

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO CANOASPREV

RESOLUÇÃO Nº 05, DE 29 DE MARÇO DE 2019

Institui a Política de Segurança da Informação (PSI) do Instituto de Previdência e Assistência aos Servidores Municipais de Canoas -CANOASPREV.

O Presidente do Instituto de Previdência e Assistência dos Servidores Municipais de Canoas – CANOASPREV, no uso das atribuições que lhe confere o inciso IV, do artigo 7º, e o inciso I, do artigo 7º-A, da Lei Municipal nº 4.739, de 3 de fevereiro de 2003,

Considerando o Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social da União, dos Estados, do Distrito Federal e dos Municípios, instituído pela portaria MPS nº 185, de 14 de maio de 2015,

Considerando o disposto na Portaria SPREV MF nº 3, de 31 de janeiro de 2018;

Considerando a Portaria nº 232, de 28 de agosto de 2018, alterada pela Portaria nº 088, de 1º de março de 2019;

Considerando conteúdo do memorando eletrônico nº2019013966, de 29 de março de 2019;

RESOLVE:

Art.1º Fica instituída a Política de Segurança da Informação (PSI) do Instituto de Previdência e Assistência aos Servidores Municipais de Canoas (CANOASPREV), na forma do Anexo Único desta Resolução.

Art.2º Esta Resolução entra em vigor na data da sua publicação.

CANOASPREV, em vinte e nove de março de dois mil de dezenove (29.3.2019).

Aires Vigel
Presidente em exercício do CANOASPREV

1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO DE PREVIDÊNCIA E ASSISTÊNCIA DOS SERVIDORES MUNICIPAIS DE CANOAS - CANOASPREV

1.1. ESCOPO

A Política de Segurança da Informação (PSI) tem por finalidade estabelecer diretrizes para a segurança do manuseio, tratamento e controle e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio pelos sistemas de informação a serem, obrigatoriamente, observadas na definição de regras operacionais e procedimentos no âmbito do Instituto de Previdência e Assistência dos Servidores Municipais de Canoas - CANOASPREV.

Constitui-se como objetivo o estabelecimento de mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados e a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confidencialidade e autenticidade das informações no CANOASPREV.

Esta Política aplica-se a todos os conselheiros, servidores e estagiários do CANOASPREV e demais agentes públicos ou particulares que oficialmente executem atividade(s) vinculada(s) à atuação institucional do CANOASPREV.

1.2. CONCEITOS E DEFINIÇÕES

Para os fins desta PSI, considera-se:

Acesso Lógico: acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação;

Acesso Remoto: ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;

ADSL (Asymmetric Digital Subscriber Line): (Linha Digital Assimétrica para Assinante) tecnologia de transmissão que possibilita o transporte de voz e dados a alta velocidade através da rede telefônica convencional, analógica ou digital;

Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

Ativo da Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

Ativo Sigiloso: qualquer bem tangível ou intangível que possa conter informações sigilosas que, se acessadas por pessoas não autorizadas, podem causar danos significativos à organização;

Auditoria: verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas inefficientes ou ineficazes;

Autenticação: é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

Banco de Dados (ou Base de Dados): é um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações;

Biometria: uso de mecanismos de identificação para restringir o acesso a determinados lugares ou serviços. Exemplos de identificação biométrica: através da íris (parte colorida do olho), da retina (membrana interna do globo ocular), da impressão digital, da voz, do formato do rosto e da geometria da mão;

Bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso;

Chefe da Unidade de Informática: servidor público ocupante de cargo efetivo ou de órgão ou entidade da Administração Pública Municipal, incumbido de chefiar e gerenciar a equipe da Unidade de Informática;

Classificação da informação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

Contingência: descrição de medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à corporação;

Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

Controle Interno: conjunto de recursos, métodos e processos adotados pelos próprios gestores, com vistas a impedir o erro, a fraude e a ineficiência, visando a dar atendimento aos princípios constitucionais e administrativos, em especial os da legalidade, impessoalidade, moralidade, publicidade e eficiência;

Cópia de Segurança (Backup): copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade, sendo essencial para dados importantes;

Correio Eletrônico: é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;

Credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha;

Criptografia: é a técnica pela qual a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta");

CTIC: Comissão de Tecnologia da Informação do CANOASPREV;

Dado: representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;

Diretriz: descrição que orienta o que deve ser feito, e como, para se alcançar os objetivos estabelecidos nas políticas;

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

Download: (Baixar) copiar arquivos de um servidor (site) na internet para um computador;

Espelhamento: Sistema de proteção de dados onde o conteúdo é espelhado em tempo real. Todos os dados são duplicados entre as áreas de armazenamento disponíveis.

