HOSPITAL UNIVERSITÁRIO
PROF. ALBERTO ANTUNES
HUPAA-UFAL

Política de Segurança da Informação

Objetivo

Prestar serviços de rede de alta qualidade e ao mesmo tempo desenvolver um comportamento extremamente ético e profissional. Assim, para assegurar os altos padrões de qualidade na prestação desses serviços, faz-se necessária a especificação de uma política de utilização da rede.

Essa Política de Utilização da Rede descreve as normas de utilização e atividades que entendemos como violação ao uso dos serviços e recursos, os quais são considerados proibidos.

Definição

Podemos definir como serviços e recursos os equipamentos utilizados pelos funcionários tais como: computadores, e-mails do domínio hu.ufal.br acesso a Internet e afins.

As normas descritas no decorrer deste documento não constituem uma relação exaustiva e podem ser atualizadas com o tempo, sendo que qualquer modificação será avisada em tempo hábil para remodelação (se necessário) do ambiente.

Tais normas são fornecidas a título de orientação ao funcionário. Em caso de dúvida sobre o que é considerado, de alguma forma, violação, o usuário deverá enviar previamente um e-mail para nti@hupaaufal.org visando esclarecimentos e segurança.

Nos termos da Política de Utilização da Rede, a instituição procederá ao bloqueio do acesso ou cancelamento do usuário caso seja detectado uso em desconformidade com o aqui estabelecido ou de forma prejudicial à Rede.

Caso seja necessário advertir o funcionário, será informado ao departamento de recursos humanos para interagir e manter-se informado da situação.

Atitudes que são consideradas violação à Política de Utilização da Rede foram divididas nos seguintes tópicos:

1. Utilização da Rede;
2. Utilização de E-Mail;
3. Utilização de acesso a Internet;
4. Utilização de equipamentos de informática;
5. Acesso ao ambiente físico do NTI;
6. Procedimentos de Backup.

Abaixo descreveremos as normas mencionadas e informamos que tudo o que não for permitido e/ou liberado é considerado violação à Política da Utilização da Rede.

1. Utilização da Rede

Esse tópico visa definir as normas de utilização da rede que engloba desde o *login*, manutenção de arquivos no servidor e tentativas não autorizadas de acesso.

1.1. Concessão de acesso

a) O solicitante deverá preencher o formulário de conta de usuário (Anexo I) onde consta também o aceite da politica de segurança que pode ser encontrado no site da instituição (www.hu.ufal.br) e no NTI.

b) O nome da conta (*login*) será o primeiro nome do usuário seguido pelas iniciais do seu sobrenome. De forma alguma essa conta poderá ser um nome genérico como, por exemplo, um setor ou departamento.

c) A senha obrigatoriamente deverá conter no mínimo 6 (seis) caracteres e terá que ser alterada a cada 3 (três) meses. Haverá o bloqueio da conta do usuário caso a senha seja digitada errada por 3 (três) vezes. O usuário que não utilizar a sua conta por mais de 90 (noventa) dias será desativado.

d) A conta do usuário não poderá ser utilizada em mais de um computador simultaneamente.

e) Quando o usuário for desligado da instituição sua conta será desativada. O setor de recursos humanos deverá informar ao NTI para que tal ação seja efetuada.

f) A conta de estagiário deverá ser renovada a cada 6 (seis) meses.

g) A conta de usuário, independente do sistema a ser acessado ou rede, é pessoal e intransferível, não podendo em hipótese alguma ser cedido para outros usuários sob pena de revogação da mesma.

1.2. Manutenção de acesso

1.1. Independentemente do sistema acessado pelo usuário, existe por parte da área de TI uma revisão periódica de todos os usuários e seus respectivos perfis de acesso, com isso podemos suspender tempestivamente os acessos indevidos a transações críticas.

2. Concessão de acesso à rede

a) Todo equipamento de rede (*access point*, roteador, switch, etc.) deverá ser configurado pelo NTI (Núcleo de Tecnologia da Informação).

b) Não é permitido que ninguém coloque equipamentos na rede HUPAA sem prévia autorização do NTI.

c) O solicitante deverá preencher o formulário de acesso à rede (Anexo I) onde consta também o aceite da política de segurança que pode ser encontrado no site da instituição (www.hu.ufal.br) e no NTI.

d) Não é permitido tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes.

e) Não é permitido tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo "negativa de acesso", provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor.

f) Não é permitido o uso de qualquer tipo de programa ou comando designado a interferir com sessão de usuários.

