Política de Protección de Datos Personales

Política de Protección de Datos Personales

Objetivo

PTM International Logistics, SA de CV y cada una de sus empresas afiliadas y subsidiarias en Mexico y mundial (en lo sucesivo "PTI") ("**Phoenix Tower**" o "**PTI**"), como responsable de uso y protección de los Datos Personales ("**DP**") que trate con motivo de sus operaciones, pone a disposición de su personal, contratistas, proveedores, socios comerciales y demás terceros relacionados la presente Política de Protección de Datos Personales ("**Política**") para demostrar el compromiso que tiene respecto de la protección de los DP, así como el compromiso de la gerencia con el aprendizaje y la mejora continua.

PTI está comprometido con la protección y confidencialidad de la privacidad y de los DP que trate, incluyendo aquellos de su personal, candidatos y proveedores, de conformidad con lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, su Reglamento, los Lineamientos del Aviso de Privacidad, así como con la normativa y disposiciones aplicables en materia de protección de datos personales (la "**Ley**"). Asimismo, PTI tratará los DP observando en todo momento los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.

Alcance

Esta política se aplica a todos los empleados, contratistas, proveedores, socios comerciales o cualquier otro tercero que apoyen o interactúen con Phoenix Tower para el tratamiento de DP.

Generalidades

Phoenix Tower considera la protección de DP como uno de los aspectos más importantes de su negocio.

- La alta dirección de Phoenix Tower liderará el ejemplo asegurando que se le dé una alta prioridad a la protección de DP en todas las actividades e iniciativas empresariales actuales y futuras.
- La Política será revisada anualmente por los funcionarios autorizados de Phoenix Tower para asegurar que sean relevantes, actualizadas y adecuadas a la luz de la evolución de la tecnología, las necesidades del negocio y la legislación aplicable.
- La Gerencia comunicará la revisión de la Política a todo el personal por diversos medios, tales como actualizaciones electrónicas, sesiones de información, capacitación, boletines informativos, etc.
- La finalidad de esta política es establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los DP contra cualquier daño, pérdida, alteración, vulneración, destrucción, uso, acceso o tratamiento no autorizado.

- Por otra parte, la Política tiene el objetivo de ayudar a los empleados, contratistas y proveedores, según corresponda, a determinar qué información se puede revelar a terceros, así como la sensibilidad de la información que no se divulgará fuera de Phoenix Tower sin la debida autorización.

Con el fin de cumplir o superar estos objetivos, se han puesto en marcha las siguientes prácticas:

- Las herramientas de concientización se distribuyen al contratar y durante toda la relación laboral o contractual con Phoenix Tower.

- Los empleados, consultores contratados y/o seleccionados y los empleados temporales firmarán un aviso de recepción de la Política.

- El entendimiento del personal se reforzará continuamente para que las cuestiones de protección de DP sean un eje rector durante la conducción de sus actividades laborales.

- La capacitación individual en materia de datos personales es obligatoria, con cualquier capacitación técnica apropiada a las responsabilidades de la función del trabajo. Cuando el personal cambia de puesto de trabajo, sus necesidades de formación en materia de protección de datos personales deben ser reevaluadas y cualquier nueva formación proporcionada como una prioridad.

Definiciones

Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de los DP de un Titular.

Datos Personales (DP): Cualquier información concerniente a una persona física identificada o identificable, incluyendo:

- Número de Seguridad Social;
- Número de Clave Única de Registro de Población;
- Número de Registro Federal de Contribuyentes;
- Número de Credencial de Elector;
- Números de licencia de conducir nacional o extranjera;
- Números de pasaporte o copias de pasaportes;
- Fecha de nacimiento; y
- Información de contacto personal (vgr., números de teléfono, direcciones).

Datos Personales (DP) financieros: Aquellos datos personales concerniente a una persona física identificada o identificable en materia financiera o patrimonial, incluyendo:

- Número de tarjeta de crédito o de débito corporativo o personal (Incluyendo PIN o números de acceso);
- Historial crediticio;
- Cuentas bancarias; e
- Información de las propiedades de un Titular.

