EBSERH
HOSPITAIS UNIVERSITÁRIOS FEDERAIS

Empresa Brasileira de Serviços Hospitalares

GT – Padrão de redes

Daniel da Silva Farias (Sede)
Brunner Salgado Martins (HUCAM)
Deive Correa Lima (HCTM)
Helton Carlos Lima Godoy (HUJM)
Leandro Marcel Freitas e Santos (HUGD)
Paulo Henrique de Assis (HU-UFJF)

JULHO DE 2018

SUMÁRIO

NORMA OPERACIONAL DE PADRÃO DE REDES

Regulamenta a padronização da infraestrutura de redes lógica, Plano de Infraestrutura Lógica da Rede de Computadores - PILRC-EBSERH, no âmbito da EBSERH.

O Diretor de Administração e Infraestrutura da Empresa Brasileira de Serviços Hospitalares - EBSERH, no uso das atribuições que lhe são conferidas pelo inciso I do artigo 45 do 2º Regimento Interno, aprovado na 30º reunião do Conselho de Administração, realizada no dia 26 de novembro de 2014, resolve:

CAPÍTULO I - DAS DISPOSIÇÕES PRELIMINARES

SEÇÃO 1: DO OBJETIVO E DA APLICAÇÃO

Art. 1º. A presente Norma Operacional tem como objetivo regulamentar e implementar o **Plano de Infraestrutura Lógica da Rede de Computadores - PILRC-EBSERH**, no âmbito da EBSERH.

§ 1º. De acordo com o mapa estratégico da EBSERH, 02 (dois) dos objetivos habilitadores da empresa tratam sobre viabilizar a infraestrutura física e tecnológica necessária para o funcionamento dos Hospitais Universitários Federais - HUF's, que fazem parte da rede EBSERH, e implementar soluções de TI para gestão da EBSERH.

Parágrafo único: A EBSERH objetiva definir esses padrões e conceitos relacionados ao seu ambiente tecnológico a fim de garantir a difusão dessas informações e definições em toda a sua rede de hospitais e na sede.

§ 2º. A melhoria contínua proposta para os hospitais está diretamente relacionada com a gestão da TIC e da Segurança da Informação (SI). A padronização proporcionará um alinhamento dos hospitais com as estratégias da SEDE e uma organização para implementação de novas tecnologias para reestruturação da rede computacional.

§1º. O PILRC-EBSERH faz parte da estratégia da EBSERH da implantação da Rede de Gestão do Hospitais Universitários (RGHU) em cada um dos HUF´s sob gestão dela.

Art. 2º. As definições estabelecidas nesse documento deverão ser aplicadas e implementadas por todas as unidades da EBSERH.

Art. 3º. O PILRC-EBSERH faz parte do **ANEXO I** a esta norma operacional.

SEÇÃO 2: DA VIGÊNCIA E ATUALIZAÇÃO

Art. 4º. Esta Norma Operacional tem vigência por prazo indeterminado.

Art. 5º. Este documento entra em vigor a partir da data de sua publicação e deve ser revisto em intervalos planejados, não excedendo o prazo de 12 (doze) meses a partir de sua data de publicação ou em caso de ocorrência de algumas das condições obrigatórias de atualização do documento.

Art. 6º. Condições obrigatórias de atualização do documento:

I. surgimento ou alteração de leis e/ou regulamentações vigentes;

II. mudança estratégica da instituição;

III. expiração da data de validade do documento;

IV. mudanças de tecnologia na organização; ou

V. a partir dos resultados das análises de riscos realizadas pela EBSERH que venham a impactar/provocar necessária mudança nesse normativo para readequação da empresa aos riscos encontrados (mitigação).

SEÇÃO 3: DAS DEFINIÇÕES

Art. 7º. Para efeitos desta Norma Operacional, foram adotadas as seguintes definições:

I. **AD (***Active Directory***)**: é uma implementação de serviço de diretório no protocolo LDAP que armazena informações sobre objetos em rede de computadores e disponibiliza essas informações a usuários e administradores desta rede. É um software da Microsoft utilizado em ambientes Windows, presentes no ***active directory***;

II. **LDAP (***Lightweight Directory Access Protocol***)**: é um protocolo de aplicação aberto, livre de fornecedor e padrão de indústria para acessar e manter serviços de informação de diretório distribuído sobre uma rede de Protocolo da Internet (IP);

III. **CDC (***Container Data Center***):** são data centers modulares. Ao invés de construir enormes instalações para acomodar ***racks*** de servidores e ***storage*** usa-se o container como um modulo completo de processamento. Sua expansão é simples, basta adicionar mais módulos quando necessário. Os containers podem ser empilhados, otimizando o espaço do prédio;

IV. **COBIT 5 (***Control Objectives for Information and Related Technology***) - Versão 5**: é um guia de boas práticas apresentado como ***framework***, dirigido para a gestão de tecnologia de informação (TI). Mantido pelo ISACA ***(Information Systems Audit and Control Association***), possui uma série de recursos que podem servir como um modelo de referência para gestão da TI, incluindo um sumário executivo, um ***framework***, objetivos de controle, mapas de auditoria, ferramentas para a sua implementação e principalmente, um guia com técnicas de gerenciamento;

V. **IP** *(Internet Protocol)*: endereço IP, de forma genérica, é uma identificação de um dispositivo (computador, impressora, etc) em uma rede local ou pública. Cada computador na internet possui um IP ***(Internet Protocol*** ou Protocolo de internet) único, que é o meio em que as máquinas usam para se comunicarem na Internet;

VI. **IPS** *(Intrusion Prevent System)*: é um sistema, similar ao IDS (***Intrusion Detection System***), voltado para a prevenção de ataques a redes de computadores. A diferença básica entre um IPS e um IDS é que o primeiro, além de detectar um tráfego anômalo, é capaz de tratá-lo;

VII. **ITIL v3** *(Information Technology Infrastructure Library)* - Versão 3: é o ***framework*** para gerenciamento de serviços de TI (ITSM) mais adotado mundialmente. A utilização das melhores práticas contidas na ITIL V3 (versão atual) ajuda as organizações a atingirem seus objetivos de negócio utilizando apropriadamente os serviços TI;

VIII**. NBR ISO/IEC** *(International Organization for Standardization)*: é a sigla de Norma Brasileira aprovada pela ABNT, de caráter voluntário, e fundamentada no consenso da sociedade. Torna-se obrigatória quando essa condição é estabelecida pelo poder público;

IX. **POSIC (Política de Segurança da Informação e Comunicação)**: é um documento aprovado pela autoridade responsável pela EBSERH, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da Segurança da Informação e Comunicações;

X. **RGHU (Rede de Gestão de Hospitais Universitários)**: rede de dados viabilizada pela RNP, que tem o objetivo de interligar as unidades hospitalares da rede EBSERH e a sede;

XI. **RNP (Rede Nacional de Pesquisa)**: é uma organização social que provê a integração global e a colaboração apoiada em tecnologias de informação e comunicação para a geração do conhecimento e a excelência da educação e da pesquisa;

XII. **SSL (***Secure Socket Layer***)**: é um padrão global em tecnologia de segurança desenvolvida pela Netscape em 1994. Ele cria um canal criptografado entre um servidor web e um navegador (***browser***) para garantir que todos os dados transmitidos sejam sigilosos e seguros.

XIII. **VPN (***Virtual Private Network***)**: é uma sigla, em inglês, para "Rede Virtual Privada" e que funciona criando uma rede de comunicações entre computadores e outros dispositivos que têm acesso restrito a quem tem as credenciais necessárias.

CAPÍTULO II - A QUEM SE DESTINA

Art. 8º. Destina-se a toda estrutura da EBSERH (sede e HUF´s) que possuam rede de computadores e/ou equipamentos que precisem trabalhar com o protocolo IP.

Parágrafo único: Todos os equipamentos que possuam comunicação de dados, tanto através de rede cabeada, quanto através da rede wifi, deverão seguir obrigatoriamente as definições dessa norma.

Art 9º. É obrigação do Gestor de TI, tanto da sede como dos HUF´s seguirem e implementarem obrigatoriamente o processo de padronização da rede lógica da EBSERH.

Art. 10º. Não será permitida a mudança no escopo definido para o plano de infraestrutura lógica da rede de computadores da EBSERH-Sede e suas filiais (PILRC-EBSERH).

CAPÍTULO III - DAS DEFINIÇÕES DO DOCUMENTO

Art. 11º. O documento orientador para a implantação do PILRC-EBSERH, pode ser acessado através do link: http://sape.ebserh.gov.br/projects/normatizacao-da-padronizacao-da-rede-logica-da-ebserh.

Art. 12º. O acesso ao documento será controlado por motivos de segurança. Somente os Gestores de TI e a equipe responsável pela implantação e implementação poderão ter acesso aos mesmos, assim como a equipe do **Serviço Orientado ao Usuário (CSOU)** que ficará a cargo de atualizar a documentação.

Parágrafo único: Caso haja necessidade de acesso ao referido documento, deverá ser solicitado formalmente, ao Coordenador de Infraestrutura e Segurança de TI (CISTI) para que possa ser liberado.

Art. 13º. A revisão do PILRC-EBSERH ficará a cargo do CSOU que juntamente com a equipe deverá rever, modificar, eliminar ou acrescentar alterações no documento.

Art. 14º. Toda alteração do documento deverá ser informada pelo Diretor de Gestão de Processos e Tecnologia da Informação (DGPTI) a todos os gestores responsáveis pela implementação do PILRC-EBSERH na sua respectiva unidade.

Art. 15º. O acesso ao PILRC-EBSERH por pessoal terceirizado deverá ser feito somente após a ciência do Termo de Sigilo e Confidencialidade, garantindo a não violabilidade das informações do documento.

Parágrafo único: Caso o terceirizado ou a empresa terceirizada não tenha assinado o Termo de Sigilo e Confidencialidade, o Gestor de TI da unidade deverá providenciar imediatamente a assinatura do documento em 2 (duas) vias, sendo que uma fica com o Gestor de TI da unidade e a outra com o prestador do serviço.

