Políticas de Uso da Rede do Instituto de Informática

NRC - Núcleo de Recursos Computacionais

Fevereiro de 2014

Sumário

1 Introdução

Este documento abrange as políticas de uso dos recursos computacionais do Instituto de Informática. Todos os computadores conectados à rede do Instituto de Informática estão sujeitos a essas políticas. Elas abrangem itens relacionados à segurança da informação e ao uso dos recursos computacionais sob a tutela do NRC (Núcleo de Recursos Computacionais).

2 Políticas de utilização da rede do Instituto de Informática

Esse tópico define as normas de utilização da rede que abrangem o acesso à rede cabeada, o acesso à rede sem fio, a manutenção de arquivos no servidor home.inf.ufg.br, o uso do *webmail*, as tentativas não autorizadas de acesso e outros assuntos correlatos.

2.1 Políticas gerais

1. Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer computador ou servidor de rede sob a tutela do NRC. Isso inclui a tentativa de acesso a dados cujo acesso não seja expressamente autorizado ao usuário ou ainda colocar à prova a segurança da rede do Instituto de Informática;

2. Não é permitido o uso da infraestrutura do Instituto de Informática para tentativas de penetração em outras redes. Isso inclui ataques, tentativas de provocar congestionamentos ou tentativas deliberadas de sobrecarregar um servidor de rede;

3. Conteúdos de natureza pornográfica, preconceituosa, ofensiva ou ilegal (inclui-se aqui conteúdos oriundos de práticas de pirataria) não podem ser obtidos, mantidos ou distribuídos por meio dos recursos computacionais do Instituto de Informática;

4. A equipe de redes do NRC oferece suporte limitado à utilização de equipamentos de informática particulares, tais como: computadores, notebooks, roteadores, impressoras e dispositivos correlatos;

5. É proibido a inclusão de equipamentos de rede sem autorização explícita da equipe de redes e sistemas do NRC, tais como: switches, pontos de acesso sem fio, *media centers* e dispositivos correlatos;

6. O acesso aos sistemas sob a tutela do NRC deve ser feito por meio de uma conta de usuário, devidamente cadastrada no Instituto de Informática. A seção 2.2 trata das políticas das contas.

2.2 Políticas das contas

Ao ingressar no Instituto de Informática, todo docente, técnico-administrativo ou discente receberá os dados de seu cadastro na infraestrutura de TIC (Tecnologias da Informação e Comunicação) do Instituto de Informática. Esses dados

incluem o endereço de e-mail, o usuário (login) e uma senha gerada aleatoriamente.

O ingressante receberá estes dados após preenchimento e assinatura de um termo de compromisso, por meio do qual se comprometerá a utilizar os recursos computacionais do Instituto de Informática conforme as Políticas de Uso instituídas por este documento.

O preenchimento do termo de compromisso é obrigatório, com atenção aos seguintes itens: o nome completo do ingressante deve ser preenchido sem abreviações e no termo de compromisso deve constar o e-mail alternativo do ingressante.

Os dados cadastrais do ingressante no Instituto de Informática garante a ele acesso aos sistemas mantidos pela equipe do NRC, tais como:

1. Serviço de e-mail institucional;
2. Rede sem fio;
3. Diretório pessoal;
4. Intranet (Wiki, tutoriais e documentação em geral);
5. Serviço de conversação (*chat*);
6. Outros serviços de acesso restrito.

Após o primeiro acesso aos sistemas, o usuário deverá mudar a sua senha, seguindo as regras especificadas neste documento.

O e-mail alternativo, fornecido durante o preenchimento do termo de compromisso, tem por objetivo a recuperação automática de acesso ao recursos computacionais do Instituto de Informática, caso o usuário perca sua senha.

Em casos excepcionais, visitantes poderão fazer uso de contas temporárias. Os dados das contas temporárias deverão ser solicitadas junto à coordenação administrativa.

2.3 Políticas de uso do e-mail

Esta seção tem por objetivo definir as normas de utilização do e-mail institucional que engloba desde o envio e recebimento de e-mails até o gerenciamento da conta.