Datos Personales (DP) sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, la autoridad competente en materia de protección de datos personales en los Estados Unidos Mexicanos.

Titular: La persona física a quien corresponden los datos personales.

Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.

Tratamiento de los Datos Personales

Recolección de DP

Antes de llevar a cabo la recolección de los DP, se debe analizar detalladamente si existe la necesidad de negocio para llevar a cabo dicha recolección, así como de las finalidades de su tratamiento. Posteriormente, si por cuestiones de negocio Phoenix Tower requiere tratar DP; entonces, las áreas de negocio o administrativas (por ejemplo, Recursos Humanos para el caso de DP de candidatos) se encargaran de entregar los Avisos de Privacidad a los Titulares y de obtener su consentimiento, según sea aplicable, antes de llevar a cabo la recolección de los DP.

De acuerdo con la Ley, se requerirán diferentes tipos de consentimiento, dependiendo del tipo de DP que vayan a ser recabados:

- Consentimiento tácito para el caso de recolección de DP;
- Consentimiento expreso para el caso de recolección de DP financieros; y
- Consentimiento expreso y por escrito para el caso de recolección de DP sensibles.

Únicamente se recabarán los DP que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido. Dichas finalidades se establecerán en los Avisos de Privacidad aplicables.

Los DP no deben recolectarse por medios inapropiados; solo podrán recolectarse mediante los formularios o documentos de PTI y contra la entrega del Aviso de Privacidad, y obtención del consentimiento, según

corresponda. Si la información personal es recopilada por un Encargado y es dudoso si el Encargado la recolectó por medios apropiados, la información no debe recabarse.

Uso de la información personal

La información personal solo se utilizará y tratará para cumplir las finalidades para los que se obtuvo la información personal. En caso de que requieran ser utilizados para finalidades distintas a las señaladas en los Avisos de Privacidad, se obtendrá el consentimiento del Titular antes de llevar a cabo el tratamiento respectivo.

Finalidad del Tratamiento de los DP

Los DP recolectados por PTI o sus Encargados serán tratados para las finalidades legales y de negocio que requiera Phoenix Tower, mismas que quedarán establecidas en los Avisos de Privacidad correspondientes. Por otra parte, Phoenix Tower podrá tratar los DP para las finalidades secundarias que estime convenientes, incluyendo para finalidades de mercadotecnia o estadísticas, según corresponda y únicamente si PTI cuenta con los consentimientos respectivos de los Titulares.

Los DP serán incluidos en una base de datos denominada "Base de Datos de Titulares", que le permite a Phoenix Tower, sociedades controladoras y/o filiales, recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos DP, de conformidad con la Ley.

Almacenamiento y Manejo de Información que Contiene Datos Personales

Los DP, y por lo tanto la Base de Datos de Titulares, pueden ser contenidos en documentos impresos o electrónicos. Ambas formas de DP están comprendidas dentro del alcance de esta Política.

DP almacenados en medios electrónicos

Los DP pueden ser guardados electrónicamente por una variedad de métodos y dispositivos, incluyendo de forma enunciativa mas no limitativa, lo siguiente:

- *Dispositivos móviles (vgr., computadores portátiles, teléfonos y tabletas inteligentes, PDAs)*. Los DP se pueden guardar en dispositivos móviles, pero dichos dispositivos deben estar protegidos con contraseña, encriptados y con opciones de borrado remoto. Este no es un método preferido para almacenar DP y la información almacenada en dispositivos móviles debe ser vista como una ubicación de almacenamiento temporal y los DP deben ser trasladados a un servidor PTI tan pronto como sea posible.

- *Correo electrónico, Internet y programas de mensajería instantánea*. PTI no recomienda la transmisión de DP por correo electrónico, Internet o programas de mensajería instantánea. Sin embargo, sSi se van a transferir DP por correo electrónico, se deben tomar las siguientes medidas para garantizar una transmisión segura y minimizar el riesgo de que se produzca una vulneración después de que se confirme que se han guardado los DP en el servidor local:

1. Proteger el documento con una contraseña, ya sea en PDF, Word o Excel. Si el documento está en un formato que no esté fácilmente protegido (es decir, gif o jpeg), convierta el documento en un archivo PDF, proteja con contraseña en este formato y vuelva a guardarlo. El formato "original" puede ser borrado en este momento y eliminado de la papelera.

