Politica

Protección de Datos Personales

El Objetivo de la presente Política es proteger datos personales tratados por el Grupo Tawa en Perú, preservando la confidencialidad, disponibilidad e integridad de estos en cumplimiento al marco normativo dado por la Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento, aprobado mediante DS 003-2013-JUS (en adelante, la "Normativa de Protección de Datos Personales")

BASE LEGAL

Constitución Política del Perú

El artículo 2 de la Constitución Política del Perú contiene una lista enunciativa y no taxativa de los derechos fundamentales que tiene toda persona por su propia naturaleza. Así pues, dentro de aquella lista, el numeral 6 del mencionado artículo indica expresamente que "toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".

Ley de Protección de Datos Personales y su Reglamento

Con la promulgación de la Ley y el Reglamento, el Perú cuenta con un marco jurídico que busca garantizar el respeto al derecho fundamental a la protección de datos personales a través de un adecuado tratamiento. De esta manera, ambas normas no sólo buscan proteger los derechos de los titulares de aquellos datos, sino también se ocupan de las obligaciones de los referidos titulares de los bancos de datos personales, como es el caso de las empresas que conforman el Grupo Tawa en el Perú. En tal sentido, lo que se pretende conseguir es que la actuación de los titulares de los bancos de datos personales, en relación con el tratamiento de datos personales se ajuste al contenido del nuevo marco jurídico y a los principios rectores que a partir de ahora guían todo tratamiento de información personal.

DISPOSICIONES GENERALES

- La política de protección de datos personales se alinea con los objetivos de la empresa y da soporte a las exigencias legales y regulatorias.
- El Titular de datos personales podrá ejercer sus derechos ARCO frente a las empresas del Grupo Tawa en su condición de propietario de estos. Estos derechos se podrán ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Las empresas del Grupo Tawa en su condición de titulares de los bancos de datos personales deberán facilitar el ejercicio de los derechos ARCO al titular de la información contenida en dichos repositorios de datos.
- Todo colaborador de las empresas del Grupo Tawa que acceda al banco de datos personales deberá preservar la confidencialidad, disponibilidad e integridad de estos en cumplimiento de la Normativa de Protección de Datos Personales.
- El Oficial de Seguridad de la Información debe revisar y monitorear la implementación y ejecución de los controles y políticas de protección de datos personales.

Politica

Protección de Datos Personales

Las empresas del Grupo Tawa mantendrán actualizado los controles de seguridad para el banco de datos personales, basándose en un proceso de identificación y evaluación de riesgos de seguridad de la información.

Las empresas del Grupo Tawa mantendrán la información contenida en los bancos de datos personales bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

El Oficial de Seguridad de la Información deberá revisar y proponer la actualización de documentos normativos referidos a la Normativa de Protección de Datos Personales para su aprobación.

La presente política deberá formar parte del proceso de inducción de nuevos colaboradores, y en el caso de terceros debe ser anexado al contrato.

Las empresas del Grupo Tawa, así como todos sus colaboradores que efectúen tratamiento de datos personales, deberán facilitar el ejercicio de los derechos ARCO a los titulares de la información que generan, administren o usen información personal.

PRINCIPIOS RECTORES

Principio de Calidad:

Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

Principio de consentimiento:

Para el tratamiento de los datos personales debe mediar el consentimiento de su titular.

Principio de finalidad:

Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

Principio de disposición de recurso:

Todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuanto estos sean vulnerados por el tratamiento de sus datos personales.

Principio de legalidad:

El tratamiento de los datos personales se hace conforme a lo establecido en la Ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos.

Principio de nivel de protección adecuado:

Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección de datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por la Ley o por los estándares internacionales en la materia.

Principio de proporcionalidad:

Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

Principio de seguridad:

El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con los datos personales que se traten.

Principio de transparencia:

El titular del banco de datos y el encargado del tratamiento deben asegurar que la información sobre el tratamiento de datos personales sea clara, accesible y comprensible. Deben informar de manera precisa sobre la finalidad, plazos, transferencias y derechos de los titulares, empleando un lenguaje sencillo y formatos adecuados.

