Dezembro de 2024

POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO DO MUNICÍPIO DE NAVIRAÍ

Naviraí - MS

Histórico de atualizações

Versão Publicada	Data de Disponibilização
Versão I Política Corporativa de Segurança da Informação do Município de Navirai	16/12/2024

Naviraí – MS

CAPÍTULO I

1. OBJETIVO

A presente política tem o objetivo de estabelecer condutas e procedimentos a serem adotados dentro de cada departamento ligado a administração municipal de Naviraí, com o intuito de manter a sua conformidade com a Lei Geral de Proteção de Dados em todos os processos e rotinas laborais, respaldada nas seguintes premissas norteadores:

a) Assegurar a confidencialidade, integridade e disponibilidade das informações da organização, mediante utilização de mecanismos de segurança da informação e cibernética, balanceando fatores de risco, tecnologia e custo.

b) Garantir a proteção adequada das informações e dos sistemas contra acessos indevidos, cópias, leituras, modificações, destruição e divulgação não autorizados.

c) Assegurar que os ativos de informação sejam utilizados apenas para as finalidades aprovadas pela instituição, estando sujeitos ao monitoramento, rastreabilidade e auditoria interna e externa.

d) Assegurar a participação do quadro de pessoal dos departamentos ligados a administração municipal de Naviraí no Programa Corporativo de Conscientização e educação em Segurança da Informação e Cibernética.

e) Assegurar a existência de processos para continuidade das atividades e gestão de incidentes de segurança para proteção, detecção, resposta e recuperação contra ataques cibernéticos.

f) Informar aos usuários sobre as precauções a serem adotadas na área de Segurança da Informação e Cibernética por meio de medidas necessárias nos processos internos do Município de Naviraí.

g) Garantir o cumprimento desta Política e das Normas e Padrões Corporativos de Segurança da Informação dentro dos departamentos, gerências, núcleos e órgãos vinculados a administração municipal de Naviraí.

h) Assegurar o comprometimento dos gestores e de todos os demais servidores do Município de Naviraí com a melhoria contínua dos processos e recursos necessários para Segurança Cibernética.

2. ABRANGÊNCIA

As regras aqui estabelecidas aplicam-se a todos os servidores, prestadores de serviço, fornecedores, estagiários e demais pessoas ligadas ao Município de Naviraí em seus diferentes regimes de trabalho, independentemente da duração do contrato ou natureza da prestação do serviço, desde que que participantes de processos de tratamento ou que envolvam acesso a informações dos bancos de dados do município.

3. OBRIGAÇÃO DE CONHECER E CUMPRIR A POLÍTICA

Todos os servidores e demais pessoas ligadas ao Município de Naviraí, tem a obrigação de conhecer e cumprir o que prescreve o presente documento, bem como cooperar com sua implantação, comunicando imediatamente ao seu superior hierárquico qualquer descumprimento ou fato que possa se assemelhar a tanto, assim que tiver ciência, para que seja feita com a maior brevidade a comunicação do incidente ao responsável imediato, departamento de tecnologia da informação e ao Encarregado de Dados do município, o qual procederá com todos os protocolos de segurança previstos em Lei.

Os servidores, contratados, prestadores de serviço e demais pessoas envolvidas no processo de tratamento de dados, independente do regime de trabalho, funções e responsabilidades, além de ter total conhecimento do conteúdo desta Política, necessitam ainda possuir conhecimento sobre a Política de Proteção e Privacidade de Dados e da Política de Contenção e Resposta a Incidentes do Município de Naviraí.

CAPÍTULO II

4. DESCRIÇÃO DE RESPONSABILIDADES

4.1. Dos servidores em geral:

Os servidores aqui tratados, são aqueles responsáveis por realizar seus trabalhos nos departamentos, núcleos, gerências e órgãos vinculados ao Município de Naviraí, independente da jornada e regime de trabalho, bem como fornecedores de produtos e serviços, ficando todos cientes das seguintes normas de segurança:

I) Da utilização de aparelhos celulares e de informática:

Para garantir a segurança de todos os equipamentos e as informações neles contidas, o usuário deverá dispensar total cuidado para com o equipamento fornecido pelo Município para o exercício de suas funções. Além disso, todos os aparelhos institucionais utilizados para atendimento ao público ou mesmo para atividades interna de trabalho via *WhatsApp* ou similares, deverão:

i) instituir uma pessoa responsável pelo aparelho, de forma que este tenha um responsável pelo uso e fiscalização, assinando termo de responsabilidade correspondente;

ii) ao final do expediente serem recolhidos para guarda em local seguro e de acesso restrito, permanecendo trancado;

iii) O aparelho celular cedido pelo município, não deve ser compartilhado com terceiros estranhos ao Município de Naviraí e suas gerências.

iv) ser configurados com senha de desbloqueio e recuperação de dois fatores no aplicativo de WhatsApp, a qual deve ficar aos cuidados da pessoa eleita como responsável pelo aparelho.