2. Envíe por correo electrónico el documento con la palabra "** CONFIDENCIAL **" como etiqueta seguido del nombre del sujeto en la línea de asunto.

3. Póngase en contacto con el destinatario por teléfono para confirmar que el destinatario haya recibido el correo electrónico y proporciónele la contraseña. ***NUNCA ENVÍE LA CONTRASEÑA EN EL MISMO CORREO ELECTRÓNICO***

4. Elimine el archivo adjunto del correo electrónico enviado.

Si cualquier DP es recibido por PTI por cualquiera de los medios anteriores (correo electrónico, Internet o programas de mensajería instantánea), la información debe ser transferida inmediatamente al servidor local (primera opción) o trasladada al almacenamiento de un dispositivo móvil y luego deberá ser borrado permanentemente del programa en el que se recibió.

- *Medios electrónicos extraíbles (vgr., controladores USB, controladores de discos compactos, discos duros externos)*. Los DP pueden guardarse en medios electrónicos extraíbles con el fin de transportar información. Los dispositivos de medios extraíbles deben estar protegidos con contraseña y encriptados. Este no es un método preferido para almacenar DP. La información almacenada en medios electrónicos extraíbles debe ser vista como una ubicación de almacenamiento temporal y los DP deben ser trasladados a un servidor local de PTI tan pronto como sea posible.

- *Servidor local propiedad de PTI*. El lugar de preferencia para el almacenamiento de los DP será en servidores locales propiedad de PTI y este método de almacenamiento siempre debe utilizarse cuando esté disponible. Los servidores locales deben configurarse con protección de cortafuegos (*firewall*) para impedir el acceso externo no autorizado a la red. Además, todas las carpetas y datos que contengan DP estarán claramente etiquetados como tales y el acceso a estas carpetas estará restringido sólo a aquellas personas que deban tener acceso en función de sus actividades de trabajo.

- *Servidores en la nube de terceros*. En algunos casos, los datos de PTI que contienen DP, tendrán que residir en servidores en la nube de terceros (vgr., Siterra y Microsoft AX). Antes de contratar a terceros, el equipo de TI verificará, a través de procesos de diligencia debida, que el tercero haya implementado medidas para proteger los DP del acceso, adquisición y divulgación no autorizados y que cumplan por lo menos con las medidas de seguridad señaladas en la Ley y aquellas que mantengan para el manejo de su información. IT puede confiar en cualquier certificación aceptada por la industria obtenida por el tercero dentro de los 12 meses anteriores como validación de controles de seguridad efectivos.

No se permitirá en ningún caso que los dispositivos que no sean propiedad, arrendados o administrados por PTI: (i) contengan DP; o (ii) acceder por medio de ellos a servidores locales, en la nube o eliminar servidores que contengan DP.

DP almacenados en medios físicos

Ahora bien, los DP pueden ser guardados físicamente, incluyendo de forma enunciativa mas no limitativa, lo siguiente:

- *Almacenamiento físico (interno)*. Los DP almacenados localmente deben ser asegurados en cajones cerrados con llave y preferentemente en cuartos bajo llave. El acceso a estas ubicaciones debe limitarse a aquellas personas que requieran tratar los DP con motivo de sus funciones de trabajo. Las llaves a tales localizaciones seguras deben ser guardadas solamente por el jefe de departamento y cualquier acceso deberá ser documentado en un formato de registro. En ningún caso saldrán documentos con DP de la oficina, salvo en casos extraordinarios y con la previa aprobación del CEO.

  Toda la información, los datos y los documentos que contengan DP deben estar claramente etiquetados para que todos los usuarios estén al tanto de la propiedad, la clasificación y el valor de la información. La información, los datos y los documentos que contengan DP serán transportados con seguridad y destruidos de manera segura para protegerlos de ser divulgados. La información, los datos y los documentos que contengan DP se almacenarán de forma segura cuando no sean utilizados.