CAPÍTULO IV - DA UTILIZAÇÃO DO SERVIÇO

Art. 16º. A padronização da rede deve ser executada em toda estrutura local que tenha necessidade de acesso à rede de dados, tanto interna como externa da EBSERH.

Art. 17º. Somente pessoal autorizado poderá alterar qualquer parâmetro de configuração definido pela PILRC-EBSERH.

§ 1º. O pessoal autorizado a alterar parâmetros de rede será definido pelo gestor de TI local;

§ 2º. Qualquer necessidade de alterar parâmetros de rede lógica, o usuário deverá contatar a área de TI local e solicitar o serviço;

§ 3º. Obrigatoriamente, cada divisão da rede e endereçamento estabelecido no PILRC-EBSERH deve ser seguido, e não serão aceitas alterações ou adaptações aos ditames estabelecidos.

Parágrafo único: Casos especiais devem ter autorização expressa do Gestor de TI local e anuência da DGPTI, toda alteração revisada, documentada e guardada para consultas futuras.

CAPÍTULO V - DAS COMPETÊNCIAS

Art. 18º. O CSOU é responsável pela manutenção da PILRC-EBSERH atualizada.

Art. 19º. Compete ao CSOU:

I. rever, modificar, eliminar ou acrescentar alterações no documento do PILRC-EBSERH;

II. orientar as equipes dos HUF´s sobre a utilização do documento;

III. orientar as equipes dos HUF´s sobre a implementação dos parâmetros definidos na PILRC-EBSERH, em caso de dúvidas;

IV. o acompanhamento da adequada implantação do definido no PILRC-EBSERH;

V. controlar e verificar a implantação do PILRC-EBSERH garantindo sua interoperabilidade juntamente com a sede e demais HUF´s.

Art. 20º. Aos gestores de TI de cada unidade:

I - obedecer às determinações do PILRC-EBSERH;

II - zelar pelo uso correto da estrutura de rede lógica, evitando que a utilização errada cause indisponibilidade local ou até remota, por duplicidade de endereçamento;

III - zelar pela segurança do documento, não devendo disponibilizar para pessoas que não tem e guarda do aparelho, bem como prestar as informações e os esclarecimentos que lhes forem solicitados relacionados com as despesas decorrentes da utilização dos serviços.

Art. 21º. Ao colaborador envolvido nos procedimentos descritos nessa norma não é dado o direito de desconhecimento, devendo seguir rigorosamente o que é definido.

Art. 22º. A inobservância dessas regras acarretará a apuração das responsabilidades funcionais na forma da legislação em vigor, podendo haver responsabilização penal, civil e administrativa.

CAPÍTULO VI - DAS DISPOSIÇÕES FINAIS

Art. 23º. É obrigação do Gestor de TI seguir as especificações do PILRC-EBSERH.

Art. 24º. Deverá o Gestor de TI local verificar se sua estrutura está aderente ao PILRC-EBSERH. Qualquer não conformidade deverá ser imediatamente corrigida.

Art. 25º. Os casos omissos e não cobertos pelas orientações emanadas por esta norma serão resolvidos pela DGPTI.

Art. 26º. Revogam-se as disposições em contrário.

ANEXO I - PROCEDIMENTO PARA PADRONIZAÇÃO DA REDE LÓGICA DA EBSERH

1. INTRODUÇÃO

A Empresa Brasileira de Serviços Hospitalares (EBSERH), empresa pública vinculada ao Ministério da Educação e Cultura (MEC), tem como missão aprimorar permanentemente a gestão dos Hospitais Universitários Federais

(HUF's) para prestarem atenção de qualidade à saúde no âmbito do Sistema Único de Saúde (SUS) e fornecerem um cenário de prática adequado ao ensino e pesquisa para docentes e discentes.

As empresas do século XXI utilizam no seu cotidiano as ferramentas da Tecnologia da Informação e Comunicação (TIC) e da mobilidade tecnológica como meio fundamental para produzir resultados positivos agregando valor para o seu negócio. Logo, surge a necessidade de aderir novos modelos de decisão para realizar um alinhamento estratégico entre negócio e TI, incorporando assim as boas práticas de mercado de gestão e governança.

De acordo com o mapa estratégico da EBSERH 2015-2016, 02 (dois) dos objetivos habilitadores da empresa tratam sobre viabilizar a infraestrutura física e tecnológica necessária para o funcionamento dos HUF's e implementar soluções de TI para gestão da EBSERH. Sendo assim, a melhoria contínua proposta para esses hospitais está diretamente relacionada com a gestão da TIC e da Segurança da Informação (SI).

Em suma, a EBSERH está focada em aperfeiçoar a gestão dos hospitais que fazem parte da sua rede, porém, para isso, é necessário definir padrões e conceitos relacionados ao seu ambiente tecnológico a fim de difundir essas informações a toda a sua rede de hospitais. Por fim, essa padronização proporcionará um alinhamento dos hospitais com as estratégias da SEDE e uma organização para implementação de novas tecnologias para reestruturação da rede computacional.

Nos capítulos abaixo, serão apresentados padrões, definições e conceitos de tecnologias relacionadas à rede de dados, bem como conhecimentos fundamentais envolvidos na comunicação entre computadores e equipamentos de rede. Será realizada uma revisão bibliográfica das tecnologias da área de rede, trazendo citações e conteúdo para contextualizar, qualificar e embasar essa documentação e toda rede computacional da EBSERH.

2. CONTEXTUALIZAÇÃO

O presente procedimento para padronização da rede lógica foi baseado no trabalho realizado por servidores do Hospital Universitário do Maranhão (HUMA), Hospital Universitário de Grande Dourados (HUGD), Hospital Universitário de Santa Maria (HUSM) e da EBSERH-Sede.

O plano de infraestrutura lógica faz parte da estratégia da empresa pública de implantação da Rede de Gestão do Hospitais Universitários (RGHU) em cada hospital universitário sob gestão da EBSERH.

3. PLANO DE ARQUITETURA LÓGICA

Com base nos levantamentos do cenário atual e na definição de necessidades deverá ser elaborado um planejamento que contemple uma organização global do ambiente de TIC da EBSERH e suas filiais, considerando-se as seguintes premissas em seu desenvolvimento:

• Contemplar crescimento futuro, garantindo uma arquitetura escalável;

• Disponibilidade, prevendo redundâncias lógicas adequadas que visem a alta disponibilidade dos serviços prestados;

• Segurança, prevenindo contra ameaças a confidencialidade, disponibilidade e integridade dos dados e sistemas providos; e

• Organização e padronização, visando redução de complexidade e agilidade em qualquer tipo de ação de TIC.

O resultado irá consistir em um documento que contenha todas as regras, definições, políticas e/ou metodologias que deverão ser adotadas no ambiente de TIC da EBSERH e suas filiais. Servirá como um documento norteador para as soluções tecnológicas adotadas pela empresa.

Para elaboração do Plano de Arquitetura Lógica, deverão ser levados em consideração os documentos técnicos e as boas práticas de mercado, devidamente referenciados no documento de detalhamento das tecnologias adotadas.

3.1. OBJETIVOS DO PLANO DE ARQUITETURA LÓGICA

O objetivo deste plano, é relatar o modo de funcionamento de cada HUF dentro da Rede de Gestão de Hospitais Universitários (RGHU), provendo alta disponibilidade e redundância dos ativos e serviços.

Para atender esta premissa, a arquitetura lógica da rede RGHU será estruturada em IP's privados, utilizando o bloco 10.0.0.0/8. Cada HUF será estruturado com 02 (dois) blocos 10.X.X.X/16, sendo um bloco par e outro ímpar. Todos os HUF's e a EBSERH-Sede farão parte de uma rede privada a ser estabelecida sobre a infraestrutura da Rede Nacional de Pesquisa (RNP), conforme contrato. Inicialmente a rede será

implementada sobre o protocolo IPv4, no entanto, deve-se prepará-la para futuramente suportar o protocolo IPv6.

Recomenda-se em cada HUF a utilização de link redundante para suportar o acesso à Internet em caso de falha na rede RGHU. O Setor de Gestão de Processos e Tecnologia da Informação (SGPTI) deverá juntamente com a equipe de Governança de cada HUF's, prover um link redundante. A rede interna deverá ser constituída de:

• Comutadores de núcleos redundantes;

• Enlaces internos entre racks redundantes (anel) sobre um comutador diferente daquele conectado ao comutador de núcleo;

• Comutadores de núcleo e distribuição configurados e com suporte à prevenção de loops na rede;

• Firewall com alta disponibilidade/redundância para conexão com a Rede RGHU, com o link redundante e com os comutadores de núcleo; e

• Os comutadores que suportarão a rede de servidores, deverão ser constituídos de um empilhamento de 02 (dois) ou mais comutadores, sendo que a conexão com os servidores deverá estar configurada sobre um Link Aggregation de portas ou algum outro mecanismo ativo-passivo entre 02 (duas) ou mais interfaces dos servidores.

