

Política de Uso do Projeto iINTERNET SEM FIO

Sumário

1	Introdução.....	2
2	Público alvo.....	2
3	Objetivo.....	3
4	Política de uso.....	3
4.1	Usuários.....	4
4.2	Autenticação dos Usuários.....	5
4.3	Captive Portal.....	6
4.4	Regras gerais para usuários.....	6
4.5	Violação das regras.....	7
4.6	Penalidades.....	8
5	Considerações finais.....	9

1 Introdução

A rede sem fio do projeto Wi-Fi Paraná foi concebida para complementar a rede cabeada. Ela não deve ser vista como uma rede exclusiva ou substituta à rede cabeada atual. O propósito da infraestrutura da rede sem fio é permitir acesso a rede de dados e a Internet através de dispositivos móveis e também cobrir certas áreas com ausência de infraestrutura de rede cabeada.

Ela é adequada ao uso em pequenos intervalos de tempo, como consultas de email ou navegação na web. O uso para transferência de grandes arquivos, aplicações cliente-servidor ou de conexões constantes não é recomendado na rede sem fio. Estas atividades terão melhor desempenho através da rede cabeada.

O serviço estará disponível 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana nas dependências das instituições, entretanto poderá, eventualmente, sofrer quedas de desempenho ou interrupções devido as seguintes circunstâncias externas:

- Manutenções técnicas e/ou operacionais que exijam o desligamento temporário do sistema ou impossibilitem o acesso;
- Casos fortuitos ou força maior;
- Falta de fornecimento de energia elétrica;
- Defeitos, falha ou pane nos equipamentos;
- Ocorrências de falhas no link de acesso à Internet;
- Em função de condições técnicas e/ou ambientais que podem interferir com o sinal emitido pelos roteadores, não há garantia na manutenção do mesmo em condições adversas e os usuários devem estar cientes da possibilidade de perda de comunicação ou de informações.

Seu uso deve estar de acordo com esta política.

2 Público alvo

Professores, alunos, funcionários administrativos e visitantes.

3 Objetivo

O propósito desta política é oferecer acesso seguro em rede sem fio nas Universidades e Faculdades Estaduais do Paraná e prover acesso à Internet de acordo com os termos e condições descritas neste documento.

Nos locais onde houver cobertura da rede sem fio fornecida pelo projeto Wi-Fi Paraná não será permitida a instalação de outras redes sem fio. Em locais sem cobertura da rede sem fio somente será permitida a instalação de dispositivos para rede sem fio com a orientação do responsável pela rede local na instituição.

4 Política de uso

A política de utilização da rede sem fio tem como objetivo estabelecer regras e normas de utilização e ao mesmo tempo desenvolver um comportamento ético e profissional aos usuários desta rede nas dependências das Universidades e Faculdades do Estaduais do Paraná.

Assim, para assegurar a qualidade na prestação dos serviços da rede sem fio, faz-se necessária a especificação de uma política de utilização.

Tal política e normas fornecidas têm teor informativo e de orientação ao usuário, quanto ao uso da solução de rede sem fio.

Nos termos da política de utilização da rede, quanto ao aspecto de “violação” e uso indevido dos recursos, a direção da instituição poderá proceder ao bloqueio de acesso ou cancelamento da conta do usuário, caso seja detectado e evidenciado o uso em desconformidade com o estabelecido e que tenha causado prejuízo aos serviços da rede sem fio.

Ao efetivar seu cadastro para o uso da rede sem fio, o usuário aceita expressamente, sem reservas ou ressalvas, todas as condições estipuladas neste documento, aderindo ao presente contrato.

O usuário é responsável por todos os atos oriundos da utilização deste serviço, quer seja de acesso, visualização, divulgação, legal ou ilegal, devendo manter seu login e senha em absoluto sigilo.

O usuário compromete-se a fazer uso da senha de forma segura e confidencial, zelando por sua guarda e confidencialidade, declarando-se ciente de que não poderá vender, transferir, ceder ou emprestar a outrem, a qualquer título, a senha que é de caráter pessoal e intransferível.

A instituição poderá suspender ou cancelar o acesso do usuário, sem prévio aviso, na hipótese de identificar o mesmo como divulgador de imagens de pedofilia, crimes financeiros, disseminação de vírus, malwares, trojans, que violem direitos autorais ou práticas ilícitas, que induzam ou provoquem riscos a terceiros, práticas enganosas, etc.

