NORMAS DE ACESSO A INTERNET

Sumário

Prefácio

A presente norma está de acordo às diretrizes da Política de Segurança da Informação e Comunicação da Secretaria de Desenvolvimento Humano e Social do Distrito Federal - PoSIC/SEDHS.

1 Objetivo

Estabelecer responsabilidades e requisitos básicos de uso dos serviços de acesso à Internet no âmbito da SEDHS.

2 Regras Gerais

Como regra geral, o acesso à Internet é permitido apenas para navegação em sítios cujo conteúdo esteja adequado aos termos desta norma.

Com o intuito de promover a eficiência e o uso racional dos recursos de comunicação de dados com a Internet, a SEDHS poderá bloquear e/ou limitar o acesso a sítios de Internet, priorizando o uso institucional.

O acesso à Internet só será permitido a usuários cadastrados e identificados. O cadastro para acesso é de uso pessoal e intransferível.

Usuários que tiverem acesso à Internet provido pela SEDHS não poderão utilizar quaisquer outras conexões simultaneamente, no mesmo dispositivo, tais como: 3G, Cabo ou ADSL.

Devem ser reservados todos os direitos do autor a qualquer conteúdo disponibilizado na Internet, a menos que explicitamente especificado, sendo proibida a cópia, reprodução ou distribuição sem prévia autorização.

A possibilidade de acesso a qualquer serviço da Internet não implica na autorização para acessá-lo.

2.1 Do Acesso à Internet

A disponibilização de acesso à Internet para uso de visitantes ou equipamentos particulares, como laptops, smartphones e tablets, deverá ser separada da rede corporativa ou comunicada a Diretoria de Informática se necessitar acessar a rede interna.

O acesso à Internet com destino a portas TCP/UDP será limitado àquelas de uso comum e relacionadas ao uso institucional, tais como 80, 443, 8080 e 21. As exceções serão tratadas conforme o caso, e as liberações de acesso poderão ser solicitadas à unidade responsável por intermédio do chefe do setor, justificando a necessidade.

2.2 Visitantes

A disponibilização de acesso à Internet para uso de visitantes deverá ser separada da rede corporativa, mediante cadastro junto ao setor responsável.

2.3 Redes Sem Fio

A conexão através de redes sem-fio (Wi-Fi) deverá ser feita apenas nos pontos de acesso (Access Points) identificados em diversos pontos da edificação. O usuário nunca deverá conectar-se em redes abertas (sem senha), sob o risco de ter suas informações interceptadas por um usuário malicioso.

2.4 Categorias não permitidas

Sites ou serviços que se relacionem aos conteúdos a seguir não são permitidos, exceto por necessidade do serviço devidamente comprovada. O acesso que se enquadre em qualquer das seguintes categorias caracterizará uma violação a PoSIC/SEDHS:

- Material obsceno, ilegal, ofensivo, antiético, preconceituoso ou discriminatório;
- Conteúdo que incite prática delituosa;
- Proxy / Web Proxy;
- Conteúdo viole direitos de propriedade intelectual;
- Vírus ou qualquer outro tipo de programa malicioso;

2.5 Categorias limitadas

As categorias a seguir poderão ter limitação de acesso, seja pela largura de banda disponibilizada, seja pelo horário.

- Entretenimento;
- Propaganda;
- Redes Sociais;
- Streaming (fluxo de mídia) como rádio, TV ou vídeos online.

Estas categorias poderão, eventualmente e sem aviso prévio, serem bloqueadas em detrimento do uso institucional.

3 Responsabilidades

3.1 Das Chefias

As chefias deverão orientar seus subordinados quanto ao uso racional e consciente da conexão com a Internet e atentar quanto a possíveis violações.

3.2 Do Usuário

São responsabilidades do usuário:

- Não se utilizar do acesso à Internet para tentar comprometer a segurança (integridade, confidencialidade ou disponibilidade) de computadores, sistemas ou serviços de organização governamental ou privada.
- Não permitir que outros usuários façam uso da Internet com suas credenciais. O acesso concedido ao usuário é pessoal e intransferível.
- Certificar-se de que dados ou informações pessoais e sigilosas sejam transmitidas de forma segura, por meio de uma conexão segura, normalmente identificada com a denominação HTTPS:// na barra de endereço e o símbolo de um cadeado.
- Procurar desconectar-se com segurança de sistemas web, utilizando links específicos para este fim, como “Sair”, “Logoff” ou “Desconectar”. Evite

simplesmente fechar o navegador, pois isso mantêm sua conexão ativa por alguns minutos, podendo ser utilizada por um usuário mal-intencionado.

- Não se utilizar do recurso de "salvar" ou "lembrar" senhas disponíveis em muitos navegadores de Internet, tais como Microsoft Internet Explorer, Mozilla Firefox e Google Chrome.

3.3 Da DITEC

3.3.1 Monitoramento e registro de Logs

A DITEC deverá prover meios para registrar e monitorar o acesso à Internet, de modo a detectar violações a esta norma, respeitando-se as limitações quanto ao sigilo de informações classificadas ou protegidas por lei.

O registro deverá conter, no mínimo: endereçamento de origem e destino; e data / hora de início e término de conexões com a respectiva referência GMT. Adicionalmente poderão ser registradas o tipo a quantidade de tráfego gerado e outras informações necessárias para a otimização do link acesso e realização de auditoria.

O prazo mínimo para retenção dos logs de acesso será de 01 (um) ano.

Caberá a DITEC informar às chefias violações a norma e a PoSIC cometidas em suas respectivas áreas de gerência.

A DITEC deverá prover controle e cadastro de usuários para acesso à Internet. Para redes sem-fio,

3.3.2 Manutenção do serviço

A DITEC deverá comunicar os usuários quanto a realização de manutenções programadas no serviço que venham a causar indisponibilidade no link de comunicação de dados.

Bibliografia

ABNT. NBR ISO/IEC 27002:2005 - Tecnologia da Informação - Técnicas de segurança - Código de prática para a Gestão da Segurança da Informação. Rio de Janeiro: ABNT, 2005.

BRASIL. Marco Civil da Internet. Lei n. 12.965, de 23 de abril de 2014 <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em: 05 set. 2014.

_____. Ministério do Planejamento, Orçamento e Gestão. Governo Federal. Padrões Web em Governo Eletrônico e-PWG: Guia de administração de sítios. Disponível em: <http://epwg.governoeletronico.gov.br/guia-administracao>. Acesso em: 18 jun. 2012.

CERT.BR (São Paulo). Comitê Gestor da Internet No Brasil. Cartilha de Segurança para Internet. versão 4.0. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 11 junho 2012.

MICROSOFT (Usa). Central de Proteção e Segurança: Proteção do Computador, Privacidade Digital e Segurança Online. Disponível em: <http://www.microsoft.com/pt-br/security/resources/activex-whatis.aspx>. Acesso em: 12 jun. 2012.

REGISTRO.BR (Brasil). FAQ (Perguntas Frequentes). Disponível em: <http://registro.br/suporte/faq/faq1.html#1>. Acesso em: 25 maio 2012.