



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL FLUMINENSE
REITORIA
RUA CORONEL WALTER KRAMER, Nº 363, PARQUE SANTO ANTONIO, CAMPOS DOS GOYTACAZES / RJ, CEP 28080-565
Fone: (22) 2737-5600

INSTRUÇÃO NORMATIVA DGTIREIT/IFFLU Nº 1, DE 1 DE FEVEREIRO DE 2024

A DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO DA REITORIA DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA FLUMINENSE - IFFLUMINENSE, no uso das atribuições legais que lhes são conferidas.

CONSIDERANDO:

- A Política de Segurança da Informação e Comunicação do IFFluminense (POSIC) - Portaria N.º 1767, de 6 de dezembro de 2018;
- A Portaria Nº 852 de 1 de Setembro de 2023 que instituiu o Grupo de Trabalho na Câmara de TIC para revisão e atualização das normas da Infraestrutura de rede do Instituto Federal Fluminense
- Reunião da Câmara de TIC realizada no dia 19 de Dezembro de 2023 onde foi apresentado o resultado do trabalho do Grupo de Trabalho de revisão e atualização das normas da Infraestrutura de redes do Instituto Federal Fluminense

RESOLVE:

CAPÍTULO I

DOS OBJETIVOS

Art. 1º A presente instrução normativa, no âmbito do Instituto Federal Fluminense, estabelece orientações quanto a padronização da infraestrutura de rede, a fim de assegurar que todas as unidades do instituto utilizem os mesmos mecanismos de controle e segurança de redes e possam prover, com níveis similares de qualidade e confiabilidade, serviços de TIC inerentes à referida infraestrutura.

Parágrafo único. Esta instrução normativa deve ser revisada bianualmente ou sempre que houver alguma mudança significativa na infraestrutura de rede do instituto, por meio da formação de um grupo de trabalho multicampi designado para esse fim.

CAPÍTULO II

DA REDE FÍSICA

Art. 2º Estabelece-se que a rede das unidades do IFFluminense deva ser isolada fisicamente ou logicamente (por meio de VLANs), mantendo-se separadas as redes administrativas, acadêmicas (laboratórios) e de acesso livre.

Art. 3º Dispositivos “embarcados” devem estar isolados fisicamente ou logicamente das VLANs supracitadas.

Parágrafo único. Ativos tais como **switches**, DVR, câmeras, impressoras e/ou **scanners** e **access point** podem estar em uma única VLAN ou distribuídos em VLANs específicas.

Art. 4º Considerando as redes de acesso livre (para alunos e/ou visitantes), tendo as mesmas **firewall** dedicado ou não, o tráfego proveniente dessas redes não será roteado para outras redes e/ou unidades do IFFluminense, ficando apenas liberado para acesso à internet.

Art. 5º Para situações não previstas neste documento, outras VLANs podem ser criadas a critério do setor de TIC dos campi.

CAPÍTULO III

DA REDE LÓGICA

Seção I

Dos Links

Art. 6º As unidades do IFFluminense deverão dispor de um link principal (prioritário) fornecido pela RNP para acesso à rede mundial de computadores, provido de velocidade síncrona e com IPs públicos (com quantidade de acordo com cada campus), sendo suas subredes do bloco 200.143.198.0/24.

Art. 7º A Reitoria e os campi também contarão com um link secundário, licitado pelo Instituto Federal Fluminense, objetivando a redundância no acesso à internet para suas unidades e aos serviços sistêmicos hospedados no **data center** institucional.

Seção II

Do Balanceamento e Redundância

Art. 8º No caso de queda do link principal, o link secundário será utilizado até que o principal seja restabelecido.

Parágrafo único. Para que não ocorra ociosidade quanto à utilização do link secundário, o mesmo servirá de balanceamento ao link principal.

Art. 9º Sistemas hospedados no Serpro e que são utilizados pelos setores administrativos do IFF devem ter saída prioritária pelo link secundário. Os blocos podem ser atualizados consultando o endereço http://bgp.he.net/AS10954#_prefixes, e são os seguintes:

I - 161.148.0.0/16;

II - 189.9.0.0/16; e

III - 200.198.192.0/18.

Seção III

Do Endereçamento Privado

Art. 10. Os campi devem ter sua respectiva documentação de rede e devem mantê-la atualizada. A documentação básica pode ser acessada, mediante login e senha do sistema OTRS, em [https://centraldeservicos.iff.edu.br/otrs/index.pl?Action=AgentFAQExplorer;CategoryId=146;Nav=.](https://centraldeservicos.iff.edu.br/otrs/index.pl?Action=AgentFAQExplorer;CategoryId=146;Nav=)

Art. 11. As redes destinadas a visitantes devem possuir o padrão 10.XX3.0.0/16.

CAPÍTULO IV

DA AUTENTICAÇÃO

Seção I

Do DNS e Subdomínios

Art. 12. Cada unidade deverá utilizar como domínio da sua rede local o subdomínio <campus>.iffuminense.edu.br para todos os serviços, como o de diretórios, DHCP, DNS etc.

Parágrafo único. Para serviços web externos é possível a delegação da zona <campus>.iff.edu.br, entretanto, para que seja possível, o campus deve disponibilizar um servidor DNS com IP público.

Seção II

LDAP

Art. 13. Para a autenticação das redes, será utilizada a base LDAP do idIFF, por meio do conjunto CPF/senha.