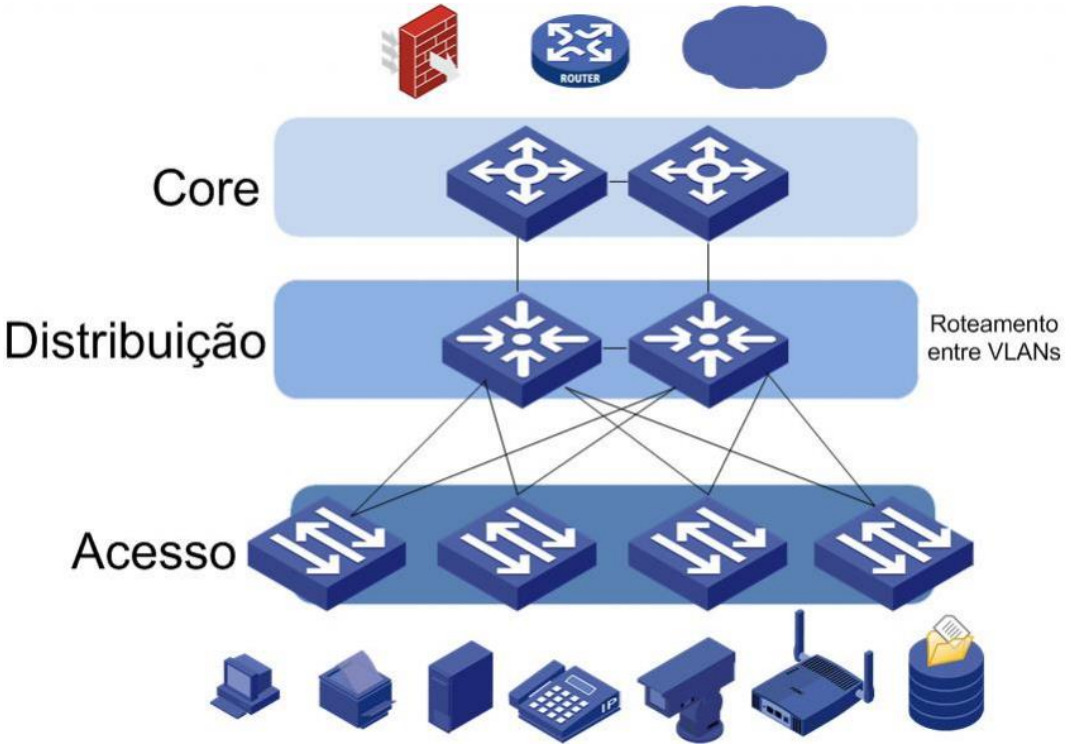


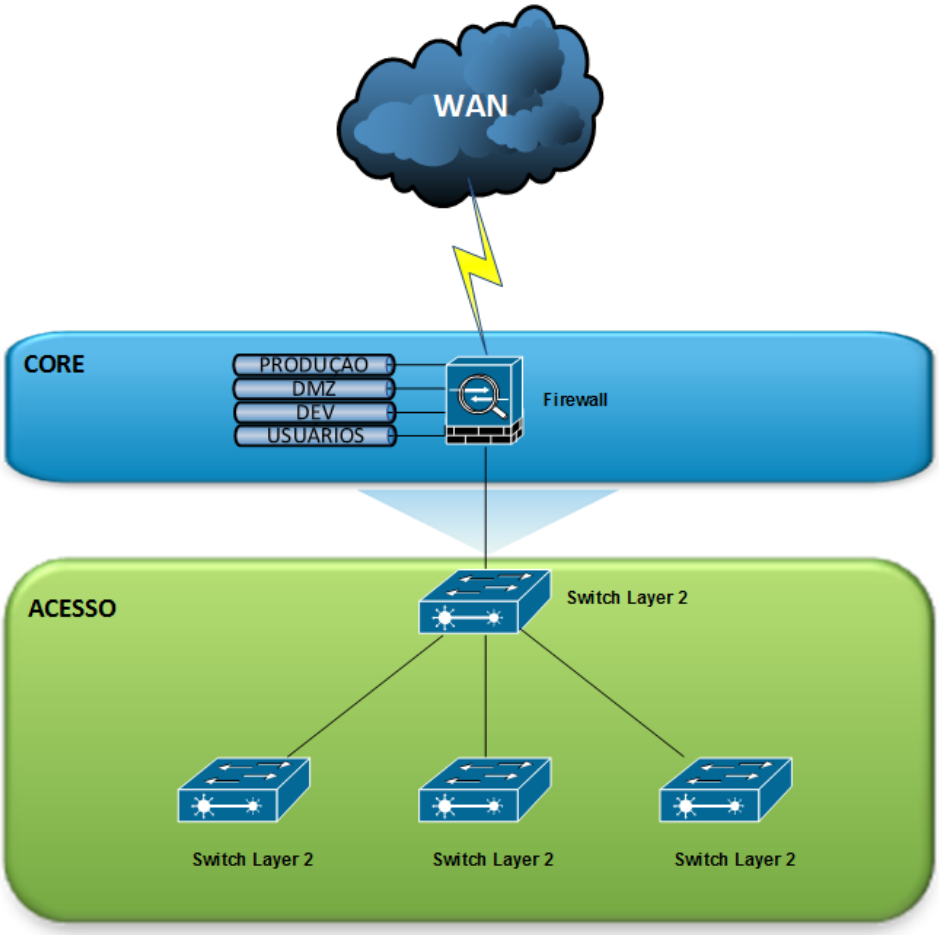
Figura: Switches core, distribuição e acesso.

Sugere-se que seja utilizado um único ativo com no mínimo essas funcionalidades. O Firewall/IPS/Controle de Acesso, devem ser configurados conforme a Política de Segurança da Informação e Comunicação (POSIC) vigente. A configuração dos ativos deverá ser mantida de acordo com a Política de Backup, assim como toda documentação deve seguir o modelo de documentação proposto neste projeto.

Para redundância no caso do hospital possuir provedor que não seja a RNP, pode ser configurado para em caso de indisponibilidade da rede RGHU o estabelecimento da VPN com a sede seja automático.

3.1.1 INFRAESTRUTURA BÁSICA

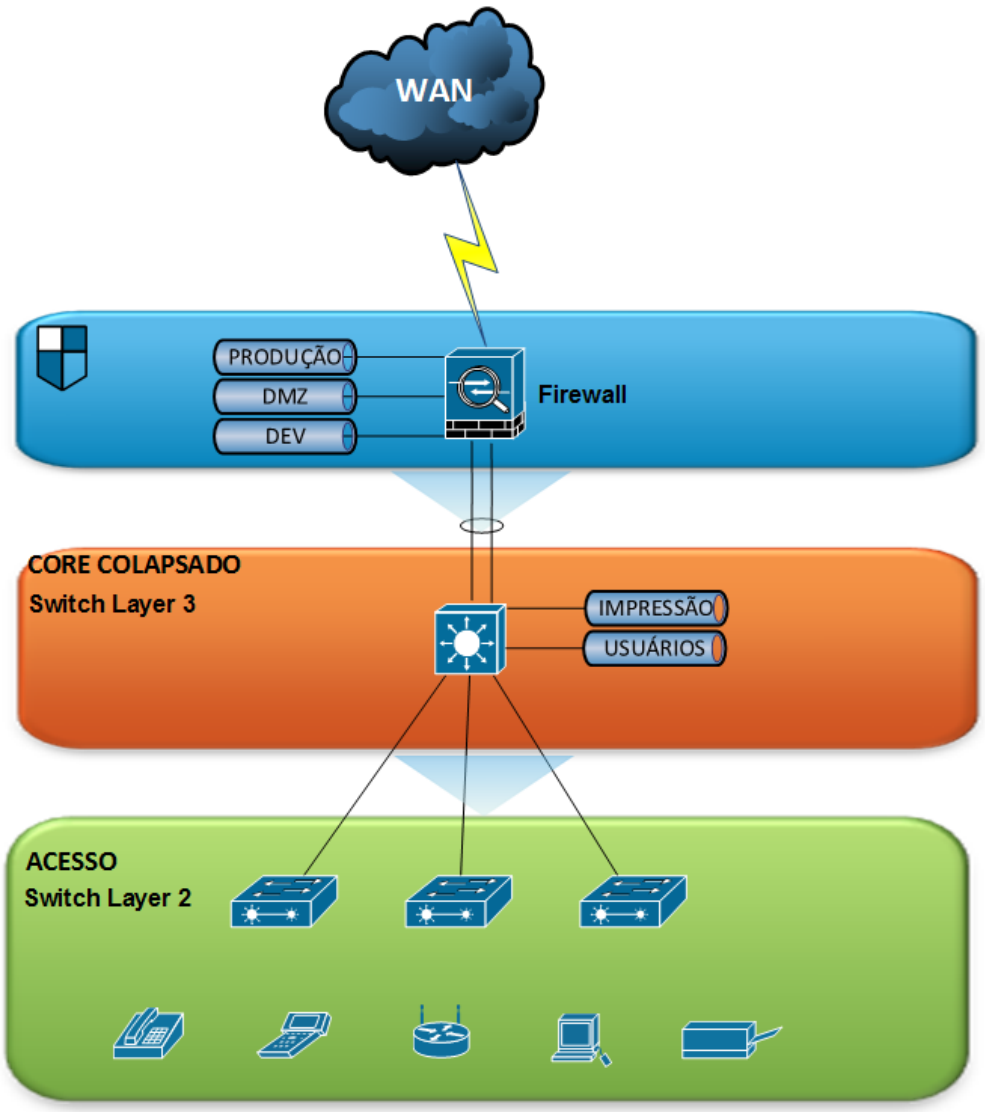
Para os hospitais que não contam ainda com infraestrutura adequada, sugere-se a adoção da arquitetura demonstrada abaixo.



