MANUAL INTERNO DE PROTECCIÓN DE DATOS PERSONALES

ZOHU ZONAS HUMEDAS S.A.S. ha desarrollado este manual interno en respuesta a la exigencia de la Ley 1581 de 2012, la cual establece las disposiciones generales para la protección de datos personales. Específicamente, se busca cumplir con el deber, señalado en el artículo 17, de adoptar políticas y procedimientos internos para asegurar el adecuado cumplimiento de la ley y la atención de consultas y reclamos de los titulares de los datos.

En su rol de responsable del tratamiento de datos personales (definido por la ley como la entidad que decide sobre las bases de datos y su uso), **ZOHU ZONAS HUMEDAS S.A.S.** reconoce la relevancia de la gestión eficiente de la información personal para sus operaciones y el cumplimiento de sus objetivos corporativos, abarcando áreas como la gestión de personal y la atención a diversos grupos de interés.

El manual se fundamenta en el derecho fundamental al habeas data, que busca garantizar a los ciudadanos el control sobre su información personal, incluyendo su uso y destino. En este sentido, el derecho a la protección de datos personales otorga a los titulares diversas facultades para controlar su información. El presente documento tiene como objetivo implementar las garantías e instrumentos que la Ley 1581 de 2012 desarrolla para asegurar la vigencia de este derecho, estableciendo los procedimientos de recolección y tratamiento de datos personales que **ZOHU ZONAS HUMEDAS S.A.S.** aplicará en cumplimiento de la ley.

OBJETIVOS

Establecer lineamientos claros para el tratamiento de datos personales en todas las actividades de la Organización, definir roles y responsabilidades en materia de protección de datos**, i**mplementar procedimientos efectivos para garantizar los derechos de los titulares, minimizar los riesgos asociados al tratamiento inadecuado de información personal, asegurar el cumplimiento de la normativa vigente en materia de protección de datos y **f**omentar una cultura organizacional de respeto a la privacidad y protección de datos.

ALCANCE

Este manual es de obligatorio cumplimiento para:

- Todos los colaboradores de la Organización, independientemente de su tipo de contratación o nivel jerárquico.
- Terceros que realicen tratamiento de datos personales a nombre de la Organización (encargados del tratamiento).
- Todas las bases de datos y archivos que contengan información personal, independientemente de su formato (físico o digital).
- Todos los procesos organizacionales donde se recolecten almacenen, usen o circulen datos personales.

DEFINICIONES

1. Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
2. Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
3. Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento.
4. Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.
5. Titular: Persona natural cuyos datos personales sean objeto de tratamiento.
6. Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

MARCO NORMATIVO

El presente manual se fundamenta en la Constitución Política, artículo 15, que consagra el derecho a la intimidad personal y familiar y al buen nombre, Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales y el Decreto 1377 de 2013, que reglamenta parcialmente la Ley 1581 de 2012.

PRINCIPIOS RECTORES.

Todo tratamiento de datos personales debe regirse por los siguientes principios:
1. Principio de legalidad: El tratamiento de datos personales es una actividad reglada que debe sujetarse a lo establecido en la ley y en las demás disposiciones que la desarrollen.
2. Principio de finalidad: El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley.
3. Principio de libertad: El tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular.
4. Principio de veracidad o calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
5. Principio de transparencia: En el tratamiento debe garantizarse el derecho del titular a obtener información sobre sus datos.
6. Principio de acceso y circulación restringida: El tratamiento se sujeta a los límites derivados de la naturaleza de los datos personales y de la ley.
7. Principio de seguridad: La información sujeta a tratamiento debe manejarse con las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros.
8. Principio de confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales están obligadas a garantizar la reserva de la información.

