PREFEITURA MUNICIPAL DE CHAPECÓ / SC

SECRETARIA DE COORDENAÇÃO DE GOVERNO E GESTÃO

PSI – Política de Segurança da Informação

Gerencia de Projetos Estruturantes e Sistemas

V 2.0

Sumário

Introdução

A fim de prestar aos colaboradores e servidores públicos municipal do Município de Chapecó serviços simultâneos de rede de alta qualidade e ao mesmo tempo prover a segurança da informação, assegurando altos padrões de qualidade na prestação desses serviços, faz-se necessária a adoção de uma *PSI - Política de Segurança da Informação*.

Esta visa descrever as boas práticas, as formas de utilização e as atividades que entendemos como violação ao uso dos serviços e recursos, que são consideradas proibidas.

Podemos definir como serviços e recursos os programas e equipamentos utilizados pelos servidores, tais como: computadores, switches, impressoras, Scanners, Nobreaks, Internet, Correio Eletrônico (e-mails) do domínio *chapeco.sc.gov.br*, Rede Institucional, Intranet, Pastas e Arquivos.

As normas descritas podem ser atualizadas e adequadas com as necessidades, sendo que qualquer modificação será avisada em tempo hábil para remodelação (se necessário) do ambiente.

Em caso de dúvidas sobre o que é considerado, de alguma forma violação, o usuário deverá enviar previamente um e-mail para ti@chapeco.sc.gov.br visando esclarecimentos.

Objetivo

O objetivo é estabelecer diretrizes que permitam aos servidores públicos municipais do Município de Chapecó seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e da proteção legal da instituição, preservando as informações no tocante a:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. Dessa forma, busca-se desenvolver um comportamento ético e profissional, para que todos possam utilizar da melhor forma, as ferramentas de TI e as informações por elas geradas, ao mesmo tempo, busca-se reduzir ameaças através da adoção de medidas preventivas para evitar possíveis incidentes que tragam prejuízos à instituição.

E também quanto à classificação da informação:

- **Pública –** É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.
- **Interna –** É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.
- **Restrita –** É o nível médio de confidencialidade. São informações estratégicas que devem estar disponíveis apenas para grupos restritos de colaboradores/servidores. Podem ser protegidas, por exemplo, restringindo o acesso a uma pasta ou diretório da rede.
- **Confidencial –** É o nível mais alto de segurança dentro deste padrão. As informações confidenciais são aquelas que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem da empresa. É comum que estas sejam protegidas, por exemplo, por criptografia.

Conceitos e Definições

Para os fins dessa Política, considera-se:

- **Acesso Não Autorizado** - Acesso indevido ou não previsto obtido, por quaisquer meios, procedimentos e a qualquer título, à revelia da política ou do controle de acesso vigentes, ou ainda decorrente de falhas ou imperfeições nos mecanismos de controle de acesso. Contrasta com acesso autorizado.
- **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.
- **Acesso Físico** – acesso a locais e setores com equipamentos considerados críticos (Datacenter, Servidores, Racks, Central de Lógica e etc.) a TI.
- **Ameaça** – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.
- **Análise/avaliação de riscos** – processo completo de análise e avaliação de riscos.
- **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.
- **Auditoria** – verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes 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.
- **Bloqueio de acesso** – processo que tem por finalidade suspender temporariamente o acesso.
- **Cadastro -** procedimento de criação de usuário para acesso a rede Institucional, computadores, Internet e/ou ter direito a utilização de e-mail Institucional;
- **Classificação da informação** - atribuição, pela autoridade competente, degrau de sigilo dado à informação, documento, material, área ou instalação.

- **Colaborador** – servidores, empregados, contratados por tempo determinado, estagiários e prestadores de serviços que exercem atividades no âmbito do Município de Chapecó e suas autarquias.
- **Confidencialidade** – propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade autorizada.
- **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 instituição.
- **Controle de Acesso** - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.
- **Cópia de Segurança (Backup)** – copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. 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 o estudo dos princípios e técnicas pelas quais 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");
- **Dado** – representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;
- **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 pessoal.
- **Gestão de Continuidade de Negócios** - Processo de gestão global que identifica às potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia-a-dia.
- **Gestão de Risco** – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

