**Normas de Infraestrutura de TIC (exemplo)**

## A- Nomenclatura de estações

### 1 NOMENCLATURA DAS ESTAÇÕES CLIENTES

| 1° CAMPO | 2° CAMPO | 3° CAMPO |
|---|---|---|
| Sigla do Equipamento | Campus | Numero patrimônio |

**1.1 1° campo:** o primeiro identificador é constituído por um único caractere que define qual o tipo de equipamento que está sendo nomeado. A tabela abaixo define os valores para os equipamentos.

| Identificador | Equipamento |
|---|---|
| **M** | Estação de Trabalho |
| **N** | *Notebook* |
| **I** | Impressora |

**1.2 2° campo:** o segundo identificador é constituído por 3 caracteres. Este campo distingue o campus no qual a estação está instalada, utilizando sua respectiva sigla.

**1.3 3° campo:** o terceiro identificador é constituído de 5 ou 6 dígitos. Este campo é formado pelo número da placa de patrimônio afixada no equipamento.

**Exemplos:** MGYN50799 – Estação (patrimônio) 50799 do Campus Goiânia
NGYN50750 – Notebook (patrimônio) 50750 do Campus Goiânia
IGYN10850 – Impressora (patrimônio) 10850 do Campus Goiânia

### 2 NOMENCLATURA DOS ELEMENTOS ATIVOS

| 1° CAMPO | 2° CAMPO | 3° CAMPO |
|---|---|---|
| Sigla do equipamento | Campus | Numero sequencial |

Tabela 7

**2.1 1° campo**: o primeiro identificador é constituído por um único caractere que define qual o tipo de equipamento que está sendo nomeado. A tabela abaixo define os valores para os equipamentos.

| Identificador | Equipamento |
|---|---|
| **R** | Roteador |
| **W** | *Switch* |
| **H** | *Hub* |
| **A** | *Access Point* |

**2.2 2° campo:** o segundo identificador é constituído por 2 caracteres. Este campo distingue o campus, utilizando sua respectiva sigla.

**2.3 3° campo:** o terceiro identificador é constituído por 4 dígitos. Este campo é composto por um número sequencial.

**Exemplos:** RGYN0004 – Roteador número 4 do Campus Goiânia
WGYN0001 – Switch número 1 do Campus Goiânia
AGYN0001 – *Access Point* número 1 do Campus Goiânia

## B- Infraestrutura de rede LAN

### 3 Definições gerais

**3.1** Manter todas as redes locais a serem utilizadas de acordo com os padrões de topologias de rede.

**3.2** Seguir, para o cabeamento das redes locais, os padrões de cabeamento estruturado utilizados nas melhores práticas de mercado.

**3.3** Prover backup para todos os arquivos de configuração dos elementos ativos rede local, armazenando o backup em servidor de arquivos, de forma a serem usados caso aconteçam incidentes graves.

**3.4** Nomear os elementos ativos de rede local seguindo as Regras de Nomenclatura, do item 1 desta norma.

**3.5** Seguir, para o endereçamento IP (Internet Protocol), o Esquema de Endereçamento IP definido pelas normas internas.

**3.6** Documentar todas as informações de endereçamento utilizadas na rede local, contendo no mínimo as seguintes informações:

a) registro de utilização das faixas de endereçamento IP utilizadas, bem como para IPs fixos;

b) definição das VLANs utilizadas, contendo a definição das máscaras, dos *gateways* e das faixas de endereçamento atribuídas para cada uma das VLANs especificadas;

c) faixa de endereçamento destinada a cada grupo de clientes, projetos e laboratório: caso haja distinção entre eles.

**3.7** Realizar os acessos aos elementos ativos de rede local por meio de SSH (Secure Shell), provendo segurança na atividade de administração destes elementos.

**3.8** Dotar os elementos de rede local de senha forte, com no mínimo 8 (oito) caracteres.

**3.9** Acondicionar os elementos ativos de rede local em racks com chaves, considerando:

a) o controle de acesso físico aos elementos ativos deverá ficar a cargo do respectivo chefe do órgão de TI do campus;

b) o chefe do órgão de TI também terá o papel de autorizar a entrada e saída de equipamentos de redes locais e acompanhar as manutenções dos elementos ativos.

c) Os racks deverão estar localizados em salas de com acesso restrito e controlado sendo permitido o acesso regular apenas à equipe técnica.

**3.10** Manter os elementos ativos de rede local sob condições de temperatura estabelecidas no seu manual de instalação.

