OT 002 - Interconectividade de Rede

Fornece informações para que se possa avaliar qual a tec nologia mais adequada para implantar a interconectividade no Órgão Setorial, bem como o modelo mais adequado de contratação, em consonância com os requisitos de negócio e a viabilidade técnica de modo que garanta a segurança para a conexão física e lógica e possibilite o tráfego controlado de dados entre redes. Em seu conteúdo constam informações a respeito dos tipos de tecnologias de interconectividade, requisitos gerais, diferentes classificações de conexão entre sites, autenticação de usuários e serviços, segurança da informação, recomendações sobre redes Wi-Fi e IoT e plano de respostas a incidentes.

DEFINIÇÕES

SOBRE DEFINIÇÕES

RPCD: Rede privada de comunicação de dados da Administração Pública Municipal, administrada pelo Integrador Estratégico, nos termos do Art. 12, inciso III, do Decreto 57.653 de 07 de abril de 2017. No âmbito desta OT, é a infraestrutura de comunicação, hospedagem e armazenamento gerida pelo Integrador Estratégico, que não seja nem site interno nem externo.

Site interno: rede privada, ou conjunto de redes privadas, de um Órgão do SMTIC.

Site interno independente: site interno gerido de maneira autônoma pelo Órgão do SMTIC.

Site interno dependente: site interno gerido pelo Integrador Estratégico em nome do Órgão do SMTIC, mediante autorização deste último, incluindo quando a gestão do Integrador Estratégico se limita à alocação de intervalos de endereços IP do site interno.

Sites externos: referem-se às redes que não pertencem à PMSP e não estão sob a sua gestão. Exemplos: redes de parceiros, empresas contratadas, bancos, entidades governamentais externas à PMSP.

TECNOLOGIA DE INTERCONECTIVIDADE

SOBRE TECNOLOGIA DE INTERCONECTIVIDADE

A interconectividade de redes pode ser realizada de diversas maneiras, utilizando-se de diferentes tecnologias.

Algumas tecnologias típicas para implantar a conexão propriamente dita são:

- Circuitos dedicados (dedicated circuit network), que são links contratados para que haja uma conexão dedicada ponto-a-ponto entre dois sites.
- Site-to-site Virtual Private Network (VPN), que é um canal criptografado e privado de comunicação sobre a internet para que dois sites possam trocar dados.
- Links de comunicação MPLS (Multiprotocol Label Switching), uma tecnologia de transmissão de dados de alto desempenho.

A tabela a seguir oferece um comparativo **bastante simplificado** entre as três tecnologias de acordo com quatro fatores: custo financeiro, segurança da conexão, confiabilida-de (qualidade de serviço e disponibilidade) e escalabilidade.

Fator	Circuito dedicado	Site-to-Site VPN	MPLS
Custo	Alto	Baixo	Médio
Segurança	Alto	Baixo	Dependente do serviço contratado
Confiabilidade	Alto	Baixo	Médio
Escalabilidade	Baixo	Médio	Alto

A escolha da tecnologia de implantação do link de comunica-ção deverá ser feita com base nas necessidades de negócio e na viabilidade técnica de operacionalização do link, sendo que a escolha não está restrita às três tecnologias supra-citadas[1]. A tabela acima visa meramente servir de subsídio eventual à análise técnica do responsável técnico de TI do Órgão do SMTIC.

Além disso, o responsável técnico de TI do Órgão do SMTIC poderá levar em consideração diferentes modelos de con-tratação, avaliando possibilidades como a contratação de um managed services provider (MSP) que forneça inclusive os ativos de rede (roteadores e demais materiais)

para o acesso físico à conexão.

> 1: Outras tecnologias possíveis são, por exemplo, SD-WAN (Software Defined WAN) e a Broadband bonding.

Acrescenta-se ainda que a tecnologia SD-WAN permite a combinação de diversos links, por exemplo um link dedicado e uma conexão 4G de forma a obter melhor performance, e ao mesmo tempo uma mais alta disponibilidade. Traz uma abordagem programática e automatizada para gerenciar a conectividade de rede e os custos de circuito de empresas.