FTP (File Transfer Protocol): (Protocolo de Transferência de Arquivo) é um protocolo da internet para transferência de arquivos;

Hardware: É a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressora, teclado e outros;

HTTP (Hyper Text Transfer Protocol): (Protocolo de Transferência de Hipertexto) é uma linguagem para troca de informação entre servidores e clientes da rede;

HTTPS (HyperText Transfer Protocol Secure): (Protocolo de Transferência de Hipertexto Seguro) é uma linguagem para troca de informação entre servidores e clientes da rede, com recursos de criptografia, autenticação e integridade;

Incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

Informações Críticas: são as informações de extrema importância para a sobrevivência da instituição;

Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

Instant messenger: (Mensageiro instantâneo) é uma aplicação que permite o envio e o recebimento de mensagens em tempo real;

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

Internet: rede mundial de computadores;

Internet protocol: (Protocolo de Internet) é um protocolo de comunicação usado entre duas ou mais máquinas em rede para encaminhamento dos dados;

Intranet: rede de computadores privada que faz uso dos mesmos protocolos da internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;

Log: é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;

Logon: Procedimento de identificação e autenticação do usuário nos recursos de tecnologia da informação. É pessoal e intransferível;

On line: (Estar disponível ao vivo) no contexto da Internet significa estar disponível para acesso imediato, em tempo real;

Perfil de acesso: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

Peer-to-peer (P2P): (Ponto a ponto) permite conectar o computador de um usuário a outro, para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, entre outros;

Política de Segurança da Informação (PSI): documento aprovado pela autoridade responsável pela entidade com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

Protocolo: convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;

Proxy: é um serviço intermediário entre as estações de trabalho de uma rede e a Internet. O servidor de rede proxy serve para compartilhar a conexão com a Internet, melhorar o desempenho do acesso e bloquear acesso a determinadas páginas;

Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

Recursos computacionais: recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

Rede corporativa: conjunto de todas as redes locais sob a gestão da instituição;

Rede pública: rede de acesso a todos;

Replicação: é a manutenção de cópias idênticas de dados em locais diferentes. O objetivo de um mecanismo de replicação de dados é permitir a manutenção de várias cópias idênticas de um mesmo dado em vários sistemas de armazenamento;

Roteador: equipamento responsável pela troca de informações entre redes;

Sala segura: sala que proporciona um ambiente seguro no Datacenter, oferecendo maior garantia no armazenamento de informações eletrônicas.

Segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

Servidor de rede: recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;

Sistemas de informação: conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção;

Sistema de segurança da informação: proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento;

Software: programas existentes em um computador, como sistema operacional, aplicativos, entre outros;

Site: conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;

Streaming: transferência de dados (normalmente áudio e vídeo) em fluxo contínuo por meio da Internet;

Switches: um switch de rede é um equipamento eletrônico de comutação que funciona como um nó central numa rede no formato estrela, armazenando em memória o endereço físico de todos os computadores conectados a ele, relacionando cada endereço físico a uma de suas portas e permitindo assim a interligação entre os dispositivos conectados;

Termo de Responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

Tratamento da informação: toda operação realizada com dados, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Tratamento de Incidentes de Segurança em Redes Computacionais: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

Trilhas de auditoria: são rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (logs) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários não autorizados;

Unidade de Informática (UI): Setor que compõe a estrutura organizacional e administrativa da Diretoria Administrativa, composta por servidor(es) municipal(is) e estagiários, tendo entre suas responsabilidades a competência de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores, assim como outras tarefas relacionadas com a Tecnologia da Informação;

Usuário: servidores públicos, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação, formalizada por meio da assinatura do Termo de Responsabilidade;

VLAN (Virtual Local Area Network ou Virtual LAN): (Rede Local Virtual) é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local;

VPN (Virtual Private Network): (Rede Privada Virtual) é uma rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública de uma maneira que emula uma conexão ponto a ponto privada;

Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;

Wireless (rede sem fio): rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

1.3. PRINCÍPIOS

São princípios da PSI:

1.3.1 A garantia ao direito pessoal e coletivo à intimidade e ao sigilo da correspondência e das comunicações individuais;

1.3.2 A proteção dos dados, informações e conhecimentos produzidos no CANOASPREV, em observância com o que dispõe a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI);

1.3.3 A proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural no tratamento de dados pessoais, em observância com o que dispõe a Lei nº 13.709, de 14 de agosto de 2018.

1.4. DIRETRIZES GERAIS

São diretrizes gerais da PSI:

1.4.1 A preservação da disponibilidade, integridade, confiabilidade e autenticidade dos dados, informações e conhecimentos que compõem o ativo da informação do CANOASPREV;

1.4.2 Continuidade das atividades;

1.4.3 Economicidade da proteção dos ativos de informação;

1.4.4 Pessoalidade e utilidade do acesso aos ativos de informação; e

1.4.5 A responsabilização do usuário pelos atos que comprometam a segurança do sistema da informação.

1.5 ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

1.5.1 A Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos da Instituição, com vistas à garantia de integridade, disponibilidade, conformidade e confidencialidade;

1.5.2 Todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos para preservar a continuidade do negócio e regular o exercício das funções institucionais;

1.5.3 O gerenciamento dos ativos de informação deverá observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua;

1.5.4 O cumprimento desta PSI, bem como das normas complementares e procedimentos de segurança da informação no CANOASPREV será auditado periodicamente, de acordo com os critérios definidos pelo Controle Interno ou pela CTIC;

1.5.5 As medidas de proteção devem ser planejadas e os gastos na aplicação de controles devem ser compatíveis com valor do ativo protegido;

1.5.6 O acesso às informações, sistemas e instalações depende da apresentação de identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento;

1.5.7 A aquisição, contratação de serviços de desenvolvimento, instalação e uso de sistemas e equipamentos devem ser homologados e/ou autorizados pelo Presidente da Diretoria Executiva com apoio da CTIC;

1.5.8 Para garantir o cumprimento das normas, os responsáveis pelas unidades deverão auxiliar no controle do uso dos recursos computacionais;

1.5.9 Os requisitos de segurança da informação devem estar explicitamente citados em todos os termos de compromisso celebrados entre o órgão e terceiros;

1.5.10 Todos os conselheiros, servidores e estagiários do CANOASPREV e demais agentes públicos ou particulares que oficialmente executam atividade vinculada à atuação institucional do CANOASPREV e sejam usuários dos ativos sigilosos, devem assinar Termo de Compromisso quanto ao sigilo dos dados, informações e conhecimentos do CANOASPREV.