4.1 Usuários

Quatro tipos de usuários foram definidos para este projeto:

- Professores;
- Funcionários Administrativos;
- Alunos;
- Visitantes.

Cada um destes usuários possuem perfis diferenciados para acesso à rede sem fio.

No caso específico deste projeto apenas dois SSIDs serão utilizados:

- SSID com valor “wifiXXX”, onde XXX é o nome da instituição;
- SSID com valor “visitante”.

Os usuários visitantes irão se conectar ao SSID “visitante” e serem direcionados ao CaptivePortal.

Os professores, alunos e funcionários administrativos irão se conectar ao SSID “wifiXXX”.

Quem desejar usufruir desta tecnologia deverá preencher um formulário com as informações necessárias ao cadastramento.

O usuário receberá um username ("nome do usuário") e uma senha gerada pelo sistema; no primeiro acesso, é recomendável orientá-lo para que efetue a troca da senha atribuída pelo sistema.

Visitantes deverão obter autorização da instituição, em tempo hábil, no sentido de viabilizar o uso provisório da rede sem fio. A viabilidade será analisada individualmente.

4.2 Autenticação dos Usuários

O projeto segue a recomendação 802.11i do IEEE para a autenticação dos usuários utilizando 802.1x e WPA2 Enterprise.

O 802.1x é um padrão do IEEE que define uma estrutura de autenticação para WLANs utilizando o protocolo EAP (Extensible Authentication Protocol) para a troca de mensagens durante o processo de autenticação.

Neste projeto foi definido o PEAP (Protected EAP) utilizando o método PEAP-MSCHAP-v2 (PEAP-Microsoft Challenge Handshake Authentication Protocol Version 2) que utiliza TLS (Transport Layer Security) para criar um túnel criptografado entre o usuário a ser autenticado e o servidor de autenticação.

Já o WPA2 (WiFi Protected Access version 2) utiliza AES (Advanced Encryption Standard) para a criptografia dos dados do usuário que trafegam na interface aérea.

O uso de EAP-PEAP-MSCHAPv2 requer a instalação do certificado digital do servidor AAA nos dispositivos sem fio que irão utilizar a rede.

Este certificado digital é único e será disponibilizado pela Celepar às instituições de ensino do projeto, que tem a responsabilidade de distribuir e instalar nos dispositivos dos usuários da rede sem fio.

Os usuários do SSID "visitante" não utilizarão 802.1x e WPA2. Durante o processo de autenticação terão seu login e senha protegidos por SSL (Secure Socket Layer) provido pela página do Captive Portal, porém uma vez autenticados não contarão com a criptografia de seus dados transmitidos via interface aérea, este método é conhecido como autenticação aberta.

4.3 Captive Portal

A funcionalidade Captive Portal permite a um cliente da rede sem fio se autenticar via um portal baseado em HTTPS.

Neste projeto foi implementado um Captive Portal para o SSID “visitante”. Um ponto de contato de cada instituição terá acesso à página de registro dos usuários visitantes, cadastrando um login e uma senha para os mesmos.

No caso específico da funcionalidade de Captive Portal, os dados referentes aos usuários cadastrados serão armazenados em banco de dados.

O tráfego de dados dos usuários visitantes não são criptografados.

4.4 Regras gerais para usuários

O acesso à rede sem fio somente será permitido aos usuários devidamente cadastrados no sistema de controle de acesso.

O login e senha de acesso cadastrado no ato da formalização do acesso à rede sem fio da instituição é pessoal e intransferível, sendo o usuário o único responsável por qualquer ato (legal ou ilegal) decorrente do uso da Internet utilizando seu login e senha.

Nenhum funcionário das instituições tem acesso ao login e senha do usuário e nem estará autorizado a solicitar ao mesmo essa informação, em nenhuma hipótese.

