INTERMUD

Acuerdo de Datos Privados

Versión 1 –

Junio 2022

0. Cláusulas iniciales

0.1. Este Acuerdo de Datos Privados (ADP) se establece entre la empresa especificada (en lo sucesivo denominada "Proveedor") e INTENACIONAL DE MUDANZAS S.A. (En adelante INTERMUD), con domicilio en 20 av. 18-01 zona 11, ciudad de Guatemala**.**

0.2. ***INTERMUD requiere su aceptación sobre este acuerdo***. De esta forma, el proveedor se compromete a cumplir con los requisitos establecidos por INTERMUD para todos los productos y servicios entregados. Se recomienda discutir la información incluida en este ADP con todos los empleados operativos y líderes de equipo de la empresa del proveedor.

0.3. Cualquier aspecto no mencionado en el presente documento DEBE ser autorizado por INTERMUD antes de la entrega del producto o servicio, de lo contrario, INTERMUD se reservará el derecho de no pagar los cargos derivados de acciones, productos o servicios no autorizados.

0.4. Toda información proporcionada al proveedor por INTERMUD y / o sus empleados será confidencial y el proveedor solo podrá divulgar a terceros aquellos datos necesarios para la entrega de productos o servicios. Esta obligación no tiene fecha de vencimiento.

0.5. El proveedor debe proteger la confidencialidad, integridad, privacidad, disponibilidad y disposición de la información de INTERMUD y sus clientes. Al aceptar este ADP, el proveedor acepta que es responsable, en caso de incumplimiento, de cualquier falla en la seguridad de la información de acuerdo con la legislación internacional sobre protección de la información.

0.6. El proveedor se compromete a no ofrecer, prometer, otorgar, aceptar o solicitar ventajas indebidas de cualquier valor como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño de las obligaciones de dicha persona.

0.7. Al aceptar este documento, el proveedor entiende que INTERMUD puede finalizar el presente Acuerdo De Nivel De Servicio Y Seguridad en caso de:

0.7.1. Ser sancionado por la comisión de delitos relacionados con el comercio internacional, tales como, pero no limitado a:

- terrorismo
- tráfico de drogas
- trata de personas
- contrabando
- corrupción
- otros delitos similares no mencionados en este ADP

0.8. No existe exclusividad entre la relación comercial de INTERMUD con el proveedor, ambos pueden realizar negocios y pactar acuerdos con cualquier otra empresa, siempre que esté apegado al derecho nacional e internacional.

0.9. La firma de este acuerdo no garantiza negocios futuros y se mantendrá vigente hasta que sea aprobado un nuevo acuerdo que cubra los mismos aspectos del actual.

0.10. Todos los cambios futuros se comunicarán por escrito y cada revisión se resaltará para una fácil identificación.

1. índice

2. Responsabilidad empresarial

2.1. Aplicabilidad

INTERMUD solicita a sus proveedores a comprometerse con:

- Proteger los bienes y la información de sus clientes, proveedores y de quienes conforman su capital humano e infraestructura.
- Hacer negocios de forma correcta, ética, justa e incluyente con sus empleados, clientes, proveedores y entidades gubernamentales.

2.2. Privacidad de la información

El proveedor se compromete a proteger la información de los clientes de INTERMUD a través del cumplimiento del *Reglamento General de Protección de Datos,* aprobado por el Parlamento Europeo y el Consejo de la Unión Europea, así como a los principios de protección de la información y la privacidad de mayor aceptación en el mundo.

2.2.1. Datos personales

Se entiende como datos personales toda la información sobre una persona identificable. Se define una persona identificable como aquella cuya identidad pueda determinarse directa o indirectamente, en particular mediante un identificador, como por ejemplo su nombre, número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiología, genética, psíquica, económica, cultural o social de esta persona.

2.2.2. Tratamiento

Cualquier operación o conjunto de operaciones realizadas con datos personales o conjuntos de datos personales de los clientes y empleados de Internacional de Mudanzas S.A. tales como, recopilación, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

2.2.3. Responsable del tratamiento o responsable

Internacional de Mudanzas S.A.

2.2.4. Encargado del tratamiento o encargado

El proveedor de productos y servicios de INTERMUD

2.2.5. Destinatario

La persona física o jurídica, autoridad, servicio u otro organismo al que se comuniquen datos personales de los clientes y empleados de INTERMUD. No obstante, no se considerarán destinatarios las autoridades que puedan recibir datos personales en el marco de una investigación concreta de conformidad con la ley aplicable.