1.6. SEGURANÇA EM RECURSOS HUMANOS

1.6.1 As responsabilidades pela segurança da informação devem ser definidas nas descrições de cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos do CANOASPREV;

1.6.2 Todos os usuários devem ser conscientizados e treinados nos procedimentos de segurança da informação;

1.6.3 O controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa;

1.6.4 Quando do afastamento, mudança de responsabilidades e de lotação ou atribuições dentro da organização faz-se necessária a revisão imediata dos direitos de acesso e uso dos ativos;

1.6.5 Quando da efetivação do desligamento de usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos a ele atribuído;

1.6.6 Todo ativo produzido pelo usuário, desligado, deverá ser mantido pelo CANOASPREV garantindo o reconhecimento e o esclarecimento da propriedade do acervo para Instituição;

1.7. COMPETÊNCIAS E RESPONSABILIDADES

1.7.1 Esta PSI, as normas complementares e os procedimentos de segurança se aplicam a todos os conselheiros, servidores e estagiários do CANOASPREV e demais agentes públicos ou particulares que oficialmente executam atividade vinculada à atuação institucional desta Autarquia.

1.7.2 Compete ao Gabinete do Presidente do CANOASPREV:

1.7.2.1 Assegurar que a implementação dos controles de segurança da informação tenha uma coordenação e permeie toda a organização;

1.7.2.2 Assegurar os recursos necessários para a implementação e gestão da PSI do CANOASPREV;

1.7.2.3 Instituir e designar os integrantes da Comissão de Tecnologia da Informação, o Chefe da Unidade de Informática e os servidores que integram a Unidade de Informática.

1.7.2.4 Decidir, por ato do Presidente do CANOASPREV, sobre a necessidade de abertura de sindicância ou Processo Administrativo Disciplinar na forma da legislação, nos casos de não atendimento da presente PSI.

1.7.3 Compete à Comissão de Tecnologia da Informação do CANOASPREV:

1.7.3.1 Sugerir critérios para auditoria periódica destinada a aferir o cumprimento da PSI do CANOASPREV, suas normas complementares e procedimentos.

1.7.3.2 Manifestar-se sobre a PSI, com posterior encaminhamento ao Presidente do CANOASPREV, para aprovação.

1.7.3.3 Assessorar na implementação das ações relacionadas a esta PSI;

1.7.3.4 Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

1.7.3.5 Propor alterações a esta PSI;

1.7.3.6 Propor normas complementares a esta PSI e relativas à segurança da informação.

1.7.4 Compete ao Chefe da Unidade de Informática do CANOASPREV:

1.7.4.1 Promover a cultura de segurança da informação e comunicações;

1.7.4.2 Acompanhar as apurações e as avaliações dos danos decorrentes de quebras de segurança;

1.7.4.3 Propor os recursos necessários às ações de segurança da informação e comunicações;

1.7.4.4 Coordenar a Comissão de Tecnologia da Informação do CANOASPREV e a Unidade de Informática;

1.7.4.5 Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

1.7.4.6 Manter contato direto com a Diretoria Administrativa para o trato de assuntos relativos à segurança da informação e comunicações;

1.7.4.7 Propor normas complementares a esta PSI e que sejam relativas à segurança da informação;

1.7.4.8 Propor estratégias para a implantação da PSI;

1.7.4.9 Propor normas complementares e procedimentos de segurança da informação e das comunicações, cabendo a CTIC a recomendação de alteração normativa;

1.7.4.10 Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança;

1.7.4.11 Apurar os incidentes de segurança críticos e encaminhar o resultado dos fatos apurados a Diretoria Administrativa, que encaminhará o resultado ao Gabinete da Presidência;

1.7.4.12 Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;

1.7.4.13 Manter a análise de risco atualizada, refletindo o estado corrente da organização;

1.7.4.14 Identificar controles físicos, administrativos e tecnológicos para mitigação de riscos;

1.7.4.15 Recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança, recomendando aos respectivos gestores as ações corretivas ou de contingência em cada caso;

1.7.4.16 Produzir relatórios síntese de incidentes de segurança da informação para a Diretoria Administrativa e para a CTIC;

1.7.4.17 Planejar, coordenar, supervisionar e orientar a execução das atividades da UI.

1.8. NORMAS COMPLEMENTARES

1.8.1 O regimento da PSI no âmbito do CANOASPREV está estruturado na seguinte relação de Normas Complementares, constantes no anexo único desta Política, que tratam especificamente da gestão dos recursos de tecnologia da informação, e que, portanto, devem ser expressamente cumpridas:

