# AUTENTICAÇÃO DE USUÁRIOS E SERVIÇOS

# SOBRE AUTENTICAÇÃO DE USUÁRIOS E SERVIÇOS

A interconectividade de redes pode prever a autenticação, unidirecional ou bidirecional, entre as redes envolvidas, utilizando tecnologias como Kerberos ou Active Directory. A autenticação e a autorização relativa a acessos em sistemas e similares está fora do escopo desta Orientação Técnica.

A competência para definir os mecanismos e/ou procedimentos de autenticação para acesso à rede é:

- Do Integrador Estratégico, para a interconectividade externo-rpcd;
- Dos respectivos Órgãos do SMTIC, para interconectividade externo-interno.

A autenticação na RPCD, para acesso aos recursos computacionais e informações, será realizada mediante criação de credenciais no domínio rede.sp ou através do estabelecimento de relação de confiação com o diretório gerido pelo órgão.

Cabe ressaltar, no entanto, que o sistema de Controle de Acesso Corporativo (CAC) não está contemplado como um meio hábil à autenticação na RPCD.

Para as interconectividades interno-interno e interno-rpcd, os mecanismos e procedimentos de autenticação poderão ser acordados mutuamente de maneira prévia entre as partes envolvidas, considerando-se às capacidades de infraes-trutura dos sites envolvidos e à necessidade de restringir os acessos às necessidades de negócio que justificam a interconectividade.

Em particular, para as interconectividades interno-interno e interno-rpcd, pode-se realizar a integração dos mecanismos de autenticação mediante o estabelecimento de relação de confiança entre domínios, caso haja compatibilidade entre as partes envolvidas e a implantação de tais mecanismos seja tecnicamente viável.

Para isso, devem-se tomar, no mínimo, os seguintes passos:

1. Caracterizar a relação de confiança a ser estabelecida, considerando as seguintes dimensões: tipo, transitividade e direcionalidade.
   - O tipo pode ser:
     1. Hierárquico: uma relação de subordinação entre uma rede e outra (ex: relações de confiança pai-filho e árvore-raiz).
     2. Não-hierárquico: uma relação de confiança entre uma rede e outra em nível de igualdade (ex: relações de confiança externo e floresta).
   - A transitividade pode ser transitiva ou intransitiva (não transitiva).
   - A direcionalidade pode ser unidirecional ou bidirecional (mútua).

2. Realizar testes para validar a infraestrutura e a relação construída antes de colocar em ambiente de produção.
    - Incluindo testes para verificar se os acessos e privilégios estão de acordo com as regras de negócio que justificam.

# QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Para interconectividade interno-interno ou interno-rpcd, disponibilizar no Portal de Governança um guia ou lista atualizada periodicamente (periodicidade mínima anual) dos mecanismos e/ou procedimentos de autenticação para acesso aos respectivos sites ou à RPCD, excetuando os dados e informações consideradas necessárias à manutenção da segurança das informações.
- Remover relações de confiança redundantes ou expirados.
- Revisão constante dos usuário de rede ativos (revogação dos não ativos)

# QUAIS SÃO AS NOSSAS SUGESTÕES?

- Evitar relações de confiança muito profundas, mantendo-as no máximo com um nível de profundidade.
- Ter na documentação uma representação gráfica da relação de confiança, usando de diagramas, mapas e similares, para facilitar a visualização e entendimento.
- Implementar uma verificação periódica para detectar relações de confiança redundantes ou expirados.
- Criar processo interno, idealmente com o Departamento de Pessoal (RH), com o objetivo de obter informação sobre desligamento/licença de pessoal, de forma a bloquear ou revogar os usuários de rede.