Principio de responsabilidad proactiva:

El titular del banco de datos y el encargado del tratamiento deben adoptar medidas preventivas y correctivas para garantizar el cumplimiento normativo, documentando y evaluando continuamente su efectividad. Deben demostrar su cumplimiento ante la ANPDP, implementando controles, auditorías y políticas que minimicen riesgos en el tratamiento de datos personales.

DISPOSICIONES ESPECÍFICAS

- Los usuarios que crean o usan bancos de datos que contengan información personal tienen la responsabilidad de garantizar la integridad, confidencialidad y disponibilidad de los bancos de datos personales que producen o utilizan en el marco de sus competencias.

- Cada Propietario del banco de datos personales, en coordinación con el Oficial de Datos Personales debe proponer, diseñar y coordinar la implementación de controles eficaces en sus procesos y actividades, manteniendo un equilibrio entre la productividad y la protección de datos personales.

- Las empresas del Grupo Tawa deben realizar campañas de sensibilización de manera anual a los colaboradores en temas, métodos y herramientas de protección de datos personales. Asimismo, en caso de terceros, sean estos personas naturales o jurídicas, y en caso de empresas con las que hayamos firmado convenios de colaboración se debe comunicar los lineamientos de protección de datos personales de la empresa.

Politica

Protección de Datos Personales

- Todo contrato, convenio de personal o compañía de servicios involucrada en los procesos de las empresas del Grupo Tawa, debe contar con una cláusula que exprese el acuerdo en el cumplimiento de la confidencialidad de la información, según el nivel de sensibilidad de la información que administrará el contrato. Estas cláusulas deben señalar las sanciones en caso de incumplimiento.

- En caso de incumplimientos relacionados a protección de datos personales, se sancionará a los responsables teniendo como referencia el Reglamento Interno de Trabajo de cada una de las empresas pertenecientes al Grupo Tawa, contratos y convenios firmados. Los incumplimientos serán reportados al Oficial de Datos Personales y las Gerencias respectivas, en caso del personal con copia a la Unidad de Gestión Humana y en caso de terceros a la Gerencia Legal para la aplicación de las sanciones correspondientes.

- Los accesos a los bancos de datos personales; se realizará en base a perfiles de acceso elaborados en función a las responsabilidades asignadas.

- El Oficial de Datos Personales como responsable de la seguridad del banco de datos personales, coordinará en la empresa la implementación la Normativa de Protección de Datos Personales, además de las disposiciones relativas a la materia.

- La Gerencia General en su calidad de responsable ante el órgano judicial por el tratamiento de los datos personales contenidos en las diferentes bases de datos declaradas; nombrará en sesión de Directorio a los encargados del tratamiento interno de las mismas cuyas responsabilidades son:

    - Velar por el cumplimiento de los parámetros de seguridad lógica y de identificación en los accesos a los sistemas de almacenamiento de los bancos de datos.
    - Llevar y resguardar en los medios de soporte correspondiente el registro de altas y bajas de usuarios con acceso a los bancos de datos y los niveles de acceso brindados.
    - Supervisar la correcta asignación de permisos y accesos a los bancos de datos según el perfil correspondiente al nivel del usuario.
    - Supervisar y auditar los niveles de seguridad de los bancos de datos de la compañía.

- Toda recuperación de datos personales, desde su copia de respaldo, debe contar con la autorización expresa del encargado del banco de datos personales o del responsable de su tratamiento a través del SI-FOR-01Solicitud de copia de banco de datos personales.

- Las empresas del Grupo Tawa en su labor de prevención y en cumplimiento de lo dispuesto por la Ley han tomado las siguientes medidas preventivas:

    - Determinar una estructura organizacional con roles y funciones determinados con el objeto de resguardar el correcto tratamiento de los datos personales contenidos en sus diversos bancos de datos.
    - Mantener con sus trabajadores acuerdos de confidencialidad referidos a los datos personales que pudiesen tomar conocimiento como parte de sus funciones.
    - Implementar el acceso a los bancos de datos personales mediante el uso de usuarios y contraseñas personalizados, únicos e intransferibles.
    - Elaborar perfiles determinados para acceso a los bancos de datos según las funciones de cada trabajador y resguardando el acceso a la información estrictamente necesaria para el cumplimiento de sus funciones.
    - Registrar la actividad desarrollada por cada uno de los usuarios de los bancos de datos.