- *Almacenamiento físico (externo)*. No está permitido bajo ninguna circunstancia almacenar documentos físicos que contengan DP fuera de las oficinas de Phoenix Tower. Los datos que contengan DP en formato impreso no deben enviarse a instalaciones externas, incluyendo en los hogares de los empleados.

- Toda la información, los datos y los documentos que contengan DP deben estar claramente etiquetados para que todos los usuarios estén al tanto de la propiedad, la clasificación y el valor de la información. La información, los datos y los documentos que contengan DP serán transportados con seguridad y destruidos de manera segura para protegerlos de ser divulgados. La información, los datos y los documentos que contengan DP se almacenarán de forma segura cuando no sean utilizados.

- *Transporte de impresiones*. Cuando haya documentos que contengan DP que deban ser transportados fuera de las oficinas de PTI, solo podrán ser realizadas por empleados directos de PTI y una vez que se haya obtenido la autorización correspondiente. Debe asegurarse de que los datos que contengan DP estén asegurados (maletín cerrado, etc.) y que dichos datos estén siempre en posesión del empleado durante el transporte.

- *Impresiones en papel*. La impresión de datos que contienen DP (almacenados electrónicamente) debe evitarse en la medida de lo posible. Solo en situaciones extraordinarias, el empleado que imprimirá dichos documentos, necesitará recibir la aprobación previa del jefe del departamento, indicando qué materiales se están imprimiendo y por qué razón. El empleado también será

responsable de la destrucción de las copias impresas y proporcionará al jefe del departamento una declaración que incluya la fecha de destrucción, descripción del material destruido y el método utilizado.

Acceso a DP por parte de empleados

Cada jefe de departamento es responsable de identificar y mantener una lista de usuarios de su departamento que d eban tener acceso a los archivos (electrónicos o impresos) que contengan DP. La lista debe actualizarse según sea necesario y, como mínimo, debe revisarse mensualmente. La lista se proporcionará al departamento de TI, que a su vez será responsable de garantizar que el acceso a los archivos impresos y en papel que contengan DP esté restringido de acuerdo con la lista. Los gerentes de departamentos deben revisar el acceso de los usuarios en cualquier cambio en las funciones y responsabilidades de un individuo afectado, o el estado de empleado/contratista independiente (incluyendo la terminación) y comunicar cualquier cambio oportuno a TI.

Transferencias y Uso de Encargados

Consentimiento para llevar a cabo las Transferencias de DP

PTI podrá transferir los DP cuando por cuestiones razonables de negocio se requiera o cuando así lo establezca la Ley. Por regla general, Phoenix Tower deberá obtener el consentimiento del Titular antes de realizar una Transferencia, salvo en los supuestos de excepción establecidos en la Ley y que son los que se describen a continuación:

- Cuando la Transferencia esté prevista en una ley o tratado en los que México sea parte;
- Cuando la Transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
- Cuando la Transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable (vgr., PTI), o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
- Cuando la Transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del Titular, por el responsable y un tercero, incluyendo en el caso de la contratación e instrucción a un Encargado;
- Cuando la Transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
- Cuando la Transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; y
- Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

En cualquier otro caso, PTI deberá obtener el consentimiento y la Transferencia únicamente podrá llevarse a cabo conforme a lo señalado en el Aviso de Privacidad y para las finalidades a las que el Titular sujetó su Tratamiento. Independientemente de que la Transferencia requiera o no del consentimiento del Titular, todas las Transferencias de DP deberán ser formalizadas mediante un contrato o clásulas contractuales que permitan a PTI demostrar que hizo del conocimiento del receptor de los DP las condiciones aceptadas por los Titulares para el Tratamiento de sus Datos Personales, así como el papel que sume el receptor por virtud de dicha Transferencia.