- **Gestão de Segurança da Informação e Comunicações** - conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.
- **Gestor da Informação** - pessoa responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades;
- **Operador da Informação** – Pessoa responsável pela gerência de e-mails que atua dentro da Gerência de Projetos Estruturantes e Sistemas.
- **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;
- **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;
- **Informação sigilosa** - informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Município, e aquelas abrangidas pelas demais hipóteses legais de sigilo;
- **Integridade** – propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- **Internet** – rede mundial de computadores.
- **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;
- **Norma** - Documento interno que regulamenta formal e administrativamente, de maneira geral ou específica, aspectos ou diretrizes expressas na PSI, no todo

ou em parte da instituição. As normas mapeiam a PSI na organização técnico-administrativa da instituição, estabelecendo regras para a sua implementação.

- **Negação de Acesso**– ato ou tentativa proposital ou acidental de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Também conhecido pelo termo em inglês: *DoS (Denial of Service).*
- **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;
- **Perfil de acesso** - conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;
- **Política de Segurança da Informação (PSI)** – documento aprovado pela autoridade responsável pelo órgão, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação na instituição;
- **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, bloquear acesso a determinadas páginas;
- **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 Institucional Municipal** - conjunto de todas as redes locais sob a gestão do Município de Chapecó;
- **Rede Pública** – rede de acesso a todos;
- **Responsabilidade** - Obrigações e deveres decorrentes da legislação vigente, ofício, cargo, função ou por força de contrato, na proteção dos ativos de informação de qualquer natureza.
- **Restrição de Acesso** – processo que tem por finalidade restringir ou limitar por tempo determinado ou indeterminado o acesso à algum ativo, rede ou site.
- **Senha ou Credencial de Acesso**- Credencial que concede, de maneira prevista, o direito de acesso, físico ou lógico, a determinado ativo de informação de qualquer natureza, ou local que o abrigue. Uma senha ou credencial fraca é toda aquela que não obedece aos critérios e requisitos mínimos de qualidade vigentes.

- **Servidor de Rede** - recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;
- **Software** - são todos os 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;
- **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 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;
- **Usuário** - servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Municipal 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.

Âmbito da PSI

As diretrizes aqui estabelecidas estão baseadas na família ISO 27000 (Norma Brasileira ABNT NBR / ISO/IEC 27002) as quais deverão ser seguidas por todos os colaboradores que exercem atividades no âmbito do Município de Chapecó e suas autarquias ou qualquer pessoa e/ou empresa que venha a ter acesso a dados ou informações e em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes do órgão poderão ser monitorados e gravados conforme previsto nas leis brasileiras, de acordo com o Marco Civil e da Lei de Garanta e Proteção de Dados Pessoais.

É também a obrigação de cada colaborador se manter atualizado em relação a esta **PSI** e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de tecnologia da informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

É considerada como REDE INSTITUCIONAL MUNICIPAL, toda a rede e/ou computador de domínio público municipal.

Diretrizes Gerais

Todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos para preservar a continuidade do negócio.

Toda informação gerada pelos colaboradores, utilizando integralmente ou parcialmente recursos do Município de Chapecó, é de propriedade do órgão;

Ameaças e riscos devem ser reavaliados periodicamente para garantir que a organização esteja efetivamente protegida.

O acesso às informações, produzidas ou recebidas pelo Município de Chapecó e suas autarquias, deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos usuários internos;

Os processos de aquisição ou contratação de bens e serviços de tecnologia da informação, a qualquer título, devem refletir esta PSI e seus documentos acessórios, sem prejuízo da observância da legislação em vigor;

Os equipamentos de informática e comunicação, sistemas e informações deverão ser utilizados para a realização das atividades profissionais.

Esta Política de Segurança da Informação pode ser revisada periodicamente e eventualmente atualizada sempre que eventos ou fatos relevantes ocorrerem.

Os colaboradores devem evitar a circulação das informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

Define-se assim que está *PSI - Política de Segurança da Informação* é considerada um código de boas práticas.

Competências e Responsabilidades

1. **Secretário (a) de Governo**

- Assegurar que a implementação dos controles de segurança da informação tenha uma coordenação e permeie toda a organização.
- Apoiar a Política e manter compromisso com sua continuidade e resultados.

2. **Secretários Municipais**

- Solicitar cadastro, bloqueio, permissão, ou ainda a exclusão de usuários institucionais, bem como informar quaisquer alterações referentes ao perfil de acessos dos servidores vinculados a sua pasta ou delegar tal função a pessoa oficialmente designada, através de e-mail para suporteti@chapeco.sc.gov.br, com os seguintes dados: nome completo, matrícula, cargo e telefone para contato.

