GERED/COSEI

CÓDIGO	TÍTULO	VIGÊNCIA	VERSÃO
NORMA 003/2020	NORMA DE ACESSO À INTERNET	30/10/2020	1

1 PREFÁCIO

A presente norma está de acordo às diretrizes da Política de Segurança da Informação e Comunicação do CIASC.

2 OBJETIVO

Estabelecer responsabilidades e requisitos básicos de uso dos serviços de acesso à Internet no âmbito do CIASC.

3 ESCOPO

Esta norma se aplica a qualquer pessoa utilizando a infraestrutura do CIASC para acesso à internet.

4 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, o CIASC 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 pelo CIASC 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.

4.1 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 e 21.

Todo dispositivo, estação de trabalho e laptops corporativos só poderão acessar a Internet após efetuar a autenticação no *Proxy* através do *Captive Portal* (Página de Autenticação).

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.

4.2 Visitantes

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

4.3 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;

A Coordenadoria de Segurança da Informação (COSEI) deverá prover controle e cadastro de usuários para acesso à Internet para redes sem fio.

4.4 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 à Política de Segurança da Informação e Comunicação do CIASC:

I. Material obsceno, ilegal, ofensivo, antiético, preconceituoso ou discriminatório;
II. Conteúdo que incite prática delituosa;
III. *Proxy* / *Web Proxy*;
IV. Conteúdo viole direitos de propriedade intelectual; e
V. Vírus ou qualquer outro tipo de programa malicioso;

4.5 Categorias Limitadas

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

I. Entretenimento;
II. Propaganda;
III. Redes Sociais; e
IV. *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.

5 RESPONSABILIDADES

5.1 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.

5.2 Do Usuário

São responsabilidades do usuário:

I. 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;
II. Não permitir que outros usuários façam uso da Internet com suas credenciais. O acesso concedido ao usuário é pessoal e intransferível;
III. 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;
IV. 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;
V. 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*; e
VI. É proibido utilizar os recursos do CIASC para fazer o download ou distribuição de *software* ou dados não legalizados.

5.3 Da COSEI

5.3.1 Monitoramento e Registro de *Logs*

A COSEI 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 COSEI informar às chefias violações a norma e a Política de Segurança da Informação e Comunicação do CIASC cometidas em suas respectivas áreas de gerência.

5.3.2 Manutenção do Serviço

A COSEI deverá comunicar os usuários quanto a realização de manutenções programadas no serviço que venham a causar indisponibilidade no acesso à Internet.

6 REFERÊNCIAS BIBLIOGRÁFICAS

DITEC-SEDES (Distrito Federal). Secretaria de Estado de Desenvolvimento Humano e Social do Distrito Federal. Normas de Acesso a Internet. Disponível em: <http://www.sedes.df.gov.br/wp-conteudo/uploads/2018/02/Normas-de-Seguran%C3%A7a.pdf>. Acesso em: 18 jul. 2020.

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.

7 HISTÓRICO DE VERSÕES

Alterações	Data de aprovação	Versão gerada
Diretoria Executiva dia 29/10/2020 - ATA 084/2020	29/10/2020	V 1.0