1.8.1.1 NC 01 – SEGURANÇA FÍSICA E DO AMBIENTE;

1.8.1.2 NC 02 – ACESSO REMOTO EXTERNO;

1.8.1.3 NC 03 - CONTAS DE ACESSO E SENHAS;

1.8.1.4 NC 04 - CORREIO ELETRÔNICO;

1.8.1.5 NC 05 - UTILIZAÇÃO DA INTERNET E DA INTRANET.

1.8.2 As Normas Complementares devem ser divulgadas no Diário Oficial do Município de Canoas (DOMC) e disponibilizadas na Internet para todos os usuários dos recursos de tecnologia da informação do CANOASPREV (conselheiros, servidores e estagiários e demais agentes públicos ou particulares que oficialmente executam atividade vinculada à atuação institucional da autarquia);

1.8.3 Em nenhuma hipótese será permitido o descumprimento das Normas Complementares pela alegação de desconhecimento das mesmas por parte dos abrangidos pela presente PSI.

1.9. PENALIDADES

1.9.1 O não cumprimento das determinações desta PSI e nas normas complementares sujeita o infrator às penalidades previstas na legislação;

1.9.2 O descumprimento, por servidores públicos, das disposições constantes nesta PSI e nas normas complementares sobre segurança da informação poderá ser caracterizada como desconformidade, a ser apurada por meio de processo administrativo de apuração de desconformidade (PADES), ou infração funcional, a ser apurada em processo administrativo disciplinar (PAD), sem prejuízo das responsabilidades penal e civil;

1.10. ATUALIZAÇÃO

1.10.1 Esta PSI deve ser revisada e atualizada periodicamente no período não superior de 5 (cinco) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

1.11. VIGÊNCIA

1.11.1 Esta PSI entra em vigor na data de sua publicação.

1.12. DISPOSIÇÕES FINAIS

1.12.1 Os casos omissos, as excepcionalidades e as dúvidas com relação a esta PSI serão submetidos à análise da CTIC e decididos pela Diretoria Executiva.

ANEXO ÚNICO - NORMAS COMPLEMENTARES

NC 01 - SEGURANÇA FÍSICA E DO AMBIENTE

1. Campo de aplicação

Esta norma se aplica no âmbito do CANOASPREV.

2. Objetivo

Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e nas informações do Instituto.

3. Diretrizes Gerais

a) Perímetro de Segurança Física

- Os perímetros de segurança física do instituto devem estar bem definidos, localizados em locais com uma construção que evite a entrada de pessoas não autorizadas.
- Os acessos às dependências do prédio devem ser controlados por uma área de recepção, além de sistemas de segurança e de combate a incêndios.

b) Controles de Entrada Física

- As áreas que contenham material de acesso restrito só podem ser acessadas por pessoas autorizadas, com a aplicação de um controle de entrada e saída.
- Crachás de identificação de funcionários, de visitantes e prestadores de serviço devem ser utilizados.
- O acesso às áreas internas do Instituto é controlado pelo serviço de recepção e catraca, com registro de entrada e saída de visitantes e de prestadores de serviços.
- O registro de acesso e saída de servidores é realizado pela catraca ou pelo ponto biométrico.

c) Segurança em escritórios, salas e instalações - Os escritórios, salas e instalações devem ser acessados apenas por pessoas autorizadas.

- O acesso para a entrega e o carregamento de materiais, assim como a prestação de serviços por terceiros, deve ser controlado e supervisionado.

- As áreas em que é realizado o processamento e/ou armazenamento de informações sempre que não estiverem ocupadas, devem ser devidamente trancadas

d) Localização e proteção de equipamentos

- Os equipamentos do instituto devem estar sempre protegidos de ameaças e perigos do meio ambiente e de acesso não autorizado.

- Os equipamentos devem ser protegidos contra falhas no fornecimento de energia elétrica.

- Devem ser instaladas iluminação de emergência nas dependências do Instituto.

- Devem ser adotados controles para minimizar o risco de ameaças físicas potenciais e ambientais

e) Segurança do cabeamento

- O cabeamento de energia e de telecomunicações deve estar protegido contra interceptação, interferência e danos.

- Deve-se manter um acesso controlado aos painéis de conexões e às salas de cabos.

f) Manutenção dos equipamentos

- A manutenção dos equipamentos deve ser realizada nos intervalos recomendados pelo fornecedor e de acordo com as suas especificações, por pessoal de manutenção autorizado.

- Sempre que possível, e que não comprometa a segurança das informações, essas devem ser eliminadas do equipamento que sofrerá a manutenção.

- Todos os equipamentos devem ser testados após manutenção ou troca.

g) Remoção de ativos

- Equipamentos, informações ou software não devem ser retirados do local sem autorização prévia.

- Em caso de remoção necessária, ela deve ser autorizada pelos servidores públicos responsáveis pelos ativos em questão e sua retirada e devolução deve ser controlada, por meio de registro.

- Fora das dependências do instituto deve-se sempre avaliar o risco das informações importantes contidas em equipamentos (computadores e dispositivos de armazenamento de informações em geral) e caso necessário, recomenda-se supervisão na sua utilização.

h) Reutilização ou descarte seguro de equipamentos

- Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes de sua reutilização ou descarte para assegurar a remoção de informações sensíveis.