- Establecer los medios necesarios para comunicar a los titulares de datos personales el tratamiento que se dará a sus datos y obtener el consentimiento para el mencionado tratamiento.
- Establecer y hacer público el procedimiento para el ejercicio de los derechos de los titulares de datos personales. Supervisar la correcta asignación de permisos y accesos a los bancos de datos según el perfil correspondiente al nivel del usuario.
- Implementar canales de atención para la solución de controversias, reclamos y solicitudes de los titulares de datos personales contenidos en los diversos bancos de datos.

Condiciones para el Tratamiento de Datos Personales

Autorización del titular

Para que las empresas del Grupo Tawa realicen cualquier acción de tratamiento de datos personales, se requiere la previa autorización expresa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al titular su manifestación automatizada o pueden ser por escrito o de forma oral. En el caso de datos sensibles, el consentimiento para efectos de su tratamiento deberá efectuarse por escrito. El consentimiento deberá cumplir con las siguientes características:

- Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos personales.

- Previo: Con anterioridad al tratamiento de los datos personales.

- Expreso e Inequívoco: Cuando el consentimiento haya sido manifestado en condiciones que no admitan dudas de su otorgamiento. Tratándose del entorno digital, también se considera expresa la manifestación consistente en “hacer clic”, “cliquear” o “pinchar”, “dar un toque”, “touch” o “pad” u otros similares. En este contexto el consentimiento escrito podrá otorgarse mediante firma electrónica, mediante escritura que quede grabada, de forma tal que pueda ser leída e impresa, o que por cualquier otro mecanismo o procedimiento establecido permita identificar al titular y recabar su consentimiento, a través de texto escrito. También podrá otorgarse mediante texto preestablecido, fácilmente visible, legible y en lenguaje sencillo, que el titular pueda hacer suyo mediante una respuesta escrita, gráfica o mediante clic o pinchado, o mediante manifestación verbal la cual podrá constar en grabaciones.

- Informado: Al titular de los datos personales se le debe comunicar de manera clara, expresa e indubitablemente, con lenguaje sencillo, cuando menos lo siguiente:

  a. La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento y/o ejercer sus derechos.
  b. La finalidad o finalidades del tratamiento a las que sus datos serán sometidos.
  c. La identidad de los que son o pueden ser sus destinatarios, de ser el caso.
  d. La existencia del banco de datos personales en que se almacenarán.
  e. El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso.
  f. Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.
  g. En su caso, la transferencia nacional e internacional de datos que se efectúen.
  h. El tiempo durante el cual se conservarán sus datos personales.
  i. La posibilidad de ejercer los derechos que la Ley le concede y los medios previstos para ello.

En consecuencia, las empresas del Grupo Tawa adoptarán los procedimientos necesarios a fin de que la autorización del Titular para el tratamiento de los mismos cumpla con las características antes señaladas. .

Ubicación de los Bancos de Datos y Traslado Transfronterizo

Las empresas del Grupo Tawa señalan que todos sus bancos de datos se encuentran alojados en un servicio de almacenamiento en la nube en cuyo contrato se especifican las normas de seguridad que adopta dicho servicio para resguardar la confidencialidad, integridad y disponibilidad de la información sensible contenida. Asimismo, dicho servicio facilita la aplicación de los derechos ARCO de los propietarios de la información personal contenida.

Como parte de sus políticas, las empresas del Grupo Tawa transfieren a título gratuito y previo consentimiento, determinados datos personales, principalmente los contenidos en sus bancos de datos de candidatos a empleos, a su filial ubicada en Chile y a sus empresas clientes ubicadas en el extranjero. En los países donde se transfieren datos personales, las empresas destinatarias de dicha información deberán garantizar niveles de protección de datos personales adecuados conforme a lo establecido en la Ley y Reglamento.

