AVISO DE PRIVACIDAD

PARA LOS EFECTOS DE ESTE AVISO DE PRIVACIDAD, SE ENTIENDE POR “ARKANGELES”, “NOSOTROS”, “NUESTROS” O “NUESTRAS” A ANGELES EN ARK, S.A.P.I. DE C.V.

AL ACEPTAR ESTE AVISO DE PRIVACIDAD, SE ENTIENDE QUE USTED HA REVISADO, LEÍDO Y ACEPTADO LOS TÉRMINOS DEL MISMO, POR LO QUE OTORGA SU CONSENTIMIENTO PARA EL TRATAMIENTO DE SUS DATOS PERSONALES, POR PARTE DE ARKANGELES, CONFORME LO AQUÍ ESTABLECIDO.

ARKANGELES, en cumplimiento a lo dispuesto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante la “Ley de Datos”) y su Reglamento, hace de su conocimiento el presente Aviso de Privacidad (en adelante el “Aviso”).

1. Responsable de los datos personales recabados y datos de contacto.

ANGELES EN ARK, S.A.P.I. DE C.V., con domicilio en Calle Goldsmith 40, Colonia Polanco Reforma, Delegación Miguel Hidalgo, C.P. 11550, Ciudad de México, Estados Unidos Mexicanos, es el responsable de los datos personales que se recaban a través del sitio de Internet www.arkfund.co (en adelante “la Plataforma”) y de la prestación de nuestros productos y servicios. ArkAngeles se encargará de recabar, manejar, procesar, tratar y conservar los datos personales de los particulares (en adelante los “Usuarios”)

2. Datos personales recabados de los Usuarios.

Con el propósito de integrar los expedientes de los Usuarios de ArkAngeles, Usted deberá proporcionar a ArkAngeles la siguiente información (en adelante y en conjunto, los “Datos Personales Recabados”):

Datos personales generales (identificación y de contacto)	I. Apellido paterno, apellido materno y nombre(s); II. Fecha de nacimiento; III. País de nacimiento; IV. País de nacionalidad; V. Actividad, ocupación, profesión, actividad o giro del negocio al que se dedique el Usuario; VI. Domicilio en el lugar de residencia, compuesto de los siguientes datos: nombre de la calle, avenida o vía de que se trate, debidamente especificada; número exterior y, en su caso, interior; colonia o urbanización; demarcación territorial, municipio o demarcación política similar que corresponda, en su caso; ciudad o población, entidad federativa, estado, provincia, departamento o demarcación política similar que corresponda, en su caso; código postal y país; VII. Número(s) de teléfono, incluyendo la clave de larga distancia y, en su caso, extensión; VIII. Correo electrónico; IX. Clave Única de Registro de Población y la clave del Registro Federal de Contribuyentes; y X. Datos de la identificación con la que se identificó, consistentes en: nombre de la identificación; autoridad que la emite, y número de esta.

	XI. Identificación; XII. Constancia de la Clave Única de Registro de Población, expedida por la Secretaría de Gobernación o Cédula de Identificación Fiscal expedida por el SAT; XIII. Comprobante que acredite el domicilio; XIV. Fotografía; XV. Número de pasaporte; XVI. Perfil de Linkedin.
Datos personales financieros y patrimoniales	Actividad profesional o comercial, datos de cuentas bancarias y presupuesto de inversión en ArkAngeles anual.
Datos de ubicación geográfica	Geolocalización del dispositivo electrónico utilizado para el acceso a la Plataforma.
Datos personales sensibles	ArkAngeles no recaba datos personales sensibles.

ArkAngeles recibe, recaba, maneja, procesa, trata y conserva los Datos Personales Recabados en su carácter de Titulares, bajo los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad a efecto de asegurar la privacidad, confidencialidad e integridad de conformidad con lo dispuesto por la Ley de Datos.

3. Medidas de Seguridad en el Tratamiento de Datos Personales Recabados

Los Datos Personales Recabados serán almacenados con las medidas de seguridad administrativas, técnicas y físicas necesarias que permiten garantizar su privacidad y confidencialidad. Dichas medidas de seguridad administrativas, permiten que los Datos Personales Recabados estén protegidos contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado de los mismos.