Com a SD-WAN, a TIC pode fornecer roteamento e proteção contra ameaças, além de economizar custos com circuitos caros e simplificar o gerenciamento das redes WAN. Os benefícios com uso dessa tecnologia são:

- Melhor experiência de aplicação.
- Alta disponibilidade, com serviço previsível, de todas as principais aplicações empresariais.
- Vários links ativos para todos os cenários de rede.
- O roteamento dinâmico é programável e automatizado a fim de permitir controlar o tráfego com base em políticas de aplicativos, condições de rede ou prioridade do circuito WAN.
- OpEx aprimorado, substituindo os serviços de MPLS (Multiprotocol Label Switching) por uma banda larga mais econômica e flexível (incluindo conexões VPN seguras).

Mais segurança

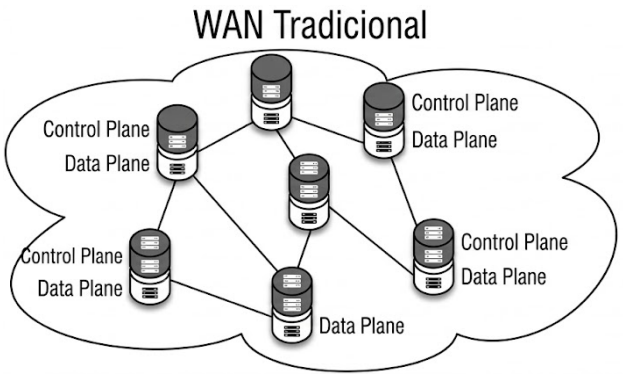
- Políticas de reconhecimento de aplicações com segmentação de ponta a ponta e controle de acesso em tempo real.
- Proteção integrada contra ameaças.
- Tráfego seguro no ambiente de Internet de banda larga e na nuvem.
- Segurança distribuída para a filial e os endpoints remotos com NGFW, segurança DNS e NGAV.

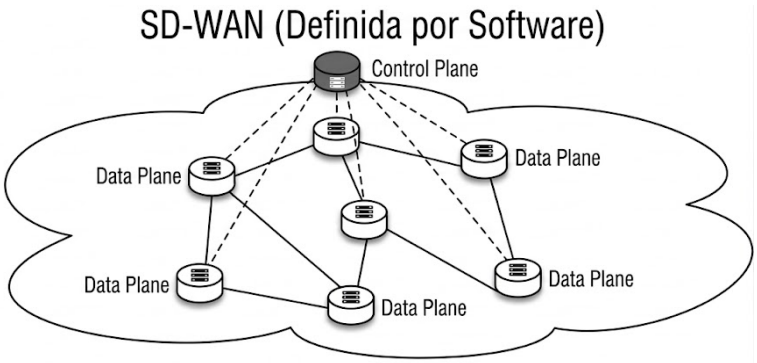
Conectividade de nuvem otimizada

- Fácil ampliação da WAN para várias nuvens públicas.
- Desempenho otimizado em tempo real no Microsoft Office 365, Salesforce e outras aplicações importantes de SaaS.
- Fluxos de trabalho otimizados para plataformas de nuvem, como serviços Web da Amazon (AWS) e Microsoft Azure.

Gerenciamento simplificado

- Um painel de gerenciamento único e centralizado.
- Provisionamento automatizado.
- Relatório detalhado de aplicações e desempenho.


WAN Tradicional
Control Plane
Data Plane
Control Plane
Data Plane
Control Plane
Data Plane
Control Plane
Data Plane
Data Plane


SD-WAN (Definida por Software)
Control Plane
Data Plane
Data Plane
Data Plane
Data Plane
Data Plane

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Avaliar qual a tecnologia mais adequada para implantar a interconectividade, bem como o modelo mais adequado de contratação, em aderência com os requisitos de negócio e a viabilidade técnica.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Avaliar tecnicamente a opção de contratar ou não um provedor de serviços gerenciados (managed services provider) para a implantação do serviço de conexão.
- Para Órgãos do SMTIC com maturidade inferior à Série C, adotar uma tecnologia de interconectividade com segurança média ou alta.
- Avaliar a possibilidade de utilização da SD - WAN a fim de trazer benefícios operacionais visando suporte a várias conexões seguras para também minimizar danos em caso de violações, elevar o desempenho e obter redução de custos.