3. **Gerencia de Projetos Estruturantes e Sistemas**

- Gerenciar os endereços de e-mail e os perfis de acessos conforme solicitação;
- Promover cultura de segurança da informação e comunicações;
- Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- Propor recursos necessários às ações de segurança da informação e comunicações;
- Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
- Propor Normas Complementares e Procedimentos de Segurança da Informação e das Comunicações;
- Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança da informação;
- Apurar os incidentes de segurança críticos e encaminhar os fatos apurados para aplicação das penalidades previstas;
- Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;
- Identificar controles físicos, administrativos e tecnológicos para mitigação do risco;

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

4. Cabe aos Servidores Públicos do Município de Chapecó:

- Cumprir com todas as diretrizes e normas estabelecidas por esta política;
- Estar sempre atualizado e ciente das políticas, normas e procedimentos vigentes do Município de Chapecó;
- Não divulgar, compartilhar, transmitir ou deixar-se conhecer informações a pessoas que não tenham nível de autorização suficiente.
- Não conduzir, transportar, enviar, transmitir, compartilhar ou deixar que dados e informações alcancem ambiente ou destinatário fora das dependências ou controle do Município de Chapecó sem a devida autorização.
- Zelar e fazer bom uso do equipamento disponibilizado para o trabalho.

5. Cabe à Diretoria de Gestão de Pessoas

- Conforme o fluxo estabelecido com cada Secretaria, Fundação e/ou Autarquia comunicar à Gerência de Projetos Estruturantes e Sistemas todos os desligamentos, afastamentos, retornos e modificações no quadro funcional do Município de Chapecó.
- Repassar, no ato da contratação, e mediante termo de recebimento, a política de segurança da informação e do tratamento de dados.

6. Cabe à Procuradoria Geral do Município

- Prestar assessoramento de natureza jurídica, supervisionar e coordenar as atividades de natureza jurídica, inclusive aquelas relacionadas com a elaboração de atos normativos.
- Prestar apoio de natureza jurídica, na análise do não cumprimento pelo colaborador das normas estabelecidas para a utilização da Rede Institucional do Município de Chapecó.

Normas Complementares

Com a finalidade de detalhar à *PSI - Política de Segurança da Informação* e para melhorar seu entendimento, foram segmentadas as seguintes Normas e Complementares:

1. NC 01 – Política de Controle de Acesso;
2. NC 02 – Política de Acesso à Internet;
3. NC 03 – Política de Uso de Equipamentos de Informática;
4. NC 04 – Política para Uso de E-mail Institucional;

Penalidades

O descumprimento das disposições constantes nessa Política e nas Normas Complementares sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

Considerações Finais

Os casos omissos e dúvidas serão submetidos à Gerência de Projetos Estruturantes e Sistemas.

NC 01 – Política de Controle de Acesso

1. Objetivo

Estabelecer critérios para a disponibilização e administração do acesso aos serviços de tecnologia de informação do Município de Chapecó, bem como estabelecer critérios relativos às senhas das respectivas contas e boas práticas no que tange Controle de Acesso a Sistemas de Informação e Rede de Computadores.

2. Diretrizes Gerais

A conta de acesso é o instrumento para identificação do usuário na rede do Município de Chapecó e caracteriza-se por ser de uso individual e intransferível.

Todo cadastramento de conta de acesso à rede do Município de Chapecó deverá ser realizado por meio de solicitação do Secretário Municipal ou por pessoa por ele designada, através do e-mail suporteti@chapeco.sc.gov.br.

O login de acesso deverá estar vinculado à função exercida pelo servidor, não sendo permitida a utilização de e-mails com nomes pessoais dos usuários.

Excepcionalmente, poderão ser solicitados e-mails com a manutenção do nome do servidor, desde que devidamente justificados, por escrito, pelo superior hierárquico junto ao departamento de TI.