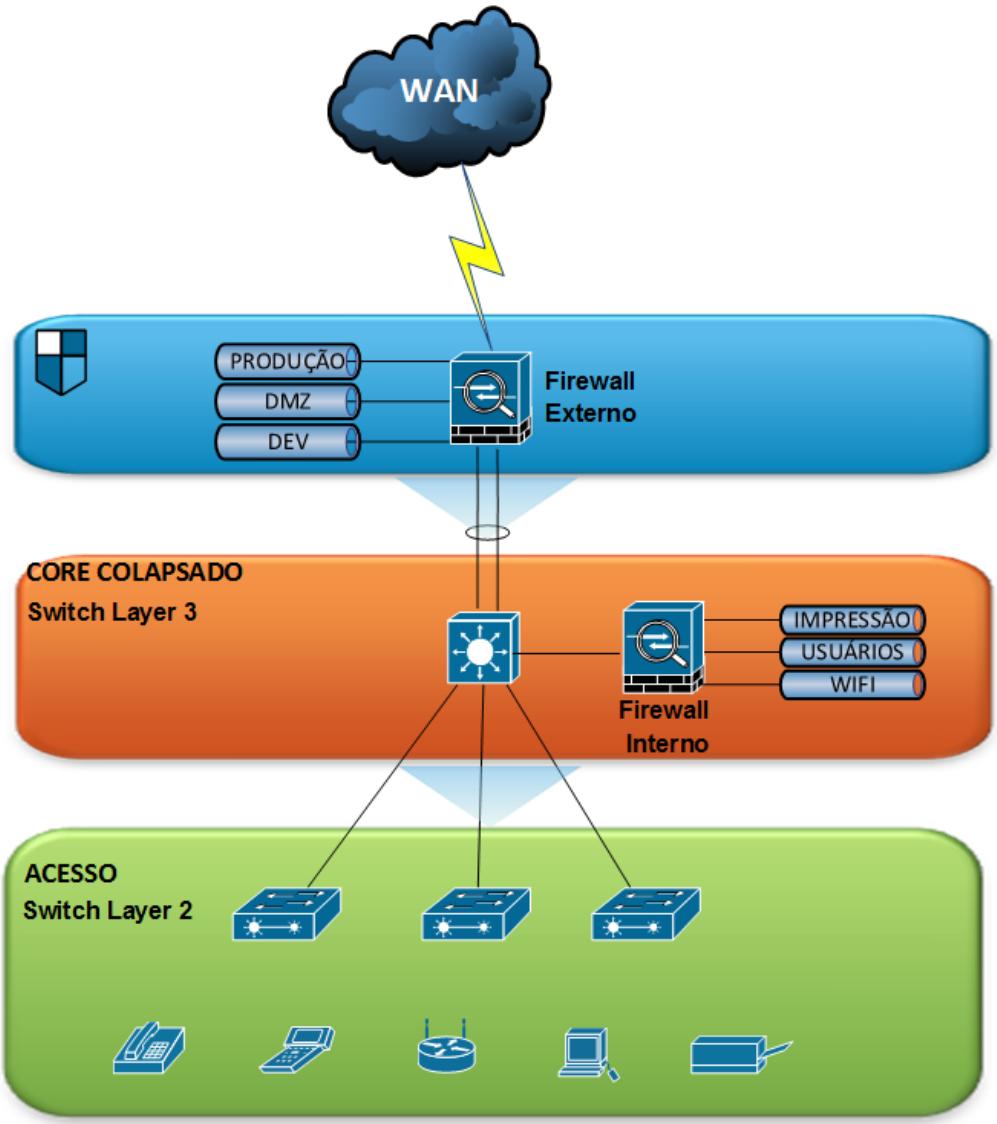
Neste modelo, considera-se que o hospital não possui switches com capacidade de roteamento, desta forma, o roteamento será realizado pelo firewall.

3.1.2 INFRAESTRUTURA INTERMEDIÁRIA

Este modelo é indicado para hospitais que já possuem switches com capacidade de roteamento, neste modelo recomenda-se que as rede de usuários sejam interfaces Layer 3 no switch, e o firewall tenha as redes de produção (DMZ, DESENVOLVIMENTO etc.)



O controle do tráfego de dados pode ser realizado por ACLs no switch que possui a interface Layer 3, caso o entendimento seja de que a administração das ACLs via command line é trabalhosa, pode ser adotado também um firewall interno para controlar o tráfego da rede interna (Usuários, Impressoras, WiFi etc) de forma gráfica.



3.2. PROPRIEDADES E PADRÕES

3.2.1. VIRTUALIZAÇÃO

• Definir os recursos de virtualização que devem estar presentes na solução;

• Definir o padrão de configuração do posicionamento das interfaces de rede;

• Definir o padrão de conectividade com o switches (LACP, Link Aggregation);

• Definir o tipo de configuração para as interfaces (trunk, VLAN etc.), bem como para a configuração do equipamento (Storage);

• Definir nomenclatura e empilhamento;

• Quando for utilizado mais de um comutador para conectividade do pool, os comutadores devem ser empilhados; e

• Deve-se prover agrupamento de portas no comutador (empilhado) para que exista redundância das interfaces do pool de virtualização.

3.2.2. SISTEMAS LEGADOS

• Definir onde ficarão hospedados (VLAN);

• Definir para exceções (Ex. Equipamentos conectados aos equipamentos médicos); e

• Definir informações que devem ser mantidas sobre o sistema (empresa, contato, telefone, responsável dentro do HUF etc.).

3.2.3. ESTRATÉGIAS DE MONITORAMENTO

Todos os servidores e ativos de rede devem ser configurados para enviar seus respectivos logs a um servidor Syslog local e depois concentrados na sede da EBSERH, para backup e gerenciamento, sendo que o gerenciamento dos ativos de rede será configurado no Zabbix. Sistemas de monitoramento:

• IMC/Network Director;

• Servidor Syslog;

• Zabbix.

Todos os ativos de rede, deverão ser monitorados pelo sistema especificado neste documento, sendo que para cada ativo, deve-se monitorar minimamente:

1. Switches: monitorar erros, taxa de dados, disponibilidade, carga de processamento/memória e portas em uso/desuso.

2. Pontos de acesso sem fio: monitorar erros, taxa de dados, disponibilidade, carga de processamento/memória, números de usuários conectados no ponto; SSID configurados.

3. Roteadores: monitorar erros, taxa de dados, disponibilidade, carga de processamento/memória.

4. Servidores físicos: espaço em disco, memória, processamento, taxa de erros das interfaces, disponibilidade.

5. Servidores virtuais: espaço em disco, memória, processamento, disponibilidade.

6. Televisores: disponibilidade.

7. Impressoras: disponibilidade, erros.

8. Câmeras: disponibilidade, processamento, memória.

9. Nobreaks: carga, potência, erros.

10. Storages: espaço em disco, memória, processamento, disponibilidade, portas em uso/desuso, taxa de dados.

Ativos	Disponibilidade	CPU	Memória	Espaço em Disco	Trafego Tx/Rx Dados	Interfaces / Portas	Usuários Conectados	SSID Configurados	Carga	Potência	Monitorar Erros
Switch											
Pontos de Acesso sem Fio											
Roteadores											
Servidores Físicos											
Servidores Virtuais											
Televisores											
Impressoras											
Câmeras IP											
Nobreaks											
Storage											

3.2.4. DATA CENTER

• Uso de KVM com suporte a gerenciamento remoto e empilhamento;

• Uso de nobreaks redundantes, sendo que cada servidor deve possuir fontes de energia redundante;

• Cada fonte do servidor deve ser ligada ao circuito elétrico de somente um nobreak; e

• Deve existir dispositivos para o monitoramento ambiental, provendo minimamente informações sobre a temperatura e a umidade.

4. PLANO DE ENDEREÇAMENTO IP

O plano de endereçamento IP (Internet Protocol) tem como foco definir o mapa de endereços IP para organização da rede de dados, facilitando a identificação de cada ativo de rede que a compõe e o entendimento da interligação dos seus componentes. Além disso, este planejamento conceituará os principais termos utilizados na comunicação da rede de computadores, fornecendo um guia e um padrão à rede de dados da EBSERH.

4.1. ENDEREÇAMENTO IP

O endereçamento IP permite definir o conjunto de endereços que fazem parte da rede de dados, estruturando o conjunto de números de um endereço IP para definir o campo que identifica a rede e o campo que identifica um host (nó de uma ligação na rede de dados). Outra característica é a de segmentação da rede que consiste em dividir a rede de dados em partes definindo o conjunto de endereços IP que compõe cada segmento, proporcionando uma maior segurança na comunicação entre os hosts e um controle mais eficiente do tráfego de dados.

4.2. IPV4 E IPV6

Atualmente existem duas versões de endereço IP, a versão 4 (IPv4) e a versão 6 (IPv6). A quantidade de bits que compõe um endereço é o que difere as versões, determinando a quantidade de redes e hosts possíveis de se endereçar.

No IPv4, cada um dos endereços é composto por 4 blocos de 8 bits, totalizando 32 bits, sendo representados por números que variam de 0 a 255, porém, quando processados, são transformados em binários variando entre 0 e 1. Por exemplo: 192.168.1.10 (decimal) e 11000000.10101000.00000001.00001010 (binário).

O IPv6 foi oficializado em 6 de junho de 2012, sendo fruto do esforço do IETF para criar a "nova geração do IP" (IPng: Internet Protocol next generation).

O endereçamento no IPv6 é de 128 bits, e inclui prefixo de rede e sufixo de host. No entanto, não existem classes de endereços, como acontece no IPv4. Assim, a fronteira do prefixo e do sufixo pode ser em qualquer posição do endereço.

A longo prazo, o IPv6 tem como objetivo substituir o IPv4, que só suporta cerca de 4 bilhões (4x109) de endereços IP, contra cerca de 340 undecilhões (3,4x1038) de endereços do novo protocolo. O governo brasileiro recomenda a adoção do protocolo no documento e-PING, dos Padrões de Interoperabilidade de Governo Eletrônico.

4.3. IP PRIVADO E IP PÚBLICO

Basicamente, IP privado é endereço utilizado para a identificação de um dispositivo dentro de uma rede. Eles não são válidos na internet. Por outro lado, o IP público é para dispositivos acessíveis na internet.

A maioria dos endereços IP são públicos, permitindo assim que as nossas redes (ou pelo menos o nosso roteador que faz a fronteira entre a nossa rede e a Internet) estejam acessíveis publicamente através da Internet, a partir de qualquer lado.

Quanto a endereços privados, estes não nos permitem acesso direto à Internet, no entanto esse acesso é possível, mas é necessário recorrer a mecanismos de tradução como o NAT (Network Address Translation) que traduzem o nosso endereço privado para um endereço público.

