POLÍTICA INTERNA DE PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES

Medina & Rivera Ingenieros Asociados S.A.S.

Fecha de entrada en vigencia: 16 /04 /2019
Revisión / actualización: 04/01/2025

1. OBJETIVO

Establecer los lineamientos, responsabilidades y procedimientos que rigen el tratamiento de datos personales dentro de *Medina & Rivera Ingenieros Asociados SAS*, incluyendo el uso de cámaras de vigilancia y correos electrónicos corporativos, con el fin de garantizar la legalidad, transparencia, seguridad y derechos de los titulares, de conformidad con la Ley 1581 de 2012 y normativa aplicable.

2. ALCANCE

Esta política aplica a todos los colaboradores (empleados, contratistas, pasantes), proveedores, visitantes y terceros que interactúen con los sistemas, instalaciones físicas y procesos de la empresa. Incluye todos los datos recolectados, almacenados, usados, transmitidos o eliminados en el marco de las actividades de la empresa.

3. DEFINICIONES CLAVE

Para efectos de esta política se adoptan las definiciones establecidas por la Ley 1581 de 2012:

- **Dato personal**: cualquier información vinculada o que pueda asociarse a una persona natural determinada o determinable.
- **Responsable del Tratamiento**: quien decide sobre los fines y medios del tratamiento de los datos.
- **Encargado del Tratamiento**: quien realiza el tratamiento por cuenta del responsable.
- **Titular**: la persona natural a quien se refieren los datos.
- **Tratamiento**: cualquier operación o conjunto de operaciones sobre datos personales, como recolección, almacenamiento, uso, circulación, supresión.
- **Datos sensibles**: aquellos que afectan la intimidad, como origen racial, convicciones religiosas, datos de salud, orientación sexual, datos biométricos, entre otros.

4. PRINCIPIOS QUE RIGEN EL TRATAMIENTO

El tratamiento de datos personales dentro de la empresa se sujetará a los siguientes principios:

Principio	Descripción aplicable
Legalidad	El tratamiento se debe ajustar a la ley y normativa colombiana.
Finalidad	Los datos solo serán tratados para propósitos explícitos, legítimos e informados (por ejemplo: seguridad, control interno, gestión laboral) y no para fines incompatibles.
Libertad / consentimiento	El tratamiento de datos requerirá autorización previa, expresa e informada del titular, salvo las excepciones legales.
Transparencia	El titular tiene derecho a conocer en qué consiste el tratamiento, los fines, destinatarios, derechos y mecanismos para ejercerlos.
Veracidad / calidad	Los datos deben ser exactos, completos, actualizados, coherentes con la realidad.
Acceso y circulación restringida	El tratamiento solo puede hacerse por personas autorizadas, y los datos no pueden circular libremente sin control.
Seguridad	Se deben adoptar medidas técnicas, humanas y administrativas para proteger los datos de acceso no autorizado, pérdida o alteración.
Confidencialidad	Las personas que intervengan en el tratamiento deben guardar reserva y no divulgar información no autorizada, incluso después de terminada su relación laboral.

5. TRATAMIENTO DE DATOS A TRAVÉS DE CÁMARAS DE VIGILANCIA

- Uso justificado: Las cámaras se instalan con el fin legítimo de seguridad física, protección de bienes, control de acceso y prevención de riesgos.
- Señalización: Se deberán colocar avisos visibles que informen a las personas que ingresan al área de que existe vigilancia por cámaras, con indicación de contacto para consultas.

- Áreas prohibidas: No se podrán instalar cámaras en sitios que comprometan la intimidad, como baños, vestuarios, áreas privadas de descanso.
- Acceso a grabaciones: Solo personal autorizado (Gerencia, Seguridad, Jefaturas) podrá acceder a las grabaciones, previa solicitud justificada.
- Conservación: Las imágenes serán conservadas solo durante el tiempo necesario (30 días), salvo requerimiento legal o judicial que justifique ampliación.
- Eliminación segura: Cumplido el periodo de conservación, las grabaciones deberán ser eliminadas o destruidas de manera segura, garantizando que no puedan recuperarse.
- Auditoría: Se llevarán registros de quién, cuándo y por qué ingresó a las grabaciones.

6. TRATAMIENTO DE CORREOS ELECTRÓNICOS CORPORATIVOS

- Uso exclusivo laboral: Los correos corporativos deben usarse para funciones asociadas al trabajo, no para asuntos personales, actividades ilícitas o que contravengan políticas internas.
- Monitoreo responsable: La empresa podrá revisar, auditar o acceder al contenido de los correos, en casos de ausencia del colaborador, auditorías internas, investigaciones disciplinarias o legales.
- Notificación previa: Los titulares serán informados con antelación del monitoreo o acceso al correo, salvo situaciones excepcionales debidamente justificadas.
- Respaldo y almacenamiento: en casos especiales se realizara copia de seguridad de los correos que se considere necesario, o para poder liberar espacio y mantener el buzón vigente o reasignarlo.
- Seguridad en el sistema: Uso de mecanismos técnicos de protección (cifrado, contraseñas robustas, autenticación multifactor) para prevenir accesos indebidos.