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

Todas as senhas, de usuários comuns, para autenticação na rede do Município de Chapecó devem seguir os seguintes critérios mínimos:

1. Toda senha deve ser constituída de, no mínimo, 8 caracteres sendo obrigatório o uso de caracteres alfanuméricos (letras e números);
2. A senha não poderá conter parte do nome do usuário, por exemplo: se o usuário se chama Joana dos Santos, sua senha não pode conter partes do nome como "1234joana" ou "1516Sant";
3. Deverá conter pelo menos de um caractere especial: @, *, !, #, $, %, +, =, -, _
4. Será obrigatória a troca de senha ao efetuar o primeiro logon;

A base de dados de senhas deve ser armazenada com criptografia.

O acesso aos serviços de tecnologia de informação do Município de Chapecó deve ser disponibilizado aos servidores que oficialmente executem atividade vinculada à atuação institucional do Município de Chapecó, suas autarquias e fundações.

O processo de aprovação do acesso deve ser iniciado pelo superior do usuário e os privilégios garantidos continuarão em efeito até que o usuário mude suas atividades ou deixe o

Órgão Público. Se um desses dois eventos ocorrer, a chefia imediata tem que notificar imediatamente a unidade responsável.

Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de tecnologia da informação deve ser imediatamente comunicada a Gerencia de Projetos Estruturantes e Sistemas.

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

Em caso de comprometimento comprovado da segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas.

3. Acesso Remoto

O acesso remoto aos serviços institucionais somente deve ser disponibilizado aos servidores que, oficialmente, executem atividades vinculadas à atuação institucional do Município de Chapecó, desde que solicitado pela gerência responsável pela informação.

A liberação de acesso remoto só será efetivada após avaliação e aprovação do Setor de Informática, para que se evitem ameaças à integridade e sigilo das informações contidas na rede do Município de Chapecó.

As Conexões remotas à rede do Município de Chapecó devem ocorrer da seguinte maneira:

a) Utilização de autenticação;
b) As senhas e as informações que trafegam entre a estação remota e a rede do Município de Chapecó devem estar criptografadas;
c) É vedada a utilização do acesso remoto para fins não relacionados às atividades da instituição.

Quanto ao cancelamento do serviço de acesso remoto deve ser efetuado sob as seguintes condições:

a) Finalização do período solicitado ou término do Contrato;
b) Perda da necessidade de utilização do serviço;
c) Transferência do usuário para outras unidades;
d) Identificação de vulnerabilidade, risco ou uso indevido.

É vedado ao usuário o acesso à base de dados institucionais com o objetivo de:

a) Compartilhar sem autorização da chefia imediata, no todo ou em parte, as informações contidas na base de dados institucionais;

É de responsabilidade do usuário que possui acesso a qualquer base de dados Institucional:

I. Manter em sigilo sua senha de acesso à base de dados;
II. Fechar o aplicativo de acesso à base de dados toda vez que se ausentar, evitando o acesso indevido;
III. Fazer bom uso da ferramenta e/ou sistema de acesso a base de dados;
IV. Não prejudicar desempenho, a usabilidade e o acesso ao sistema causando lentidão ou negação de acesso.

4. Acesso Remoto Externo

Quanto aos acessos remotos externos, estes normalmente se originam de fora da Rede Institucional do Município de Chapecó, e deverão ser efetuadas por meio de ferramentas e/ou softwares específicos que garanta uma comunicação ponto a ponto de maneira isolada e criptografada.

Todas as ferramentas e/ou softwares para acesso remoto deverão ser informados e homologados pela Gerência de Projetos Estruturantes e Sistemas.

Todo e qualquer acesso remoto externo que utilizar a tecnologia VPN (Virtual Private Network) para acesso à Rede Institucional do Município de Chapecó deverá ocorrer da seguinte maneira:

I. Efetuar a solicitação de acesso para suporteti@chapeco.sc.gov.br com a devida autorização do Secretário ou pessoa por ele designada.
II. Encaminhar e-mail para suporteti@chapeco.sc.gov.br com a autorização do Secretário ou pessoa por ele designada solicitando a criação de usuário e senha.
III. Acesso deverá ser efetuado através de um login para a identificação e autenticação do usuário.
IV. Toda conexão deverá ser criptografada.
V. Todo acesso será registrado em um histórico de eventos (log).
VI. O acesso somente deverá ser efetuado quando existir a necessidade.
VII. Fica vedado o acesso contínuo e ininterrupto da conexão.

O serviço de acesso remoto via VPN deve ser cancelado sob as seguintes condições:

I. Finalização do período solicitado ou término do Contrato;
II. Perda da necessidade de utilização do serviço;
III. Transferência do usuário para outras unidades;
IV. Identificação de vulnerabilidade, risco ou uso indevido.

