LOZADA & PARTNERS
ACCOUNTING, TAXES & HR SOLUTIONS

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Versión 1.0 | Marzo 2026
Cajicá., Colombia

1. INTRODUCCIÓN

LOZADA & PARTNERS SAS (en adelante "LOZADA"), como firma de outsourcing contable estratégico que gestiona información financiera, tributaria y laboral de alto valor para sus clientes, establece el presente Manual de Políticas de Seguridad de la Información con el fin de garantizar la protección integral, disponibilidad y confidencialidad de toda la información durante su ciclo de vida, ya sea física, electrónica o verbal.

2. OBJETIVO

Establecer las políticas de seguridad de la información en LOZADA, garantizando los principios de integridad, reserva, disponibilidad, legalidad y confiabilidad, previniendo riesgos operacionales y estratégicos en el manejo de la información contable, tributaria y laboral de nuestros clientes y de la Compañía.

3. ALCANCE

Esta política es de obligatorio cumplimiento para todos los directivos, socios, empleados, clientes, contratistas, proveedores y terceros que presten servicios o tengan algún tipo de vinculación con LOZADA, aplicable desde el momento de su publicación.

4. MARCO LEGAL

- Constitución Política de Colombia, Artículos 15 (Habeas Data) y 20 (Libertad de Información).
- Ley 527 de 1999 – Comercio electrónico y firmas digitales.
- Ley 1266 de 2008 – Habeas Data y bases de datos personales.
- Ley 1273 de 2009 – Delitos informáticos y protección de datos.
- Ley 1581 de 2012 – Protección de datos personales.
- Decreto 1074 de 2015 – Reglamentación de protección de datos.
- Ley 23 de 1982 – Derechos de autor y propiedad intelectual.

5. POLÍTICA GENERAL DE SEGURIDAD

LOZADA protege la información mediante controles administrativos, técnicos y jurídicos, impidiendo que personas no autorizadas puedan acceder, distribuir, modificar o alterar información protegida bajo los principios de confidencialidad, integridad y disponibilidad. Dada la naturaleza de nuestros servicios contables, tributarios y laborales, la información financiera de clientes recibe el más alto nivel de protección.

6. POLÍTICAS ESPECÍFICAS

6.1. Política de Estructura Organizacional

La información estará bajo la responsabilidad directa de LOZADA para evitar conflictos y reducir oportunidades de acceso no autorizado. La Compañía mantendrá contacto con grupos especializados en

protección de información para capacitar a su personal. Los servicios en la nube están permitidos cumpliendo los acuerdos de confidencialidad vigentes. Los datos extraídos de bases de datos de clientes a través de medios removibles deben permanecer bajo custodia en condiciones de seguridad. LOZADA renovará equipos que hayan cumplido su vida útil y representen un punto vulnerable.

6.2. Política de Bases de Datos

LOZADA establece acciones para evitar la divulgación, modificación, retiro o destrucción no autorizada de información almacenada en bases de datos, velando por la disponibilidad y confidencialidad. Cualquier acceso a la información física o virtual deberá ser autorizado por la Gerencia General o el área responsable designada.

- Se realizan procedimientos de mantenimiento preventivo en los equipos que contienen información protegida.
- Bajo ninguna circunstancia LOZADA entregará copia de las bases de datos en dispositivos externos (discos duros, USB, CD, DVD), salvo requerimiento de autoridad judicial o administrativa.
- El titular puede solicitar la supresión total o parcial de sus datos cuando estos no estén siendo tratados conforme a la normatividad vigente, o cuando transcurran más de ocho (8) años desde la recolección.
- LOZADA podrá negar la supresión cuando esta obstaculice actuaciones judiciales o administrativas, exista deber legal o contractual de permanencia, o los datos sean necesarios para proteger intereses jurídicos.

6.3. Política de Uso de Internet

Internet es un instrumento de trabajo cuyo uso se monitorea y controla bajo las siguientes reglas:

- Su uso es exclusivo para actividades relacionadas con las funciones de la Compañía.
- Queda prohibido generar, reproducir o introducir código malicioso diseñado para dañar equipos o redes.
- LOZADA implementa herramientas para impedir la descarga de software no autorizado y controla el acceso a portales de almacenamiento en línea.
- El acceso a redes sociales, mensajería instantánea y cuentas de correo no institucional está restringido, salvo autorización expresa de la Gerencia General.
- Se prohíbe la navegación en sitios de contenido sexualmente explícito, discriminatorio o que implique delito informático.
- No está permitida la descarga de música, videos o software no relacionado con actividades laborales.
- Se prohíbe el uso de cuentas de correo personales para enviar o recibir información institucional o de clientes.
- LOZADA se reserva el derecho de monitorear tiempos de navegación y páginas visitadas.

6.4. Política de Seguridad de Acceso Físico y Red

- El acceso a carpetas físicas y documentos está bajo custodia de la Gerencia General.
- Todo trabajador deberá portar de manera visible su identificación dentro de las instalaciones.
- Visitantes, clientes y proveedores deberán estar acompañados permanentemente por un trabajador autorizado.

- Las contraseñas son de uso personal e intransferible y su cambio debe ser solicitado al área responsable.
- Ningún tercero tendrá acceso a equipos o documentos sin autorización de la Gerencia General.
- Los equipos, sistemas y servicios de red provistos a trabajadores son activos de LOZADA destinados exclusivamente al cumplimiento de funciones laborales.