Procedimiento para el Registro, Consulta, Modificación y Supresión de Datos Personales en los Bancos de Datos del Grupo Tawa

Del registro:

Al registrar los datos del titular, las empresas del Grupo Tawa solicitarán al titular la autorización y deberán informarle de manera clara y expresa lo siguiente:

- El tratamiento al cual serán sometidos sus datos personales y la finalidad de este.
- El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre datos de menores de edad.
- Los derechos que le asisten como titular.
- La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos.
- La identidad de los que son o pueden ser sus destinatarios, de ser el caso.
- La existencia del banco de datos personales en que se almacenarán.
- Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.
- En su caso, la transferencia nacional e internacional de datos que se efectúen.
- El tiempo durante el cual se conservarán sus datos personales.

De la(s) consulta(s) y/o solicitud(es) del titular (actualización, rectificación, inclusión y supresión de datos personales):

- Los titulares de datos personales tienen derecho a la actualización, inclusión, rectificación y supresión de sus datos personales materia de tratamiento cuando estos sean parcial o totalmente inexactos, incompletos, o cuando se hubiere advertido omisión o falsedad de los mismos, o cuando ya no sean necesarios o pertinentes para la finalidad que fueron recopilados.

- El titular de datos personales que considere que la información contenida en un banco de datos debe ser objeto de corrección, actualización o supresión, o cuando advierta el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley, podrá presentar a la empresa del Grupo Tawa que corresponda, una solicitud de corrección, actualización o supresión de datos personales, la cual debe contar con la siguiente información:
- Nombre del solicitante.
- Copia del DNI.
- Solicitud o requerimiento referente a sus datos personales, de manera clara y explícita (debe de especificarse qué datos se desea rectificar, incluir o actualizar).
- Fecha y firma.
- Domicilio o dirección (puede ser electrónica) de notificación.
- Las solicitudes realizadas por el titular o su representante serán atendidas por la empresa del Grupo Tawa que corresponda y las respuestas a estas se trasladarán por el mismo medio que fue formulada la solicitud.
- El titular puede realizar solicitudes por los siguientes medios:
- Mediante documento físico entregado en las oficinas de cada empresa del Grupo Tawa según corresponda.
- Mediante correo electrónico a la siguiente dirección electrónica: cumplimiento@grupotawa.com

De la revocatoria de autorización para el tratamiento de datos y supresión de datos personales

La revocatoria (total o parcial) de autorización para el tratamiento de datos personales podrá solicitarse en cualquier momento, sin justificación previa y sin que le atribuyan efectos retroactivos. En caso de que la revocatoria afecte la totalidad del tratamiento, la empresa del Grupo Tawa que corresponda gestionará la supresión de los datos personales correspondientes al solicitante.

La solicitud de revocatoria se realizará mediante los siguientes canales de atención:

- Mediante documento físico entregado en las oficinas de cada empresa del Grupo Tawa, según corresponda.
- Mediante correo electrónico a la dirección: cumplimiento@grupotawa.com

La solicitud deberá contener de forma clara y legible los siguientes datos:

- Nombre completo.
- Copia del DNI.
- Datos que solicita se supriman del banco de datos de la empresa del Grupo Tawa, según corresponda.
- Fecha y firma.
- Domicilio o dirección (puede ser electrónica) de notificación.

La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando los datos que el titular requiere suprimir sean necesarios para el cumplimiento de los servicios ofertados y contratados con las empresas del Grupo Tawa, a menos de que el contrato entre las partes no se encuentre vigente.

Plazos de atención a consultas y solicitudes del titular

Las solicitudes y consultas del titular serán absueltas en el término de plazos razonables y según lo estipulado en la Ley.

- Consultas referentes al derecho de la información: ocho (08) días hábiles, contados desde el día siguiente a la presentación de la solicitud.
- Solicitudes referentes al derecho de acceso: veinte (20) días hábiles, contados desde el día siguiente a la presentación de la solicitud.
- Rectificación, Cancelación, u oposición de datos: diez (10) días hábiles, contados desde el día siguiente a la presentación de la solicitud.

De la recepción, subsanación o requerimiento de información adicional para la atención de solicitudes

De la recepción de solicitudes:

Las empresas del Grupo Tawa implementarán los medios para la recepción de todas las solicitudes de los titulares de dato y contará con los medios necesarios para dejar constancia de la recepción de documentos y la fecha correspondiente a la misma.