REQUISITOS GERAIS DE INTERCONECTIVIDADE

SOBRE REQUISITOS GERAIS DE INTERCONECTIVIDADE

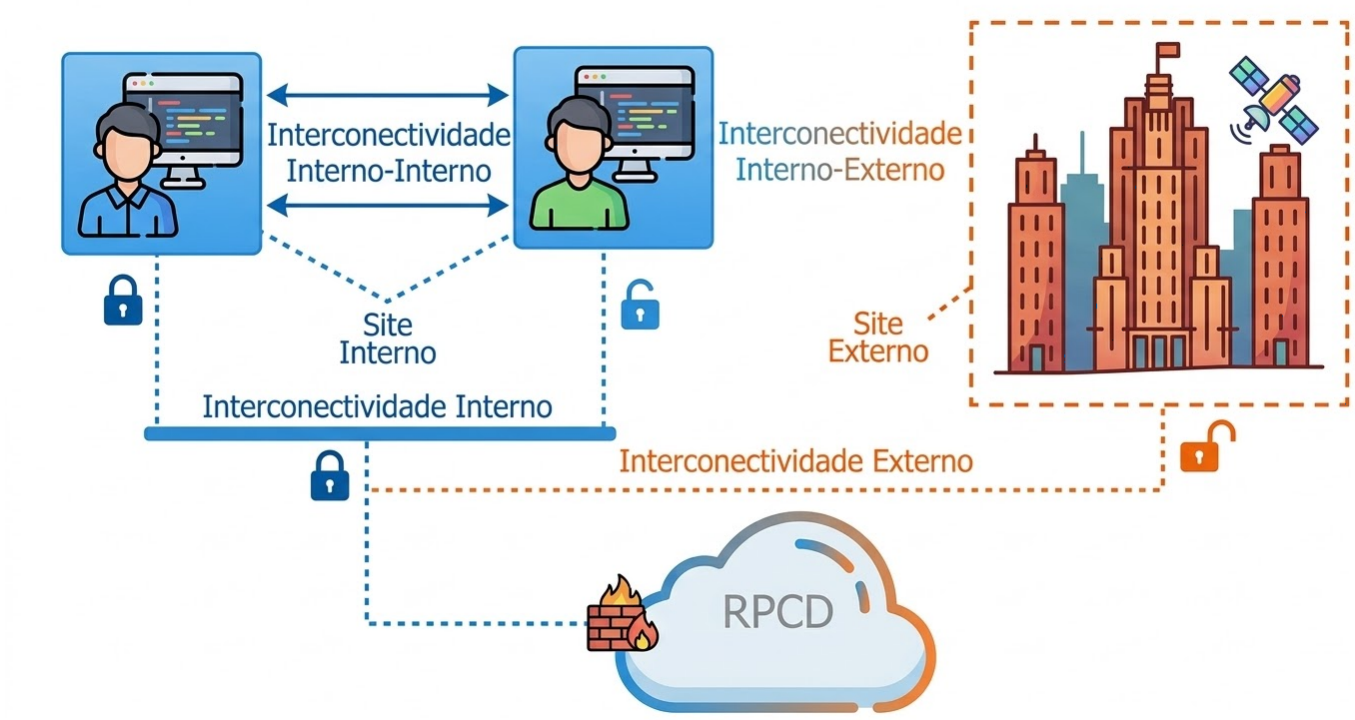
A RPCD e cada um dos sites, internos ou externos, são con-siderados como perímetros distintos, que podem conter um ou mais subperímetros para fins de segurança da informação e/ou de infraestrutura.

Em particular, datacenters são considerados como um subperímetro do site interno no qual estão inseridos.