- As mídias de armazenamento que contenham informações confidenciais ou de direitos autorais devem ser destruídas fisicamente, ou as suas informações apagadas ou sobregravadas por meio de técnicas que tornem as informações originais irrecuperáveis.

- Em caso de dispositivo defeituoso, recomenda-se a destruição física da unidade de armazenamento, visando a eliminação das informações antes do descarte.

- Recomenda-se também encriptação de unidades de armazenamento com dados sensíveis, a fim de evitar problemas de segurança em casos de descarte das mesmas.

i) Equipamento de usuário sem monitoramento

- Os usuários devem assegurar que os equipamentos não monitorados tenham proteção adequada, encerrando as sessões ativas ou utilizando tela de proteção com senha sempre que não estiverem presentes no ambiente.

j) Política de mesa limpa e tela limpa - Informações sensíveis ou críticas em papel ou mídia de armazenamento eletrônica devem sempre estar em local seguro quando não utilizadas, principalmente quando o escritório estiver desocupado.

- Os computadores devem sempre estar desligados ou protegidos por senha quando não estiverem em uso.

- Impressoras e outros equipamentos com tecnologia de reprodução são utilizadas mediante autorização, e qualquer documento com informação sensível deve ser retirado imediatamente após sua impressão.

NC 02 - ACESSO REMOTO EXTERNO

1. Campo de Aplicação

Esta norma se aplica no âmbito do CANOASPREV.

2. Objetivo

Estabelecer critérios para a disponibilização do serviço de acesso remoto externo à rede do CANOASPREV, bem como as regras para a sua utilização, visando à prevenção do acesso não autorizado às informações do Instituto.

3. Diretrizes Gerais

a) Permissão de acesso remoto aos serviços corporativos - O acesso remoto aos serviços corporativos somente deve ser disponibilizado aos conselheiros, servidores, estagiários e demais agentes públicos ou particulares que oficialmente executam atividade vinculada à atuação institucional do CANOASPREV e que necessitam deste serviço para execução de suas atividades institucionais, desde que autorizados.

b) Permissão aos servidores públicos da UI

- Os administradores da rede do CANOASPREV lotados na UI, para o desempenho de suas atribuições, poderão ter permissão de acesso remoto a todos os recursos computacionais da entidade quando necessário.

c) Avaliação e aprovação do acesso remoto

- A liberação de acesso remoto, só será efetivada após avaliação da CTIC e aprovação pelo Presidente da Diretoria Executiva, para que se evitem ameaças à integridade e sigilo das informações contidas na rede do CANOASPREV.

- Será feita uma análise criteriosa, podendo ser negado o acesso remoto caso comprometa a segurança da rede da Autarquia.

d) Solicitação de acesso remoto

- A solicitação do acesso remoto deve conter, no mínimo, as seguintes informações:

- I. Data da solicitação;
- II. Tipo de solicitação;
- III. Tempo de validade do acesso remoto;
- IV. Justificativa;
- V. Identificação do solicitante;
- VI. Identificação do usuário.
- e) Acesso remoto para outras organizações
 - A disponibilização de acesso remoto à rede do CANOASPREV para outras organizações deve obedecer às seguintes regras:
 - I. Direitos de acesso definidos por contrato formal entre as partes;
 - II. Acesso temporário e limitado às necessidades de negócio;
 - III. Revisão periódica dos direitos de acesso;
 - IV. Utilização de solução que permita a implementação e controle de regras de acesso.
- f) Cancelamento do acesso remoto
 - O serviço de acesso remoto deve ser cancelado sob as seguintes condições:
 - I. Finalização do período especificado na solicitação ou contrato;
 - II. Perda da necessidade de utilização do serviço;
 - III. Transferência do usuário para outras unidades;
 - IV. Identificação de vulnerabilidade, risco ou uso indevido no acesso concedido.
- g) Condições de utilização do acesso remoto
 - As conexões remotas à rede do CANOASPREV devem ocorrer da seguinte maneira:
 - I. Utilização de autenticação;
 - II. As senhas e as informações que trafegam entre a estação remota e a rede da Autarquia devem estar criptografadas;
 - III. Cada usuário deve manter suas credenciais de acesso (login e senha) em sigilo absoluto e não fornecê-lo a outra pessoa, garantindo assim, a impossibilidade de acesso indevido por pessoas não autorizadas;
 - h) Vedações quanto ao acesso remoto - É vedada a utilização do acesso remoto para fins não relacionados às atividades da instituição.

NC 03 - CONTAS DE ACESSO E SENHAS

1 Campo de Aplicação

Esta norma se aplica no âmbito do CANOASPREV.

2 Objetivo

Estabelecer critérios para a disponibilização e administração do acesso aos serviços de tecnologia de informação do CANOASPREV, assim como estabelecer critérios relativos às senhas das respectivas contas.