De la subsanación de solicitudes:

En caso las solicitudes no cuenten con los datos señalados en el punto 14.2 del presente documento y/o los señalados en el artículo 50 del Reglamento, la empresa del Grupo Tawa que corresponda deberá notificar la omisión al solicitante en un plazo máximo de cinco (05) días contados desde el día siguiente a la recepción de la solicitud. El titular deberá subsanar las omisiones en el plazo de cinco (05) días después de recibida la notificación, en caso no lo hiciera se tendrá por no presentada la solicitud.

Del requerimiento por ampliación de información:

En el caso que la información proporcionada en la solicitud sea insuficiente o errónea de forma que no permita su atención, las empresas del Grupo Tawa podrán requerir dentro de los siete (7) días siguientes de recibida la solicitud, documentación adicional al titular de los datos para atenderla.

En un plazo de diez (10) días de recibido el requerimiento, contado desde el día siguiente de la recepción del mismo, el titular de datos personales acompañará la documentación adicional que estime pertinente para fundamentar su solicitud. En caso contrario, se tendrá por no presentada dicha solicitud.

De la Gestión de Incidentes de Seguridad de Datos Personales

Del Registro

Todo incidente de seguridad de datos personales deberá ser reportado de inmediato al Oficial de Datos Personales (ODP) o al área de Seguridad de la Información.

La empresa del Grupo Tawa que corresponda deberá registrar el incidente en el Registro de Incidentes de Seguridad de Datos Personales, consignando:

- Fecha y hora del incidente.
- Tipo de incidente (acceso no autorizado, pérdida de datos, alteración, divulgación indebida, etc.).
- Datos personales comprometidos.
- Medidas preliminares adoptadas.

La empresa del Grupo Tawa que corresponda clasificará el incidente de acuerdo con su impacto y alcance:

- Incidente menor: No compromete datos sensibles ni un volumen significativo de información.
- Incidente grave: Involucra datos sensibles o un número importante de titulares.
- Incidente crítico: Puede generar un alto impacto en los derechos de los titulares o en la seguridad de los sistemas.

De la Evaluación y Mitigación del Incidente

- La empresa del Grupo Tawa que corresponda realizará un análisis del incidente para determinar su origen, impacto y posibles riesgos adicionales.

- Se implementarán medidas inmediatas de contención y mitigación, tales como:
  - Bloqueo de accesos no autorizados.
  - Restauración de datos.
  - Refuerzo de controles de seguridad.
  - Implementación de acciones correctivas para prevenir la recurrencia del incidente.

Notificación a la ANPDP y a los Titulares Afectados

- Si el incidente afecta datos sensibles, involucra un gran volumen de información o compromete derechos fundamentales, la empresa del Grupo Tawa que corresponda notificará a la Autoridad Nacional de Protección de Datos Personales (ANPDP) dentro de las 48 horas posteriores a su detección, conforme al artículo 34 del Reglamento.

- Si el incidente involucra datos personales tratados en entornos digitales, se notificará también al Centro Nacional de Seguridad Digital.

- La empresa del Grupo Tawa que corresponda informará a los titulares de los datos afectados, indicándoles:

  - Naturaleza del incidente y datos comprometidos.
  - Posibles consecuencias.
  - Medidas adoptadas para mitigar riesgos.
  - Recomendaciones para proteger su información.

Plazos de Atención y Registro

- Toda acción tomada en respuesta al incidente deberá documentarse en el Registro de Incidentes de Seguridad.

- Las medidas correctivas deberán implementarse en un plazo máximo de 10 días hábiles desde la detección del incidente.

- La información del incidente deberá conservarse por un período mínimo de 2 años.

Canales de Recepción de Reportes de Incidentes

Los colaboradores y terceros podrán reportar incidentes de seguridad de datos personales a través de los siguientes medios:

- Correo electrónico: cumplimiento@grupotawa.com
- Documento físico entregado en las oficinas de la empresa del Grupo Tawa correspondiente.