1. O e-mail deve ser utilizado de forma responsável, evitando qualquer tipo de perturbação a outras pessoas, seja por meio de linguagem inapropriada, frequência ou tamanho das mensagens.
2. O *webmail* fornecido pela equipe de redes do NRC é a forma recomendada de acesso ao e-mail institucional.
3. Clientes de e-mail, tais como, Microsoft Outlook, Mozilla Thunderbird, Kmail, Evolution e outros podem ser utilizados por meio da configuração das portas seguras de envio e recebimento de e-mail. No entanto, o NRC não é responsável pela configuração dos clientes e nem mesmo pelos erros decorrentes da má configuração dos mesmos.

4. O redirecionamento de e-mails para servidores não hospedados no Instituto de Informática não é uma prática recomendada. Caso o usuário resolva utilizá-la, deve estar ciente de que o NRC não se responsabiliza por perda de mensagens, erros de configurações ou por períodos de indisponibilidade ou instabilidade de servidores externos para os quais o usuário redirecionou e-mails institucionais.

5. É proibido o envio de grande quantidade de mensagens de e-mail (*spam*), isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política.

6. É proibido o envio de e-mail mal-intencionado, correntes, golpes, boatos ou sobrecarregar um usuário, site ou servidor de e-mail com e-mails muito extensos ou dividido em numerosas partes.

7. É proibido o envio de e-mail que configure a prática de *phishing*, ou seja, a tentativa de conseguir de forma ílicita os dados pessoais de outrém.

8. É proibido o envio por e-mail de *virus*, *worms*, *trojans*, *keyloggers* ou quaisquer outros tipos de *malware*.

9. É proibido forjar qualquer das informações do cabeçalho do remetente de uma mensagem.

10. É dever do usuário do e-mail institucional estar atento a sua cota de e-mail. As cotas de e-mail são definidas da seguinte forma:

    - Alunos de graduação, alunos de especialização e alunos especiais dos programas de pós-graduação: 500MB;
    - Alunos de mestrado: 1GB;
    - Alunos de doutorado e funcionários técnico-administrativos: 2GB;
    - Docentes: 4GB.

11. O e-mail institucional não pode ser utilizado para veicular conteúdo pornográfico, preconceituoso, ofensivo ou ilegal.

12. O usuário que se desligar do Instituto de Informática terá sua conta excluída e seus dados mantidos por um período de 6 meses.

2.4 Políticas de uso do diretório pessoal

1. O acesso ao diretório pessoal é feito por meio da porta 22, utilizando os dados da conta pessoal e o endereço de destino home.inf.ufg.br.

2. Não são permitidas tentativas de obter acesso a outras contas, não autorizadas, independente do meio utilizado para tal ou ainda colocar à prova a segurança do servidor home.inf.ufg.br.

3. Não é permitido o uso do servidor home.inf.ufg.br para tentativas de penetração em outras redes. Isso inclui ataques, tentativas de provocar congestionamentos ou tentativas deliberadas de sobrecarregar um servidor de rede.

4. O usuário deve fazer manutenção no diretório pessoal que dispõe no servidor home.inf.ufg.br, evitando acúmulo de arquivos desnecessários.

5. É dever do usuário estar atento a sua cota do diretório pessoal. As cotas do diretório pessoal são definidas da seguinte forma:

   - Alunos de graduação, alunos de especialização e alunos especiais dos programas de pós-graduação: 200MB;
   - Alunos de mestrado: 1GB;
   - Alunos de doutorado: 2GB;
   - Funcionários técnico-administrativos: 5GB;
   - Docentes: 15GB.

6. Conteúdos de natureza pornográfica, preconceituosa, ofensiva ou ilegal não podem ser obtidos, armazenados ou distribuídos por meio do servidor home.inf.ufg.br.

7. O subdiretório public_html, disponível no diretório pessoal, pode ser utilizado para disponibilizar conteúdo acadêmico, o que inclui códigos escritos em html. No entanto, por questões de segurança, códigos escritos em php não são interpretados pelo servidor home.inf.ufg.br.

8. O subdiretório public_html não pode ser utilizado para disponibilizar conteúdo sigiloso. Devem estar disponíveis apenas informações públicas.

