## 1. POLÍTICAS DE ASEGURAMIENTO

### 1.1 Gestión de Dominios

- 1.1.1 Configuración y administración de dominios
- 1.1.2 Políticas de seguridad del dominio
- 1.1.3 Controladores de dominio y redundancia

### 1.2 Administración de Grupos

- 1.2.1 Clasificación y tipos de grupos
- 1.2.2 Políticas de creación de grupos
- 1.2.3 Gestión de permisos por grupos

### 1.3 Gestión de Equipos

- 1.3.1 Políticas de incorporación de equipos
- 1.3.2 Configuración de seguridad en estaciones de trabajo
- 1.3.3 Políticas de actualización y mantenimiento

### 1.4 Gestión de Usuarios

- 1.4.1 Políticas de creación de cuentas
- 1.4.2 Gestión de credenciales y contraseñas
- 1.4.3 Control de accesos y privilegios

### 1.5 Conectividad a la Nube

- 1.5.1 Políticas de acceso a servicios cloud
- 1.5.2 Seguridad en almacenamiento cloud
- 1.5.3 Gestión de identidades en la nube

### 1.6 Conectividad a Dispositivos Móviles

- 1.6.1 Políticas BYOD (Bring Your Own Device)
- 1.6.2 Gestión de dispositivos móviles (MDM)
- 1.6.3 Seguridad en aplicaciones móviles

---

## 2. CONTROLES A SER IMPLEMENTADOS

### 2.1 Controles de Acceso

- 2.1.1 Control de acceso físico
- 2.1.2 Control de acceso lógico
- 2.1.3 Autenticación multifactor

### 2.2 Controles de Seguridad de Red

- 2.2.1 Firewalls y segmentación de red
- 2.2.2 Sistemas de detección y prevención de intrusos
- 2.2.3 VPN y conexiones seguras

### 2.3 Controles de Protección de Datos

- 2.3.1 Cifrado de datos
- 2.3.2 Respaldo y recuperación
- 2.3.3 Prevención de pérdida de datos (DLP)

### 2.4 Controles de Monitoreo y Auditoría

- 2.4.1 Registro de eventos (logging)
- 2.4.2 Monitoreo continuo
- 2.4.3 Auditorías periódicas

### 2.5 Controles de Gestión de Incidentes

- 2.5.1 Plan de respuesta a incidentes
- 2.5.2 Procedimientos de escalamiento
- 2.5.3 Análisis post-incidente