Revisión y Actualización del Procedimiento

Este procedimiento será revisado anualmente y actualizado conforme a cambios normativos o nuevos riesgos en seguridad de datos personales.

Bancos de Datos Declarados

Las empresas que conforman el Grupo Tawa en el Perú cuentan con los siguientes Bancos de Datos Personales debidamente registrados ante la Dirección de Protección de Datos Personales del MINJUS:

Empresa	Código de registro	Nombre	Finalidad
TAWA CONSULTING S.A.C	4717	PROVEEDORES	Administrar la información de proveedores para la adquisición de bienes o servicios, así como contar con una lista de proveedores con los que contrata la empresa.
TAWA CONSULTING S.A.C	4718	RECURSOS HUMANOS	Administrar la información de los trabajadores y practicantes para fines de compensación, bienestar social, salud y control interno del recurso humano.

Politica

Protección de Datos Personales

GrupoTawa

Empresa	Código de registro	Nombre	Finalidad
TAWA CONSULTING S.A.C	4719	MATRIZ DE CANDIDATOS A EMPLEOS	Recopilar datos personales de los postulantes para realizar la selección y evaluación del personal
TAWA CONSULTING S.A.C	16480	VIDEOVIGILANCIA	Recopilar los datos personales para brindar seguridad interna y externa.
TAWA PERU S.A.C.	5243	RECURSOS HUMANOS	Administrar la información de los trabajadores y practicantes para fines de compensación, bienestar social, salud y control interno del recurso humano.
ROM OUTSOURCING S.A.C	4715	CLIENTES	Venta de productos a personas naturales o empresas unipersonales.
ROM OUTSOURCING S.A.C	4716	RECURSOS HUMANOS	Administrar la información de los trabajadores y practicantes para fines de compensación, bienestar social, salud y control interno del recurso humano.
LIMTEK SERVICIOS INTEGRALES S.A.	13728	POSTULANTES Y CANDIDATOS	Recopilar los datos personales de los postulantes y candidatos a puestos laborales para realizar evaluaciones, elaborar perfiles y determinar la idoneidad para el puesto.

Politica

Protección de Datos Personales

GrupoTawa

Empresa	Código de registro	Nombre	Finalidad
LIMTEK SERVICIOS INTEGRALES S.A.	13729	RECURSOS HUMANOS	Administrar la información de los trabajadores y practicantes para fines de compensación, bienestar social, salud y control interno del recurso humano.
LIMTEK SERVICIOS INTEGRALES S.A.	13730	ACCIDENTES DE TRABAJO	Recopilar los datos personales de los empleados y terceros que sufran accidentes e incidentes en las instalaciones de la empresa a fin de realizar las investigaciones respectivas, fortalecer la seguridad y remitir información al Ministerio de Trabajo cuando corresponda en cumplimiento del mandato legal.
LIMTEK SERVICIOS INTEGRALES S.A.	13731	EXAMEN OCUPACIONAL Y NO OCUPACIONAL	Recopilar los datos personales para realizar exámenes médicos, determinar las enfermedades de los trabajadores en cumplimiento a la normativa vigente.
LIMTEK SERVICIOS INTEGRALES S.A.	13732	CLIENTES	Recopilar los datos personales de los clientes para realizar transacción de compras, análisis de riesgos crediticios, financieros, comerciales, publicidad y prospección comercial.

Politica

Protección de Datos Personales

GrupoTawa

Empresa	Código de registro	Nombre	Finalidad
LIMTEK SERVICIOS INTEGRALES S.A.	13733	REGISTRO DE VISITAS	Recopilar los datos personales de los visitantes así como del personal visitado a fin de controlar la entrada y salida por medidas de seguridad.
LIMTEK SERVICIOS INTEGRALES S.A.	13734	VIDEOVIGILANCIA	Recopilar los datos personales para prevenir riesgos, registrar incidencias y accidentes por medidas de seguridad.
LIMTEK SERVICIOS INTEGRALES S.A.	13964	PROVEEDORES	Recopilar los datos personales de los proveedores para cumplir con las relaciones y negociaciones contractuales y profesionales, realizar análisis de riesgos crediticios, financieros y comerciales.