O usuário deverá, ainda, dispensar total cuidado para com o equipamento fornecido pelo Município para o exercício de suas funções, mantendo-o em pleno funcionamento e não compartilhando-o com terceiros estranhos às funções desempenhadas pelo servidor e que não possuam vínculo com a Prefeitura Municipal de Naviraí.

A instalação de aplicativos nos aparelhos institucionais só deverá ser feita mediante autorização do responsável pela Tecnologia da Informação (DTI), que fará verificações de rotina. Os acessórios que acompanham o aparelho, tais como, carregadores de parede, carregadores veiculares, cabos de conexão, etc., sempre serão fornecidos pelo município, sendo proibido ao usuário utilizar qualquer outro tipo de acessório.

II) Da utilização de celulares para foto/filmagem das atividades internas.

O Município de Naviraí preza pela privacidade de todos os titulares dos dados, bem como dos dados pessoais tratados, inclusive de voz e imagem.

Portanto, toda e qualquer imagem de servidores e da rotina laboral, somente poderá ser capturada por meio dos telefones corporativos, preferencialmente pela equipe responsável pelo Departamento de Comunicação e Assessoria de Imprensa do município e para finalidades determinadas e justificadas em seus propósitos legais.

O material somente poderá ser produzido em equipamento institucional, devendo o responsável certificar-se de que os munícipes, servidores ou demais titulares envolvidos, deram sua autorização expressa para tanto, a qual deverá ser requerida no ato do evento que deu causa a coleta, observando-se, quanto às crianças e adolescentes, o procedimento de coleta de consentimento por meio dos seus representantes legais. A negativa de consentimento, se houver, deverá ser por todos respeitada.

Recomenda-se a não utilização de celulares pessoais durante expediente, especialmente para atividades de trabalho ou captação de imagem dos servidores e demais titulares de dados sob responsabilidade do Município de Naviraí, durante as atividades internas e independe do horário.

Ademais, fica proibida a captura, reprodução e compartilhamento de imagens de telas de computadores, principalmente quando as telas espelharem sistemas internos onde estão armazenados os dados pessoais tratados. De igual forma, fica proibida a divulgação de qualquer imagem, foto ou vídeo da rotina de trabalho e colaboradores nas redes sociais pessoais dos servidores e prestadores de serviço, sem a devida autorização da pessoa veiculada a imagem, exceto aqueles materiais institucionais produzidos em eventos abertos ao público, sob pena de responsabilidade pessoal daquele que infringir à presente política publicando em suas redes sociais privadas conteúdos não autorizados pelo titular do dado.

III) Da criação de perfis em redes sociais e sua administração

A criação e administração de perfis em redes sociais em nome das gerências, departamentos ou órgãos ligados ao Município de Naviraí, deverá ser precedida de termo de responsabilidade assinado pelo administrador da conta, o qual ficará igualmente responsável pelo conteúdo veiculado.

Outrossim, em relação aos perfis existentes, fica orientado aos dirigentes a transferência da gestão da conta e demais dados cadastrais para os meios institucionais, em especial ao uso de e-mail corporativo nos cadastros desses perfis, com consequente troca das senhas, devendo ser elegido um responsável para administrá-lo, o qual deve ser cientificado por meio expresso quanto aos encargos oriundos de referido gerenciamento.

Restando devidamente advertido a todos servidores que a criação e administração de perfis sem a devida formalização do procedimento retromencionado, será considerada clandestina, portanto desautorizada e não abrangida pela responsabilidade do município, mas sim exclusivamente pela de seu criador, o qual responderá por todos prejuízos causados.

Aos indicados como responsáveis das redes sociais institucionais, compete administrar e assegurar o cumprimento da Lei Geral de Proteção de Dados, analisando o conteúdo veiculado ao perfil, restringindo conteúdos inapropriados e validando as publicações no concernente a não violação dos direitos dos titulares de dados.