Todos os casos omissos serão tratados pela Gerência de Projetos Estruturantes e Sistemas e o setor envolvido.

5. Do acesso a base de dados:

Deverá ser firmado termo de responsabilidade, pelo órgão solicitante, sobre as informações disponibilizadas.

A responsabilidade da guarda dos dados obtidos através de integrações entre sistemas deverá ser do órgão solicitante.

6. Controle de Acesso Físico

O acesso físico ao ambiente da Prefeitura Municipal de Chapecó deve ser controlado para prevenir o acesso não autorizado e a ocorrência de danos e interferências nos ativos da organização.

Todos os visitantes devem ser acompanhados por servidor, a não ser que o seu acesso tenha sido previamente aprovado.

6.1. Datacenter

O acesso ao Datacenter, salas de rack e somente poderá ser feito por pessoas autorizadas;

O acesso de visitantes ou terceiros ao Datacenter somente poderá ser realizado com acompanhamento de um colaborador da área de tecnologia de informação do Setor de Informática;

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração da Gerência de Serviços Gerais;

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto famígero e/ou inflamável;

6.2. Arquivos Físicos

O arquivo físico deve ser protegido por controles apropriados de entrada (chave, cartão de acesso, tags, biométrica, senha etc.) para assegurar que somente pessoas autorizadas tenham acesso permitido, bem como que esses controles sejam auditáveis.

Onde possível deve-se implantar uma área de recepção, ou outro meio para controlar o acesso físico ao local ou ao edifício, podendo-se ter o apoio de câmera de vigilância para monitoramento do ambiente.

NC 02 – Política de Acesso à Internet

1. Objetivo

Estabelecer critérios para administração e utilização de acesso aos serviços de Internet no âmbito do Município de Chapecó, em consonância com o Marco Civil da Internet e a LGPD.

2. Diretrizes Gerais

O acesso à Internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pelo Órgão.

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

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta Política de Segurança da Informação.

Toda alteração de nível de acesso somente será realizada mediante solicitação formal, através de formulário disponibilizado em https://ti.chapeco.sc.gov.br/psi/formulario.php, pela chefia imediata do usuário, contendo a devida justificativa, que será avaliada pelo Setor de Informática, podendo esta solicitação ser negada em caso de risco ou vulnerabilidade a segurança e a integridade da rede do Município de Chapecó.

3. Proibições

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

a) Pornografia, pedofilia, preconceitos, vandalismo, entre outros;
b) Acessar ou obter na Internet arquivos que apresentem vulnerabilidade de segurança ou possam comprometer, de alguma forma, a segurança e a integridade da rede da Institucional do Município de Chapecó;
c) Uso recreativo da internet em horário de expediente;
d) Uso de proxy anônimo;
e) Acesso à rádio e TV em tempo real, exceto os canais institucionais em horário de expediente;
f) Acesso a jogos;

g) Acesso a outros conteúdos notadamente fora do contexto do trabalho desenvolvido;
h) Envio a destino externo de qualquer software licenciado ao Município de Chapecó ou dados de sua propriedade ou de seus usuários, salvo expressa e fundada autorização do responsável pela sua guarda;
i) Contorno ou tentativa de contorno às políticas de Controle e Restrição de Acesso automaticamente aplicadas pelas ferramentas sistêmicas do Município de Chapecó;
j) Utilização de softwares de compartilhamento de conteúdo na modalidade peer-to-peer (P2P);
k) É proibido utilizar os recursos do Município de Chapecó para fazer o download ou distribuição de software ou dados não legalizados;
l) Efetuar upload de qualquer software licenciado ao Município de Chapecó ou de dados de propriedade desta e de seus usuários sem expressa autorização do Gestor da informação.

4. Controle e Restrição de Acesso

Caso o órgão julgue necessário, haverá controle e restrições de acesso a arquivos e sites não autorizados ou que comprometam o uso de banda da rede, o desempenho e produtividade das atividades do colaborador, bem como, que exponham a rede ariscos de segurança;

5. Auditoria

Quando necessário haverá auditoria dos sites acessados por usuário para verificação da adequação à política vigente;

Comprovada a utilização irregular, o usuário envolvido poderá ter o seu acesso à Internet bloqueado, sendo comunicado o fato à chefia imediata, podendo incorrerem processo administrativo disciplinar e nas sanções legalmente previstas, assegurados o contraditório e a ampla defesa.