2.5 Políticas de acesso à Internet

Esta seção tem por objetivo definir como deverá ser o acesso à Internet por meio da infraestrutura de rede sob tutela do NRC, englobando desde a navegação por sites até *downloads* e *uploads* de arquivos.

1. O acesso à Internet feito dentro do Instituto de Informática é uma ferramenta de trabalho, estudo, pesquisa, extensão e administração universitária e, portanto, deve ser usado para esses fins.

2. É expressamente proibido utilizar os recursos da rede para obtenção ou distribuição de *software* ou dados que infrinjam alguma lei, licença ou patente.

2.6 Políticas de acesso à rede sem fio

Existem duas redes sem fio sob tutela do NRC, sendo elas: INFWLAN e PROFINFWLAN.

A INFWLAN é aberta a toda a comunidade de discentes, docentes e funcionários técnico-administrativos do Instituto de Informática.

A PROFINFWLAN é restrita aos docentes e funcionários técnico-administrativos.

O acesso à rede sem fio deverá ser feito conforme o que é estabelecido a seguir:

1. Assim como a rede cabeada, a rede sem fio é uma ferramenta de trabalho, estudo, pesquisa, extensão e administração universitária e, portanto, deve ser usada para esses fins.

2. Assim como o acesso ao *webmail*, o acesso à rede sem fio é feito por meio de usuário e senha, previamente cadastrados, conforme o que foi estabelecido na seção 2.2.

3. É expressamente proibido utilizar os recursos da rede sem fio para obtenção ou distribuição de *software* ou dados que infrinjam alguma lei, licença ou patente.

4. Os dados utilizados para acesso à rede sem fio são pessoais e intransferíveis.

3 Políticas de uso da rede nos laboratórios de pesquisa

Com o objetivo de prover maior flexibilidade e menos restrições aos laboratórios de pesquisa do Instituto de Informática, foi configurada uma rede lógica que é isolada do restante da infraestrutura do Instituto de Informática. Doravante chamada rede externa.

Sob o ponto de vista da rede sob tutela do NRC, a rede externa é tão hostil quanto a Internet.

No entanto, do ponto de vista da UFG e do restante do mundo, a rede externa pertence ao Instituto de Informática e, portanto, a rede externa também está sujeita às políticas de uso e segurança definidas pelo equipe de redes e sistemas do NRC. Assim, os docentes que gerenciam os laboratórios de pesquisa são responsáveis por observar e fazer cumprir tais políticas.

Caso o responsável pelo laboratório de pesquisa não deseje manter um servidor em suas dependências, e assim usufruir de flexibilidade e menos restrições, ele poderá optar por ter o laboratório sob sua responsabilidade incluso na mesma rede dos laboratórios de ensino e assim ficar sujeito às regras específicas desse ambiente.

3.1 Regras gerais

O laboratório de pesquisa receberá um endereço IP público e deverá, por sua conta, criar, configurar e manter um servidor que forneça os serviços mínimos para o funcionamento do laboratório, dentre eles: NAT e Firewall. O servidor deverá ser mantido dentro das dependências do laboratório.

Além disso, as regras abaixo devem ser observadas:

1. O pleno funcionamento do servidor localizado no laboratório é de inteira responsabilidade do responsável pelo laboratório;

2. A senha de administrador/root do servidor deverá ter as seguintes caracteristicas:

    - Ser memorizada pelo administrador do laboratório, o que implica que ela não deverá ser encontrada escrita em agendas, memorandos ou similares;
    - Ter um comprimento mínimo de 8 caracteres;
    - Ser formada por letras, números e caracteres especiais;

- Não ser derivada de dados pessoais, tais como nomes de membros da família;
- Ser periodicamente trocada.

