

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	POLÍTICA DE MEDIDAS DE SEGURIDAD DE SOPORTE PARA TELETRABAJO	
VIGENCIA: 25/06/2024	VERSIÓN: 1	PÁG. 1 de 3

1. Objetivo

Establecer las medidas de seguridad mínimas necesarias para proteger la información y los activos tecnológicos durante la ejecución de actividades laborales en modalidad de teletrabajo, garantizando la confidencialidad, integridad y disponibilidad de la información.

2. Alcance

Aplica a todo el personal interno, externo o contratado que realice actividades laborales de forma remota utilizando sistemas de información, infraestructura tecnológica o acceso a datos de la organización.

3. Responsabilidades

- **Usuarios:** Cumplir con las medidas de seguridad definidas y reportar incidentes de seguridad.
- **Área de TI:** Brindar soporte, implementar controles y mantener actualizado el entorno tecnológico seguro.
- **Responsable de Seguridad de la Información:** Supervisar el cumplimiento de esta política y realizar revisiones periódicas.

4. Requisitos Generales de Seguridad para el Teletrabajo

4.1. Dispositivos aprobados

- Solo se permitirá el uso de equipos autorizados por el área de TI.
- Todo equipo debe tener software de seguridad actualizado (antivirus, firewall, etc.).

4.2. Redes Seguras

- El acceso remoto debe realizarse exclusivamente mediante redes seguras (preferiblemente con cable o Wi-Fi protegido con contraseña WPA2/WPA3).
- Queda prohibido el uso de redes públicas sin túneles cifrados (VPN) (Si aplica).

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	POLÍTICA DE MEDIDAS DE SEGURIDAD DE SOPORTE PARA TELETRABAJO	
VIGENCIA: 25/06/2024	VERSIÓN: 1	PÁG. 2 de 3

4.3. Control de Acceso

- Autenticación de múltiples factores (MFA) obligatoria para acceso remoto.
- Las contraseñas deben cumplir los requisitos de complejidad definidos por la organización.
- No se permite compartir credenciales de acceso bajo ninguna circunstancia.

4.4. Gestión de la Información

- La información sensible debe almacenarse solo en plataformas autorizadas (servidores, nube corporativa).
- Se prohíbe el uso de memorias USB no autorizadas o servicios de almacenamiento en la nube no autorizados (Google Drive personal, Dropbox, etc.).
- Todos los documentos deben cifrarse si se almacenan localmente (Utilizando AVG Antivirus).

4.5. Uso de Videollamadas y Comunicación

- Utilizar únicamente herramientas corporativas autorizadas para videollamadas y mensajería (Google Meet, Microsoft Teams).
- Evitar compartir datos sensibles a terceros.
- Asegurar que el entorno físico no permita que terceros escuchen conversaciones confidenciales.

4.6. Soporte Técnico

- El área de TI proporcionará asistencia remota a través de canales seguros (Anydesk, Any Viewer).
- No se permitirá el acceso remoto de soporte externo sin previa validación.
- Todos los accesos de soporte deben registrarse.

5. Concienciación y Formación

Todo el personal en modalidad de teletrabajo debe participar en capacitaciones periódicas sobre ciberseguridad y uso seguro de herramientas digitales.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	POLÍTICA DE MEDIDAS DE SEGURIDAD DE SOPORTE PARA TELETRABAJO	
VIGENCIA: 25/06/2024	VERSIÓN: 1	PÁG. 3 de 3

6. Gestión de Incidentes

Cualquier anomalía, intento de acceso no autorizado, pérdida de datos o fallo de seguridad deberá ser reportado inmediatamente al área de TI o Seguridad de la Información.

7. Revisión y Actualización

Esta política será revisada anualmente o ante cualquier cambio significativo en las condiciones de trabajo o infraestructura tecnológica.



CARLOS HUMBERTO TRONCOSO AYALDE
GERENTE GENERAL

VERSIÓN	CAMBIO	VIGENCIA
1	Primera versión	25/06/2024