### 4 Cabos de Rede Utilizados

**4.1** Utilizar, no caso de pares trançados, sempre cabos UTP de 4 pares de fios de condutores sólidos em cobre recozido, de bitola AWG N22 ou 24, flexíveis, com capa de proteção do tipo não propagante de chamas, categoria 5E ou superior, e que atendam plenamente a todos os requisitos físicos e elétricos da norma EIA/TIA-568 e correlatas.

**4.2** Utilizar, na conectorização dos cabos UTP, sempre conectores RJ-45 com o material dos contatos em bronze fósforo e revestimento dos contatos em ouro, com espessura mínima de 30 micrômetro, de categoria 5e ou superior, e que atendam plenamente a todos os requisitos físicos e elétricos da norma EIA/TIA-568 e correlatas.

**4.3** Recusar reaproveitamento e emendas de cabos UTP. Ocorrendo do comprimento não atingir a distância desejada, o cabo deve ser substituído por outro de maior comprimento, porém não deve ultrapassar o comprimento máximo permitido pela norma de cem metros.

## 5 CONTROLE DOS PONTOS DE REDE

**5.1** Todos os pontos de rede local desocupados (não conectados a estações) deverão estar inativos, salvo os pontos críticos.

**5.2** Os pontos críticos devem estar restritos e serem tolerados, somente em locais de acesso controlado, ou seja, ambientes de laboratório, auditórios, salas de reunião e salas de treinamento

**5.2.1** Para a ativação de pontos desocupados o responsável pela área interessada deverá preencher formulário de solicitação de ativação de ponto com as devidas justificativas para sua habilitação.

**5.3** Devem existir controles, por parte do chefe do órgão de TI, para que os pontos críticos não sejam utilizados sem autorização.

**5.4** Quaisquer modificações na infraestrutura da rede, que impactem em acréscimos e/ou mudanças nos mapas de pontos de rede local, devem ser notificados ao respectivo chefe do órgão de TI.

**5.5** Os dados referentes aos pontos de rede local devem ser armazenados em uma planilha de situação de pontos de rede local, informando a quantidade de pontos de rede local ativos, desocupados e críticos.

**5.6** A planilha de situação de pontos de rede local deve ser atualizada com periodicidade que atenda aos requisitos operacionais exigidos, com uma tolerância máxima permitida de um mês.

# C- Acesso a Internet

## 6 ACESSO A SITES NA INTERNET

**6.1** O acesso à Internet disponibilizado pela instituição aos seus usuários internos pode, a qualquer momento, sofrer restrições por parte da mesma.

**6.2** Os serviços que provenham da Internet não podem inserir vulnerabilidades na rede corporativa, nem tampouco, acarretar riscos para os negócios da instituição.

**6.3** Poderão ser bloqueados os sites da Internet não considerados de interesse dos negócios e atividades da instituição quando houver manifesto devidamente justificado pelas áreas competentes.

**6.4** O bloqueio de acesso aos sites poderá ser efetivado com base na atividade desempenhada pelo usuário, sendo diferente para as atividades: administrativa, docente e discente.

**6.5** Caberá ao Departamento de TI promover restrições de acesso à Internet, como por exemplo, áudio, vídeo e outros sites, quando julgar necessário em caso de comprometimento da segurança da rede e da performance da infraestrutura tecnológica.

## 7 USO PARA ACESSO A SITES NA INTERNET

**7.1** Grupo de contas de rede de usuários das unidades administrativas: cada campus deverá possuir um grupo global, no seu respectivo domínio de contas, chamado Internet. A esse grupo pertencerão os usuários das Unidades Administrativas.

**7.2** Grupo de contas de rede de usuários docentes e discentes: cada campus deverá possuir um grupo global, no seu respectivo domínio de contas, chamado Docentes e Discentes, relativamente aos usuários lotados em cargo docente ou matriculados no corpo discente. A esse grupo, pertencerão os usuários professores e alunos, respectivamente, cada um com o seu tipo de acesso.

**7.3** Havendo alterações no quadro de professores e alunos, o responsável pelo Departamento Acadêmico deverá solicitar à área de tecnologia as modificações referentes às permissões, no grupo Docentes ou Discentes, de forma a manter o cadastro dos usuários sempre atualizado.

**7.4** Regras de acesso para usuários administrativos e docentes: à exceção das categorias de sites bloqueados, todos os demais, em princípio, estão liberados para acesso.
**7.5** Regras de acesso para discentes: além das categorias de sites bloqueados, estarão bloqueados todos os outros que não sejam os seguintes: sites de universidades e instituições de ensino, , sites governamentais (.GOV), sites categorizados como Educacionais e todos os sites autorizados pelos departamentos acadêmicos, observando o não-comprometimento da segurança e impacto na rede corporativa.