§ 1º Destaca-se que a base LDAP do idIFF faz parte do Serviço da RNP Comunidade Acadêmica Federada (CAFe), a fim de possibilitar o acesso dos servidores do IFFluminense às redes de outros órgãos participantes do projeto eduroam e ao Portal de Periódicos da CAPES.

§ 2º A referida base pode, ainda, ser replicada para servidores samba4, para que exista uma base de autenticação localizada em cada unidade do instituto, evitando, com isso, que um servidor tenha que se cadastrar em vários campi.

§ 3º Cada unidade que desejar utilizar seu próprio domínio deverá usar o padrão <campus>.iffuminense.edu.br.

§ 4º A documentação para implantação e operação do serviço Domínio Unificado está disponível, mediante login e senha do sistema OTRS, em <https://centraldeservicos.iff.edu.br/otrs/index.pl?Action=AgentFAQExplorer;CategoryID=52;Nav=>.

Seção III

Controles de Gestão de Acesso

Art. 14. O controle de acesso de usuários deve ser feito por controlador(es) de domínio(s), conforme descrito na seção anterior.

Parágrafo único. Todos os controladores de domínio e servidores de autenticação devem estar informados no documento em <https://centraldeservicos.iff.edu.br/otrs/index.pl?Action=AgentFAQExplorer;CategoryID=150;Nav=>, acessível por login e senha do sistema OTRS.

Seção IV

DHCP

Art. 15. Para máquinas institucionais, tanto as de uso administrativo quanto as de uso acadêmico, as mesmas devem estar cadastradas num servidor DHCP por meio do seu endereço físico (endereço MAC). Já o acesso de outros dispositivos deve ser autenticado via 802.1x ou via autenticação web (**hotspot**), evitando assim que máquinas não autorizadas obtenham endereços IP.

CAPÍTULO V

DAS REDES SEM FIO

Art. 16. Para evitar o cadastramento dos usuários e a reconfiguração dos dispositivos, serão utilizadas apenas as redes especificadas a seguir:

I - wIFF: rede para servidores autenticada via idIFF - WPA2 **Enterprise**;

II - wIFF_administrativa: rede WPA2 PSK oculta para equipamentos institucionais que não estão próximos à rede cabeada;

III - wIFF_visitantes: rede para visitantes com autenticação via **voucher** gerado pela controladora ou **OpenSystem** em conjunto com **captive** portal;

IV - wIFF_academica: rede para alunos autenticada via idIFF, utilizando WPA2 **Enterprise**; e

V - eduroam: rede para visitantes de outras instituições que participam do projeto - WPA2 Enterprise (utiliza servidor radius do projeto).

Art. 17. Para a rede wIFF recomenda-se utilizar o domínio integrado ao idIFF e implementar um radius próprio.

Parágrafo único. Também é possível utilizar o radius da Reitoria, porém em caso de queda do IPSEC a rede não irá autenticar.

Art. 18. As redes sem fio de acesso livre (para alunos ou visitantes), conforme política de acesso da rede cabeada (Capítulo II), devem ter seu tráfego isolado fisicamente ou logicamente (por VLANs), e ter apenas saída para a internet.

CAPÍTULO VI

DO FIREWALL

Art. 19. A liberação de tráfego, tanto de entrada quanto de saída, deve seguir os padrões especificados no documento “Documentação da Rede IFF”, disponível em <https://centraldeservicos.iff.edu.br/otrs/index.pl?Action=AgentFAQZoom;ItemID=312;Nav=>, com acesso através do login e da senha do sistema OTRS.

Parágrafo único. O **framework** utilizado para este controle será o pfSense®.

CAPÍTULO VII

ENDEREÇAMENTO IPV4 E IPV6 PÚBLICO

Art. 20. Os endereços públicos, tanto IPv4 quanto IPv6, para endereçamento WAN e DMZ, devem seguir o especificado no documento “Documentação da Rede IFF”, disponível em <https://centraldeservicos.iff.edu.br/otrs/index.pl?Action=AgentFAQZoom;ItemID=312;Nav=>, mediante login e senha de acesso ao sistema OTRS.

CAPÍTULO VIII

GESTÃO DE REGISTROS DE AUDITORIA

Art. 21. O controle de log deve ser centralizado, por campus, utilizando o **framework** Graylog e deve seguir a política de retenção de logs do instituto. Para garantir a sincronização de hora desses logs, serão utilizados os servidores NTP da Reitoria conforme a documentação disponível em <https://centraldeservicos.iff.edu.br/otrs/index.pl?Action=AgentFAQZoom;ItemID=312;Nav=>, acessível através do login e da senha do sistema OTRS.

CAPÍTULO IX

DAS DISPOSIÇÕES FINAIS

Art. 22. Os procedimentos complementares relativos à padronização da infraestrutura de rede do IFFluminense devem estar harmonizados com as demais disposições desta instrução normativa.

Art. 23. Esta instrução normativa entra em vigor na data de sua publicação.

Documento assinado eletronicamente por:

- **Ronaldo Amaral Santos, DIRETOR(A) - CD3 - DGTIREIT, DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO**, em 01/02/2024 15:44:08.

Este documento foi emitido pelo SUAP em 01/02/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse <https://suap.iff.edu.br/autenticar-documento/> e forneça os dados abaixo:

Código Verificador: 523179

Código de Autenticação: e9dfea20cc