Transferencia de información que contienen DP a Encargados

Esta sección aplica a todos los Encargados (vgr., *land acquisition specialists*) que tratan, almacenan, procesan o transmiten DP o de otro modo tienen acceso a dichos DP en nombre y por cuenta de PTI:

- El Encargado deberá firmar un contrato o acuerdo que contenga requisitos específicos para que él implemente, mantenga y verifique los controles de seguridad para proteger los DP del acceso, adquisición, vulneración, destrucción, uso, modificación y divulgación no autorizados de DP.

- El Encargado únicamente podrá tratar los DP conforme a las instrucciones de PTI y deberá guardar su confidencialidad en todo momento. El Encargado deberá abstenerse de tratar los DP para finalidades distintas a las instruidas por PTI, así como de transferir los DP sin la autorización de PTI o cuando así lo requiera la autoridad competente.

- Antes de contratar Encargados, el departamento de TI verificará, a través de un proceso de debida diligencia, que el Encargado haya implementado medidas razonables, siendo como mínimo los estándares señalados en la Ley y los que ellos ocupen para el resguardo de su información, para proteger los DP del acceso, adquisición, destrucción, vulneración, modificación y divulgación no autorizados. El equipo de TI puede confiar en cualquier certificación aceptada por la industria obtenida por el Encargado en los últimos 12 meses como validación de controles de seguridad efectivos. En caso de que el Encargado no tenga representación independiente de controles de seguridad efectivos, o las pruebas presentadas se consideren inadecuadas, no se permitirá la transmisión de DP a este tercero.

- El Encargado deberá suprimir los DP objeto de tratamiento una vez cumplida la relación jurídica con PTI o según lo instruya PTI.

- Los Encargados serán auditados anualmente para asegurar el cumplimiento con el mantenimiento de los requisitos de acceso no autorizado.

- Toda transmisión de DP a terceros estará en cumplimiento con la sección anterior titulada “Almacenamiento y manejo de información que contiene DP”.

- El departamento de TI mantendrá una lista de todos los terceros que hayan recibido o tengan acceso a DP.

Derechos de los Titulares

Derechos ARCO

De conformidad con la Ley, los Titulares tienen derecho a conocer qué datos personales tiene PTI, para qué los utiliza y las condiciones del uso que les da (Acceso). Asimismo, es su derecho solicitar la corrección de su información personal en caso de que esté desactualizada, sea inexacta o incompleta (Rectificación); que PTI la elimine de sus registros o bases de datos cuando considere que la misma no está siendo utilizada conforme a los principios, deberes y obligaciones previstas en la normativa (Cancelación); así como también los Titulares podrán oponerse al uso de sus DP para fines específicos (Oposición). Estos derechos se conocen como derechos ARCO.

Para el ejercicio de cualquiera de los derechos ARCO, los Titulares deberán presentar una solicitud a los funcionarios que PTI designe, enviada a la dirección física o electrónica que PTI especifique en los Avisos de Privacidad respectivos.

Los Titulares deberán incluir la siguiente información en las solicitudes: (i) su nombre y domicilio; (ii) teléfono fijo y celular; (iii) correo electrónico; (iv) una copia de su identificación oficial (pasaporte, credencial de elector o licencia de conducir); (v) la descripción clara y precisa de los datos personales a los que desea acceder, rectificar, cancelar u oponerse o cualquier otro elemento que facilite la localización de sus datos; (vi) el requerimiento o trámite a solicitar; (vii) su firma autógrafa; y (viii) cualquier otro requisito establecido por la Ley y demás disposiciones aplicables.

La respuesta de PTI indicará si la solicitud de acceso, rectificación, cancelación u oposición es procedente y, en su caso, PTI hará efectiva la determinación dentro de los 15 días hábiles siguientes a la fecha en que comunique la respuesta al titular de los DP o a su representante en su caso. Los plazos podrán ser ampliados en los términos que señale la Ley. PTI proporcionará copias electrónicas de los DP en caso de que el Titular ejerza su derecho de acceso.

Revocación de consentimiento

Los Titulares podrán revocar el consentimiento que hayan otorgado a PTI para el Tratamiento de sus DP. Sin embargo, no en todos los casos PTI podrá atender dicha solicitud o concluir el uso de forma inmediata, ya que es posible que por alguna obligación legal se requiera seguir tratando los DP. En ciertos casos, la revocación del consentimiento implicaría que PTI no pueda seguir con la relación contractual o laboral con el Titular.