IV) Da utilização do WhatsApp e demais aplicativos de conversa

Toda comunicação com servidores, fornecedores, prestadores de serviço e munícipes que utilizem os serviços prestados pelo Município de Naviraí, deve ser realizada exclusivamente pelos canais oficiais disponibilizados pelo Município.

Fica, portanto, vedado aos servidores a troca de mensagens por meio de seus celulares ou aplicativos pessoais em nome do Município de Naviraí. Caso sejam recepcionadas de forma espontânea, deverão ser transferidos para ambiente institucional seguro, orientando aquele a quem compete, o envio de informações e solicitações exclusivamente por meio dos canais oficiais.

Deve ser evitado ainda, mesmo que por meio dos canais oficiais, o envio desnecessário de imagens e dados pessoais em conversas realizadas por meio desses aplicativos, visando evitar o tratamento desnecessário de dados.

Todo e qualquer compartilhamento de dados com órgãos ou pessoas externas à Município de Naviraí, deve vir instruído por requerimento formal, o qual deve trazer a identificação do solicitante, a descrição dos dados requeridos e a finalidade do compartilhamento da informação, sob pena de indeferimento. Para análise dos requerimentos, o Encarregado de Dados fica à disposição do Município de Naviraí.

O uso de grupos de WhatsApp institucional deve ser realizado de maneira prudente pelos seus membros e com observância a finalidade institucional a ele inerente. Fica indicado que todo e qualquer conteúdo pessoal e/ou desvinculado à finalidade institucional encaminhado em grupos institucionais sejam removidos pelos Administradores do grupo.

Fica recomendado aos servidores a não criação de grupos desautorizados em aplicativos para as atividades de trabalho, especialmente para o compartilhamento de dados, uma vez que nem a gerência correspondente, nem o Município de Naviraí, se responsabilizarão pelas informações nestes grupos veiculadas, nem por eventuais divulgações indevidas. Fica vedado o envio de atestados médicos em grupos de *WhatsApp*, ainda que corporativo ou em ambiente privado do aplicativo, devendo estes serem pessoalmente apresentados ao responsável pelo Departamento de Recursos Humanos da unidade ou Gestor imediato, assim que possível.

Todos os departamentos da prefeitura que tiverem aparelhos institucionais para atendimento ao público via WhatsApp, deverão configurar o aplicativo com autenticação de dois fatores, a ser validada pelo responsável pelo aparelho. Nos departamentos da prefeitura que tiverem aparelhos institucionais para atendimento ao público via WhatsApp, deverão instituir uma pessoa responsável pela utilização da aparelho, o qual deverá configurar cópias de segurança (backup) das conversas para o e-mail institucional do departamento ou, caso não haja, para o e-mail da Central de Processamento de Dados (T.I).

Sempre que possível, após a utilização dos dados pessoais e documentos enviados pelo público via aplicativo de WhatsApp *(transcrição ou upload para sistema, atualização cadastral, instrumentalização de processo, etc.)* deverá ser o arquivo eliminado do celular de atendimento, mantendo-se, se necessário, o registro da conversa e do documento, em local adequado no servidor ou na própria plataforma de atendimento, caso se tratar de chatbot institucional do município.

Periodicamente os aparelhos institucionais passarão por monitoramento do Município de Naviraí e/ou do responsável pela Tecnologia da Informação (TI), sendo realizada a exclusão de dados e imagens que não tiverem mais justificativa para permanência nos aparelhos. Deste modo, aquelas informações que precisem ficar armazenadas, deverão ser objeto de comunicação imediata ao responsável pela T.I e Suporte da unidade para que promova a transferência para local adequado, sob pena de perda.

V) Do uso exclusivo de e-mail institucional e restrição de compartilhamento

Aos servidores vinculados ao Município de Naviraí fica vedada a utilização de e-mails de domínio privado e pessoal para o trabalho, restando orientados acerca do dever de utilização exclusiva de e-mails de domínio institucional para armazenamento de dados, envio e compartilhamento de informações. Inexistindo usuário de e-mail nestes moldes, deverá ser imediatamente formalizado requerimento ao setor responsável para providências quanto a criação e fornecimento do e-mail ao servidor solicitante.