O usuário deve conhecer as regras e penalidades, sendo elas:

- Não se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais;
- Responsabilizar-se pela sua identidade eletrônica, senha, credenciais de autenticação, autorização ou outro dispositivo de segurança, negando revelá-la a terceiros;
- Responder pelo mau uso dos recursos computacionais em qualquer circunstância;
- Responder por atos que violem as regras de uso dos recursos computacionais,

estando, portanto, sujeito às penalidades definidas na política de uso desses recursos;

- O usuário deve manter seus computadores pessoais com software (patches, erratas) e antivírus atualizados, conforme orientação do administrador de rede.

4.5 Violação das regras

Considera-se violação das regras o seguinte:

- Infringir qualquer lei ou regulamento local, estadual, nacional ou internacional aplicável;
- Mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos;
- Utilizar o acesso à Internet para instigar, ameaçar ou ofender, abalar a imagem, invadir a privacidade ou prejudicar outros membros da comunidade Internet;
- Acessar sites pornográficos, jogos on-line, bate papo da Internet, sites de relacionamento, ou quaisquer outros sites cujo conteúdo não seja informativo ou educacional;
- Efetuar ou tentar qualquer tipo de acesso não autorizado aos recursos computacionais da instituição;
- Utilizar os recursos computacionais da instituição para acesso não autorizado a recursos de terceiros;
- Violar ou tentar violar os sistemas de segurança, quebrando ou tentando adivinhar a identidade eletrônica de outro usuário, senhas ou outros dispositivos de segurança;
- Interceptar ou tentar interceptar a transmissão de dados através de monitoração, exceto quando autorizado explicitamente e com prévio conhecimento do departamento de Informática;
- Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais da instituição;

- Desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos aos sistemas e às informações armazenadas, tais como criação e propagação de vírus e worms, criação e utilização de sistemas de criptografia que causem ou tentem causar a indisponibilidade dos serviços e/ou destruição de dados, e ainda, engajar-se em ações que possam ser caracterizadas como violação da segurança computacional;
- Utilizar os recursos computacionais da instituição para fins comerciais ou políticos, tais como mala direta, spams ou propaganda política;
- Utilizar os recursos computacionais da instituição para ganho indevido;
- Consumir inutilmente os recursos computacionais da instituição de forma intencional.

4.6 Penalidades

O usuário é responsável por qualquer atividade a partir de sua conta (login) e também por seus atos no uso dos recursos computacionais oferecidos. Assim, o mesmo responderá por qualquer ação judicial e administrativa apresentada à instituição e que o envolva.

O descumprimento de qualquer um dos itens desta regra sujeita o infrator às penalidades apresentadas a seguir:

- 1ª falta: advertência verbal;
- 2ª falta: advertência formal;
- 3ª falta: suspensão do acesso por período de 15 dias úteis;
- 4ª falta: suspensão do acesso por um período a ser determinado;
- 5ª falta: suspensão permanente do uso da rede sem fio.

Caso alguma violação de regra seja identificada, através do sistema de monitoramento, o usuário será bloqueado e notificado pelo e-mail de contato.

5 Considerações finais

Em caso de necessidade, troca, ou uso indevido da senha de acesso por terceiros, favor procurar imediatamente a administração dos laboratórios para solicitar sua troca.

O login de acesso à rede sem fio só terá validade enquanto perdurar o vínculo do aluno, funcionário, ou professor com a instituição.

A configuração do equipamento será de responsabilidade do usuário. Orientação sobre como proceder poderá ser obtido junto ao Departamento de Tecnologia da Informação da instituição.

O uso da internet estará vinculado à conta de acesso (login e senha) do usuário na instituição. Caso constem outros acessos e estes forem indevidos, os usuários serão notificados e as punições serão aplicadas ao infrator e também ao proprietário do equipamento.

A instituição se reserva o direito de suspender o acesso do equipamento que estiver consumindo excessivamente o link de internet devido à existência de programas maliciosos nos equipamentos autorizados, tais como: vírus, spyware, worm, entre outros.

Medidas de segurança do equipamento do usuário como antivírus, firewall, anti-spyware são de sua exclusiva responsabilidade. Em nenhum caso a instituição se responsabilizará por qualquer dano e/ou prejuízo que o usuário possa sofrer ao utilizar o serviço.

A instituição se reserva o direito de cancelar este serviço sem prévio aviso.

As regras aqui estabelecidas não concorrem com medidas disciplinares que as IEES (Instituições Estaduais de Ensino Superior) resolvam tomar e aplicar no seu âmbito de atuação.