A interconexão de redes se trata da ligação entre tais perímetros e pode ser classificada na seguinte conformidade:

- Interno-interno: ligação entre dois sites internos.
- Interno-rpcd: ligação entre um site interno e a RPCD.
- Externo-interno: ligação entre um site externo e um site interno.
- Externo-rpcd: ligação entre um site externo e a RPCD.

A figura a seguir ilustra as diferentes classificações listadas acima.



A sua concretização deverá atender, prévia e cumulativamente, os seguintes requisitos, sem prejuízo de outros requisitos formais e de negócio:

- Acordo prévio entre as entidades a serem interconectadas, explicitando a forma pela qual a interconectividade será realizada e os serviços a serem providos/consumidos por meio da interconectividade;
- Cumprimento dos requisitos e medidas para a interconectividade definidos nesta Orientação Técnica, além de eventuais requisitos adicionais acordados entre as entidades cujas redes serão interconectadas;
- Definição do plano de endereçamento privativo de rede pelo Órgão do SMTIC, quando aplicável.

A competência para definir o plano de endereçamento pri-vativo de rede, incluindo as faixas de endereçamento IP e eventuais sub-redes a serem concedidas aos sites, internos ou externos, é:

- Do Integrador Estratégico, quando a interconexão envolver a RPCD. Uma vez alocado o range de endereço IP pelo Integrador estratégico para o Órgão, este terá autonomia no que diz respeito à gestão das subnets dentro do range fornecido.
- Dos respectivos Órgãos do SMTIC, sem prejuízo de eventuais acordos mútuos, quando a interconexão não envolver a RPCD, sendo que os Órgãos que possuem sites internos poderão delegar explicitamente sua competência ao Integrador Estratégico.

Sempre que necessário ou conveniente para a concretização da interconexão, o Integrador Estratégico deverá alocar um range contínuo de endereços IP para os Órgãos do SMTIC para interconexões envolvendo a RPCD.

O tamanho do range deverá ser em função da dimensão do Órgão e adequado para atender às necessidades de negócio da interconectividade, e deverá ser implementado de maneira tempestiva pelo Integrador Estratégico.

Os órgãos com sites independentes deverão, sempre que possível, coordenar com o Integrador Estratégico a alocação de novos ranges de modo a minimizar possíveis conflitos de ranges IPs entre os diversos órgãos, de modo a facilitar uma possível integração futura.

Os requisitos tecnológicos básicos de interconectividade são:

- Ter uma conexão, ou serviço de conexão, gerenciada de maneira a ter qualidade adequada para suportar os serviços que utilizarão a interconectividade.
- Implementar mecanismos de segurança de informação para restringir o acesso à interconectividade apenas aos serviços previstos e aos serviços de suporte para gestão e manutenção da conexão (vide item 7).

A qualidade da conexão, ou serviço de conexão, inclui fatores como:

- A largura de banda (bandwidth).
- A velocidade efetiva de conexão (throughput).
- A confiabilidade (perda de pacotes).

- A disponibilidade da conexão.
- A latência (demora na transmissão de dados).

O responsável técnico de TI do Órgão do SMTIC também poderá incluir análises sobre modelagem de tráfego (traffic shaping) e a priorização de tráfego, para avaliar se a qualidade de serviço (QoS – quality of service) oferecida é compatível com os requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações.

Dentre os mecanismos de segurança, o uso de uma solução de firewall controlando o tráfego no link de interconectividade é o requisito básico mínimo para a interconexão de redes quando se tratar de órgãos distintos ou entre o mesmo órgão e a RPCD, sem prejuízo dos demais mecanismos.

Apenas para a interconectividade entre dois sites internos pertencentes ao mesmo Órgão do SMTIC, o requisito acima poderá ser flexibilizado mediante análise de risco do responsável de TI do Órgão. A análise de risco deverá levar em consideração as vulnerabilidades de segurança e poderá ser feita apenas por um Órgão que esteja na Série C ou acima na Escala de Maturidade, ou por um Órgão de maturidade mais baixa, mas que tenha na sua equipe de TI um membro com capacitação formal em gestão de redes e/ou de segurança de informação.