Fica vedado o uso compartilhado de e-mail pelas equipes de trabalho do Município de Naviraí, bem como de seus *logins* e senhas, os quais são restritos, intransferíveis e de uso individualizado, sob responsabilidade de cada servidor. Caso necessário, nos e-mails centralizadores que representem um determinado órgão, equipes de trabalho ou setor, poderá ser designado um responsável para administrar a conta e redirecionar as demandas aos demais membros da equipe no local, evitando contudo o acesso compartilhado.

VI) Da utilização de computadores, rede de internet e sistemas *(Logins e Senhas)*

Na utilização dos computadores, notebooks e redes de internet cedidos pelo Município, deverão ser observadas as finalidades institucionais das máquinas e da rede, sendo vedado o acesso por meio destes aparelhos para finalidades pessoais ou desvinculadas das atividades de trabalho. Caso seja necessário o acesso a página que possua conteúdo bloqueado, a sua liberação será feita pelo Departamento de Tecnologia da Informação, desde que seja justificada pelos fins institucionais.

Todas as vezes que for necessário utilizar-se dos aparelhos institucionais, sistemas, aplicativos e da rede, os servidores deverão utilizar seus *logins* e senhas individuais de acesso, que são intransferíveis. O compartilhamento indevido desses *logins* e senhas será de total responsabilidade de seu proprietário, que responderá pelos danos causados por pessoa a quem tiver cedido, independentemente de ter ou não colaborado com conduta irregular praticada por terceiro.

Não será tolerada a utilização da aparelhos e computadores pessoais para o trabalho ou da rede de internet fornecida pelo Município para atividades da vida pessoal pelo servidor, e, caso identificada a utilização retro ou o acesso a sites e endereços eletrônicos inadequados à finalidade pública do fornecimento, o servidor estará sujeito as penalidades legais do regime de trabalho ao qual estiver atrelado. Ao setor de Tecnologia da Informação (T.I) fica terminamente vedado a concessão e manutenção dos acessos às áreas e sistemas institucionais por meio de computadores e aparelhos pessoais dos servidores do Município de Naviraí, devendo ser imediatamente revogado os acessos, caso existentes.

Todos computadores devem ser configurados para possuir bloqueio de acesso com solicitação obrigatória de credenciais ao adentrar a área de trabalho, sendo referida programação de alteração exclusiva do administrador de T.I, evitando assim, a retirada posterior do bloqueio por qualquer usuário desautorizado com intuito de acessar livremente as máquinas. Fica vedado o armazenamento de arquivos na área de trabalho dos computadores do Município de Naviraí, devendo ser mantidos em ambiente seguro e monitorado. Além disso, é indicado a todos servidores, o uso de senhas fortes com caracteres especiais, letras maiúsculas, minúsculas e números em sistemas, computadores e especialmente na rede *Wifi* do Município de Naviraí.

VII) Do gerenciamento de acessos aos sistemas e servidor de dados

O acesso aos sistemas e servidor de dados da instituição será concedido apenas a colaboradores autorizados, que tenham passado por um processo de autenticação e autorização de acordo com os princípios da segurança da informação, abrangendo os seguintes pontos:

a) **Controle de acesso do usuário** – deve ser mantido processo formal para conceder, modificar e revogar o acesso dos usuário ao servidor de dados e sistemas da informação baseado na necessidade e nas funções atribuídas;

b) **Gerenciamento de privilégios do sistema** – o acesso deve ser baseado em uma abordagem de necessidade mínima, devendo ser realizada a revisão regular dos níveis de acesso, de modo a garantir que que apenas as pessoas autorizadas tenham acesso às informações;

c) **Revogação de acesso do usuário** – deverá ocorrer quando o acesso do usuário à aquela informação não é mais necessário ou quando a relação do mesmo com a Município de Naviraí se encerrar, devendo haver a sua remoção imediata;

d) **Revisão de direitos de acesso** – O setor de Tecnologia da Informação (T.I) ou gestor imediato quando couber, deverá conduzir revisões periódicas dos direitos de acesso dos usuários para garantir que eles continuem alinhados com as funções e responsabilidade atuais de cada servidor;

e) **Gerenciamento de acesso de terceiros** – o acesso concedido a terceiros, como contratados ou prestadores de serviços, deve ser rigorosamente controlado e gerenciado por meio de um processo formal de autorização e revisão, bem como revogação ao fim do cumprimento de sua finalidade.

VIII) Da Restrição de Compartilhamento de Login e Senha de Acesso

O acesso aos sistemas do Município e outros sistemas externos utilizados para o desenvolvimento das atividades dos departamentos, tem em seu gerenciamento de acessos a premissa da utilização pessoal e intransferível daquele acesso, sendo determinante para a garantia da segurança das informações e a apuração de responsabilidades.