2.2.6. Tercero

Persona física o jurídica, autoridad, servicio u organismo distinto del cliente de INTERMUD, distinto de INTERMUD, distinto del proveedor de productos y servicios, distinto de las personas autorizadas para tratar los datos personales de los clientes de INTERMUD.

2.2.7. Consentimiento del interesado

Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el cliente de INTEMUD acepta, ya que sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos que le conciernen.

2.2.8. Violación de la seguridad de los datos personales

Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

2.3. Política de privacidad y protección de la información de INTERMUD

Por este medio, INTERMUD define, documenta y comunica su política de privacidad y protección de la información y también asigna responsabilidad para tales políticas y procedimientos.

2.3.1. Información recopilada

INTERMUD recopilará información personal con el objeto de proveer a sus clientes un servicio dedicado, sin embargo, requerimos de su consentimiento explícito[1] (por escrito) para captar tal información. Entre los datos que serán recopilados se encuentran:

- Nombre completo
- Dirección de domicilio, ciudad y país de origen y/o destino
- Dirección de correo electrónico
- Números de teléfono móvil y/o residencial
- Detalles de contacto de su empleador (cuando sea necesario)
- Fotografía de algunos de sus bienes para efectos de seguro e inventario
- Fotocopia de cédula y pasaporte.
- Título de propiedad de vehículos (cuando sea necesario).
- Número de seguro social de los Estados Unidos (cuando sea necesario).

2.3.2. Uso de la información recopilada

El proveedor podrá recopilar datos personales del cliente de INTERMUD con el fin de estimar las dimensiones, pesos y condiciones que determinarán la presentación de una cotización de servicio. Durante una visita de estimación de peso y volumen, puede ser necesario fotografiar piezas frágiles y valiosas ubicadas dentro de la residencia del cliente, tales imágenes serán suministradas al área operativa para confeccionar cajas de madera (cuando sea necesario).

El proveedor podrá solicitar copia de algún documento de identidad del cliente que sea necesario para los trámites de exportación / importación de sus enseres. Esto también aplica para la documentación de un vehículo.

Cuando el embarque tenga como destino Estados Unidos, el proveedor podrá solicitar al cliente de INTERMUD su número de seguro social.

[1] El cliente de INTERMUD tiene derecho a revocar su consentimiento explícito (por escrito) para el uso de su información personal.

2.3.3. Divulgación de información personal a terceros

Siempre que cuente con el consentimiento explícito de INTERMUD y sus clientes, el proveedor podrá divulgar información personal (de tales clientes) a terceros.

2.3.4. Elección y consentimiento explícito del interesado

El proveedor necesita autorización de INTERMUD antes que pueda recopilar cualquier tipo de información personal de los clientes de INTERMUD. Dicho consentimiento explícito podrá ser **revocado** en cualquier momento por el cliente o INTERMUD.

El consentimiento explícito jamás podrá deducirse del silencio o inacción de las personas.

2.3.5. Disposición de la información personal

Al finalizar cualquier servicio entregado a un cliente de INTERMUD, el proveedor debe eliminar toda la información personal recopilada anteriormente para mitigar riesgos de fuga de información personal.

2.3.6. Acceso a la información personal

Los proveedores deben asegurar a los clientes de INTERMUD:

- Acceso a su información personal cuando estas lo soliciten para su revisión, actualización y en otras situaciones cuando así se requiera
- Adhesión a los derechos a olvidar su información (borrarla)
- Portabilidad de datos (entregar la información personal cuando le sea solicitado)

2.3.7. Monitoreo y cumplimiento de la política de privacidad y protección de la información

INTERMUD supervisará el cumplimiento de sus proveedores respecto con esta política y cuenta con procedimientos para abordar las quejas y disputas relacionadas con la privacidad.

2.3.8. Responsabilidad sobre las consecuencias de la divulgación de información a terceros

INTERMUD establece acuerdos de seguridad con sus proveedores para definir límites en las responsabilidades compartidas sobre la protección de la información personal de los clientes de INTERMUD.

Si una empresa incumple estos requisitos podría ser procesada bajo las leyes de la Unión Europea, incluso cuando se encuentre fuera de Europa.

2.3.9. Brechas de seguridad

El proveedor notificará a INTERMUD cuando se confirme una brecha de la seguridad de la información personal. Ante esta situación, el proveedor deberá activar un *protocolo de seguridad ante brechas de seguridad de los datos personales*.