3 Diretrizes Gerais

a) Criação de Contas de Acesso

- Todo cadastramento de conta de acesso à rede do CANOASPREV deve ser efetuado mediante solicitação formal;
 - Contas de acesso de terceirizados do CANOASPREV devem ser solicitadas pelos fiscais dos contratos e ter prazo de validade no máximo igual ao período de vigência do contrato ou período de duração de suas atividades;
 - As solicitações relativas à criação de cada conta devem ser mantidas registradas e armazenadas de forma segura pela UI;
 - Todos os usuários devem assinar um termo de responsabilidade pela utilização da conta de acesso, devendo ser entregue junto com a solicitação de criação de conta de acesso;
 - A nomenclatura das contas de acesso de usuários deve seguir padrão definido pela UI.
 - Excepciona-se do disposto na presente NC o simples acesso dos segurados ao portal do CANOASPREV com o objetivo de consultar, imprimir, ou gerar, os seus contracheques e os seus informes de rendimentos, observando, nas situações referidas, regras específicas definidas pela CTIC.
- b) Eventos relacionados à falhas e anormalidades percebidas
- A chefia imediata da área a qual pertence o usuário deve ser informada formalmente, pela UI, a respeito de qualquer evento relacionado a falhas de segurança referentes à conta do usuário e senha;
 - Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de tecnologia da informação deve ser imediatamente comunicada ao UI.
- c) Exclusão e Bloqueio de Contas de Acesso
- Toda exclusão ou bloqueio de conta de acesso à rede do CANOASPREV deve ser efetuado mediante solicitação formal;
 - A exclusão da conta de acesso do usuário deve ser solicitada caso haja:
 - I. Falecimento;
 - II. Aposentadoria; e
 - III. Outros afastamentos que caracterizem encerramento do vínculo com a instituição;
 - Contas sem utilização por mais de 45 (quarenta e cinco) dias devem ser bloqueadas;
 - As contas deverão permanecer bloqueadas até que haja nova solicitação formal para desbloqueio;
 - As contas de serviços utilizadas em servidores de rede, backup, correio eletrônico, banco de dados, aplicações, entre outros, devem ser utilizadas somente para execução de ações ligadas à sua natureza, de forma automática, sem intervenção manual através de login/acesso;
 - As contas com privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades atribuídas, em equipamentos previamente definidos.
 - As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos administradores dos equipamentos de rede e chefia respectiva.
- d) Senhas
- Todas as senhas, para autenticação na rede do CANOASPREV devem seguir os seguintes critérios mínimos:

I. Toda senha deve ser constituída de, no mínimo, 6 caracteres alfanuméricos (letras e números), contendo obrigatoriamente maiúsculas, minúsculas, numerais e caracteres especiais;

II. A senha não poderá conter parte do nome do usuário, por exemplo: se o usuário chama-se Jose da Silva, sua senha não pode conter partes do nome como "1221jose" ou "1212silv";

III. A data de expiração, terá tempo de vida útil determinada pela equipe de segurança, devendo o mesmo ser respeitado, caso contrário o usuário ficará sem acesso aos sistemas;

IV. É obrigatória a troca de senha ao efetuar o primeiro login;

V. É proibida a repetição das 5 últimas senhas já utilizadas;

- Os critérios definidos acima serão auditados pelo Controle interno e pela CTIC, por meio de ferramentas adequadas e suporte operacional da UI;

- A base de dados de senhas deve ser armazenada com criptografia;

- O usuário poderá solicitar alteração de sua senha, caso não se recorde da mesma, mediante solicitação formal;

- Caso o usuário desconfie que sua senha não está mais segura, tem liberdade para alterá-la, mesmo antes do prazo determinado de validade.

e) Utilização de Contas de Acesso e Senhas

- A conta de acesso é o instrumento para identificação do usuário na rede do CANOASPREV e caracteriza-se por ser de uso individual e intransferível e sua divulgação é vedada sob qualquer hipótese.

- Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário aos quais as informações estão vinculadas.

- O acesso aos serviços de tecnologia de informação do CANOASPREV deve ser disponibilizado aos conselheiros, servidores, estagiários e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional da Autarquia.

- Para fins de auditoria, às contas de administradores locais das estações de trabalho ou de servidores de rede só devem ser utilizadas quando estritamente necessário.

f) Movimentação de Pessoal

- A Unidade de Apoio Administrativo e de Recursos Humanos (UAARH) deve comunicar à UI, imediatamente, os ingressos, os desligamentos, as aposentadorias, os afastamentos e as movimentações de usuários que impliquem mudanças de lotação.

NC 04 - CORREIO ELETRÔNICO

1 Campo de Aplicação

Esta Norma se aplica no âmbito do CANOASPREV.

2 Objetivo

Constitui como objetivo desta NC a disponibilização do serviço de correio eletrônico corporativo do CANOASPREV aos usuários.

3 Diretrizes Gerais

a) Finalidade

- O serviço de correio eletrônico tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais do CANOASPREV.

b) Usuários

- São usuários do serviço de correio eletrônico corporativo os conselheiros e servidores do CANOASPREV, os estagiários e os demais agentes públicos ou particulares que oficialmente executam atividade vinculada à atuação institucional da Autarquia.

c) Concessão

- A concessão de contas de correio eletrônico depende de pedido fundamentado da autoridade responsável pela respectiva área, demonstrando a necessidade, para a Autarquia, da utilização do serviço pelo agente.

d) Listas de distribuição

- Pode ser solicitada a criação de listas de distribuição, visando atender o funcionamento de unidades da estrutura administrativa do CANOASPREV, ou, ainda, Comissões ou Grupos de Trabalho, restritas aos seus respectivos âmbitos de atuação, mediante solicitação fundamentada, e subscrita por integrante da Diretoria Executiva.

e) Responsabilidade de tramitação

- A tramitação das mensagens emitidas e/ou recebidas por meio do endereço do correio eletrônico institucional do Conselho Deliberativo do CANOASPREV é de responsabilidade do Presidente do Conselho Deliberativo, sendo facultado ao mesmo a designação de outros conselheiros para a sua tramitação.

