1. CONTROL DE REVISIÓN Y APROBACIÓN DEL DOCUMENTO

Oscar Emilio Muñoz Gonzalez	**Mauricio Rojas Giraldo**
REVISÓ	APROBÓ
Director Tics	**Presidente**
CARGO	CARGO

2. OBJETIVO

MILENIO PC. S.A., empresa de servicios gestionados de tecnología que organiza componentes adecuados de Hardware, Software, Nube y Talento Humano en paquetes de valor adaptables para los clientes con flexibilidad, rapidez y conveniencia establece el compromiso con la protección, confidencialidad, integridad, disponibilidad y uso responsable de la información en todos los procesos administrativos, operativos y de atención al cliente, la protección de los datos personales y el fortalecimiento de la ciberseguridad, garantizando la continuidad del negocio y el cumplimiento de los requisitos legales, contractuales y normativos aplicables, en la prestación de los servicios de alquiler y administración de equipos de cómputo, impresoras, dispositivos de red, soporte técnico y administración de infraestructura tecnológica.

3. ALCANCE

Aplica a todo el personal de la organización, incluyendo personal administrativo, técnico, proveedores, contratistas, terceros autorizados y visitantes que tengan acceso físico o lógico a la infraestructura, sistemas de información o datos de la compañía y sus clientes.

4. COMPROMISOS DE MILENIO PC

La Presidencia y la Dirección de MILENIO PC se comprometen a:

1. **Confidencialidad:** Proteger la información propia y la de clientes frente a accesos no autorizados, con especial énfasis en los datos personales, técnicos, comerciales y financieros.
2. **Integridad:** Garantizar que la información no sea alterada de manera indebida, asegurando la calidad y confiabilidad de los datos gestionados.
3. **Disponibilidad:** Asegurar que la información, servicios y sistemas estén disponibles de acuerdo con los requerimientos de los procesos críticos de negocio y las necesidades de clientes.
4. **Cumplimiento legal y normativo:** Dar cumplimiento a la legislación vigente en materia de Seguridad de la información y protección de datos personales, firma electrónica, propiedad intelectual y demás normativas aplicables.
5. Continuidad del negocio: Mantener, actualizar y probar planes de continuidad y recuperación ante desastres, asegurando la prestación ininterrumpida de los servicios de soporte técnico y alquiler de equipos.
6. Protección de Datos Personales: Garantizar el tratamiento adecuado de los datos personales de clientes, colaboradores, proveedores y demás titulares de la información, conforme a la legislación vigente, las políticas internas de privacidad y los principios de confidencialidad, integridad, disponibilidad y uso autorizado de la información.
7. Ciberseguridad: Fortalecer las capacidades de prevención, detección, respuesta y recuperación frente a amenazas cibernéticas, mediante la implementación de controles técnicos y administrativos, la gestión de vulnerabilidades, el monitoreo de eventos de seguridad, la concienciación de los usuarios y la mejora continua de los mecanismos de protección.
8. Gestión de incidentes: Garantizar que todos los incidentes de seguridad de la información y de ciberseguridad, reales o sospechosos, sean reportados oportunamente, analizados, contenidos, tratados y gestionados para minimizar su impacto, prevenir su recurrencia y fortalecer la resiliencia de la organización.

9. Capacitación y concientización: Implementar programas continuos de formación en seguridad de la información para todos los empleados, con contenidos específicos para el personal técnico que interactúa directamente con los clientes.
10. Uso responsable de recursos tecnológicos: Asegurar que los sistemas de correo electrónico, redes, plataformas y equipos sean utilizados de manera ética, prohibiendo el envío de cadenas, material ofensivo, político, religioso o que degrade la dignidad humana.
11. Atención segura al cliente: Establecer protocolos de interacción técnica con clientes que garanticen la confidencialidad de la información tratada durante la prestación de servicios y soporte.
12. Mejora continua: Revisar y actualizar periódicamente esta política y el Sistema de Gestión de Seguridad de la Información (SGSI), promoviendo la mejora continua y la adaptación a nuevas amenazas, tecnologías y regulaciones.

5. RESPONSABILIDADES

- Presidencia: Asegurar la aprobación, difusión y cumplimiento de la política.
- Responsable de Seguridad de la Información: Supervisar la implementación y actualización de controles de seguridad.
- Personal técnico: Cumplir los lineamientos de seguridad en la interacción con clientes y en la gestión de equipos e infraestructura.
- Todos los empleados y terceros: Cumplir con esta política, reportar incidentes y participar activamente en la protección de la información.

6. OBLIGACIÓN DE CUMPLIMIENTO

El cumplimiento de esta política es obligatorio para todas las partes interesadas internas y externas. Su desconocimiento no exime de responsabilidad y puede generar sanciones disciplinarias o contractuales.

Revisada agosto 1 de 2026

MAURICIO ROJAS GIRALDO
Presidente