2.3.10. Protocolo ante brechas de seguridad de los datos personales

Cuando se identifique una violación de seguridad de los datos personales retenidos en sus servidores, el proveedor responderá de la siguiente manera:

- Informar a INTERMUD sobre la fuga de información de inmediato
- Evaluar el riesgo de brechas de seguridad de la información de los clientes de INTERMUD
- Notificar al área de tecnología de información (TI) sobre la violación de seguridad dentro de 72 horas desde el momento que ha identificado la fuga de información
- Suministrar al área de TI toda la información sobre la brecha de seguridad
- Proveer a los clientes de INTERMUD toda información sobre la fuga de su información personal y asesorarlos para ayudarlos a protegerse contra los efectos de tal brecha en la seguridad
- Documentar todas las violaciones de seguridad, incluso las que no necesitan ser reportadas

2.4. Control de acceso a las instalaciones de su empresa

El control de acceso a las instalaciones del proveedor previene el ingreso no autorizado, mantiene el control de sus empleados, visitantes y protege los activos de su empresa. El proveedor debe tener un procedimiento implementado que incluya los siguientes aspectos:

2.4.1. Acceso del personal

El proveedor debe:

a) Proveer identificación a sus colaboradores
b) Controlar el acceso a sus instalaciones
c) Limitar el acceso a áreas críticas (cuando sea necesario)

2.4.2. Acceso para visitantes, contratistas y terceros

Todo los visitantes, contratistas y terceros del proveedor deben:

a) Presentar una identificación oficial con fotografía
b) Mantener un registro de entrada y salida
c) Solicitar autorización para su admisión
d) Dar una identificación temporal controlada
e) Asegurar de que estén acompañados durante su estadía en la empresa
f) Limitar el acceso a áreas restringidas

2.4.3. Recepción de correo y paquetería

El proveedor debe:

- Inspeccionar el correo y los paquetes recibidos antes de distribuirlos
- Mantener registro que incluya la información de identidad de quién recibe y a quién está destinado el correo o paquete

2.4.4. Otros controles

El proveedor debe controlar la operación dentro de sus instalaciones, a través de:

- Entregar una identificación temporal a los visitantes para que la exhiban en un lugar visible, bajo las regulaciones de seguridad industrial aplicables.
- Identificar y retirar personas no autorizadas.

2.5. Política ambiental

Los proveedores de INTERMUD deberían contar con una política ambiental que:

- Incluya un compromiso de la alta dirección con la reducción del impacto sobre el ambiente
- Sea comunicada a todos sus empleados

2.6. Políticas contra la discriminación y el acoso, garantía de un ambiente libre de alcohol y drogas.

2.7. Anticorrupción y antisoborno

INTERMUD establece como referencia el ABC[2] de FIDI y los requisitos relacionados con el soborno; dejando en claro que la empresa está decidida a prevenir la corrupción y luchar contra ella. INTERMUD cree en valores fundamentales, tales como la honestidad, el respeto hacia el estado de derecho, la responsabilidad y la transparencia para promover el desarrollo y hacer de nuestro mundo un lugar mejor para todos.

A menudo, se piensa que la corrupción y el soborno son “sólo un modo de vida”, pero todas las sociedades, así como todos los sectores e individuos, saldrían ganando si se dijera “NO” a estos delitos. La erradicación de la corrupción permite el desarrollo social y económico de una nación. Para luchar contra la corrupción y el soborno, INTERMUD exige a sus proveedores de productos y servicios:

- Educar a sus colaboradores acerca de la responsabilidad de la organización de erradicar la corrupción. Una justicia igualitaria e imparcial para todos es decisiva para la estabilidad y el crecimiento de un país. También ayuda a combatir eficazmente la delincuencia.

[2] FIDI ABC: FIDI Anti-Bribery & Anti-Corruption Charter (Carta Anticorrupción y Antisoborno de FIDI).

- ¿Cómo? Esta educación se proveerá dentro de las instalaciones de la organización y los facilitadores serán gerentes y supervisores de la organización.

3. Requisitos generales cuando se trata directamente con clientes de INTERMUD

3.1. Al tener contacto directo con los clientes de INTERMUD, debe dirigirse a ellos de manera profesional. Por ejemplo, evite usar nombres de pila, en su lugar, diríjase a ellos como señor(a) señorita, o cualquier otro título representativo.

3.2. No proporcione ningún tipo de factura, costo o información de tarifas a clientes de INTERMUD, cuentas ni a ninguna otra persona que pueda llamar, escribir o solicitar de cualquier manera. Debe notificar a Internacional de Mudanzas S.A. si esto ocurre.