O Integrador Estratégico é responsável pela administração do firewall da RPCD na interconexão com a mesma, sem prejuízo de disponibilização de outros ativos ou equipamentos de segurança.

Uma conexão direta de um outro site, interno ou externo, ao datacenter de um Órgão do SMTIC é uma conexão crítica em termos de Segurança da Informação. Desta forma, é necessário ter a aprovação prévia do responsável técnico de TI do Órgão do SMTIC para que ela seja realizada, e deve atender aos requisitos técnicos necessários definidos pelo Órgão gestor do datacenter.

Uma vez interconectados, por padrão os sites terão acesso aos serviços acordados.

Os Órgãos do SMTIC poderão desativar ou remover as interconectividades redundantes ou que não estejam mais em uso.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Adotar medidas de segurança adicionais para proteção física e lógica dos datacenters e demais perímetros relevantes, conforme as necessidades e capacidades técnicas do Órgão do SMTIC.
- Monitorar periodicamente os firewalls da conexão, dentro das capacidades técnicas e de pessoal do Órgão do SMTIC, visando manter o alinhamento das regras e configurações implementadas nos firewalls com as necessidades de segurança.
- Manter um inventário atualizado periodicamente (periodicidade mínima anual) acerca dos circuitos de comunicação de interconectividade, registrando no mínimo a identificação/ descrição do circuito e a sua finalidade e disponibilizando essas informações em uma área de armazenamento corporativo adequado.
- Manter registros atualizados periodicamente (periodicidade mínima anual) dos contatos das partes relevantes envolvidos na interconectividade, incluindo outros Órgãos Setoriais e fornecedores dos links físicos e lógicos de conexão e disponibilizando essas informações em uma área de armazenamento corporativo adequado.
- Adotar mecanismos para criptografar os dados trafegados pelo canal de comunicação, no caso de um ou mais Órgãos do SMTIC envolvidos na interconectividade avaliar tecnicamente que o canal é inseguro ou potencialmente inseguro.
- Estabelecer um acordo prévio sobre o rol dos serviços disponibilizados por meio da interconexão e implantar medidas de segurança de forma a cumprir o acordo, mitigando o risco de acontecer o consumo não previsto de serviços.
- Em caso de contratação de serviços de conexão, avaliar previamente a necessidade de cláusulas que tratem sobre a modelagem de tráfego (traffic shaping) e a priorização de tráfego, sempre que necessários aos requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações
- Desativar ou remover as interconectividades que não estejam mais em uso.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Considerar o uso de dois firewalls por link, um em cada borda do perímetro (ou seja, um em cada ponta do link), especialmente para comunicação por canais inseguros ou potencialmente inseguros.
- Avaliar a necessidade de ter conexões redundantes passando por rotas físicas distintas, se as necessidades de negócio indicarem a exigência de alta disponibilidade.
- Realizar uma análise prévia de risco em termos de Segurança da Informação, visando obter adequada visibilidade dos possíveis riscos e impactos negativos causados pela interconexão e traçar um planejamento para mitigá-los.
- Realizar um procedimento periódico para detectar se a interconectividade ainda é necessária, visando desativar interconectividades que não estejam mais em uso.

CONEXÃO ENTRE SITES INTERNOS E/OU RPCD DA PMSP

SOBRE CONEXÃO ENTRE SITES INTERNOS E/OU RPCD DA PMSP

O Órgão Central, com o apoio do Integrador Estratégico, e a Secretaria Municipal de Gestão poderão disponibilizar Atas de Registros de Preço que viabilizem ou ajudem a viabilizar a interconectividade, nos termos do Art. 16, do Decreto 57.653, de 07 de abril de 2017.

> Art. 16. Fica delegada ao Órgão Central, com o apoio da PRODAM, quando não efetuado pela Secretaria Municipal de Gestão, a realização de procedimento licitatório para fins de Registro de Preços para as aquisições de bens e contratações de serviços de Tecnologia da Informação e Comunicação.

