey NFC** utilizan exclusivamente la aplicación **Fullkey Plus** para su gestión y seguridad. Esta tecnología también se integra en las siguientes soluciones de ciberseguridad:

- **Maestro HSM NFC de PassCypher**
- **DataShielder NFC HSM Maestro y Defensa**

La integración de EviKey NFC en estas soluciones proporciona un control de acceso avanzado a los medios de almacenamiento e incluye las siguientes características:

- **Autobloqueo cuando está inactivo**
- **Gestión segura de claves**
- **Acceda a la trazabilidad a través de una caja negra**, accesible solo sin contacto a través de **un teléfono Android NFC**, gracias a la aplicación **Fullkey Plus**, **PassCypher NFC HSM** o **DataShielder NFC HSM**.

Freemindtronic no corre ningún riesgo en lo que respecta a la seguridad y no se deja sorprender: ¡aquí, **el zapatero ciertamente no es el peor calzado** ! 😉

Freemindtronic implementa **mamparas de seguridad estancas**, evitando cualquier forma de espionaje, ya sea **interno o externo**, y garantizando **la máxima** protección de los activos digitales y los datos críticos.

12.6.1.4 – Protección contra la IA y ataques avanzados :

Freemindtronic implementa tecnologías y protocolos específicos para protegerse contra los ataques asistidos por IA, incluidos los deepfakes y las manipulaciones de audio / video destinadas a comprometer la identidad digital de ejecutivos y usuarios. Estas medidas incluyen una mayor verificación de las comunicaciones y un análisis multifactorial del comercio sensible.

12.7 – Gestión de violaciones de datos :

En caso de que se produzca un compromiso de hardware o un intento de violación de seguridad que afecte a la infraestructura de Freemindtronic, los procedimientos de respuesta a incidentes se llevan a cabo de forma proactiva, independientemente de la ausencia de un sistema de detección automatizado.

Freemindtronic reconoce que no es realista garantizar una protección absoluta contra un atacante determinado, incluso con las mejores medidas de seguridad del mundo. Es por eso que el enfoque adoptado se basa en una estrategia **proactiva y preventiva**, integrando innovaciones patentadas internacionalmente desarrolladas para anticipar nuevas formas de espionaje, en particular las asistidas por **inteligencia artificial**.

Las soluciones de ciberseguridad de Freemindtronic están diseñadas para evitar que los datos sean explotados, incluso en caso de acceso físico o digital no autorizado. Este enfoque se basa en mecanismos avanzados que incluyen el autobloqueo de hardware, el cifrado de clave segmentada, el aislamiento de la infraestructura y el uso exclusivo de medios seguros como EviKey NFC, PassCypher NFC HSM y DataShielder NFC HSM.

En caso de que un incidente de seguridad afecte a un cliente o socio, Freemindtronic se compromete a **informarle lo antes posible**, de acuerdo con los requisitos de la normativa de protección de datos aplicable.

ARTÍCULO 13 – DERECHOS DE LOS USUARIOS EN VIRTUD DE LA LEGISLACIÓN ANDORRANA

De conformidad con **los artículos 16 a 21 de la Ley 29/2021**, los usuarios tienen los siguientes derechos, alineados con el **RGPD y la legislación andorrana**:

- **Derecho de Acceso** : Para verificar qué información ha sido proporcionada voluntariamente y procesada.
- **Derecho de Rectificación** : A corregir los datos inexactos o incompletos.
- **Derecho de oposición** : Impugnar el uso de sus datos.
- **Derecho de Supresión (Derecho al Olvido):** Exigir la supresión permanente de sus datos.
- **Derecho a la Portabilidad** : Recibir sus datos en un formato legible (nueva obligación reforzada por la Ley 29/2021).
- **Derecho a la restricción del procesamiento** : Restringir el procesamiento de cierta información.

13.1. Tiempo de procesamiento de las solicitudes

Freemindtronic garantiza que cualquier solicitud de ejercicio de derechos será tramitada en **un plazo máximo de 30 días**, salvo en circunstancias excepcionales que requieran una **prórroga justificada de hasta 60 días**.

Las solicitudes pueden enviarse por correo electrónico a:
contact [at] freemindtronic.com o **dpo [at] freemindtronic.com**

ARTÍCULO 14 – RECURSO EN CASO DE LITIGIO

Si un usuario considera que **no se han respetado sus derechos**, puede presentar una reclamación ante la **Agencia Andorrana de Protección de Datos (APDA),** la **autoridad de control competente en Andorra**.

14.1. Procedimiento de reclamaciones

De conformidad con **el artículo 25 de la Ley 29/2021**, cualquier persona que considere que el tratamiento de sus datos se ha realizado **infringiendo las leyes aplicables** podrá:

- **Remitir el asunto a la Agencia Andorrana de Protección de Datos (APDA)** para una investigación administrativa.
  Contacto APDA : https://www.apda.ad

- **Presentar un recurso ante los tribunales competentes de Andorra** para obtener la indemnización del daño sufrido.

Freemindtronic se compromete a cooperar **plenamente** con las autoridades de protección de datos en caso de una investigación.

ARTÍCULO 15 – CAMBIOS EN LA POLÍTICA DE PRIVACIDAD

15.1. Compromiso de actualización

Freemindtronic se compromete a actualizar esta política en caso de cambios legislativos o reglamentarios que afecten a la protección de datos. Cualquier cambio se publicará explícitamente en el sitio web oficial de Freemindtronic.

15.2. Frecuencia y transparencia de las actualizaciones

Freemindtronic publica regularmente actualizaciones de su software, aplicaciones y extensiones. Se mantiene una página de actualizaciones dedicada, que detalla explícitamente:

- **Los cambios realizados,**
- **Mejoras de seguridad,**
- **Cualquier vulnerabilidad identificada y corregida.**

El historial completo de versiones del software, las aplicaciones y las extensiones de Freemindtronic se puede encontrar aquí: Historial de versiones de Freemindtronic

15.3. Notificación a los usuarios

Los usuarios que deseen ser notificados de las actualizaciones por correo electrónico deben realizar una solicitud expresa proporcionando su dirección de correo electrónico a Freemindtronic.

15.4. Información en caso de cambios en las funcionalidades

En caso de que se produzcan cambios en las funcionalidades relacionadas con el tratamiento de datos, Freemindtronic se compromete a informar a los usuarios:

- **Mediante notificación en el sitio web oficial,**
- **A través de las aplicaciones correspondientes.**

ARTÍCULO 16 – DATOS DE CONTACTO

Freemindtronic SL
Correo electrónico : **contacto [arroba] freemindtronic.com**
Teléfono : **+376 804 500Política de cookies :** https://freemindtronic.com/cookie-policy/

Fin del documento