CATEGORÍAS DE DATOS

1. Datos Públicos. Son aquellos datos que no son de naturaleza semiprivada, privada o sensible, como los datos relativos al estado civil de las personas, su profesión u oficio y su calidad de comerciante o de servidor público.
2. Datos Semiprivados. Son aquellos que no tienen naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas, como los datos financieros y crediticios.
3. Datos Privados. Son aquellos que por su naturaleza íntima o reservada sólo son relevantes para el titular, como correos electrónicos personales, números telefónicos personales, fotografías, videos personales.
4. Datos Sensibles. Son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, como:

- Origen racial o étnico
- Orientación política
- Convicciones religiosas o filosóficas
- Pertenencia a sindicatos
- Datos relativos a la salud
- Datos biométricos
- Datos relativos a la vida sexual
- Datos de menores de edad

DERECHOS DE LOS TITULARES

Los titulares de los datos personales tienen los siguientes derechos:
1. Derecho de acceso. El titular podrá acceder de forma gratuita a sus datos personales que sean objeto de tratamiento.
2. Derecho de actualización. El titular podrá solicitar en cualquier momento la actualización de sus datos personales.
3. Derecho de rectificación. El titular podrá solicitar la corrección de sus datos personales cuando sean inexactos, incompletos o desactualizados.
4. Derecho de supresión. El titular podrá solicitar la eliminación de sus datos personales cuando:

- No exista una obligación legal o contractual que requiera conservarlos.
- Hayan dejado de ser necesarios para la finalidad para la cual fueron recolectados.
- Se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recabados.

5. Derecho de revocatoria del consentimiento. El titular podrá revocar la autorización otorgada para el tratamiento de sus datos personales, siempre que no exista un deber legal o contractual que lo impida.
6. Derecho a presentar reclamos. El titular podrá presentar reclamos ante el Responsable o el Encargado del Tratamiento cuando considere que existe un incumplimiento de la normativa de protección de datos.
7. Derecho a presentar quejas. El titular podrá presentar quejas ante la Superintendencia de Industria y Comercio por infracciones a la normativa de protección de datos personales.

8. Derecho a la portabilidad. El titular podrá solicitar la portabilidad de sus datos a otro responsable del tratamiento cuando técnicamente sea posible.

DEBERES DEL RESPONSABLE DEL TRATAMIENTO

1. Garantizar al titular el ejercicio del derecho de hábeas data.
2. Solicitar y conservar copia de la autorización otorgada por el titular.
3. Informar al titular sobre la finalidad de la recolección y los derechos que le asisten.
4. Conservar la información bajo las condiciones de seguridad necesarias.
5. Actualizar la información, rectificar cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
6. Suministrar al Encargado del Tratamiento únicamente datos cuyo tratamiento esté previamente autorizado.
7. Exigir al Encargado del Tratamiento el respeto a las condiciones de seguridad y privacidad de la información del titular.
8. Tramitar las consultas y reclamos formulados en los términos señalados en la ley.
9. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad.
10. Cumplir las instrucciones y requerimientos de la Superintendencia de Industria y Comercio.

POLÍTICAS DE TRATAMIENTO DE DATOS

1. Autorización del Titular. Toda recolección de datos personales requiere de autorización previa, expresa e informada del titular, salvo en los casos exceptuados por la ley.

2. Formas de obtener la autorización

- Por escrito
- De forma oral
- Mediante conductas inequívocas que permitan concluir de forma razonable que el titular otorgó la autorización
- Electrónicamente mediante clic o marcar casillas verificables

2. Contenido mínimo de la autorización

- Identificación del Responsable del Tratamiento
- Finalidades del tratamiento
- Derechos que le asisten al titular
- Mecanismos para conocer la política de tratamiento
- Identificación de los datos sensibles (si aplica) y consecuencias de no suministrarlos

3.Casos en que no es necesaria la autorización

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales
- Datos de naturaleza pública
- Casos de urgencia médica o sanitaria
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos
- Datos relacionados con el Registro Civil de las Personas

4. Tratamiento de datos sensibles. Se prohíbe el tratamiento de datos sensibles, excepto cuando:

- El titular haya dado su autorización explícita
- Sea necesario para salvaguardar el interés vital del titular
- Se realice en el curso de actividades legítimas por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro
- Se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial
- Tenga una finalidad histórica, estadística o científica, siempre que se adopten medidas técnicas para mantener la seguridad y confidencialidad

5. Tratamiento de datos de menores. El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando:

- Se trate de datos de naturaleza pública
- El tratamiento responda y respete el interés superior del menor
- Se asegure el respeto de sus derechos fundamentales
- Se cuente con la autorización del representante legal del menor