Os intervalos de endereços privados são:

• de 10.0.0.0 a 10.255.255.255 (10.0.0.0 /8)

• de 172.16.0.0 a 172.31.255.255 (172.16.0.0 /12)

• de 192.168.0.0 a 192.168.255.255 (192.168.0.0 /16)

4.4. SEGMENTAÇÃO DE REDE

Índi-ce	Descrição	VID	Nome	Re-de	IP Inicial	IP final	Observação
1	Servidores - Produção	100	srv_prod	/22	10.x.0.1	10.x.3.254	Para suportar serviços privados oferecidos pelo HU, onde NÃO é necessário o controle de acesso, ou é necessário ganhar desempenho

Índi-ce	Descrição	VID	Nome	Re-de	IP Inicial	IP final	Observação
							(servidor de arquivos, AD, etc.). Servidores AGHU, na faixa 10.x.1.1 a 10.x.1.254. Servidores internos, AD, DNS, DHCP, web 10.x.0.1 a 10.x.0.254.
Intervalo				/22	10.x.4.1	10.x.7.254	
2	Servidores - Desenvolvimento/ Homologação	200	srv_dev	/22	10.x.8.1	10.x.11.254	Para suportar o desenvolvimento ou homologação de novos serviços (ambiente privado).
Intervalo				/22	10.x.12.1	10.x.15.254	
3	DMZ- Interna	300	dmz_int	/22	10.x.16.1	10.x.19.254	Para suportar o confinamento de serviços privados oferecidos pelo HU, onde é necessário o controle de acesso (portas/aplicação).
Intervalo				/22	10.x.20.1	10.x.23.254	
4	DMZ- Externa/Extranet	400	dmz_ext	/22	10.x.24.1	10.x.27.254	Para suportar o confinamento de serviços públicos oferecidos pelo HU, onde é necessário o controle de acesso (portas/aplicação).
Intervalo				/22	10.x.28.1	10.x.31.254	
5	Wifi Acadêmica	500	wifi_acad	/20	10.x.32.1	10.x.47.254	Para wifi acadêmica, com controle de acesso e com bloqueio de serviços não essenciais. É possível que os

Índi-ce	Descrição	VID	Nome	Re-de	IP Inicial	IP final	Observação
							professores precisem de um servidor de arquivos para fornecimento de material.
Intervalo				/20	10.x.48.1	10.x.63.254	
6	Wifi Pública	600	wifi_pub	/20	10.x.64.1	10.x.79.254	Para wifi pública, sem controle de acesso e com bloqueio de serviços não essenciais. Preferencialmente, apenas permitir acesso a 443 e 80 (discutir).
Intervalo				/20	10.x.80.1	10.x.95.254	
7	Wifi Corporativa	700	wifi_corp	/20	10.x.96.1	10.x.111.254	Para wifi corporativa, onde essa rede pode acessar os mesmos recursos da rede de desktop.
Intervalo				/20	10.x.112.1	10.x.127.254	
8	Desktop	800	desk_ZZZ	/18	10.x.128.1	10.x.191.254	Dedicar 800 para desktops de TI, 801, 802, 803... para demais. Dedicada à rede de desktop. ZZZ: pode ser o rack, a área ou andar.
Intervalo				/22	10.x.192.1	10.x.195.254	
9	Rede para terceiros	900	rede_terc	/22	10.x.196.1	10.x.199.254	Para suportar a conexão confinada de empresas terceiras para manutenção de equipamentos, ou suportar a implantação de servidores de monitoramento dessas empresas.
Intervalo				/22	10.x.200.1	10.x.203.254	

Índi-ce	Descrição	VID	Nome	Re-de	IP Inicial	IP final	Observação
10	Impressoras	1000	impressoras	/23	10.x.204.1	10.x.205.254	Para suportar a conexão confinada de empresas terceiras para manutenção de equipamentos, ou suportar a implantação de servidores de monitoramento dessas empresas.
Intervalo				/23	10.x.206.1	10.x.207.254	
11	Telefonia IP	1100	voip	/21	10.x.208.1	10.x.215.254	Para telefones IP e central telefônica.
Intervalo				/21	10.x.216.1	10.x.223.254	
12	CFTV	1200	cftv	/22	10.x.224.1	10.x.227.254	Para câmeras, interface do servidor e outros ativos de CFTV ou monitoramento ambiental.
Intervalo				/22	10.x.228.1	10.x.231.254	
13	Gerência de Ativos de Rede e Servidores	1300	gerencia	/22	10.x.232.1	10.x.235.254	Para switches, controladoras, pontos de acesso sem fio, iDRAC ou iLO, storage e demais ativos.
Intervalo				/22	10.x.236.1	10.x.239.254	
14	Storage SAN	1400	storage_san	/24	10.x.240.1	10.x.240.254	VLAN dedicada para as interfaces dos servidores que precisam conectar à storage SAN e para as interfaces de dados da storage. (Não deve ser usada para a interface de gerenciamento da storage).
Intervalo				/24	10.x.241.1	10.x.241.254	
15	Rede de equipamentos de	1500	Pacs	/24	10.x.242.1	10.x.242.254	VLAN dedicada para

Índi-ce	Descrição	VID	Nome	Re-de	IP Inicial	IP final	Observação
	diagnósticos (imagem, tomógrafos, Desktops, etc.)						equipamentos de diagnóstico por imagem (desktops, CR, RX, tomógrafos, etc).
Intervalo				/24	10.x.243.1	10.x.243.254	
16	Controle de Acesso	1600	ctrl_acesso	/24	10.x.244.1	10.x.244.254	Para equipamentos de controle de acesso (leitores de acesso, ponto eletrônico, cancelas, etc.).
Intervalo				/24	10.x.245.1	10.x.245.254	
17	Storage NAS	1700	storage_nas	/24	10.x.246.1	10.x.246.254	VLAN dedicada para as interfaces dos servidores que precisam conectar à storage NAS e para as interfaces de dados da storage. (Não deve ser usada para a interface de gerenciamento da storage).
Intervalo				/24	10.x.247.1	10.x.247.254	
18	Redes Isoladas e Projetos	1800	proj_xxxx	/24	10.x.248.1	10.x.248.254	Para redes isoladas e projetos. XXXX: identifica o projeto.
Intervalo				/?	10.x.249.1	10.x.254.254	
19	QinQ (VLAN sobre VLAN)	1900	QinQ				Para transportar VLAN sobre VLAN.
20	RGHU (reserva técnica)	2000	RGHU				Reservada, caso necessário, para TAG da RGHU.
21	VLAN reservada a IP público	2100	IP_PUB				Possível VLAN para levar IP´s públicos para dentro do HU

4.5. VIRTUAL PRIVATE NETWORK

Rede privada virtual, do inglês Virtual Private Network (VPN), é uma rede de comunicações privada construída sobre uma rede de comunicações pública (como por exemplo, a Internet). O tráfego de dados é levado pela rede pública utilizando protocolos padrões, não necessariamente seguros.

Uma VPN é uma conexão estabelecida sobre uma infraestrutura pública ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados. VPNs seguras usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Alguns desses protocolos que são normalmente aplicados em uma VPN estão: L2TP, L2F, PPTP e o IPSec. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.

4.6. REDES WI-FI

O modelo de rede sem fio, conforme o padrão 802.11ac, deverá suportar os seguintes critérios:

• Para cada conjunto de 30 usuários ou fração deste, deverá existir um ponto de acesso sem fio;

• Em cada auditório com até 200m² ou fração deste, deverá ser instalado (no mínimo) um ponto de acesso sem fio;

• O uso de pontos de acesso sem fio externo fica a critério do Setor de Gestão de Processos e Tecnologia da Informação. Quando do uso, o equipamento deve ser do tipo "externo", com qualidade para suportar a exposição as intempéries ambientais, tais como calor, frio, chuva, umidade, poeira, etc;

• Os pontos de acesso sem fio deverão ser gerenciados por uma controladora, podendo esta ser implementada por software ou hardware. Os pontos de acesso sem fio e a controladora, deverão ser capazes de segmentar vários SSID's e implementar portais de autenticação.

• O projeto deverá ser elaborado por equipe técnica e é de responsabilidade do Setor de Gestão de Processos e Tecnologia da Informação; e

• Projetos já existentes nos HU's, poderão ser mantidos ou readequados, conforme definição da Diretoria de Gestão de Processos e Tecnologia da Informação.

As redes sem fio deverão ser:

• Públicas: e assim implementar um método de autenticação baseado em portais por login/senha ou MAC com prazo de expiração da conta. SSID: XXXX_Publica;

• Privadas: consistem em redes de uso administrativo ou restrito. Devem suportar autenticação "forte". SSID: XXXX_Corp;

• Acadêmicas: consistem em redes de uso acadêmicos, devem suportar autenticação baseado no login de rede Ebserh. SSID: XXXX_Acad; e

• Ponto-a-ponto: somente quando conectarem dois ou mais sites. Deverão suportar algum mecanismo de criptografia, além de ser configurada sobre um método de autenticação conforme redes sem fio privadas. SSID: XXXX_P2P_"Site".

Obs: XXXX é a identificação do HU, por exemplo, SEDE ou HUB ou HUGD. "Site", se refere ao site que conecta o link ponto-a-ponto, por exemplo, Almoxarifado ou Unidade_Materno. O "site" pode ser abreviado.

Os perfis de usuários e suas características de acesso são estas:

• Visitante/paciente: um dia de acesso (default) ou conforme internação; login e senha;

• Estudante: um semestre de acesso; login e senha;

• Prestador contínuo de serviço: prazo de acesso indeterminado; configurações para rede privada; login e senha ou certificado;

• Prestador esporádico de serviço: três dias de acesso; configurações para rede privada; login e senha; e

• Servidor: prazo de acesso indeterminado; configurações para rede privada; login e senha ou certificado.

O processo de concessão de acesso consistirá em:

• Visitante/paciente: através das recepções de internação

• Estudante: através da CAU;

• Prestador contínuo de serviço: através da CAU;

• Prestador esporádico de serviço: pelo setor responsável pelo acompanhamento através da CAU; e

• Servidor: através da CAU.

