Política de Seguridad de la Información (TI)

Uso Aceptable de Activos y Ciberseguridad

1. Alcance

Esta política define el uso aceptable de los recursos tecnológicos, infraestructura de red y dispositivos (laptops, tablets, smartphones) proporcionados por CGFE, garantizando la seguridad de la información corporativa e industrial (OT).

2. Uso de Activos de Información

- Los equipos computacionales y correos electrónicos corporativos son herramientas de trabajo propiedad exclusiva de la empresa. La compañía se reserva el derecho de auditar dichos medios con fines de seguridad informática, dentro del marco legal vigente.
- Está prohibida la descarga e instalación de software no autorizado, pirata o sin licencia en los equipos de CGFE.
- No se debe conectar dispositivos de almacenamiento masivo USB (pendrives) no encriptados ni provistos por TI, para prevenir la infiltración de malware (ej. Ransomware).

3. Gestión de Credenciales y Contraseñas

Seguridad de Accesos

Las contraseñas son personales e intransferibles. Deben contener al menos 12 caracteres (incluyendo mayúsculas, números y símbolos) y renovarse cada 90 días. **Nunca comparta su contraseña ni la anote en lugares visibles.**

4. Trabajo Remoto y Conectividad en Terreno

Para la gestión de proyectos en terreno o trabajo a distancia, la conexión a los servidores de CGFE, ERP (SAP) o sistemas de control (SCADA) debe realizarse obligatoriamente a través de la **Red Privada Virtual (VPN)** corporativa, que cuenta con Autenticación de Múltiples Factores (MFA).

5. Prevención de Phishing

El factor humano es la principal barrera de ciberseguridad. Todo colaborador debe estar alerta a correos electrónicos con remitentes sospechosos, enlaces desconocidos o solicitudes urgentes de transferencias de dinero. Ante cualquier duda, no haga clic y reporte el correo al área del Helpdesk de Ciberseguridad.