4. Gestión de asociados de negocio

Los asociados de negocio están conformados por las partes interesadas de su empresa, representadas por sus clientes, proveedores, proveedores y otros terceros que usted considera que tienen cierta importancia crítica para la gestión de riesgos de su empresa.

Su empresa debe contar con un procedimiento para implementar y verificar periódicamente los controles operativos de sus socios comerciales. Su empresa debe tener una lista actualizada de socios comerciales.

5. Prevención de lavado de activos y financiación de terrorismo

5.1.1. Su procedimiento de selección de asociados de negocio debe incluir criterios de prevención como, entre otros:

a) Conocimiento de sus asociados de negocio, identidad y legalidad de la empresa y sus asociados.
b) Sus antecedentes legales, criminales y financieros.
c) Monitorear sus operaciones (actividad económica, origen de sus ingresos, características de sus operaciones, sus otros clientes, cumplimiento de los contratos y su edad de mercado).
d) Cómo informar oportunamente a las autoridades, al identificar operaciones sospechosas (de sus asociados de negocio).
e) Verificación si sus asociados de negocio pertenecen a algún gremio o asociación.

5.1.2. El procedimiento de selección de socios comerciales debe considerar, como mínimo, los siguientes factores para identificar operaciones sospechosas:

a) Origen y destino de las operaciones comerciales de sus asociados de negocio.
b) Frecuencia de sus operaciones.
c) El valor y tipo de sus productos.
d) Modo de operación de transporte.
e) Forma de pago.
f) Inconsistencias en la información proporcionada por sus asociados de negocio.
g) Requisitos no establecidos.

Nota: Para reportar actividades sospechosas no es necesario estar seguro de que se trata de una actividad delictiva, ni identificar el tipo de delincuencia o que los recursos involucrados provienen de dichas actividades. Este informe debe hacerse a las autoridades de cada país.

6. Seguridad en los procesos relacionados con el personal

El personal se define como colaboradores directos, personal subcontratado y personal temporario

6.1. Procedimientos de gestión de personal

Su empresa debe tener un procedimiento en su lugar, de acuerdo con las reglamentaciones locales, que regula las siguientes actividades.

6.1.1. Verificación previa a la contratación

a) Información proporcionada por el candidato
b) referencias personales y laborales
c) antecedentes penales

6.1.2. Selección y contratación

Su compañía debe:

a) Verificar las competencias
b) Aplicar pruebas para detector el consume de alcohol y drogas ilícitas al personal que ocupará cargos críticos.
c) Mantener un registro fotográfico actualizado del personal e incluya una huella digital y un registro de firma.
d) Controlar la entrega, uso y devolución de los elementos de trabajo, identificación y uniformes cuando tengan insignias de la compañía.

Su compañía debe:

e) Realizar una visita domiciliaria al personal que ocupará puestos críticos en función de la gestión de riesgos y las reglamentaciones locales.

6.1.3. Mantenimiento del personal

Su compañía debería:

a) Actualizar los datos de personal al menos una vez al año.
b) Verificar los antecedentes del personal que ocupa cargos críticos al menos una vez al año.
c) Aplicar pruebas para detectar el consumo de alcohol y drogas ilícitas al azar, como máximo cada dos años y cuando haya sospechas.
d) Mantener un programa ilegal de prevención de adicciones.
e) Mantener un programa para prevenir el riesgo de corrupción y soborno.

Su compañía debería:

f) Realizar una visita domiciliaria al personal que ocupe puestos críticos, según la gestión de riesgos y las reglamentaciones locales, como máximo cada dos años.

6.1.4. Terminación de la relación de trabajo

Su compañía debe:

a) Retirar la identificación, uniformes y activos a partir de lo que indican los registros generados durante la entrega de estos.
b) Eliminar el acceso a los sistemas computarizados e instalaciones.

Su empresa debe, de acuerdo con su gestión de riesgos:

c) Comunicar a las partes interesadas la disociación del colaborador.

Nota: Cuando se presenta un cambio en la posición de un colaborador, se deben considerar los elementos descritos en el proceso de contratación.