Desse modo a credencial e senha é de uso pessoal e intransferível, sendo estritamente proibido o seu compartilhamento, podendo a inobservância de referido processo implicar em ações disciplinares pelo uso indevido, sendo cada usuário exclusivamente responsável pelo atos praticados durante a utilização das suas credenciais, especialmente se for cedida a terceiros.

IX) Da Criação e Gestão de Senhas

Os sistemas internos do Município, bem como bancos e servidores de dados, devem contar com o processo de criação e gestão de senhas para o seu acesso, tendo em vista os seguintes critérios:

a) **Complexidade de senha**: As senhas devem possuir complexidade relativa, contando no mínimo 8 caracteres, incluindo letras maiúsculas, números e caracteres especiais;

b) **Atualização Regular**: Deve ser estipulado prazo periódico para a atualização da senha, recomendando-se a média de 90 dias, devendo os usuários serem notificados com antecedência de sobre a mudança;

c) **Proibição de Reutilização**: O sistema deve negar a reutilização das últimas três senhas utilizadas no ambiente.

Além do processo de gestão de senha descrito, é necessária a adoção e orientação constante sobre as medidas de segurança relacionadas as senhas, tais como:

a) **Autenticação em duas etapas**: Deve ser adotada a autenticação em duas etapas para os sistemas mais críticos, quando possível;

b) **Proteção da credencial**: Não deve haver a descrição e o armazenamento de credenciais de acesso em locais acessíveis a terceiros, e se necessário, pode-se utilizar gerenciadores de senhas aprovados pelo departamento de Tecnologia da Informação.

c) **Bloqueio de sessões inativas**: Deve haver a configuração para bloqueio automático do acesso em sessões após um período determinado de inatividade, recomendando-se a média de 15 minutos.

VIII) Da utilização de Periféricos, armazenamento e compartilhamento de documentos:

Fica terminantemente proibido o uso de periféricos, especialmente particulares nos computadores do Município de Naviraí, inclusive cabos USB, *Pendrives,* HD externo e outros tipos de periféricos de armazenamento de dados.

Em caso de necessidade da transmissão de documentos, deverá ser utilizado o servidor de dados ou sistemas internos, bem como e-mails institucionais, a fim de que o compartilhamento ocorra em ambiente virtual seguro e suscetível ao rastreamento do acesso e cópias de segurança. Todos os documentos ligados à prestação do serviços devem ser mantidos no servidor de dados ou sistemas institucionais, evitando a manutenção de documentos nas áreas de trabalho dos computadores, onde não serão alcançados pelo *backup* de segurança semanal instituído pela presente política.

IX) Do armazenamento de dados e cópias de Segurança

Os dados tratados pelo Município de Naviraí estão armazenados em servidor interno do Município e de suas gerências, além de sistemas por ele operados, que ficam sob o controle do Departamento de Tecnologia da Informação ou de operador de dados no caso de softwares privados contratados pelo município, os quais deve manter padrões de segurança e monitoramento, nos seguintes termos:

b) Deverá ser mantida rede unificada de servidores de dados para armazenamento dos arquivos digitais em todas as gerências do município de Naviraí, bem como nos núcleos e órgãos ligados a administração municipal. O acesso a esta rede deverá ser realizado mediante credenciais pessoais autenticáveis com no mínimo, dois fatores.

c) Os usuários deverão ter suas configurações de acesso adequadas às atividades de rotina, de modo que só possam acessar pastas e documentos que lhe sejam necessários na rotina de trabalho, de acordo com a função exercida.

d) A rede de servidores deverá contar com cópia de segurança a ser armazenada em local seguro e diverso do local do servidor principal.

e) A rede de servidores deverá passar por permanente vigilância com relação a invasões ou ameaças internas ou externas, físicas ou digitais, com testes periódicos de vulnerabilidades para constante correção e aprimoramento, bem como controle de acessos e permissões, além da realização de cópias de segurança, tudo apto ao oferecimento das garantidas legais instituídas pela LGPD.

O ambiente institucional é monitorado, rastreável e diariamente alcançado por backup, conforme Política de Backup, sendo executado pelo Departamento de Tecnologia da Informação, que também desenvolveu e controla as rotinas de segurança do sistemas utilizados para o armazenamento de dados e informações em geral.