A conectividade interno-interno poderá ter roteamento total entre si mediante compartilhamento de tabelas de roteamento, ou seja, poderão ter comunicação direta, se as partes assim acordarem, sem prejuízo de medidas de segurança da informação dos Órgãos envolvidos.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Para os gestores de datacenter, disponibilizar no Portal de Governança uma lista atualizada periodicamente (periodicidade mínima anual) dos requisitos técnicos necessários para a interconexão interno-interno ou interno-rpcd ao seu datacenter, excentuando as informações consideradas necessárias à segurança das informações.

CONEXÃO COM SITES EXTERNOS

SOBRE CONEXÃO COM SITES EXTERNOS

Todas as interconexões com sites externos devem ser realizadas por meio de um canal adequadamente seguro de comunicação.

Para interconexão envolvendo sites externos, a competência para definir e gerir os requisitos de infraestrutura de conexão necessários para a sua concretização, bem como a operação e configuração dos filtros e a administração das contas e senhas de acesso, é:

- Do Integrador Estratégico, quando a interconexão envolver a RPCD.
- Dos respectivos Órgãos do SMTIC, sem prejuízo de eventuais acordos mútuos, quando a interconexão não envolver a RPCD, sendo que os Órgãos que possuem sites internos dependentes poderão delegar sua competência ao Integrador Estratégico.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Segregar os acessos externos da rede corporativa de forma a evitar ou minimizar seus impactos à rede interna, incluindo medidas como atribuir uma faixa de endereçamento IP específica para os acessos oriundos de sites externos.
- Conceder acessos externos apenas a recursos disponíveis nativamente para a rede externa ou a recursos disponíveis na DMZ (demilitarized zone – zona intermediária entre a rede externa e a rede interna do Órgão).

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Se houver a necessidade real de ter acessos externos a recursos disponíveis apenas na rede interna do órgão, então avaliar a possibilidade de disponibilizar um desktop virtual ou solução similar para que o acesso se dê apenas aos recursos previstos.

REDES WI-FI E IoT

SOBRE REDES WI-FI E IoT

As redes Wi-Fi e IoT devem utilizar sistemas de tunelamento para que haja autenticação do usuário, antes da liberação da conexão, acesso e enlace. Havendo acesso à internet, o mesmo será monitorado e com controle de filtro de conteúdo, nos termos da Lei 14.098/2005.

> Art. 1º. As escolas públicas, os Centros Educacionais Unificados (CEUs), bibliotecas, postos de atendimento - Telecentro e quaisquer outros locais onde funcionem computadores da Prefeitura ligados à Internet, todos da rede pública municipal, ficam obrigados a instalar a tecnologia de filtragem de conteúdo.
>
> Parágrafo único. Sites que tenham conteúdos de sexo, drogas, pornografia, pedofilia, violência e armamento, dentre outros, a critério do Executivo, devem ser proibidos.

A rede Wi-Fi corporativa interna deverá ser segregada, física ou logicamente, da rede Wi-Fi disponibilizada ao cidadão comum (conhecida como rede guest), visando reduzir o risco de acesso indevido ao ambiente corporativo. Sugere-se estudar a viabilidade de isolamento físico e lógico da rede guest para fins de segurança da informação, através da adoção de VLANs (Rede local virtual) distintas.

A rede Wi-Fi guest poderá exigir cadastro prévio de usuário para o seu usufruto, a critério do Órgão administrador. A rede Wi-Fi corporativa interna deverá exigir autenticação do usuário, conforme acima, utilizando-se no mínimo o algoritmo WPA2.