## 8 CATEGORIZAÇÃO DE SITES

**8.1** O ambiente tecnológico dos centros corporativos de dados devem possuir mecanismos para categorização de sites, conforme exemplos abaixo:
**8.1.1** Álcool: sites que promovem o uso de álcool, inclusive receitas de bebidas, métodos de fabricação caseira, anúncios, etc.
**8.1.2** Anarquia: sites contendo informações relativas a milícias, armas, grupos antigovernamentais, terrorismo, derrubadas de governo, métodos de assassinatos, etc.
**8.1.3** Anúncios: serviço de anúncios (banners) em servidores de terceiros.
**8.1.4** Autoajuda: sites que incluem informações como dieta, informações nutricionais, terapias, serviços de aconselhamento, motivação, conferências, artigos, etc.
**8.1.5** Automóvel: sites de fabricantes e negociantes de automóveis, vendas, arredamento, clubes, etc.
**8.1.6** Bate-papo (Chats): WebChats, Instant Messaging.
**8.1.7** Compras: sites que orientam o consumidor pra compras online, centros comerciais online, agências de viagens, bens imóveis, automóveis, classificados e serviços de comércio online.
**8.1.8** Consumo de Banda: sites que demandem alto consumo de banda, como: sites que ofereçam serviços de download e upload de softwares pagos e gratuitos, compartilhamento de arquivos, streaming, Peer-to-Peer, Rádio e TV, Telefonia pela Internet;
**8.1.9** Drogas: sites que promovem o uso ou a compra de drogas ilegais. Estes podem incluir ofertas de sementes de maconha para venda, métodos de plantio, técnicas e produtos para teste de pureza das drogas, informações sobre ácidos e/ou "cogumelos" e outras formas de narcóticos.
**8.1.10** Entretenimento: sites contendo assuntos como filmes, teatro, histórias em quadrinhos, televisão, música, passatempos, bandas de música e restaurantes.
**8.1.11** Esportes: sites de esportes em geral, tais como beisebol, basquete, hóquei, times de futebol americano e futebol, revistas esportivas, eventos esportivos, como Olimpíadas de inverno e verão, etc.
**8.1.12** Financeiro: sites relacionados ao comércio financeiro, bem como mercado acionário, notícias financeiras, serviços bancários online e mercado de câmbio.
**8.1.13** Humor: sites cujo propósito primário é comédia, piadas, diversão, etc.
**8.1.14** Ingressos: sites que oferecem vendas de ingressos para entretenimento: concertos, eventos esportivos, corridas, exposições, etc.
**8.1.15** Jogos: sites relacionados a jogos de computador ou outros jogos, tais como sites de downloads de jogos e sites de jogos online.
**8.1.16** Jogos de Azar: sites que encorajam jogos, como sites de apostas, loteria, bingo, corrida de cavalos/cães, apostas online em esportes, cassinos online, etc.
**8.1.17** Natureza Adulta: serviços de encontros, pertencentes a qualquer assunto que envolva maiores de 18 anos, lingerie, trajes de banho e fotos explícitas. Sites de natureza adulta, sem ser explicitamente pornográfico.

**8.1.18** Obsceno/Mau-gosto: sites que envolvem assuntos como mutilação, assassinato, horror, morte, cenas reais, execuções, violência, etc.
**8.1.19** Ódio e Discriminação: sites contendo material relativo à discriminação de quaisquer grupos de pessoas baseada na raça, religião, gênero, nacionalidade, etc.
**8.1.20** Opinião, Política e Religião: sites que pertencem a políticos, campanhas eleitorais, artigos de opinião, organizações políticas, publicações políticas, igrejas e publicações relacionadas, foros de discussão e religiões.
**8.1.21** Pessoais/Encontros: sites que estão relacionados a anúncios pessoais, sites de encontros, serviços de encontros, relacionamentos, apresentações, etc.
**8.1.22** Pornografia: sites que contêm nudez e vulgaridade de qualquer tipo, tais como Playboy, Hustler e Penthouse.
**8.1.23** Práticas Criminais: sites que promovem atividades ilegais, como pirotecnias, hackers, geração de números de cartões de crédito, quebra de senhas, investigação e assassinato.
**8.1.24** Revistas: revistas online e versões online de revistas impressas.
**8.1.25** Segurança e Risco: sites que disponibilizem conteúdos maliciosos (vírus, spyware, phishing, etc.) e que coloquem em risco a rede;
**8.1.26** Viagem: sites que oferecem passagens e reservas de viagem, agências de turismo, balcões de informação de visita, promoções, etc.
**8.1.27** Web-Based Proxies and Anonymizers: sites que oferecem serviços de navegação anônima.