NC 03 – Política de Uso de Equipamentos de Informática

1. Objetivo

Estabelecer critérios na utilização dos equipamentos de informática no âmbito do Município de Chapecó e suas autarquias.

2. Diretrizes Gerais

Os recursos computacionais somente devem ser utilizados para a execução de atividades de interesse do Município de Chapecó.

Cada estação de trabalho possui controle de IP (Protocolo Internet), os quais permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário. Por isso, sempre que ausentar do ambiente de trabalho tenha certeza de que efetuou o logoff ou bloqueou a estação de trabalho.

Todos os dados relativos às atividades das Secretarias que necessitem ser salvaguardados devem ser armazenados no servidor de rede especificado pelo Setor de Informática, onde existe sistema de backup diário e confiável.

Os arquivos gravados em diretórios temporários ou pastas públicas podem ser acessados por todos os usuários que utilizarem a rede local, portanto não garante sua integridade, podendo ser alterados ou excluídos sem prévio aviso e por qualquer usuário.

Evitar o armazenamento de assuntos sigilosos ou de natureza sensível em diretórios temporários ou pastas públicas.

Não será feito cópia de segurança dos arquivos criados no computador local dos colaboradores. O próprio usuário deve fazer cópia de segurança dos arquivos locais e verificar o que pode ser eliminado, evitando acúmulo de dados desnecessários.

É proibida a abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo deverá ocorrer pelo Setor de Informática.

Quanto à utilização de equipamentos de informática particulares (celulares, notebooks, tablets e/ou quaisquer dispositivos móveis que venham acessar a rede sem fio ou rede estruturada) o colaborador deverá comunicar a chefia imediata, que solicitará sua liberação de acesso através do Setor de Informática.

Em caso de eventos no ambiente das Secretarias e/ou autarquias que utilizem acesso à base de dados e sistemas internos do Município de Chapecó deverão ser informados ao Setor de Informática para efetuar as devidas liberações, instalações de equipamentos quando necessário.

Em eventos que acontecerem no Centro de Cultura e Eventos que são de responsabilidade do Município de Chapecó deverá ser informado o Setor de Informática com antecedência mínima de 7(setes) dias.

Em eventos realizados por terceiros no Centro de Cultura e Eventos que necessitem de internet deverá ocorrer da seguinte maneira:

I. O Setor de Informática deverá ser comunicado;
II. O acesso às salas de equipamentos de gerencia deverá ocorrer com a presença de um técnico do município;
III. Na ausência do técnico do município deverá ser preenchido um formulário com Nome Completo, Telefone, Empresa, e o que foi feito/executado.

Em caso de dano, inutilização ou extravio do equipamento o servidor deverá comunicar imediatamente o Setor de Informática e à Gerência de Patrimônio que deverá adotar as providências cabíveis.

Em caso de furto ou roubo, providenciar Boletim de Ocorrência junto à Polícia Civil e entregá-lo ao Setor de Informática e à Gerência de Patrimônio, que deverão adotaras providências cabíveis.

É proibida a colocação de adesivos com imãs nos equipamentos.

É dever do colaborador zelar pela integridade do equipamento estritamente como instrumento de trabalho, juntamente com os acessórios que foram utilizados.

Não é permitido alterar as configurações de rede e da BIOS das máquinas, bem como, efetuar qualquer modificação que possa causar algum problema futuro.

Não é permitido retirar ou transportar qualquer equipamento de informática da Rede Institucional sem autorização prévia do Setor de Informática.

Fica proibida a utilização, sem devido consentimento, da utilização de equipamentos de informática por pessoas sem vínculo com o Município de Chapecó salvo em casos extraordinários.

É vedado retirar e/ou danificar placas identificadoras de patrimônio, travas e lacres de segurança dos equipamentos de informática.

Não é permitido conectar e/ou configurar equipamento à rede, sem a prévia liberação do Setor de Informática.

O antivírus deve estar atualizado e com a autoproteção ativa na estação de trabalho.

O usuário deve obrigatoriamente executar o antivírus nos dispositivos removíveis antes de sua abertura quando inseridos na estação de trabalho.

3. Política de Instalação e Remoção de Softwares

Não é permitida a instalação de qualquer software com direitos de copyright sem o seu devido licenciamento.