Interconexões que contemplem serviços de IoT devem estar segregados, física e/ou logicamente, com a implementa-ção de regras que permitam apenas os serviços e usuá-rios atinentes à consecução do negócio.Os dispositivos ou sensores IoT são utilizados para detectar características do ambiente, gerando sinais de controle para atuadores e eventualmente podem trazer redução de custos, porém a utilização destes dependem de avaliação para atender necessidades específicas.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Substituir todas as senhas padrão de fábrica dos dispositivos geridos pelo Órgão do SMTIC por senhas adequadamente fortes, seguindo, sempre que aplicável, a política de senhas do Órgão.
- Desabilitar o recurso de WPS (Wi-Fi Protected Setup), para mitigar o risco de quebra das chaves de criptografia do WPA2.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Implementar processos de atualização periódica de firmware e de software para mitigar possíveis vulnerabilidades de segurança.
- Introduzir cadastro prévio de usuário para que este possa usufruir da rede Wi-Fi guest, para evitar que terceiros passem a utilizar a rede de forma corriqueira como se fosse a sua própria rede, exceto para os pontos de Wi-Fi livre.
- Estudar a conveniência de ter o mesmo usuário para autenticação, independentemente de ser rede Wi-Fi ou cabeada.
- Avaliar a precisão, custo, segurança, longevidade e conectividade no caso de implantação de uma solução envolva dispositivos ou sensores IoT.

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.

SEGURANÇA

SOBRE SEGURANÇA

A Segurança da Informação é uma questão de alta relevância para a interconectividade de redes.

Desta forma, além das diretrizes, recomendações e sugestões elencadas nos demais itens desta Orientação Técnica, requisitos adicionais de Segurança da Informação para a interconectividade, incluindo blacklists e whitelists de portas, protocolos, serviços e aplicações podem ser definidos:

- Pelos Órgãos do SMTIC para os seus respectivos sites internos.
- Pelo Integrador Estratégico, para interconectividade com a RPCD.

Além disso, esta OT traz as recomendações e sugestões abaixo, específicas sobre segurança, desde que haja mão de obra capacitada, disponibilidade orçamentária e disponibilidade da funcionalidade nos ativos pertinentes.

SEGURANÇA

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Controle de acesso físico aos equipamentos de rede e servidores.
- Todos os dispositivos críticos devem possuir backup da configuração (atualizado) apartado do equipamento de origem.
- Substituição das senhas padrão por senhas adequadamente fortes.
- Implementar, sempre que possível, a utilização do procotolo 802.1X para acesso aos sites internos e à RPCD.
- Usar soluções de firewall para criar perímetros que possibilitem melhor controle de acesso.
- Usar solução de antivírus em todas as estações e servidores windows conectados na rede, com atualização automática e periódica.
- Implementar processo periódico de instalação de patches de segurança de firmwares de dispositivos e equipamentos, bem como de softwares básicos, sistemas operacionais e aplicativos conectados na rede.
- Tomar como base a norma de segurança da informação em normas ISO 27099:2022 / ISO-IEC-27001-2013 /ISO/IEC 27010:2015.
- Atualizar periodicamente os firmware para mitigar vulnerabilidades de segurança.

SEGURANÇA

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Efetuar o controle do endereço físico do dispositivo (MAC address) vinculado à porta de acesso.
- Manter as portas sem uso nos equipamentos de rede em estado bloqueado.
- Implementar mecanismo de gestão centralizado das estações de trabalho, tais como policies do Active Directory ou similares. Este artifício tem como objetivo possibilitar gestão do ambiente computacional.
- Padronizar nomenclatura das estações de trabalho para as unidades.
- Usar sistema de prevenção de intrusão (IPS - Intrusion prevention system) para monitoração e bloqueio de tráfego suspeito (interconectividade externo-interno).
- Usar solução de firewall na camada de aplicações (WAF – web application firewall) para mitigar as vulnerabilidades de aplicações WEB publicadas na Internet.
- Usar solução contra ataques avançados baseados em comportamento.
- Usar solução de prevenção contra perda de dados.
- Bloquear todas as portas de sistema (0 a 1023) e as portas registradas (1024 a 49151), com exceção das portas necessárias para o provimento dos serviços utilizados por meio da interconectividade, bem como para a manutenção da própria interconectividade.
- Utilizar da Política Nacional de Segurança da Informação - PNSI para descritivo de um plano ou sugestão de segurança da informação, em atendimento ao Decreto Nº 9.637, de 26 de Dezembro de 2018.