7. Programa de entrenamiento

Su compañía debe contar con un programa anual de entrenamiento que incluya como mínimo:

a) La política de seguridad de su empresa.
b) Gestión de riesgos, controles operativos, preparación y respuesta a eventos.
c) Cumplimiento de los requisitos legales relacionados con las funciones de su personal.
d) Impacto de las actividades individuales en el cumplimiento de los indicadores de efectividad del proceso.
e) Aplicación de procedimientos de seguridad.
f) Prevención de adicciones al alcohol, drogas, juegos y otros, incluidos avisos visibles y material de lectura.
g) Prácticas de prevención de corrupción y soborno.
h) Lavado de dinero y financiamiento del terrorismo.
i) Prácticas para evitar conspiraciones internas y actividades sospechosas.

8. Seguridad física

Orientaciones: la seguridad física se refiere a las medidas de protección de las instalaciones donde se llevan a cabo los procesos críticos.

8.1.1. Su empresa debe implementar y mantener:

a) Estructuras y barreras perimetrales que impiden el acceso no autorizado.
b) Cerraduras en puertas y ventanas.
c) Sistemas de alarma que identifiquen el acceso no autorizado.

8.1.2. Su compañía debe establecer e implementar:

a) Inspecciones y reparaciones periódicas para mantener la integridad de las barreras perimetrales y la estructura de los edificios.
b) Control de llaves, dispositivos y códigos de acceso.
c) Inspecciones y reparaciones periódicas a los sistemas de emergencia.

8.1.3. Su empresa debe implementar y mantener de acuerdo con su gestión de riesgos:

a) Sistemas de CCTV monitoreados por personal competente las 24 horas del día.
b) Sistemas de respaldo de imágenes y video (grabación) con suficiente capacidad de almacenamiento para responder a posibles eventos.

Nota. Los elementos de seguridad física deben estar de acuerdo con la gestión de riesgos.

8.1.4. Su compañía debe tener un servicio de seguridad competente de acuerdo con los requisitos legales y que garantice una acción de respuesta oportuna.

9. Seguridad en los procesos de tecnología de información

Orientaciones: se considera seguridad de la información a todas las medidas y controles establecidos para que su empresa mantenga la integridad, confidencialidad, disponibilidad de documentos, registros y evidencias relacionadas con las actividades comerciales de su empresa.

9.1. Información

Su compañía debe establecer e implementar:

a) Una política para evitar que se revele información confidencial.
b) Una política para el uso de recursos informáticos.
c) Una política de privacidad y protección de datos[3].
d) Procedimientos de evaluación de riesgos para mitigar los riesgos de violaciones de seguridad de la información personal de INTERMUD.
e) Evaluación de riesgos del impacto de la protección de datos.
f) Protocolo para violaciones de seguridad de datos y comunicación a las partes afectadas.

9.2. Seguridad en las tecnologías de información (TI)

Su compañía debe:

[3] La política de privacidad y protección de datos de su compañía debe cumplir con el Reglamento General para la Protección de Datos (RGPD) y/o el Escudo de Privacidad, para tal fin, debe completar nuestro cuestionario de seguridad para proveedores.

a) Establecer políticas o contar con procedimientos establecidos para administrar la seguridad de la información y que permitan identificar, proteger y recuperar la información.
b) Usar cuentas asignadas individualmente y cada usuario que tiene acceso al sistema debe tener sus propias credenciales de acceso y mantener contraseñas; estos deben ser cambiados periódicamente.
c) Revisar periódicamente los accesos asignados a los usuarios.
d) Evitar la instalación de software no autorizado.
e) Implementar y mantener software y hardware que protegen la información de amenazas informáticas (virus, acceso no autorizado y similares).
f) Tener copias de seguridad de la información sensible y una copia debe almacenarse de forma segura fuera de las instalaciones en función de la gestión de riesgos.
g) Eliminar el acceso a la información a todos los colaboradores externos a la terminación de su contrato o acuerdo.
h) Mantener un registro actualizado de usuarios y códigos de acceso.
i) Cerrar / bloquear la sesión en computadoras desatendidas.

Su compañía debe:

a) Prohibir la conexión de dispositivos periféricos personales (teléfonos inteligentes, reproductores MP3, memorias USB, etc.) a cualquier dispositivo que esté conectado a la red informática. Los puertos USB deberían estar deshabilitados de forma predeterminada.

9.1. Control de inventario

El proveedor debe contar con procedimientos para controlar el acceso de bienes de los clientes de INTERMUD mientras se encuentren bajo su cuidado.

ACUERDO

Al recibir nuestro correo de aceptación y/o confirmación de servicio como proveedor de INTERMUD, se da por enterado y acepta estos lineamientos, de no estar de acuerdo con esta política enviar correo a intermud@intermud.com