Para el ejercicio del derecho de revocación de consentimiento, los Titulares deberán presentar una solicitud a los funcionarios que PTI designe enviada a la dirección física o electrónica que PTI especifique en los Avisos de Privacidad respectivos.

Limitación de uso o divulgación

El Titular tendrá derecho de limitar el uso o divulgación de sus DP para las finalidades que no sean necesarias para la relación jurídica con PTI, incluyendo en el caso de que el Titular ya no desee recibir comunicaciones o mercadotecnia de PTI.

Para el ejercicio de este derecho, los Titulares deberán presentar una solicitud a los funcionarios que PTI designe enviada a la dirección física o electrónica que PTI especifique en los Avisos de Privacidad respectivos. En este caso, el Titular será incluido en un listado de exclusión del cual se le otorgará una constancia.

Monitoreo de Herramientas de Trabajo

La política de herramientas de trabajo de PTI prohíbe el uso de los dispositivos propiedad o arrendados por PTI para uso de trabajo, para propósitos personales. Asimismo, PTI prohíbe el almacenamiento de información o DP en los mismos. El personal de PTI no deberá almacenar DP o información personal en dichos dispositivos proporcionados por PTI.

Toda la información almacenada en los dispositivos de PTI será propiedad de la empresa, sus filiales o subsidiarias. Por otra parte, PTI monitorea en forma regular el uso que le dé su personal al correo electrónico, archivos y páginas de Internet que reciben, escriben o visitan utilizando los dispositivos que PTI les proporcionan. PTI podrá acceder, usar, compartir, destruir y suprimir cualquier información en sus dispositivos.

PTI tiene la facultad de inspeccionar, monitorear, supervisar y compartir con terceros, todas las veces que considere necesario, los correos electrónicos, archivos y comportamiento de Internet en todos los dispositivos proporcionados por PTI, sin que ello constituya alguna invasión a la privacidad de su personal, ya que los dispositivos son herramientas de trabajo propiedad de PTI y se proporciona a su personal con la única finalidad de que cumpla con su trabajo. El personal de PTI no tendrá expectativa de privacidad alguna con respecto a los dispositivos de PTI o la información almacenada en ellos.

Protección de Información Personal y Políticas de Seguridad de la Información

Política de Seguridad de la Información

Phoenix Tower está comprometido a dar un correcto uso y tratamiento de los DP de los Titulares, evitando el acceso no autorizado de terceros que permita conocer o vulnerar, modificar, divulgar y/o destruir la información que se encuentra en las bases de datos de PTI. Por tal motivo, Phoenix Tower cuenta con protocolos de seguridad y acceso a sus sistemas de información, almacenamiento y procesamiento incluidas medidas físicas, administrativas y técnicas de control de riesgos de seguridad, las cuales se establecen en la Política de Seguridad de la Información de PTI.

El acceso a las diferentes bases de datos se encuentra restringido incluso para los empleados y colaboradores. Todos los funcionarios se encuentran comprometidos con la confidencialidad y manipulación adecuada de las bases de datos en términos de la Ley.

Las medidas de seguridad de la información serán al menos equivalentes a las medidas de seguridad de la información implementadas para proteger la información de la empresa.

Auditorías de DP

PTI realizará auditorías de información de DP mantenidas por la compañía de vez en cuando para asegurar: (i) que esta Política se mantenga vigente; (ii) para determinar la necesidad de la retención continua de la

información; y (ii) evaluar las medidas de seguridad de los DP. Cuando la necesidad ya no exista, la información de DP será destruida de acuerdo con los protocolos para la destrucción de tales bitácoras y registros mantenidos para las fechas de destrucción. Las auditorías deberán ser conducidas por cada jefe de departamento y los GCs.

Vulneraciones de Seguridad

Una vulneración de datos personales se refiere a su: (i) pérdida o destrucción no autorizada; (ii) robo o copia no autorizada; (iii) uso o acceso no autorizado; o (iv) daño o alteración o autorizada.

