1. **Definir a lista de políticas de uso e acesso à rede ou arquivos da empresa:**

- Política de Senhas Fortes
- Política de Backup de Dados
- Política de Acesso Remoto
- Política de Uso de Dispositivos Móveis
- Política de Segurança de E-mail
- Política de Atualização de Software
- Política de Controle de Acesso Físico
- Política de Proteção contra Malware
- Política de Auditoria de Segurança
- Política de Resposta a Incidentes
- Política de Privacidade de Dados
- Política de Uso Aceitável
- Política de Gestão de Riscos
- Política de Criptografia de Dados
- Política de Segurança de Rede
- Política de Gestão de Vulnerabilidades
- Política de Treinamento de Segurança
- Política de Segurança de Aplicações
- Política de Gestão de Mudanças
- Política de Segurança de Informações Confidenciais

2. **20 políticas:**

- **Política de Senhas Fortes**: Todos os funcionários devem usar senhas complexas e alterá-las regularmente.
- **Política de Backup de Dados**: Realizar backups diários de todos os dados críticos e armazená-los em locais seguros.
- **Política de Acesso Remoto**: Definir regras para acesso remoto seguro aos sistemas da empresa.
- **Política de Uso de Dispositivos Móveis**: Regulamentar o uso de dispositivos móveis para acessar dados corporativos.
- **Política de Segurança de E-mail**: Implementar medidas para proteger contra phishing e outros ataques via e-mail.
- **Política de Atualização de Software**: Garantir que todos os softwares estejam sempre atualizados com os patches de segurança mais recentes.
- **Política de Controle de Acesso Físico**: Restringir o acesso físico a áreas sensíveis da empresa.

- **Política de Proteção contra Malware**: Utilizar ferramentas de proteção contra malware e realizar varreduras regulares.
- **Política de Auditoria de Segurança**: Realizar auditorias de segurança periódicas para identificar e corrigir vulnerabilidades.
- **Política de Resposta a Incidentes**: Estabelecer procedimentos para responder a incidentes de segurança.
- **Política de Privacidade de Dados**: Proteger a privacidade dos dados pessoais de clientes e funcionários.
- **Política de Uso Aceitável**: Definir o uso aceitável dos recursos de TI da empresa.
- **Política de Gestão de Riscos**: Identificar, avaliar e mitigar riscos de segurança.
- **Política de Criptografia de Dados**: Utilizar criptografia para proteger dados sensíveis.
- **Política de Segurança de Rede**: Implementar medidas para proteger a rede corporativa contra ameaças.
- **Política de Gestão de Vulnerabilidades**: Identificar e corrigir vulnerabilidades de segurança.
- **Política de Treinamento de Segurança**: Oferecer treinamento regular de segurança para todos os funcionários.
- **Política de Segurança de Aplicações**: Garantir que todas as aplicações sejam desenvolvidas e mantidas com segurança.
- **Política de Gestão de Mudanças**: Controlar e monitorar mudanças nos sistemas de TI.
- **Política de Segurança de Informações Confidenciais**: Proteger informações confidenciais contra acesso não autorizado.