g) A estação de trabalho do usuário será bloqueada caso o sistema fique ocioso por 15 minutos e só poderá ser desbloqueada pelo usuário logado ou por um usuário administrador. D esta maneira será evitado o acesso por pessoas não autorizadas.

h) É proibido o acúmulo de arquivos inúteis no diretório pessoal, seja no servidor ou na estação.

i) Material de natureza pornográfica, preconceituosa e racista não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede.

j) Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas. As áreas de armazenamento de arquivos são designadas conforme abaixo:

Compartilhamento	**Utilização**
Diretório U: (Usuário)	Arquivos Pessoais inerentes à instituição
Diretório S: (Setor)	Arquivos do setor em que trabalha
Diretório T: (temporário)	Arquivos temporários ou de compartilhamento geral

k) Em alguns casos pode haver mais de um compartilhamento referente aos arquivos do departamento ao qual faz parte.

l) A pasta TEMPORARIO ou similar, não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível.

m) Haverá limpeza mensal dos arquivos armazenados na pasta TEMPORARIO, para que não haja acúmulo desnecessário de arquivos.

n) Não será permitido manter arquivos pessoais, tais como fotos, arquivos de música ou vídeos, documentos não inerentes a instituição nas pastas TEMPORARIO e SETORIAL. Exemplo : arquivos .mp3, .avi, .wmv.

o) É obrigatório armazenar os arquivos inerentes à instituição no servidor de arquivos para garantir o backup dos mesmos.

p) É proibida a instalação ou remoção de softwares que não forem acompanhadas pelo NTI.

q) Não será permitida a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro.

3. Utilização de E-mail

Esse tópico visa definir as normas de utilização de e-mail que engloba desde o envio, recebimento e gerenciamento das contas.

a) É proibido o assédio ou perturbação de outrem, seja através de linguagem utilizada, frequência ou tamanho das mensagens.

b) É proibido o envio de e-mail não relacionado à instituição a qualquer pessoa que não o deseje receber. Se o destinatário solicitar a interrupção de envio de e-mails, o usuário deve acatar tal solicitação e não lhe enviar qualquer e-mail.

c) É proibido o envio de grande quantidade de mensagens de e-mail ("junk mail" ou "spam") que, de acordo com a capacidade técnica da Rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política.

d) É proibido o uso de e-mails setoriais que não estejam no domínio da instituição (hu.ufal.br) exemplo : setor@gmail.com, setorhu@hotmail.com.

e) É proibido reenviar ou de qualquer forma propagar mensagens em cadeia ou "pirâmides", independentemente da vontade do destinatário de receber tais mensagens.

f) É proibido o envio de e-mail mal-intencionado, tais como "*mail bombing*" ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso ou numerosas partes de e-mail.

g) É proibido forjar qualquer das informações do cabeçalho do remetente.

h) Não é permitido má utilização da linguagem em respostas aos e-mails oficiais, tais como abreviações de palavras (Ex.: “vc” ao invés de “você”).

4. Utilização de acesso a Internet

Esse tópico visa definir as normas de utilização da Internet que engloba desde a navegação a *sites*, *downloads* e *uploads* de arquivos.

a) É proibido utilizar os recursos da instituição para fazer o *download* ou distribuição de *software* ou dados não legalizados.

b) É proibido a divulgação de informações confidenciais da instituição em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei.

c) Caso a instituição julgue necessário haverá bloqueios de acesso à:

(1) Arquivos que comprometam o uso de banda ou perturbe o bom andamento dos trabalhos;
(2) Domínios que comprometam o uso de banda ou perturbe o bom andamento dos trabalhos.

d) Haverá geração de relatórios dos *sites* acessados por usuário e se necessário a publicação desse relatório.

e) Não é permitida a utilização de *softwares* de *peer-to-peer* (P2P), tais como Kazaa, Morpheus e afins.

f) Não é permitida a utilização de serviços de *streaming*, tais como rádios *on-line*, youtube e afins.

g) É proibido a navegação em *sites* que tem a finalidade de esconder e/ou burlar o *site* que realmente é exibida, sendo este proibido na instituição.