6. Finalidades del tratamiento. Los datos personales serán tratados para las siguientes finalidades generales:

- **Clientes**
- Gestión de la relación contractual
- Prestación de servicios
- Envío de información comercial
- Evaluación de la calidad de los servicios
- Análisis de perfiles para ofrecer productos o servicios
- Gestión contable, fiscal y administrativa
- **Empleados**
- Gestión de la relación laboral
- Pago de nómina y prestaciones sociales
- Formación y capacitación
- Gestión de permisos y licencias
- Control de acceso y seguridad
- Evaluación del desempeño
- Bienestar laboral
- Prevención de riesgos laborales
- **Proveedores**
    - Gestión de la relación contractual
    - Pagos y facturación
    - Evaluación de servicios
    - Análisis de propuestas comerciales
    - Gestión contable, fiscal y administrativa

PERIODO DE CONSERVACIÓN

Los datos personales serán conservados durante el tiempo que sea necesario para cumplir con la finalidad para la cual fueron recolectados y para atender las obligaciones legales, contractuales, comerciales y de servicio.

ACTUALIZACIÓN DE LA INFORMACIÓN

Se implementarán procedimientos para mantener actualizada la información personal, incluyendo:

- Campañas periódicas de actualización
- Verificación anual de la exactitud de los datos
- Procesos para la depuración de datos obsoletos

PROCEDIMIENTOS PARA LA ATENCIÓN DE CONSULTAS Y RECLAMOS

1. Consultas. Procedimiento para atender las consultas que realicen los titulares:

1. **Recepción**: La consulta podrá ser formulada por el titular o sus causahabientes mediante los canales establecidos por la Organización.
2. **Verificación de identidad**: Se verificará la identidad del titular o de su representante.
3. **Respuesta**: La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma.
4. **Prórroga**: Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

2. Reclamos. Procedimiento para atender los reclamos relacionados con corrección, actualización, supresión o revocatoria de la autorización:

1. **Recepción**: El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del titular, la descripción de los hechos, la dirección, y acompañando los documentos que se quiera hacer valer.
2. **Reclamo incompleto**: Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.
3. **Traslado a competente**: En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.
4. **Decisión**: Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles.
5. **Respuesta**: El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo.
6. **Prórroga**: Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

3. Canales de atención. Para ejercer sus derechos, el titular puede utilizar los siguientes canales de comunicación:

- **Correo electrónico**: zonashumedasadm@gmail.com
- **Dirección física**: Trans. 39b #39 - 183, Medellín, Antioquia.

- **Teléfono**: 304 3107494 - 301 6195211
- **Página web**: https://zonashumedas.com/

MEDIDAS DE SEGURIDAD

1. Medidas técnicas

- Implementación de controles de acceso a los sistemas de información
- Cifrado de datos sensibles
- Copias de seguridad periódicas
- Actualización de software y sistemas operativos
- Protección contra malware
- Registros de eventos (logs) de seguridad
- Controles de red (firewalls, IDS/IPS)
- Segmentación de redes

2. Medidas organizativas

- Política de escritorio limpio y pantalla bloqueada
- Acuerdos de confidencialidad
- Clasificación de la información
- Gestión de incidentes de seguridad
- Procedimientos de destrucción segura de información
- Auditorías periódicas
- Gestión de accesos privilegiados

3. Notificación de incidentes

En caso de brecha de seguridad que afecte datos personales, se deberá:

- Documentar el incidente
- Notificar al Oficial de Protección de Datos
- Evaluar el impacto y alcance del incidente
- Notificar a la Superintendencia de Industria y Comercio en un término no mayor a 72 horas
- Notificar a los titulares cuando exista un riesgo significativo para sus derechos y libertades
- Implementar acciones correctivas

TRANSFERENCIA DE DATOS

1.Transferencia nacional. La transferencia de datos personales a otros responsables dentro del territorio nacional deberá cumplir con:

- Autorización previa del titular
- Existencia de relación contractual entre las partes
- Implementación de medidas de seguridad adecuadas