7. DATOS SENSIBLES Y TRATAMIENTOS EXCEPCIONALES

- En principio, el tratamiento de datos sensibles está prohibido, salvo que el titular otorgue autorización explícita, o que exista una normativa que lo permita.

- Si se requiere tratar datos sensibles (por ejemplo información médica relacionada con salud ocupacional), se debe informar claramente al titular las condiciones, finalidades, destinatarios y derechos especiales.
- Debe conservarse la mínima información necesaria y garantizar medidas de protección adicionales.

8. DERECHOS DE LOS TITULARES

Los titulares de los datos (colaboradores, contratistas, terceros) tienen los siguientes derechos, según Ley 1581 y normativa relacionada:

1. **Conocer, actualizar y rectificar** sus datos personales frente al responsable o encargado del tratamiento.
2. **Solicitar prueba de la autorización otorgada**, salvo en los casos en que la ley exceptúe esta exigencia.
3. **Ser informado** del uso que se le ha dado a sus datos cuando lo solicite.
4. **Revocar la autorización y / o solicitar la supresión de sus datos**, cuando no se respeten los principios, derechos y garantías previstas en la ley.
5. **Acceder gratuitamente** a los datos personales que hayan sido objeto de tratamiento.
6. **Interponer quejas o reclamaciones** ante la autoridad de control (Superintendencia de Industria y Comercio) por infracciones a la normativa.

9. DEBERES DE LA EMPRESA

Medina & Rivera deberá:

- Solicitar y conservar la **autorización previa, expresa e informada** de los titulares para el tratamiento de sus datos (cuando sea necesario).
- Informar claramente la finalidad del tratamiento al momento de la recolección de datos.
- Garantizar que los datos suministrados a encargados o terceros sean tratados conforme a esta política y normativa aplicable.
- Adoptar medidas de seguridad (físicas, técnicas, organizativas) para proteger los datos.

- Llevar registros de acceso, incidentes de seguridad y auditorías sobre el tratamiento de datos.
- Responder a las solicitudes de los titulares en los plazos establecidos por la ley y reglamentos.
- Notificar a la autoridad competente (SIC) y a los titulares afectados en caso de violaciones de seguridad que comprometan datos personales, en los plazos exigidos por la normativa.
- Evaluar y revisar periódicamente esta política, sus procedimientos y las medidas técnicas, para garantizar su eficacia y adecuación normativa.

10. PROCEDIMIENTOS OPERATIVOS

- **Consentimiento y autorización**: Formularios escritos o electrónicos claros donde el titular manifieste que ha sido informado sobre el tratamiento de sus datos, finalidades y derechos.
- **Registro de bases de datos**: Inscripción ante el Registro Nacional de Bases de Datos (RNBD) los datos que lo requieran, conforme al Decreto 1074 de 2015 y normativa vigente.
- **Gestión de solicitudes**: Establecer un procedimiento interno para recibir, estudiar y responder solicitudes de actualización, rectificación, supresión o revocatoria de autorización.
- **Planes de contingencia**: En caso de incidentes que comprometan datos (pérdida, robo, filtración), activar protocolo de respuesta, investigación interna y notificación a afectados y autoridad.
- **Capacitación interna**: Realizar programas de sensibilización y formación para todos los empleados sobre la protección de datos, obligaciones y buenas prácticas.
- **Evaluaciones de riesgo y auditoría**: Realizar evaluaciones periódicas de riesgos del tratamiento de datos personales, y auditorías internas o de terceros para verificar cumplimiento.

11. SANCIONES Y MEDIDAS DISCIPLINARIAS

El incumplimiento de esta política, de la normativa aplicable o de las instrucciones derivadas podrá conllevar medidas disciplinarias según el régimen interno de la

empresa, que pueden incluir amonestaciones, suspensión, terminación del contrato laboral, o sanciones administrativas según el caso.

12. COORDINACIÓN CON LA POLÍTICA INTEGRAL DE LA EMPRESA

Esta política de datos personales debe estar alineada con la política integral de gestión de calidad, medio ambiente, seguridad y salud en el trabajo que ya aparece en su página institucional para MEDINA Y RIVERA ING SAS, www.medinayrivera.com.co Las prácticas de datos personales deben integrarse al sistema de gestión integral, sin que se contradigan los objetivos de la organización.

13. VIGENCIA, REVISIÓN Y DIFUSIÓN

- La presente política entra en vigor en la fecha señalada al inicio.
- Se revisará al menos cada año o cuando cambie la normativa aplicable.
- Será difundida entre todos los colaboradores (mediante inducción, firma de acuse de recibo, publicación interna).
- Los cambios serán comunicados con antelación y de forma clara a todos los afectados.

14. CONTACTO PARA CONSULTAS, RECLAMOS Y EJERCICIO DE DERECHOS

Correo electrónico de contacto: contacto@medinayrivera.com.co
Teléfono de contacto: +57 601 6203317
Dirección: Cr. 15a # 121 – 12 ofc.318