4. Finalidad de los Datos Personales Recabados

a) Finalidad primaria: Estas finalidades son imprescindibles, puesto que dan origen y resultan necesarias para la relación jurídica entre Usted y ArkAngeles, las cuales incluyen:

Gestión de evaluación. Los Datos Personales Recabados que integran su expediente personal, se utilizarán para la atención de actividades de prospección, validación, detección y manejo de fraudes.

Gestión de Operaciones. Una vez concluida la Gestión de Evaluación se determinará si el Usuario es susceptible de realizar Operaciones con ArkAngeles, según dicho término se define en la Ley para Regular las Instituciones de Tecnología Financiera. En dicho contexto, se remitirán los Datos Personales Recabados a la Entidad Financiera o vehículo que corresponda. Para efectos de lo anterior, se entenderá que el Usuario otorgó un mandato gratuito a favor de ArkAngeles (el "Mandato") para que ArkAngeles remitiera los datos a la Entidad Financiera o vehículo en cuestión, por lo que dicha remisión será en cumplimiento al Mandato.

Gestión de las Operaciones. En caso que el Usuario celebre Operaciones con ArkAngeles, los Datos Personales Recabados podrán ser usados para contratos, realizar gestiones de mantenimiento de las Operaciones, cumplimiento de obligaciones, ceder o enajenar, parcial o totalmente derechos sobre los contratos celebrados, así como administrar la relación contractual con el Usuario, incluyendo la Transferencia de los Datos Personales Recabados a Instituciones Financieras que administren los fideicomisos mediante los cuales se realicen las Operaciones del Usuario, incluyendo todas aquellas transferencias que requiera el marco regulatorio aplicable, incluyendo la Ley para Regular las Instituciones de Tecnología Financiera.

Para efectos de lo previsto en el Reglamento de la Ley de Datos, se informa al Usuario que el tratamiento de los Datos Personales Recabados puede llevarse como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física.

b) Finalidades secundarias: Estas finalidades son distintas a la que se señala en el apartado a) que antecede, por lo que Usted podrá negar o revocar su consentimiento, así como oponerse a su tratamiento en relación con las finalidades secundarias, en términos del procedimiento descrito en el apartado 5 que sigue.

De manera adicional, los Datos Personales Recabados serán utilizados por ArkAngeles para las siguientes finalidades secundarias: (i) mercadotecnia, publicidad y prospección comercial; (ii) enviarle a los Usuarios información y documentación relativa a promociones, ofertas, publicidad e información de carácter mercadológico y publicitario, respeto de productos o servicios; (iii) para realizar análisis estadísticos, de generación de modelos de información y/o perfiles de comportamiento actual y predictivo; (iv) para participar en encuestas y promociones.

5. Revocación del consentimiento, limitación de uso o divulgación de los Datos Personales Recabados y ejercicio de los derechos de acceso, rectificación, cancelación u oposición (ARCO).

Usted, o su representante legal, podrá en cualquier momento: revocar su consentimiento para el tratamiento o uso de sus datos personales por parte de ArkAngeles, limitar su uso o divulgación, así como acceder a ellos, rectificarlos en caso de que sean inexactos o incompletos, cancelarlos y oponerse a su tratamiento en su totalidad o para ciertos fines. Para tales efectos, Usted deberá contactar al equipo de ArkAngeles a través del correo electrónico: atencion@arkangeles.com

Para revocar su consentimiento para el tratamiento o uso de sus datos personales por parte de ArkAngeles, limitar su uso o divulgación, así como acceder a ellos, rectificarlos en caso de que sean inexactos o incompletos, cancelarlos y oponerse a su tratamiento en su totalidad o para ciertos fines, deberá a través de la solicitud, señalar expresa y detalladamente: (i) que desea revocar su consentimiento para el tratamiento o uso de sus datos personales; (ii) señalar la manera mediante la cual desea limitar el uso o divulgación de los datos personales; (iii) señalar la manera en que desean acceder o rectificar sus datos personales; (iv) señalar que desean cancelar sus datos personales; y/o (v) señalar que desean oponerse al tratamiento de sus datos personales.