- A tramitação das mensagens emitidas e/ou recebidas por meio do endereço do correio eletrônico institucional do CANOASPREV é de responsabilidade do Assessor de Gestão Municipal I (AGMI), sendo facultado ao Presidente da Diretoria Executiva a designação de outras pessoas para a sua tramitação.

- A tramitação das mensagens emitidas e/ou recebidas por meio do endereço do correio eletrônico institucional do Conselho Fiscal do CANOASPREV é de responsabilidade do Presidente do Conselho Fiscal, sendo facultado ao mesmo designar outros conselheiros para a sua tramitação.

- A tramitação das mensagens emitidas e/ou recebidas por meio do endereço do correio eletrônico institucional das demais unidades administrativas do CANOASPREV é de responsabilidade do titular da respectiva unidade, ou por servidor designado pelo Diretor a que vinculada a mesma.

- A tramitação das mensagens emitidas e/ou recebidas por meio do endereço do correio eletrônico institucional pessoal é de responsabilidade do titular da respectiva conta de correio eletrônico.

f) Acesso ao conteúdo das mensagens

- O acesso ao conteúdo das mensagens tramitadas por meio do serviço de correio eletrônico institucional é vedado, salvo nas hipóteses previstas em lei.

g) Acesso indevido

- O acesso indevido às informações tramitadas por meio do serviço de correio eletrônico institucional, ou contidas em seus ambientes, sujeita o infrator às penalidades previstas no item 1.10 desta PSI.

h) Senha de acesso

- O acesso ao serviço de correio eletrônico dar-se-á por meio de senha de uso pessoal e intransferível, vedada sua divulgação.

i) Vedações

- É vedado ao usuário o uso do serviço de correio eletrônico institucional com o objetivo de:

I. Praticar crimes e infrações de qualquer natureza;

II. Executar ações nocivas contra outros recursos computacionais do CANOASPREV ou de redes externas;

III. Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e aos bons costumes;

IV. Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo “corrente”, vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possam ser considerados nocivos ao ambiente de rede do CANOASPREV;

V. Emitir comunicados gerais com caráter eminentemente associativo, sindical ou político-partidário;

VI. Enviar arquivos de áudio, vídeo ou animações, salvo os que tenham relação com as funções institucionais desempenhadas pelo CANOASPREV;

VII. Divulgar, no todo ou em parte, os endereços eletrônicos corporativos constantes do catálogo de endereços do serviço;

VIII. Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional.

j) Disponibilização do serviço

- Compete à Diretoria Administrativa, por meio da Unidade de Informática, disponibilizar o serviço de correio eletrônico institucional, diretamente ou mediante contrato, competindo-lhe, ainda, o seguinte:

I. Zelar pelo atendimento aos princípios da segurança, integridade, sigilo e disponibilidade dos serviços e dados transmitidos por meio do sistema de correio eletrônico;

II. Prover meios tecnológicos necessários à adequada utilização do serviço;

III. Definir os padrões e requisitos para cadastramento, concessão, utilização, suspensão ou exclusão das contas de correio eletrônico e listas de distribuição, definidas por essa Norma;

IV. Manter, em local seguro e restrito, dados de auditoria acerca da utilização do serviço, no sentido de garantir a recuperação de mensagens em caso de danos ao ambiente de rede, devidamente comunicado a todos os usuários do serviço;

V. Suspender motivadamente o acesso a conta de correio quando constatado o uso indevido dos recursos, dando imediata ciência ao respectivo titular e ao responsável pela apuração formal;

VI. Manter proteção contra vírus e mensagens não solicitadas (spam) nos servidores do correio eletrônico;

VII. Restringir a transmissão de arquivos que, em tese, possam significar comprometimento do serviço;

VIII. Monitorar o uso do ambiente virtual, por meio de ferramentas sistêmicas, a fim de preservar a integridade das informações e identificar possíveis violações ao disposto nesta Norma;

IX. Providenciar, sempre que necessária, a capacitação dos usuários no uso da ferramenta de correio eletrônico;

k) Movimentação de Pessoal

- Compete à Unidade de Apoio Administrativo e de Recursos Humanos (UAARH), comunicar, imediatamente, as ocorrências de ingressos, afastamentos ou desligamentos de usuários, que impliquem na necessidade de criação, suspensão ou exclusão de contas de correio eletrônico.

NC 05 – UTILIZAÇÃO DA INTERNET E INTRANET

1 Campo de Aplicação

Esta norma se aplica no âmbito do CANOASPREV.