Las bases de datos o conjuntos de datos de PTI que incluyen DP pueden ser vulnerados inadvertidamente o por intrusión incorrecta. Cualquier incidente potencial o real debe ser reportado de acuerdo con la Respuesta de Incidentes y la Política de Reporte de Vulneración de Datos señaladas en la Política de Seguridad de la Información de PTI.

En cualquier caso, en el supuesto de vulneración de DP, el tercero, Encargado o empleado deberá informar al funcionario autorizado de PTI para que: (i) se informe, según sea el caso en términos de la Ley, a los Titulares de los DP vulnerados; y (ii) se tomen las acciones de mitigación correspondientes. Si se trata de un tercero o Encargado, la vulneración deberá ser informada al funcionario autorizado de PTI en un plazo de 5 días hábiles a partir del incidente; si se trata de un empleado, la vulneración deberá ser informada al funcionario autorizado de PTI dentro de las siguientes 24 horas posteriores incidente. Los terceros, Encargados y empleados realizarán dichos informes l departamento Legal, de Compliance o de RH.

En caso de informar a los Titulares de los DP, conforme a la Ley, se deberá notificar, cuando menos lo siguiente:

- La naturaleza del incidente;
- Los DP comprometidos;
- Las recomendaciones al Titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
- Las acciones correctivas realizadas de forma inmediata; y
- Los medios donde puede obtener más información al respecto.

Retención y Destrucción de DP de los Registros de PTI

Phoenix Tower entiende la importancia de minimizar la cantidad de DP, por esta razón, mantiene y conserva dicha información sólo durante el tiempo que sea necesario, de conformidad con la Ley. Todos los datos de PTI, incluyendo los datos y la información que contengan DP, se mantendrán de acuerdo con los procedimientos estándar de retención de registros de PTI, los cuales regulan la longitud de los métodos de retención de datos y destrucción de datos tanto para documentos impresos como electrónicos.

Misceláneos

Capacitación

Todos los nuevos empleados que ingresan a la compañía reciben capacitación introductoria con respecto al contenido de esta Política, una copia de ésta y los procedimientos de implementación para el departamento al que están asignados (si los hay). Los empleados en puestos con acceso continuo regular a las DP o aquellos transferidos a tales puestos reciben capacitación que refuerza esta política y procedimientos para el Tratamiento y mantenimiento de DP y recibirán capacitación sobre seguridad y protección de DP y datos de propiedad de la compañía de vez en cuando. La capacitación será dirigida por el departamento de TI y formará parte de la orientación del nuevo empleado en el caso de los nuevos empleados. Si se incluye un empleado a la lista de acceso de DP, el empleado recibirá un entrenamiento por separado del contenido de esta Política.

Confirmación de Confidencialidad

Todos los empleados de PTI deben mantener la confidencialidad de DP así como datos de propiedad de PTI a los que puedan tener acceso y entender que tal DP debe ser restringida a sólo aquellos con una necesidad de saber basada en el negocio o conforme a las finalidades descritas en los Avisos de Privacidad correspondientes. Los empleados con acceso continuo a tales datos firmarán recordatorios de reconocimiento anualmente que verifique su comprensión de este requisito de la compañía.

Requisitos Reglamentarios

PTI tiene como política obligatoria el cumplimiento con las leyes aplicables, incluyendo la Ley, así como con cualquier otra disposición y regulación internacional, federal o estatal con respecto al acceso, uso, tratamiento y almacenamiento de DP. El departamento Legal y/o Compliance de Phoenix Tower supervisarán todos los problemas de cumplimiento de informes. Si alguna disposición de esta política entra en conflicto con la Ley o con alguna disposición de una regulación internacional, federal o estatal que regule el Tratamiento de los DP, la sección(es) de la Política que incumpla será reemplazada.

Violación de Políticas y Procedimientos de DP

Phoenix Tower considera la protección de los DP como de la mayor importancia. Las infracciones de esta Política o de sus procedimientos resultarán en acciones disciplinarias, que pueden incluir suspensión o terminación en caso de violaciones graves o repetidas.