6.5. Política de Trabajadores

- Los trabajadores deben autorizar a LOZADA para el tratamiento de sus datos personales conforme a la Ley 1581 de 2012.
- Se capacitará a todo el personal durante la inducción sobre políticas de seguridad y tratamiento de datos.
- Documentos impresos con información confidencial deben retirarse inmediatamente de impresoras.
- No deben mantenerse documentos clasificados en puestos de trabajo visibles.
- Todo incidente de seguridad debe reportarse de inmediato al área responsable.

6.6. Política de Gestión de Incidentes y Riesgos

- Se definen roles y compromisos para valorar riesgos e incidentes y mantener la continuidad operacional.
- Todo trabajador está obligado a informar cualquier situación sospechosa que comprometa la seguridad de la información.
- Se llevará un registro detallado de eventos, incidentes y riesgos para evaluación y respuesta oportuna.
- Los riesgos se tramitan por prioridad: alto, medio y bajo.
- Cualquier incidente causado por un trabajador dará lugar al proceso disciplinario correspondiente.

6.7. Política de Redes Compartidas y Carpetas Virtuales

- Se prohíbe almacenar o comercializar archivos personales de audio, video o fotografía en recursos de la Compañía.
- La información no pertinente se conserva máximo 6 meses antes de depuración.
- La eliminación de información compartida requiere autorización del área responsable.
- No se podrá almacenar información clasificada en servicios de nube públicos no autorizados.
- Los documentos confidenciales deberán ser marcados como “confidencial” o “información de acceso restringido”.

6.8. Política de Seguridad de Equipos

- Los equipos deben estar ubicados y protegidos para prevenir daño, robo o acceso no autorizado.
- Se ejecutarán mantenimientos preventivos y correctivos periódicos.
- Los equipos no deben ser prestados a personas no autorizadas.
- Todos los equipos, sistemas y servicios de red son propiedad de LOZADA.

- Está restringida la reproducción o descarga de archivos en medios removibles sin autorización.

6.9. Política de Redes Sociales y Mensajería

- La información publicada a título personal por trabajadores en redes sociales es responsabilidad exclusiva del autor.
- Toda publicación en redes sociales corporativas debe ser autorizada por la Gerencia General o el Departamento de Marketing & Comunicaciones.
- Se prohíbe vincular cuentas de correo personales a redes sociales corporativas.
- No se recomienda administrar redes sociales corporativas desde dispositivos personales.
- Las contraseñas de cuentas corporativas deben ser complejas y cambiarse periódicamente.

6.10. Política de Puesto de Trabajo

- Los escritorios deben mantenerse libres de información confidencial visible.
- Las estaciones de trabajo deben bloquearse al ausentarse el usuario.
- En horas no hábiles, la información crítica debe estar protegida bajo llave o restricción electrónica.
- Queda prohibido reutilizar papel que contenga información sensible.
- Los trabajadores son responsables de los activos informáticos asignados.

6.11. Política de Protección de Datos y Privacidad

En cumplimiento de la Ley 1581 de 2012, LOZADA propenderá por la protección de los datos personales de clientes, trabajadores, proveedores, contratistas y terceros. Se implementarán los controles necesarios para que la información sea utilizada únicamente conforme a las funciones de la Compañía y no sea revelada sin autorización.

- Para todo tratamiento de datos personales se debe obtener autorización previa del titular.
- Únicamente el personal con necesidad laboral legítima podrá acceder a datos personales.
- Los trabajadores deben guardar reserva absoluta sobre la información de LOZADA y de sus clientes.
- Es obligación corroborar la identidad de toda persona a quien se entregue información.

6.12. Política de Software No Autorizado

- Todos los equipos deben contar con software antivirus actualizado.
- Los trabajadores no pueden modificar la configuración del antivirus.
- Las herramientas de protección no pueden deshabilitarse sin autorización.
- Los archivos descargados deben proceder de fuentes acreditadas y seguras.
- Cualquier sospecha de contagio debe notificarse inmediatamente al área responsable.
- Queda prohibido instalar software no autorizado en equipos de la Compañía.

6.13. Política de Copias de Seguridad

LOZADA efectuará copias de respaldo periódicas de información crítica y reservada. Todas las áreas definirán la estrategia de backup y los períodos de conservación. Los medios magnéticos con información crítica serán resguardados en ubicación diferente a las instalaciones principales.

7. OPERACIONES QUE VULNERAN ESTA POLÍTICA

Se consideran violaciones a esta política, entre otras:

- No reportar incidentes o riesgos de seguridad.
- No almacenar de forma segura la información al ausentarse del puesto de trabajo.
- Abandonar información reservada en carpetas no autorizadas.
- Permitir acceso de personas no autorizadas a instalaciones o sistemas.
- Almacenar información de la Compañía en equipos personales.
- Modificar datos de bases de datos sin autorización.
- No mantener la confidencialidad de contraseñas.
- Instalar software no autorizado o copiar aplicaciones violando derechos de autor.
- Sustraer equipos o documentos reservados sin autorización.

8. SANCIONES

La violación de esta política dará lugar a las acciones disciplinarias correspondientes para trabajadores de LOZADA, y a la exigencia de responsabilidad solidaria para terceros. Las investigaciones disciplinarias y sanciones serán tramitadas por la Gerencia General y/o el área de Recursos Humanos.

9. ACUERDO DE CONFIDENCIALIDAD

Todos los trabajadores y contratistas están obligados a firmar un acuerdo de confidencialidad como parte integral de sus contratos laborales o de prestación de servicios. Este requerimiento es igualmente aplicable a clientes, proveedores y terceros que accedan a información de LOZADA.

Cualquier reclamo, petición o queja respecto del tratamiento de datos personales puede radicarse al correo electrónico [POR DEFINIR – ej: protecciondatos@lozada.com.co].