Identificar um número de usuários baseado no número de leitos (pacientes/visitantes)+número de funcionários. Tipo de autenticação baseado no perfil de usuário. Para cada tipo, definir um tempo limite para expirar a conexão. Para cada tipo identificar o método de autenticação. Para cada tipo identificar o processo para concessão de acesso. Definir um modelo de equipamento (com controladora, compatibilidade e recursos adicionais).

CONCEITOS E DEFINIÇÕES

FIREWALL

Firewall tem a finalidade de impedir a entrada de intrusos a máquina, alguns vem a partir de portas Transmission control protocol (TCP) que estejam abertas, vindo através do Browser, o mesmo te protege de páginas com scripts maliciosos, fazendo um contínuo monitoramento dessas portas.

A maior parte dos ataques vem de dentro do próprio Firewall, por causa que o usuário mesmo que sem malícia, ao conectar um dispositivo externo traz consigo arquivos que servirão de suporte para o ataque, por isso ele monitora a saída de dados via um gateway de aplicação.

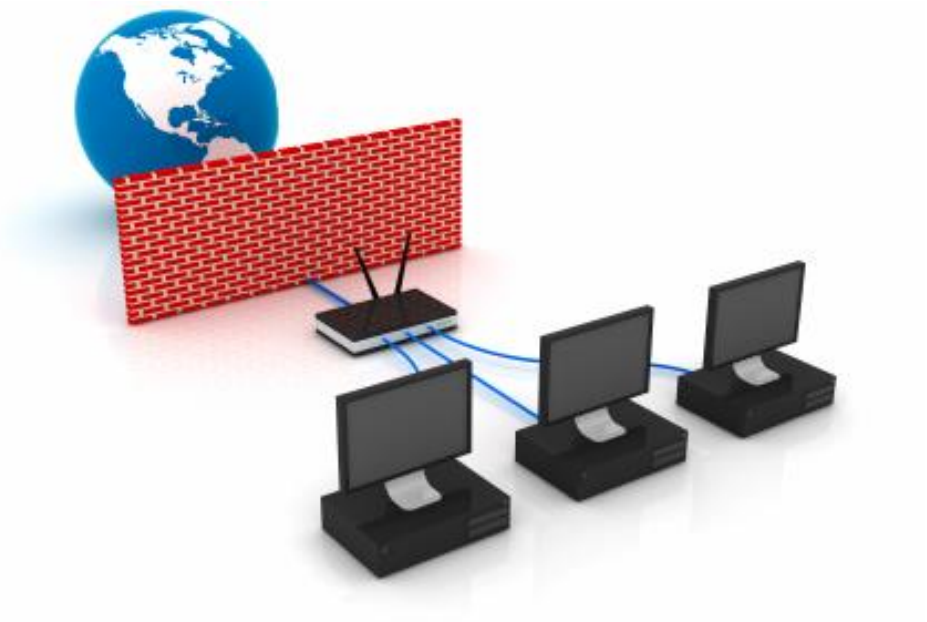


Figura – Ilustração de um Firewall bloqueando a entrada a sua rede.

Referências:

Texto: Andrew S.Tanenbaum. (2003). “Computer Networks, Fourth Edition, 582,583.”

Imagem: eBrahma. (2015). Firewall-Basic concepts. http://www.ebrahma.com/2015/04/firewall-basic-concepts/ > Acesso em: 26/09/2016

SWITCHES

Switch é um aparelho de redes que estabelece uma conexão com diferentes computadores em linhas privadas, possibilitando o envio de dados simultaneamente a todos conectados nessa rede, operando na camada de enlace e de rede.

A Cisco com intuito de otimizar a rede, deixando a mais eficiente, fácil e inteligente, dividiu os serviços em camadas:

• Switch Core (Núcleo): Faz o serviço de maneira efetiva de forma rápida e efetiva, podendo encaminhar grandes quantidades de dados com uma velocidade alta, sendo de alta importância ser redundante.

• Switch de Distribuição: Serve para estabelecer a conexão entre o Switch Core e o Switch de acesso, tendo alta redundância, e fornecendo uma segurança a quem usa o serviço.

• Switch de Acesso: Faz a interface com os dispositivos finais (PC, impressora, telefones, entre outros) para que eles tenham acesso ao restante da rede, e controlar quem terá permissão.

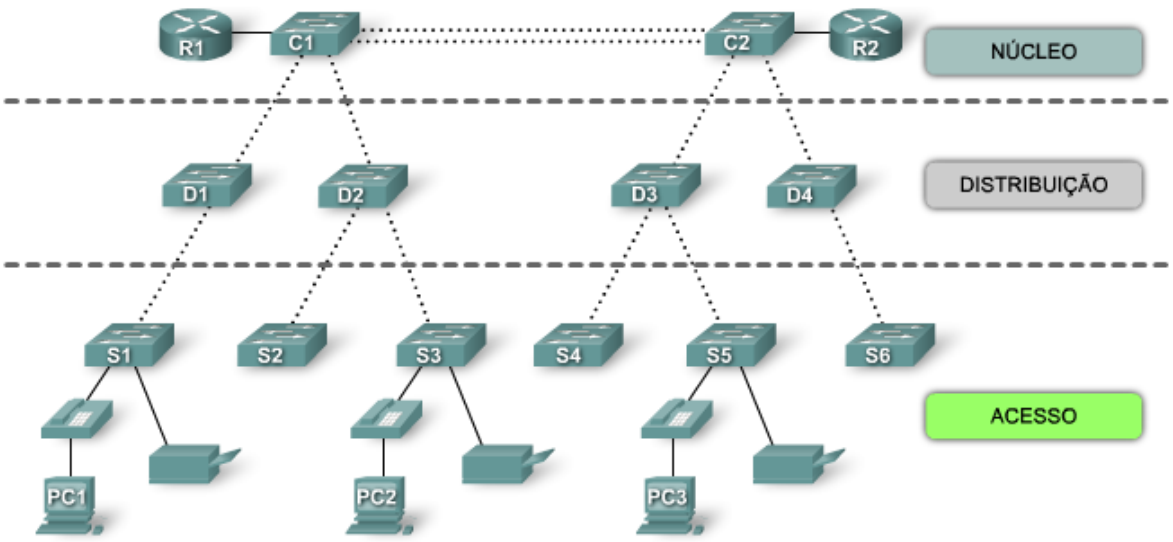


Figura – Design de rede hierárquico de um switch acordo com a norma da Cisco.

Referências:

Texto: Carlos Eduardo Morimoto. (2008). Redes: guia prático, 29.

Imagem: No Mundo das Redes. (2011). Modelo de Rede Hierárquica. http://nomundodasredes.blogspot.com.br/2011/10/modelo-de-rede-hierarquica.html > Acesso em: 23/04/2018.

VIRTUAL PRIVATE NETWORK

Virtual Private Network (VPN) é uma rede virtual privada, onde os dados e informações enviados ou recebidos serão criptografados, sendo gerenciados por certos tipos de protocolos enquanto estiverem trafegando na rede. Em sua arquitetura tem alguns modelos, dentre eles tem:

Gateway-to-Gateway (Site-to-Site): Criado para proteger a comunicação e integridade dos dados entre duas redes.

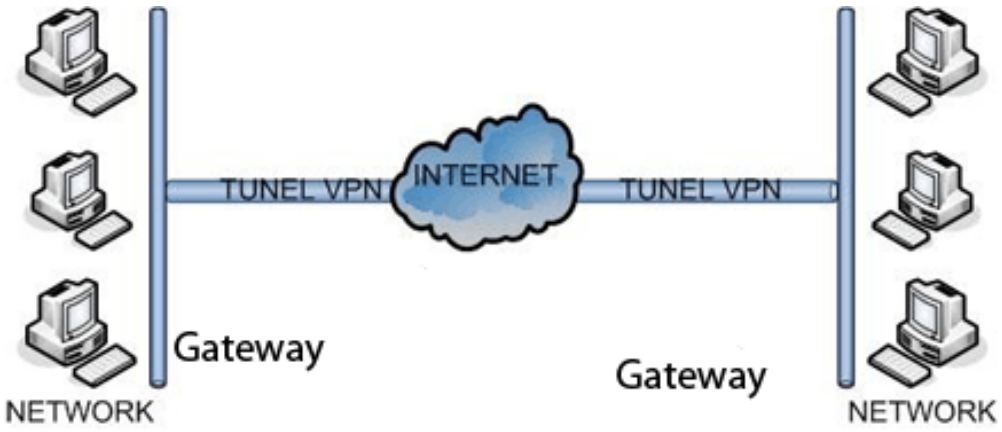


Figura – Arquitetura da conexão feita por um Gateway-To-Gateway

Gateway-to-Host (Site-to-Cliente): Criado para proteger e manter a integridade dos dados entre um usuário e uma ou mais redes.