5. Utilização de equipamentos de informática

Esse tópico visa definir as normas de utilização de equipamentos de informática disponíveis na rede interna.

a) É vedada a abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo deverá ocorrer pelo NTI.

b) É de responsabilidade do usuário do equipamento zelar pelo mesmo, mantendo a boa aparência. Não é permitido personalizar o equipamento colocando adesivos, fotos, riscar, raspar e retirar etiqueta de patrimônio.

c) É proibido alterar as configurações originais do equipamento sem a devida autorização do NTI. Exemplo: memórias, disco, unidade de CD/DVD, placa mãe, cooler ou qualquer outro componente.

d) Todo computador deverá ingressar no domínio da rede HUPAA e praticar as políticas de rede da instituição como, por exemplo, papel de parede e antivírus.

e) O NTI não se responsabiliza por prestar manutenção ou instalar softwares em computadores que não sejam os da instituição.

5.1. Utilização de notebooks e dispositivos móveis

a) Fica autorizado o uso de notebooks e dispositivos móveis na rede da instituição mediante cadastro prévio e liberação do NTI;

b) O solicitante deverá preencher o formulário de acesso à rede (Anexo I) onde consta também o aceite da política de segurança que pode ser encontrado no site da instituição (www.hu.ufal.br). O solicitante não funcionário da instituição terá seu acesso liberado por um determinado período devendo fazer uma nova solicitação ao final deste;

c) O NTI deverá fazer uma verificação das configurações de rede e do aplicativo de antivírus instalado para que o acesso a rede seja concedido. Caso o notebook não obedeça os requisitos mínimos de segurança o acesso a rede não será liberado;

d) O NTI tem o direito de, periodicamente, auditar os notebooks utilizados na instituição, visando proteger suas informações bem como garantir que aplicativos ilegais não estejam sendo executados na instituição.

e) É de reponsabilidade do proprietário a instalação do Sistema Operacional que será utlizado, bem como dos aplicativos a serem utilizados no notebook, salvo exceções de aplicativos específicos autorizados pelo NTI.

f) É de responsabilidade do proprietário manter sempre o aplicativo de antivírus atualizado em seu notebook. Caso não tenha nenhum aplicativo de antivírus instalado em seu notebook, o uso do mesmo fica proibido na instituição.

g) É de responsabilidade do proprietário usar somente aplicativos legalizados em seu notebook.

h) É de responsabilidade do NTI as configurações relativas aos dispositivos de rede e configurações de domínio no ambiente da instituição que precisam ser realizadas para o funcionamento em rede dos notebooks.

i) Não podem ser executados nos notebooks aplicativos de característica maliciosa, que visam comprometer o funcionamento da rede, bem como a captura de informações confidenciais, como por exemplo: senhas de usuários.

j) Fica proibida a apropriação de arquivos que não sejam de uso pessoal do proprietário do notebook. Todos os arquivos que pertençam a instituição não podem ser carregados nos notebooks ou dispositivos de armazenamento móvel (ex.: pendrive), sem autorização da área responsável pelos dados.

6. Acesso ao Ambiente físico do NTI

Esse tópico visa definir as normas de acesso ao ambiente físico do setor de NTI, em especial a sala dos servidores.

a) Fica a critério da coordenação do NTI, delegar quem pode ou não ter acesso a sala dos servidores e fazer utilização de qualquer equipamento que estiver no ambiente.

b) É terminantemente proibido o acesso de qualquer pessoa que não tenha sido previamente autorizada pela coordenação do NTI na sala de servidores, seja qual for o motivo.

7. Procedimentos de Backup

a) Todos os backups devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial, períodos de pouco ou nenhum acesso de usuários ou processos aos sistemas de informática.

b) Os funcionários responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

c) As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

d) As mídias de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

e) O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

f) É necessário ser mantido um estoque constante das mídias para qualquer uso emergencial.

g) Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser executados apenas mediante justificativa de necessidade.

h) Testes de restore de qualquer tipo de backup devem ser executados pelos seus responsáveis periodicamente e devidamente documentados. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

i) Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador responsável.

Disposições Gerais

Para garantir as regras mencionadas acima a instituição se reserva no direito de:

(1) Implantar *softwares* e sistemas que podem monitorar e gravar todos os usos de internet através da rede e das estações de trabalho da instituição;
(2) Inspecionar qualquer arquivo armazenado na rede, seja no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política.

Punições

O não cumprimento pelo funcionário das normas ora estabelecidas neste Documento (Políticas de segurança da Informação), seja isolada ou cumulativamente, poderá ensejar, de acordo com a infração cometida, as seguintes punições:

Comunicação de Descumprimento

A primeira notificação será encaminhada ao funcionário informando o descumprimento da norma, com a indicação precisa da violação praticada.

A segunda notificação será encaminha para a chefia do setor do infrator. Todas as notificações serão arquivadas junto ao setor de recursos humanos na respectiva pasta funcional do infrator.