Para ejercer los derechos ARCO antes descritos, Usted o su representante legal deberá presentar su solicitud en los términos que se describen en la Ley de Datos, así como presentar copia digital de una identificación oficial del Usuario y, en su caso, documento que acredite la representación legal.

En caso de solicitar la rectificación, el Usuario deberá presentar la documentación soporte de la modificación solicitada en sus datos personales.

ArkAngeles dará una respuesta a la solicitud dentro de los 20 días hábiles siguientes a la fecha en que haya sido recibido el formato debidamente requisitado, pudiendo extender por un periodo igual siempre que exista previa notificación al Usuario o su representante.

Las respuestas serán notificadas al Usuario vía correo electrónico.

La entrega de los datos personales será gratuita, debiendo cubrir el Usuario únicamente los gastos justificados de envío o con el costo de reproducción en copias u otros formatos, en los casos que lo amerite.

Así también, se informa que el Usuario o Titular tiene derecho a iniciar un Procedimiento de Protección de Derechos ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (http://inicio.inai.org.mx/SitePages/ifai.aspx) dentro de los 15 días hábiles siguientes a la fecha en que reciba la respuesta de ArkAngeles, o a partir de que concluya el plazo de 20 días hábiles contados a partir de la fecha de recepción de su solicitud de ejercicio de derechos y no hubiese recibido respuesta alguna.

6. Procedimiento para comunicar los cambios al Aviso de Privacidad.

Todo cambio efectuado al presente Aviso de Privacidad le será notificado y además, estará disponible públicamente en la página electrónica www.arkangeles.com.

7. Transferencia de los Datos Personales Recabados.

Los Datos Personales Recabados serán únicamente transferidos a las personas y con las finalidades que a continuación se describen, por lo que en términos del artículo 37, fracciones IV, V y VII de la Ley de Datos, no se requiere consentimiento alguno para en su caso, realizar dichas transferencias:

Entidades Financieras	En cumplimiento de las finalidades primarias, incluyendo la Transferencia de Datos Personales Recabados a favor de Instituciones Financieras o vehículos necesaria para: (i) celebrar el contrato de Fideicomiso con el Usuario por las Operaciones que realice o contrato que corresponda; y (ii) en cumplimiento y mantenimiento de la relación jurídica con el Usuario y ArkAngeles.

Terceros	En cumplimiento de las finalidades primarias.
Prestadores de servicios	En cumplimiento de las finalidades primarias.
Sociedades de Información Crediticia Autoridades	En cumplimiento de leyes aplicables.

8. Uso de tecnologías para recolectar información

ArkAngeles podrá utilizar diferentes tecnologías para recolectar información, y esto podrá incluir el envío de cookies a su dispositivo móvil o a través de la Plataforma . Las cookies son archivos de datos almacenados en su ordenador o dispositivo móvil, utilizado al visitar páginas Web. Las cookies se utilizan, entre otras cosas, como parte del proceso de registro, ya que permiten obtener información acerca de sus preferencias y sus ajustes de cuenta; ayudan a evaluar y resumir estadísticas de actividad de uso de los clientes, para brindarle una experiencia personalizada al utilizar la Plataforma.

Cuida tu información en la Red.

Lo que debes tomar en cuenta sobre los fraudes cibernéticos.

Los fraudes cibernéticos son aquellas estafas que se emplean a través de las redes para realizar transacciones ilícitas. El delincuente usa herramientas tecnológicas sofisticadas para acceder a distancia a tu información de identidad cibernética.

Muchas veces las personas que realizan este tipo de fraudes se aprovechan del desconocimiento o del poco cuidado que las personas llegan a tener al utilizar cualquier equipo cibernético, como pueden ser una table, un teléfono o laptop, convirtiéndose en un blanco fácil para los estafadores.