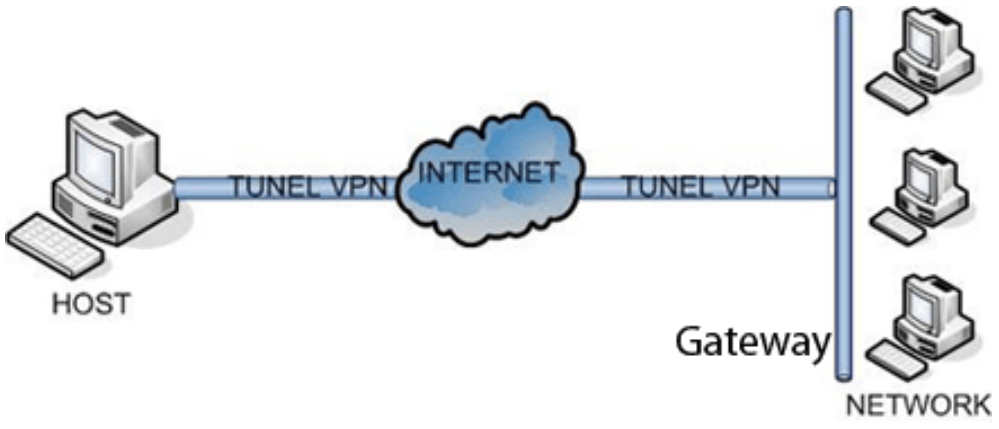


Figura – Arquitetura da conexão feita por um Gateway-To-Host

Referências:

Texto: GTA/UFRJ. (2016). Arquitetura de VPNs. Disponível em http://www.gta.ufrj.br/grad/08_1/vpn/tiposarq.html > Acesso em: 23/04/2018

Texto: DevMedia. (2016). Montando uma VPN com o OpenVPN. http://www.devmedia.com.br/montando-uma-vpn-com-o-openvpn/26670 > Acesso em: 23/04/2018

Imagem: GTA/UFRJ. (2016). Arquitetura de VPNs. Disponível em http://www.gta.ufrj.br/grad/08_1/vpn/tiposarq.html > Acesso em: 23/04/2018

IDS/IPS

IDS: Intrusion Detection System (IDS) Ou Sistema de Detecção de Intrusos, se refere a um meio usado para monitorar ações maliciosas em uma rede afim de derrubar seu serviço, fazendo uso de um software no qual é especificamente projetado para observar e detectar atividades que não são comumente feitas por um usuário qualquer.

IPS: Semelhante ao IDS, o Intrusion Prevention System (IPS) além de detectar um ataque, ele também previne prováveis ataques a rede.

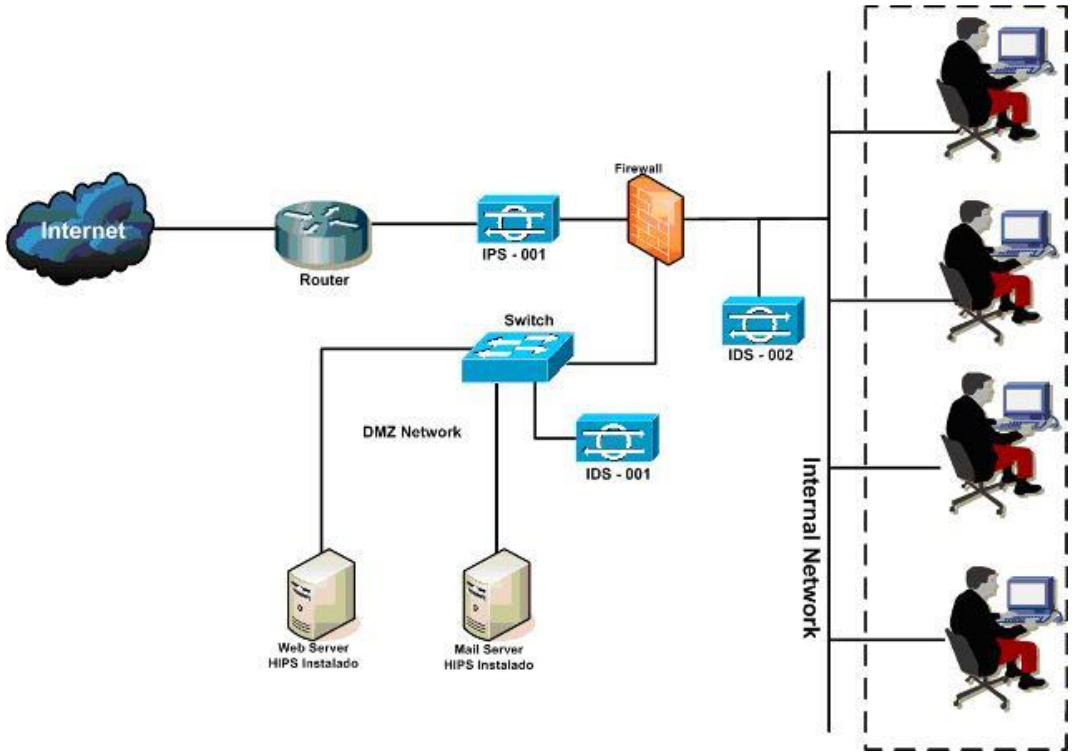


Figura – Esquematização de onde o IPS e IDS agem em uma rede.

Referências:

Texto: GTA/UFRJ. (2016). Detecção de Intrusos. Disponível em:
http://www.gta.ufrj.br/grad/07_2/rodrigo_leobons/deteccao.html > Acesso em: 23/04/2018

Imagem: For Security. (2010). Diferença entre IDS e IPS. Disponível em:
http://forsecurity.blogspot.com.br/2010/06/diferenca-entre-ids-e-ips.html> Acesso em: 23/04/2018

VLAN

As Virtual Local Area Networks (VLANs) são um mecanismo que permitem que os administradores de rede criem os domínios de transmissão lógicos que podem ser distribuídos em um único switch ou em vários, independente da proximidade física. Essa função é útil para reduzir o tamanho dos domínios de transmissão ou para permitir que grupos ou usuários sejam agrupados logicamente sem que precisem estar logicamente localizados no mesmo local.

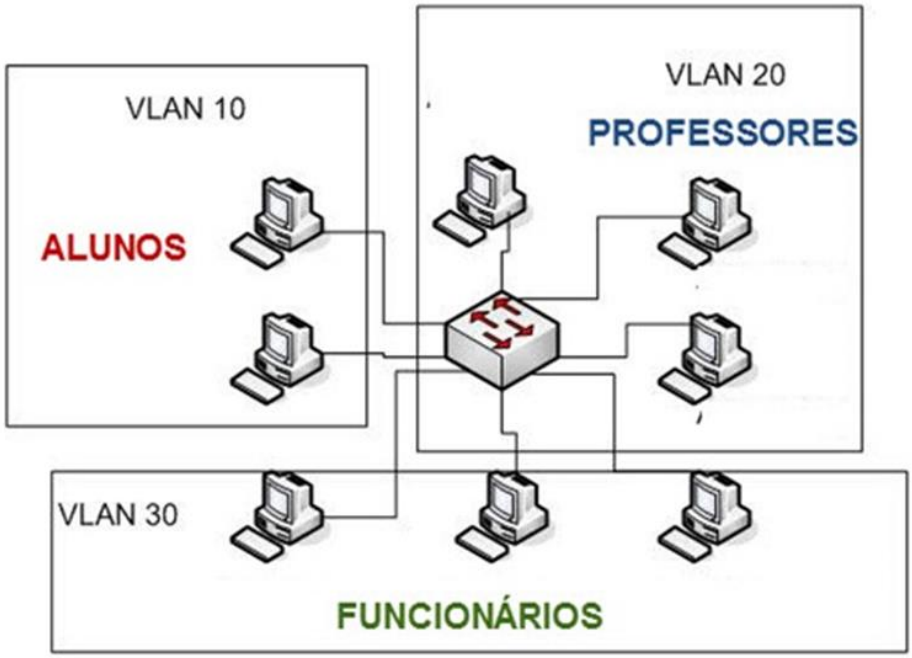


Figura – Representação de como a VLAN cria os grupos de rede.

Referências:

Texto: Cisco. (2016). Criando VLANs de Ethernet em Switches Catalyst. Disponível em: http://www.cisco.com/cisco/web/support/BR/104/1042/1042625_3.html > Acesso em: 23/04/2018

Imagem: PPL WARE. (2010). Redes – Sabe o que é uma VLAN? https://pplware.sapo.pt/tutoriais/networking/redes-sabe-o-que-uma-vlan/ > Acesso em: 23/04/2018

LISTA DE ACRÔNIMOS

A	
AD/LDAP	Active Directory/Lightweight Directory Access Protocol
C	
CDC	Container DataCenter
COBIT 5	Control Objectives for Information and Related Technology - Versão 5
D	
DGPTI	Diretoria de Gestão de Processos e Tecnologia da Informação
E	
EBSERH	Empresa Brasileira de Serviços Hospitalares
H	
HUF's	Hospitais Universitários Federais
I	
IP	Internet Protocol
IPS	Intrusion Prevent System
ITIL v3	Information Technology Infrastructure Library - Versão 3
MEC	Ministério da Educação e Cultura
N	
NBR ISO/IEC	International Organization for Standardization
P	
POSIC	Política de Segurança da Informação e Comunicação
R	
RGHU	Rede de Gestão de Hospitais Universitários
RNP	Rede Nacional de Pesquisa

S	
SI	Segurança da Informação
SGPTI	Setor de Gestão de Processos e Tecnologia da Informação
SGSI	Sistema de Gestão de Segurança da Informação
SUS	Sistema Único de Saúde
SSL	Secure Socket Layer
T	
TIC	Tecnologia da Informação e Comunicação
V	
VPN	Virtual Private Network

PADRÕES DE NOMENCLATURA

PREMISSA E RESTRIÇÕES

Para efeitos desta norma, será considerado “nome” tanto o “nome de batismo” quanto o “nome social” que é o nome adotado para identificação pela sociedade dos casos definidos pela Portaria Nº 233 de 18 de Maio de 2010, do Ministério do Planejamento, Orçamento e Gestão.

Devem ser observadas as seguintes restrições:

Não é permitido o uso de apelidos, números, ou qualquer outra forma fora dos padrões disciplinados nesse documento;

Não utilizar acentos (til, agudo, grave, circunflexo, trema), aspas simples ou duplas;

Nome, simples ou composto, pode ter no máximo 16 caracteres, podendo ser caracteres alfabéticos minúsculos, e hífen, sem espaços entre eles;

Sobrenome, simples ou composto, pode ter no máximo 40 caracteres, podendo ser caracteres alfabéticos minúsculos, e hífen, sem espaços entre eles.