3. É proibido aos usuários do laboratório de pesquisa propagar vírus de computador ou qualquer programa de computador que possa causar danos permanentes ou temporários em equipamentos de terceiros;

4. É proibido utilizar a rede de computadores do laboratório para efetuar levantamento não autorizado de informações (*scan*) na rede de computadores do laboratório, do Instituto de Informática ou de terceiros;

5. É proibido forjar endereços da camada de rede (IP) ou da camada de enlace (MAC) na tentativa de responsabilizar terceiros ou ocultar a identidade ou autoria de atos ilícitos praticados nas dependências do laboratório;

6. Materiais protegidos por direito autoral ou quaisquer outros direitos de propriedade intelectual não devem ser transmitidos, distribuídos ou armazenados nos computadores dos laboratórios;

7. Todas as regras citadas nas seções 2.1 e 2.5 devem ser cumpridas nos laboratórios de pesquisa.

3.2 Uso de rede sem fio nos laboratórios

O laboratório que desejar fazer uso de rede sem fio própria deverá estar atento às seguintes regras:

1. O roteador sem fio instalado nas dependências do laboratório funcionará em carater secundário em relação à rede sem fio do Instituto de Informática. Entende-se por caráter secundário a operação de dispositivos em canais de comunicação e em níveis de potência que não interfiram, significativamente, na operação de dispositivos que operam em caráter primário.

2. O roteador sem fio não poderá ter antenas com ganhos superiores a 3 dB, casos excepcionais serão apreciados pela equipe de redes e sistemas.

3. A conexão do roteador ao restante da rede deverá sempre ser feita por meio de uma VLAN. Em roteadores comuns, a porta WAN pode ser utilizada para este fim. O serviço de DHCP do roteador deverá servir apenas à interface *wireless*.

4. O SSID da rede sem fio dos laboratórios deverá ser oculto.

5. Os dados para acesso à rede sem fio utilizada no laboratório não poderão ser repassadas para usuários que não tenham vínculo com o Instituto de Informática.

4 Políticas de uso de servidores físicos e de máquinas virtuais para projetos de pesquisa e extensão

Equipamentos de rede, tais como, servidores, *switches*, *nobreaks* e *racks* constituem a infraestrutura física de redes e sistemas do NRC.

O espaço físico destinado a esses equipamentos será doravante chamado de *Datacenter*.

O *Datacenter* possui infraestrutura de energia elétrica, climatização e restrição de acesso essenciais para o seu funcionamento adequado.

O *Datacenter* poderá ser usado por docentes e funcionários técnico-administrativos envolvidos em projetos de pesquisa e extensão conforme dispõe os termos das seções 4.1 e 4.2.

4.1 Políticas de uso de servidores físicos

1. Respeitando os limites de espaço físco, de infraestrutura elétrica e de planejamento do NRC, o docente participante de um projeto de pesquisa ou extensão poderá pleitear a instalação de um servidor físico no *Datacenter* do Instituto de Informática. O pleito deve ser feito por meio do sistema de assistência ao usuário, antes da aquisição do servidor.

2. A critério do NRC, pautado pelas necessidades do Instituto de Informática de expansão de sua infraestrutura, poderá ser solicitado ao docente responsável pelo projeto uma contrapartida. A contrapartida poderá ser na forma de aquisição de equipamentos de rede e/ou *nobreaks* ou na forma de disponibilização de recursos do servidor instalado no *Datacenter*.

3. O servidor deverá ser necessariamente um servidor para *racks* de 19 polegadas. É recomendável que o servidor seja capaz de operar em todas as tensões do intervalo entre 100 e 230 Volts, tenha alimentação redundante e que não ocupe mais de 3 unidades de *rack* (cada unidade de *rack* possui 1,5 polegada).

4. O acesso físico ao servidor, localizado no *Datacenter*, só poderá ser feito por pessoal autorizado acompanhado de um dos analistas da equipe de redes e sistemas do NRC. A lista de pessoal autorizado deverá ter sido enviada, previamente, por meio do sistema de assistência ao usuário, à equipe de redes do NRC.

5. A senha de administrador/root do servidor deverá ter as seguintes características:

    - Ser memorizada pelo administrador do servidor, o que implica que ela não deverá ser encontrada escrita em agendas, memorandos ou similares;
    - Ter um comprimento mínimo de 8 caracteres;
    - Ser formada por letras, números e caracteres especiais;
    - Não ser derivada de dados pessoais, tais como nomes de membros da família;
    - Ser periodicamente trocada.

6. É proibido utilizar o servidor para propagar vírus de computador ou qualquer programa de computador que possa causar danos permanentes ou temporários em equipamentos de terceiros.

7. É proibido utilizar o servidor para efetuar levantamento não autorizado de informações (*scan*) na rede de computadores do laboratório, do Instituto de Informática ou de terceiros.