2 Objetivo

Estabelecer critérios para administração e utilização de acesso aos serviços de Internet e Intranet no âmbito do CANOASPREV

3 Diretrizes Gerais

a) Internet

- São usuários da Internet do CANOASPREV os conselheiros, servidores, estagiários e os demais agentes públicos ou particulares que oficialmente executem atividade vinculada à atuação institucional do CANOASPREV;

- O uso da Internet deverá priorizar a esfera profissional com conteúdo relacionado às atividades desempenhadas pela Autarquia, observando-se sempre a conduta compatível com a moralidade administrativa;

- As contas de usuários deverão ter níveis de acesso distintos, conforme a necessidade dos serviços, de acordo com os perfis definidos pela CTIC;

- Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso;

- Os usuários devem estar capacitados a utilizar os serviços de modo a garantir a sua utilização adequada;

- O uso de provedores de acesso externo ou de qualquer outra forma de conexão apenas ocorrerá mediante autorização da Diretoria Executiva;

- A Diretoria Administrativa, por meio da Unidade de Informática (UI), deverá prover o serviço de conexão à Internet implementando mecanismos de segurança adequados;

- A CTIC deverá estabelecer níveis de acesso à Internet;

- Toda alteração de nível de acesso somente será realizada mediante solicitação formal, pela chefia imediata do usuário, contendo a devida justificativa, que será avaliada pela CTIC e autorizada pela Diretoria Executiva, podendo esta solicitação ser negada em caso de risco ou vulnerabilidade na segurança e na integridade da rede do CANOASPREV;

- É vedado acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como:



CANOASPREV

INSTITUTO DE PREVIDÊNCIA E ASSISTÊNCIA
DOS SERVIDORES MUNICIPAIS DE CANOAS

- I. Pornografia, pedofilia, preconceitos, vandalismo, entre outros;
 - II. Acessar ou obter na Internet arquivos que apresentem vulnerabilidade de segurança ou possam comprometer, de alguma forma, a segurança e a integridade da rede do CANOASPREV;
 - III. Uso de IM (Instant Messenger) não homologado ou não autorizado pela CTIC;
 - IV. Uso de proxy anônimo;
 - V. Acesso a salas de bate-papo (chats), exceto aqueles definidos como ferramenta de trabalho homologada pela CTIC;
 - VI. Acesso a rádio e TV em tempo real, exceto os canais corporativos quando previamente autorizados;
 - VII. Acesso a jogos;
 - VIII. Acesso a outros conteúdos notadamente fora do contexto do trabalho desenvolvido;
 - IX. Divulgação de informações confidenciais da instituição por meio de correio eletrônico, grupos ou listas de discussão, sistemas de mensageria ou bate-papo, blogs, microblogs, ou ferramentas semelhantes;
 - X. Envio a destino externo de qualquer software licenciado ao CANOASPREV ou dados de sua propriedade ou de seus usuários, salvo expressa e fundada autorização do responsável pela sua guarda;
 - XI. Contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas do CANOASPREV;
 - XII. Utilização de softwares de compartilhamento de conteúdos na modalidade peer-to-peer (P2P);
 - XIII. Tráfego de quaisquer outros dados em desacordo com a lei ou capazes de prejudicar o desempenho dos serviços de tecnologia da informação do CANOASPREV, na forma definida pela CTIC.
 - O usuário poderá solicitar liberação de determinada página, com a devida justificada, mediante solicitação formal à UI, e autorizada pela Diretoria Administrativa, podendo ser ouvida a CTIC
 - Somente serão liberadas as páginas analisadas e autorizadas pela Diretoria Administrativa;
 - A ocorrência de qualquer hipótese de má utilização da internet deverá ser comunicada, de imediato à UI;
 - Comprovada a utilização irregular, o usuário envolvido terá o seu acesso à Internet bloqueado pela UI, sendo comunicado o fato à chefia imediata, podendo incorrer as penalidades previstas no item 1.10.
 - Poderá ser disponibilizada rede sem fio para acesso público à internet, mediante critérios de acesso que visem a proteção da rede do CANOASPREV, definidos em NC específica.
- b) Intranet
- São usuários da Intranet do CANOASPREV os Conselheiros, servidores, estagiários e os demais agentes públicos ou particulares que oficialmente executam atividade vinculada à atuação institucional do CANOASPREV;
 - A Intranet deverá ser utilizada como mecanismo de divulgação de notícias e disponibilização de serviços de caráter institucional;

- O acesso à Intranet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pela Autarquia, observando-se sempre a conduta compatível com a moralidade administrativa;

- As contas de usuários deverão ter níveis de acesso distintos, conforme a necessidade dos serviços;

- Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso;

- Os usuários devem estar capacitados a utilizar os serviços de modo a garantir a sua utilização adequada;

- O uso de provedores de acesso externos ou de qualquer outra forma de conexão apenas ocorrerá mediante autorização da Diretoria Executiva;

- As aplicações a serem disponibilizadas na Intranet devem ser previamente analisadas, homologadas e aprovadas pelo CTIC;

- As contas de serviços utilizadas em servidores de rede, backup, correio eletrônico, banco de dados, aplicações, entre outros, devem ser utilizadas somente para execução de ações ligadas à sua natureza, de forma automática, sem intervenção manual através de logon / acesso.

- As contas com privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades atribuídas, em equipamentos previamente definidos.

- As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos administradores dos equipamentos de rede e chefia respectiva.

c) Navegação e Administração

- Os navegadores de Internet e Intranet utilizados no âmbito do CANOASPREV deverão ser homologados pela UI;

- As paralisações dos serviços de Internet e Intranet, para manutenção preventiva, devem ser previamente comunicadas pela UI a todos os usuários;

- Os problemas técnicos verificados pelos usuários, ocorridos durante o acesso aos serviços de Internet e Intranet, devem ser imediatamente comunicados à UI para que sejam solucionados.