## D - Segurança da informação

### 9 Procedimentos

**9.1** Monitorar de forma periódica os recursos de infraestrutura de TIC, com foco na Segurança da Informação, identificando as possíveis vulnerabilidades e ameaças de segurança relacionadas à rede e produção, de forma a garantir que o recursos estejam com nível de segurança adequado para atender às necessidades de negócio.
**9.2** Identificar as vulnerabilidades e ameaças inerentes à segurança da informação relacionadas aos itens seguintes, observando sempre a adequação destes dispositivos ao nível de proteção requerida por requisitos legais, contratuais, estatutários e características de mercado onde o negócio da organização está inserido:
a) recursos de infraestrutura;
b) fatores que circundam a localização física e lógica dos recursos de infraestrutura;
c) processos de negócio automatizados, no que se refere aos recursos de infraestrutura que provêem essa automatização;
d) pessoas que têm acesso à localização física e/ou lógica dos recursos de infraestrutura;
e) características das tecnologias usadas.
**9.3** Avaliar as vulnerabilidades e ameaças identificadas, classificando-as em ordem de importância, considerando sua probabilidade de ocorrência.
**9.4** Definir quais controles a serem aplicados para tratar as vulnerabilidades e ameaças analisadas e quais devem ser considerados inaceitáveis.
**9.5** Definir alternativas para evitar, transferir, reter ou reduzir as vulnerabilidades e ameaças.
**9.6** Analisar tendências de riscos, de forma a garantir que o ambiente de TIC esteja protegido.
**9.7** Providenciar a implementação dos controles necessários para mitigar as vulnerabilidades e ameaças da segurança da informação.

**9.8** Estabelecer Plano de Tratamento às Ameaças e Vulnerabilidades contendo, pelo menos, as seguintes informações:
a) ações de tratamento das ameaças e vulnerabilidades;
b) a hierarquia de prioridades para o tratamento das ameaças e vulnerabilidades identificadas;

c) providencias para implementar controles necessários para mitigar as vulnerabilidades e ameaças da segurança da informação;
d) recursos necessários para a implantação das ações de tratamento;
e) responsabilidades;
f) prazos;
g) informações que permitam medir a eficiência e eficácia dos tratamentos efetivados.

## E – Usuários

### 10 Acesso a rede

**10.1** Todos os usuários de estações deverão ter identificação de usuário e senhas individuais de acesso que o identifiquem de forma única.
**10.2** NOTA: Para os usuários da rede corporativa a identificação da conta de rede deve ser formada pelo domínio, o caractere "\" e o número de matrícula padronizada.
**10.3** Desabilitar as contas de rede dos usuários da Rede Corporativa que permanecerem sem utilização por mais de 45 dias consecutivos. Em caso de demissão, desligamento ou cessão, a conta de rede do empregado deve ser bloqueada imediatamente após comunicado da área responsável.
**10.4** Excluir as contas de rede dos usuários após 120 dias do período de desabilitação da conta, exceto para os casos de afastamento por licença médica ou por solicitação do chefe imediato.

### 11 Senhas

**11.1** O critério adotado para senhas será definido como senhas fortes.
**11.2** As senhas devem possuir um comprimento mínimo de 08 (oito) caracteres e devem combinar caracteres maiúsculos, minúsculos, numéricos e caracteres especiais.
**11.3** Nos casos de renovação e alteração, as últimas oito senhas não poderão ser reutilizadas (histórico de senhas ativado).
**11.4** A conta do usuário será bloqueada, após cinco tentativas de autenticação sem sucesso e será desbloqueada, automaticamente, após 24 horas.
**11.5** As senhas são pessoais e não devem ser divulgadas sob qualquer pretexto. Todos os usuários, administradores e gestores da rede devem guardar as suas senhas com sigilo.

### 12 DA REDE CORPORATIVA

**12.1** As senhas das contas de Administradores de Rede deverão ser renovadas a cada 60 dias e as senhas das contas de usuários deverão ser renovadas a cada 120 dias.
**12.2** Ao definir sua senha o usuário deverá ser orientado a torná-la o menos óbvia possível, dificultando a sua associação com nomes, números ou seqüências comuns. O nome ou qualquer parte do sobrenome do usuário não deve ser usado, bem como o próprio nome da conta, data de nascimento, dentre outros.