Não é permitida a instalação e a remoção de softwares que não forem devidamente acompanhadas e/ou autorizadas pelo Setor de Informática qual deverá emitir uma autorização por escrito (via e-mail ou memorando).

Não é permitido gravar nas estações de trabalho e na Rede Institucional MP3, filmes, documentos, fotos e software com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria.

4. Política de Backup e Restauração de Arquivos

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente em horários em que não há nenhum ou pouco acesso de usuários ou processos aos sistemas de informática e arquivos.

Backups Incrementais Arquivos (Incremental diários) serão realizados de acordo com a rotina definida pelo Setor de Informática.

Os Backups completos Arquivos (completo semanais) serão realizados de acordo com a rotina definida pelo Setor de Informática.

Os Backups completos da Maquinas Virtuais (full semanais) serão realizados de acordo com a rotina definida pelo Setor de Informática.

Somente será restaurado os arquivos que foram gerados backup.

A restauração trará os arquivos mais antigos possíveis de acordo com a rotina de backups estabelecida pelo Setor de Informática.

Os colaboradores 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.

As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro e distantes o máximo possível do Datacenter.

Deverá ser implementada uma rotina de redundância do backup, com a finalidade de replicar o backup original em outro local seguro e distante fisicamente do Datacenter.

Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

5. Política de uso de impressoras

Todas as impressões deverão ser executadas nas suas respectivas gerências e setores.

Não é permitido imprimir documentos que não estejam dentro das atividades de trabalho.

Não é permitido deixar impressões erradas na mesa das impressoras.

Os documentos deverão preferencialmente ser impressos frente e verso, para economia de papel.

Quanto à instalação de novas impressoras deverá ser solicitada via formulário especifico com parecer da chefia imediata e remetido ao Setor de Informática para avaliação da necessidade e encaminhamentos para instalação.

NC 04 – Política de Uso de E-mail Institucional

1. Objetivo

Estabelecer critérios para disponibilização do serviço de correio eletrônico institucional do Município de Chapecó aos usuários.

2. Diretrizes Gerais

O serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais do Município de Chapecó e suas autarquias.

São usuários do serviço de correio eletrônico institucional, os colaboradores que executem atividade vinculada à atuação institucional do Município de Chapecó e suas autarquias e fundações.

A concessão de contas de correio eletrônico depende de pedido expresso do Secretário ou pessoa por ele designada.

Poderá ser solicitada a criação de listas de distribuição, restritas aos seus respectivos âmbitos de atuação.

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

O acesso ao serviço de correio eletrônico dar-se-á por meio de senha de uso pessoal e intransferível, vedada sua divulgação e através de usuário institucional sendo vedada a utilização de nome pessoal.

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 Município de Chapecó 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” e considerado como SPAM, 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 institucional;
V. Enviar arquivos de áudio, vídeo ou animações, salvo os que tenham relação com as funções institucionais desempenhadas pela Prefeitura Municipal de Chapecó;

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

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

É de responsabilidade do usuário do correio eletrônico:

I. Manter em sigilo sua senha de acesso ao correio eletrônico;

II. Fechar o aplicativo de correio (cliente) toda vez que se ausentar, evitando o acesso indevido;

III. Comunicar imediatamente a Gerência de Projetos Estruturantes e Sistemas, preferencialmente através do endereço ti@chapeco.sc.gov.br, do recebimento de mensagens com vírus ou que venham a trazer algum tipo de dano aos sistemas de informática;

IV. Efetuar a manutenção de sua caixa postal, evitando ultrapassar o limite de armazenamento e garantindo o seu funcionamento contínuo.

V. Efetuar com auxílio da Informática a criação e/ou alteração da assinatura padrão para utilização do e-mail.

É de responsabilidade da Gerência de Projetos Estruturantes e Sistemas:

I. Criar e manter cadastro dos usuários, das caixas postais e das listas de distribuição;

II. Cancelar os acessos ao serviço de correio eletrônico dos usuários que se desvincularem da Prefeitura, Secretaria e autarquias;

III. Propor a divulgação de orientação sobre o uso correto do correio eletrônico;

IV. Fiscalizar a utilização do serviço de correio eletrônico, observados os critérios estabelecidos nesta norma;

V. Desenvolver demais ações que garantam a operacionalização desta norma;