NOMES DE USUÁRIO

Tipo de conta	Regra	Padrão	Exemplo
Usuário comum	Primeira	<prenome>.<último sobrenome>	Nome: Maria de Souza Silva Conta: maria.silva
	Segunda	<prenome>.<penúltimo sobrenome>	Nome: Maria de Souza Silva Conta: maria.souza
	Terceira	<último sobrenome>.<prenome>	Nome: Maria de Souza Silva Conta: silva.maria
	Quarta	<prenome>-<último sobrenome>.<primeira letra do prenome><primeira letra do último sobrenome>	Nome: Maria de Souza Silva Conta: maria-silva.ms
	Quinta	<prenome>.<último sobrenome>.<número sequencial>	Nome: Maria de Souza Silva Conta: maria.silva.1
Usuário de Administração	Primeira	adm.<Primeira letra do primeiro nome da conta seguida do sobrenome da conta>	Nome: Ewerton Souza Filho Conta: ewerton.souza Conta adm: adm.esouza
Sistema	Primeira	<Site>srvc.<Nome do Sistema>	Sistema: Mentorh – Sistema de Gestão de RH Site: EBSERH-SEDE Conta: mentorh.sede

E-MAILS CORPORATIVOS

Tipo de E-mail	Padrão	Exemplo
Usuário comum	<Conta de Usuário comum>@ebserh.gov.br	Nome: Maria Souza Silva Conta: maria.silva Email: maria.silva@ebserh. gov.br Nome: José Moraes de Souza Conta: jose.jsouza Email: jose.jsouza@ebserh.gov.br
Departamento e grupos	<Departamento>.<Site>@ebserh.gov.br	dgpti.sede@ebserh.gov.br gerencia.hub@ebserh.gov.br ouvidoria.hupi@ebserh.gov.br webmaster.sede@ebserh.gov.br
Serviços de sistema	<site>srvc.<sistema>@ebserh.gov.br	sedesrvc.mentorh@ebserh.gov.br hupisrvc.simec@ebserh.gov.br hucamsrvc.aghu@ebserh.gov.br

SITES

Padrão	Exemplo
De acordo com o propósito da mesma	SEDE; HUPI; HUB;

ORGANIZATIONAL UNIT (OU)

Padrão	Exemplo
De acordo com o propósito da mesma	Computadores

	Impressoras SEDE HUPI

GRUPOS

Padrão	Exemplo
De acordo com o propósito da mesma	Administradores; Suporte; Desenvolvimento; Dba;

POLÍTICAS DE GRUPO (GPO)

Padrão	Exemplo
De acordo com o propósito da mesma	Acesso de painel de controle Acesso a dispositivos de rede Papel de parede

SERVIDORES / SERVIÇOS

Padrão	Exemplo
<Site>-<código serviço>-<serviço><Sequencial>	hupi-fh-vware1 (VMWare) hupi-fh-vxen1 (Xen Server) hupi-vp-mtorh1 (Mentorh) sede-vp-ad1 (AD) sede-vp-dhcp1 (DHCP) sede-vs-aghu1 (AGHU)

ESTAÇÃO DE TRABALHO / NOTEBOOKS

Padrão	Exemplo
<Site>-WK-<6 últimos dígitos patrimônio> **<Site>-NT-<6 últimos dígitos patrimônio>**	HCPA-WK-000178 MERJ-NT-000187 SEDE-WK-000301

ATIVOS DE REDE

Padrão	Exemplo
<Site>-SW-<Setor><Sequencial com 3 dígitos> **<Site>-SW-<Setor><Sequencial com 3 dígitos>**	HUJF-SW-Pediatria001 SEDE-FW-CDC001

IMPRESSORAS

Padrão	Exemplo
<Site>-PR-<Setor><Sequencial com 3 dígitos>	HUSE-PR-DC001 HCTM-PR-CASA002

ANEXO I – TABELA DE SITES EBSERH

Site	Sigla	Site de Saúde	Site Educacional	Estado
HUGV	HGV	Hospital Universitário Getúlio Vargas	Univ. Federal do Amazonas	AM
HUBFS	BFS	Hospital Universitário Bettina Ferro de Souza	Univ. Federal do Pará	PA
HUJBB	JBB	Hospital Universitário João de barros Barreto	Univ. Federal do Pará	PA
SEDE	SDE	Empresa Brasileira de Serviços Hospitalares		DF
HCUFG	CGO	Hospital das Clínicas	Univ. Federal do Goiás	GO
HUMAP	MAP	Hospital Universitário Maria Aparecida Pedrossian	Univ. Federal de Mato Grosso do Sul	MS
HUJM	UJM	Hospital Universitário Júlio Müller	Univ. Federal do Mato Grosso	MT
HUB	HUB	Hospital Universitário	Univ. de Brasília	DF
HUGD	UGD	Hospital Universitário	Univ. Federal de Grande Dourados	MT
HUPI	HPI	Hospital Universitário	Univ. Federal do Piauí	PI
HUPAA	PAN	Hospital Universitário Professor Alberto Nunes	Univ. Federal de Alagoas	AL
HUPES	PES	Hospital Universitário Professor Edgard Santos	Univ. Federal da Bahia	BA
MCO	COM	Maternidade Climério de Oliveira	Univ. Federal da Bahia	BA
HUWC	HWC	Hospital Universitário Walter Candídio	Univ. Federal do Ceará	CE
MEAC	MAC	Maternidade Escola Assis Chateaubriand	Univ. Federal do Ceará	CE
HUMA	HUM	Hospital Universitario do Maranhao	Univ. Federal do Maranhao	
HUAC	HAC	Hospital Universitário Alcides Carneiro	Univ. Federal do Maranhão	MA

Site	Sigla	Site de Saúde	Site Educacional	Estado
HULW	HLW	Hospital Universitário Lauro Wanderley	Univ. Federal da Paraíba	PB
HCPE	CPE	Hospital das Clínicas	Univ. Federal de Pernambuco	PE
HUAB	HAB	Hospital Universitário Ana Bezerra	Univ. Federal do Rio Grande Do Norte	RN
HPHFB	HFB	Hospital de Pediatria Professor Heriberto Ferreira Bezerra	Univ. Federal do Rio Grande Do Norte	RN
HUOL	HOL	Hospital Universitário Onofre Lopes	Univ. Federal do Rio Grande Do Norte	RN
MEJC	EJC	Maternidade Escola Januário Cicco	Univ. Federal do Rio Grande Do Norte	RN
HUSE	USE	Hospital Universitário	Univ. Federal de Sergipe	SE
HMRCJ	MRC	Hospital Universitário Doutor Miguel Riet Corrêa Júnior	Univ. Federal do Rio Grande	RS
HCPA	HPA	Hospital de Clínicas de Porto Alegre	Univ. Federal do Rio Grande do Sul	RS
HERS	ERS	Hospital Escola	Univ. Federal de Pelotas	RS
HUSM/RS	HSM	Hospital Universitário	Univ. Federal de Santa Maria	RS
HCPR	CPR	Hospital de Clínicas	Univ. Federal do Paraná	PR
MVFA	VFA	Maternidade Vitor Ferreira do Amaral	Univ. Federal do Paraná	PR
HEPEL	EST	Hospital Universitário Polydoro Ernani de São Thiago	Univ. Federal de Santa Catarina	SC
HUCAM	CAM	Hospital Universitário Cassiano Antônio de Moraes	Univ. Federal do Espírito Santo	ES
HUAP	HAP	Hospital Universitário Antônio Pedro	Univ. Federal Fluminense	RJ
HUCFF	CFF	Hospital Universitário Clementino Fraga Filho	Univ. Federal do Rio de Janeiro	RJ
HESFA	SFA	Hospital Escola São Francisco de Assis	Univ. Federal do Rio de Janeiro	RJ
IDT	IDT	Instituto de Doenças do Tórax	Univ. Federal do Rio de Janeiro	RJ

Site	Sigla	Site de Saúde	Site Educacional	Estado
IPPMG	PMG	Instituto Puer. Pediátrico Martagão Gesteira	Univ. Federal do Rio de Janeiro	RJ
IGRJ	GRJ	Instituto de Ginecologia	Univ. Federal do Rio de Janeiro	RJ
INDC	NDC	Instituto de Neurologia Deolindo Couto	Univ. Federal do Rio de Janeiro	RJ
IPUB	PRJ	Instituto de Psiquiatria	Univ. Federal do Rio de Janeiro	RJ
MERJ	ERJ	Maternidade Escola	Univ. Federal do Rio de Janeiro	RJ
HUGG	UGG	Hospital Universitário Gaffrée e Guinle	Univ. Federal do Estado do Rio de Janeiro	RJ
HUJF	HJF	Hospital Universitário	Univ. Federal de Juiz de Fora	MG
HCMG	CMG	Hospital das Clínicas	Univ. Federal de Minas Gerais	MG
HCTM	CTM	Hospital de Clínicas	Univ. Federal do Triângulo Mineiro	MG
HCUFU	CUB	Hospital de Clínicas	Univ. Federal de Uberlândia	MG
HSP	HSP	Hospital São Paulo	Univ. Federal de São Paulo	SP

ANEXO II – TABELA DE CÓDIGOS DE SERVIÇOS/EQUIPAMENTOS

Código	Serviço
VP / FP	Servidor Virtual/Físico de Produção
VD / FD	Servidor Virtual/Físico de Desenvolvimento
VS / FS	Servidor Virtual/Físico de Stage
VT / FT	Servidor Virtual/Físico de Teste
VZ / FZ	Servidor Virtual/Físico de DMZ
FH	Servidor físico de Hypervisor (Virtualização)
CL	Cluster de servidores/serviços
WK	Workstation (Estação de trabalho)

NT	Notebook
FW	Firewall
PR	Impressora
SW	Switch

HISTÓRICO DE REVISÕES

Versão	Data	Descrição	Colaboradores
1.0	30/04/2018	Versão inicial	Daniel da Silva Farias (Sede) Brunner Salgado Martins (HUCAM) Deive Correa Lima (HCTM) Helton Carlos Lima Godoy (HUJM) Leandro Marcel Freitas e Santos (HUGD) Paulo Henrique de Assis (HU-UFJF)
1.1	02/07/2018	Revisão: Segmentação de Rede, Redes Wi-fi, Nomes de Usuários, Serviços / Equipamentos	Brunner Salgado Martins (HUCAM)