PLANO DE RESPOSTA A INCIDENTES

SOBRE PLANO DE RESPOSTA A INCIDENTES

Em caso de surgimento de incidente com impacto na segurança do site interno ou da RPCD por causa da interconexão de redes, deverão ser tomadas ações que minimizem os riscos para a segurança da rede como um todo, mitiguem os danos já causados e evitem o causamento de novos danos.

A competência para executar medidas de proteção, mitiga-ção e contenção do dano, independente do contato prévio com outras redes, incluindo a eventual desconexão física da rede, é:

- Do Integrador Estratégico, para a interconectividade envol-vendo a RPCD.
- Dos respectivos Órgãos do SMTIC, para interconectividade que envolvam os respectivos sites internos e não envolvam a RPCD.

Em caso de ações que alterem a interconexão de alguma forma, como por exemplo a desconexão ou a aplicação de políticas mais restritivas de tráfego, o Órgão executor da ação deverá informar tempestivamente os demais Órgãos afetados, preferencialmente por meio eletrônico.

Em caso de incidentes que transcendam os limites de um site interno e/ou da RPCD, o Órgão Central deverá ser informado da ocorrência do incidente, bem como do andamento da sua resolução, de maneira tempestiva e através de meio adequado em relação à urgência do incidente.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Ter um mapeamento de risco e um plano de resposta a incidentes atualizados periodicamente, de forma que possa se ter uma resposta adequada e tempestiva em caso de incidentes de segurança.

DOCUMENTAÇÃO

SOBRE DOCUMENTAÇÃO

A documentação relativa à interconexão, bem como as informações para suporte técnico devem ser periodicamente revisadas e atualizadas para cada site interno e/ou RPCD.

A extensão e profundidade da documentação, bem como a periodicidade da revisão são definidas pelo corpo técnico de TI do respectivo Órgão responsável, mas podem incluir documentos como: topologias de rede relativas à interconexão, lista das interfaces ativas para a interconexão e as portas liberadas e o plano de resposta a incidentes.

RESOLUÇÃO DE DIVERGÊNCIAS

SOBRE RESOLUÇÃO DE DIVERGÊNCIAS

Em caso de reiteradas divergências sobre um mesmo tema, o Órgão Central é a instância de resolução inter partes. O Órgão Central poderá revisar esta Orientação Técnica para incluir a resolução e torná-la com efeito *erga omnes*[1] após aprovação do CMTIC.

> erga omnes[1]: do Latim, contra, relativamente a, frente a todos.

QUANDO AS RECOMENDAÇÕES PASSAM A VALER?

SOBRE QUANDO AS RECOMENDAÇÕES PASSAM A VALER?

Os procedimentos descritos nesta Orientação Técnica deverão ser aplicados nos procedimentos atuais e futuros, bem como nos contratos futuros e nas prorrogações con-tratuais, ainda que de contratos assinados antes do início da vigência desta OT.

Esta Orientação Técnica entrará em vigor a partir da sua aprovação pelo CMTIC.

REFERÊNCIAS

SOBRE REFERÊNCIAS

Link: https://www.cisco.com/c/pt_br/solutions/enterprise-networks/sd-wan/what-is-sd-wan.html#~why-now
Visitado em: 23/03/2026

Link: https://pt.wikipedia.org/wiki/SD-WAN
Visitado em: 23/03/2026

Link: https://technet.microsoft.com/en-us/library/cc773178(v=ws.10).aspx
Visitado em: 23/03/2026

Link: http://www.techrepublic.com/article/10-things-you-should-know-about-ad-domain-trusts/
Visitado em: 23/03/2026

Link: https://www.juniper.net/br/pt/research-topics/sd-wan-explained.html
Visitado em: 23/03/2026

Link: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm
Visitado em: 23/03/2026

Link: http://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2025/Decreto/D12572.htm
Visitado em: 23/03/2026