2. Transferencia internacional. La transferencia internacional de datos personales sólo podrá realizarse cuando:

- El titular haya otorgado su autorización expresa
- Se realice intercambio de datos de carácter médico
- Se trate de transferencias bancarias o bursátiles

- Se realice en el marco de tratados internacionales
- La transferencia sea necesaria para la ejecución de un contrato entre el titular y el responsable
- El país receptor ofrezca niveles adecuados de protección de datos

AUDITORÍA Y CONTROLES

1. Auditoría interna. Se realizarán auditorías internas de cumplimiento de las políticas de protección de datos al menos una vez al año, verificando:

- Cumplimiento de procedimientos
- Efectividad de medidas de seguridad
- Gestión de autorizaciones
- Procedimientos de atención de consultas y reclamos
- Formación del personal

2. Evaluación de impacto. Se realizará una evaluación de impacto en la protección de datos personales cuando:

- Se implementen nuevos sistemas o tecnologías
- Se modifiquen sustancialmente procesos existentes
- Se inicie un nuevo tratamiento de datos sensibles a gran escala
- Se realice perfilado o toma de decisiones automatizadas

3. Controles periódicos

- Verificación de cumplimiento de políticas y procedimientos
- Revisión de esquemas de clasificación de información
- Pruebas de vulnerabilidad técnica
- Verificación de cumplimiento de acuerdos de confidencialidad
- Monitoreo de accesos a sistemas de información

FORMACIÓN Y SENSIBILIZACIÓN

1. Inducción. Todo nuevo empleado recibirá capacitación sobre protección de datos personales como parte de su proceso de inducción.

2. Capacitación periódica. Se realizarán capacitaciones al menos una vez al año para todo el personal sobre:

- Normativa vigente
- Políticas y procedimientos internos
- Buenas prácticas de seguridad
- Gestión de incidentes

3. Comunicación y sensibilización. Se implementarán estrategias de comunicación interna para mantener la conciencia sobre la importancia de la protección de datos:

- Boletines informativos
- Charlas cortas
- Material visual (afiches, protectores de pantalla)
- Campañas temáticas

RESPONSABILIDADES

1. Alta Dirección

- Aprobar la política de protección de datos
- Asignar recursos necesarios
- Designar al Oficial de Protección de Datos
- Revisar periódicamente el sistema de gestión de protección de datos

2. Oficial de Protección de Datos

- Velar por la implementación efectiva de las políticas
- Ser el enlace con la autoridad de protección de datos
- Gestionar el registro de actividades de tratamiento
- Coordinar la atención de consultas y reclamos
- Promover la cultura de protección de datos
- Monitorear el cumplimiento normativo

3. Área de Tecnología

- Implementar medidas técnicas de seguridad
- Garantizar la seguridad en los sistemas de información
- Apoyar en la evaluación de impacto
- Gestionar incidentes de seguridad técnica

4. Área Jurídica

- Asesorar en aspectos legales de protección de datos
- Revisar contratos y acuerdos con terceros
- Actualizar políticas conforme a cambios normativos

5. Área de Recursos Humanos

- Gestionar datos de empleados
- Coordinar capacitaciones
- Incluir cláusulas de confidencialidad en contratos laborales

6. Todos los empleados

- Cumplir las políticas y procedimientos de protección de datos
- Reportar incidentes de seguridad
- Mantener la confidencialidad de la información
- Participar en las capacitaciones

INFRACCIONES Y SANCIONES

1. Infracciones disciplinarias internas. El incumplimiento de las políticas y procedimientos establecidos en este manual podrá dar lugar a:

- Llamados de atención verbal
- Llamados de atención escrita
- Suspensión temporal
- Terminación del contrato
- Acciones legales según la gravedad de la infracción

2. Sanciones legales. Las infracciones a la normativa de protección de datos pueden conllevar sanciones por parte de la Superintendencia de Industria y Comercio, que incluyen:

- Multas hasta de 2.000 SMLMV
- Suspensión de actividades relacionadas con el tratamiento de datos

- Cierre temporal de operaciones
- Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles

VIGENCIA

El presente manual entra en vigor a partir de su fecha de publicación: 28 de abril de 2025 y hasta el momento en que expresamente se revoque o modifique.