Estas estafas pueden darse de muchas maneras y en cualquier momento por eso es recomendable conocer las vertientes más típicas que utilizan estos delincuentes, entre las más frecuentes se encuentran:

1. El correo basura

Comúnmente conocido como SPAM, se trata de un mensaje enviado a varios destinatarios que usualmente no lo solicitaron, con fines aparentemente publicitarios o comerciales.

La información contenida en dicho correo te invita a visitar una página o descargar algún archivo que generalmente es un virus que roba la información de tu dispositivo.

2. Smishing

En esta modalidad de fraude, te envían mensajes SMS a tu teléfono móvil con la finalidad de que visites una página web fraudulenta, con la finalidad de obtener tu información bancaria, para realizar transacciones en tu nombre.

3. Phishing

En este tipo de fraude se hacen pasar por una Institución Financiera, enviando un mensaje indicándote un error en tu cuenta bancaria, y al ingresar tus datos financieros, obtienen tu información confidencial como: números de tus tarjetas de crédito, claves, datos de cuentas bancarias, contraseñas, etc.

Una variante a este fraude es el phishing telefónico (vishing), en donde los delincuentes simulan ser empleados de alguna Institución y te informan que tus cuentas están registrando cargos irregulares o te requieren alguna información confidencial.

4. Pharming

En esta modalidad te redirigen a una página de internet falsa mediante ventanas emergentes, para robar tu información. Suelen mostrar leyendas similares en las cuales te indican que fuiste acreedor a un apremio por visitar su página.

5. Transferencias Electrónicas

En este caso se hacen pasar por una empresa que realiza ofertas muy llamativas, por lo que al comprar te piden realizar una transferencia a cambio de dicho producto y al acudir dicha empresa te das cuenta que nunca existió dicha oferta ni compra.

6. Banca Móvil

En este tipo de fraude roban tus datos por medio de un Malware (código maligno/sotfware malicioso), el cual se inserta en tu teléfono móvil al ingresar a la aplicación de Banca móvil de tu banco de preferencia, el Malware muestra una venta falsa, en donde se solicita tus datos confidenciales como son los datos de tu tarjeta de crédito o debito los cales con enviados a los estafadores para que estos puedan hacer un uso indebido de los mismos.

7. Descarga de Software

Al descargar de una pagina poco confiable o de manera gratuita algún software este puede contener un virus que permite al estafador tomar tu información personal directamente de tu ordenador.

Pero no solo las personas físicas el “Usuario común” se ve afectado por este tipo de fraudes también se ven afectados las Empresas, quienes se enfrentan al robo de patentes, secretos tecnológicos, phishing, en otros.

¿Cómo lo puedes evitarlo?

a) Instala en tu computadora o dispositivo móvil un buen antivirus, utiliza un software tipo firewall o anti-spyware para proteger tus equipos de algún virus malicioso.

b) No des "clic" o abras vínculos sospechosos.

c) Si descargas aplicaciones y/o software realízalo por medio de las tiendas y desarrolladores oficiales

d) No respondas mensajes de correo que te dicen haber ganado un premio, viaje o sorteo

e) Verifica que el sitio en el que navegas cuente con el protocolo de seguridad "https://" y un candado cerrado en la barra de direcciones.

f) Nunca entregues tus datos por correo electrónico.

g) Las empresas y bancos nunca te van a solicitar tus datos financieros o números de tarjetas de crédito por teléfono o internet, cuando no seas tú quien inicie una operación. Si aún te queda duda del correo, llama o asiste a tu banco y verifica los hechos.

h) Desconfía de las compras en línea cuando te pidan que hagas un deposito a cuentas bancarias distintas de la empresa.

i) Cuida tus claves personales, número de identificación personal (NIP), cámbialas periódicamente.

Nota: Recuerda que las personas que realizan este tipo de fraudes son hábiles y te engañan con tácticas alarmistas o solicitudes urgentes para preocuparte y evitar que pienses bien la situación, no entres en pánico y antes de realizar cualquier acción verifica la fuente de procedencia.