8. É proibido forjar endereços da camada de rede (IP) ou da camada de enlace (MAC) na tentativa de responsabilizar terceiros ou ocultar a identidade ou autoria de atos ilícitos praticados por meio do servidor;

9. Materiais protegidos por direito autoral ou quaisquer outros direitos de propriedade intelectual não devem ser obtidos, distribuídos ou armazenados no servidor.

4.2 Políticas de uso de máquinas virtuais

1. Respeitando os limites de espaço em disco, processamento e memória RAM, o docente participante de um projeto de pesquisa ou extensão poderá pleitear uma máquina virtual (VM) dentro da infraestrutura do *Datacenter* do Instituto de Informática.

2. A máquina virtual será disponibilizada com a última versão do sistema operacional OpenSuSE, arquitetura de 64 bits e recursos de memória RAM, disco e processamento de acordo com a disponibilidade.

3. Os membros da equipe de redes terão usuários na máquina virtual e poderão instalar aplicativos de monitoramento e segurança. Esses usuários não poderão ser removidos da VM. Outros usuários poderão ser criados, sob responsabilidade do docente, desde que esses usuários façam parte do corpo técnico, docente ou discente do Instituto de Informática.

4. O pleno funcionamento da VM é de inteira responsabilidade do docente responsável por ela. Se a máquina virtual for controlada por uma máquina física também sob tutela do docente, cabe a ele a manutenção do hipervisor, dos arquivos de configuração da VM e de todos os recursos que garantam o bom funcionamento dela. Se a VM sob responsabilidade do docente for controlada por máquina física sob a tutela da equipe de redes e sistemas do NRC, essa equipe será responsável pela manutenção do hipervisor e dos arquivos de configuração da VM.

5. A VM deverá receber manutenção periódica por parte do docente. Serviços não utilizados deverão ser desativados.

6. A senha de administrador/root da VM deverá ter as seguintes características:

    - Ser memorizada pelo administrador da VM, o que implica que ela não deverá ser encontrada escrita em agendas, memorandos ou similares;
    - Ter um comprimento mínimo de 8 caracteres;
    - Ser formada por letras, números e caracteres especiais;

- Não ser derivada de dados pessoais, tais como nomes de membros da família;
- Ser periodicamente trocada.

7. É proibido utilizar a VM para propagar vírus de computador ou qualquer programa de computador que possa causar danos permanentes ou temporários em equipamentos de terceiros.

8. É proibido utilizar a VM para efetuar levantamento não autorizado de informações (*scan*) na rede de computadores do Instituto de Informática ou de terceiros.

9. É proibido forjar endereços da camada de rede (IP) ou da camada de enlace (MAC) na tentativa de responsabilizar terceiros ou ocultar a identidade ou autoria de atos ilícitos praticados por meio da VM;

10. Materiais protegidos por direito autoral ou quaisquer outros direitos de propriedade intelectual não devem ser obtidos, distribuídos ou armazenados na VM.

5 Sanções

1. O NRC poderá aplicar sanções aos que violarem esse conjunto de políticas de uso e segurança dos recursos computacionais do Instituto de Informática, sem prejuízo das sanções legais cabíveis.

2. Uma vez identificado a não conformidade com os termos desse conjunto de políticas de uso e segurança, o NRC poderá aplicar redução ou interrupção do acesso à infraestrutura de rede por prazo indefinido, para usuários e laboratórios.

3. É facultado ao NRC o direito de desativar uma conta de usuário, caso se verifique o seu mau uso. Entende-se por mau uso:

   - Incidentes suspeitos de tentativa indevida de intrusão;
   - Compartilhamento de senha;
   - Exposição de conteúdo indevido;
   - Utilização dos dados da conta pessoal para tentativas de se passar por usuário não legítimo, tanto na rede sob a tutela do NRC quanto fora dela;
   - Qualquer uso que infrinja as políticas definidas neste documento.

4. Os usuários que forem reincidentes terão suas contas excluídas definitivamente.

5. O NRC poderá excluir contas de alunos, funcionários técnico-administrativos ou docentes que tiverem contas inativas por um período superior a 6 meses.