Tanto o servidor de dados como os sistemas de gerenciamento de dados operados pelos setores e unidades de atendimento do Município, passarão por monitoramento, controle de acessos e permissões, além da realização de cópias de segurança, tudo apto ao oferecimento das garantidas legais instituídas pela Lei Geral de Proteção de Dados.

Desta forma, não serão tolerados acessos indevidos, nem armazenamento de dados mantidos fora dos ambientes institucionais citados. Ficando terminantemente proibido aos servidores à utilização de *drivers* de armazenamento pessoal para guarda ou transferência de arquivos e documentos pertencentes ao Município de Naviraí, sob pena de apuração e responsabilização daquele que incorrerem em descumprimento.

X) Do controle de solicitações e transporte de Documentos físicos

Para fins do transporte de documentos físicos internos, fica estabelecido que o translado deverá se dar de forma segura, apenas por pessoas e em processo previamente autorizados, devendo ser observadas o seguinte regramento:

i) Antes de iniciar o transporte, o emissor do documento deverá certificar-se de que este encontra-se acondicionado em envelope, pasta ou malote lacrado, com a devida identificação de seu destinatário.

ii) Todo o transporte deverá ser registrado por meio de protocolo de saída e de entrega, com a descrição do documento, destinatário e receptor.

iii) Antes de iniciar o transporte, o emissor do documento deverá certificar-se de que o meio a ser utilizado oferece condições de segurança adequadas. Se forem utilizados veículos ciclomotores, bicicletas e motocicletas, deverão estar equipados com bagageiros resistentes a impactos e munidos de trancas, cujas chaves devem ser mantidas em tempo integral com condutor.

iv) Todos os responsáveis pelo transporte, deverão firmar termo de compromisso e responsabilidade, dando ciência acerca das regras de segurança no transporte exigidas pelo Município.

v) O malote, envelope ou demais meios utilizados para comunicação interna, deverão ser lacrados e sem transparência.

Nenhum material ou documento de propriedade do Município de Naviraí, deverá ser retirado de suas dependências sem justificativa e autorização prévia do superior hierárquico direto, de modo que o servidor que agir de forma contrária a esta Política, responsabilizar-se-á pelas atividades que derem causa a incidentes de dados.

Portanto, o acesso e retirada mesmo que de cópia de documentos físicos deverá ser formalizada, permitindo a rastreabilidade e monitoramento do conteúdo, bem como dos envolvidos nos processos de requerimento e autorização. O manuseio de atesados deve ser efetivado com atenção, devendo ser apresentado pelo próprio titular, preferencialmente ao departamento de Recursos Humanos, ou a quem a administração determine, evitando-se a utilização de envio por meio de aplicativo de WhatsApp pessoal do servidor.

XI) Política da mesa limpa

Durante a execução das atividades de trabalho todos os integrantes do quadro de trabalho do Município de Naviraí são responsáveis por manter suas mesas e estações de trabalho livre de desordem, evitando a exposição de dados pessoais e informações sigilosas.

Os documentos devem ser mantidos, preferencialmente, em armários ou gavetas trancadas, quando não estiverem em uso, em especial documentos confidenciais. Sendo que, enquanto estiverem sendo utilizados e sobre as mesas, devem ser postos com o verso em branco para cima, dificultando assim a visualização de pessoas não autorizadas ao conteúdo constante na frente dos documentos.

Os computadores e dispositivos móveis que forem utilizados nas dependências das unidades vinculadas ao Município de Naviraí, devem possuir restrição de acesso por senha, devendo ser bloqueado o dispositivo sempre que o responsável pela tarefa ou aparelho se ausentar do posto de trabalho, independente do prazo de sua ausência.

Os monitores devem ficar posicionados de modo que se restrinja a visualização do conteúdo por pessoas não autorizadas que adentrarem as salas de trabalho.

Deve ser observado ainda, a eventual existência de dados pessoais em qualquer documento que possa estar sobre a mesa ou exposto na estação de trabalho, visando adotar as medidas indicadas como regra na rotina laboral.

XII) Da utilização das impressoras e scanners:

Toda vez que for realizado o download, digitalização, impressão ou cópia de documentos, é dever do funcionário que realizou o serviço providenciar o imediato descarte físico e/ou digital do mesmo.

a. O descarte físico deverá ser feito mediante destruição total dos papéis (picotadora) ou incineração;

b. O descarte digital deverá ser realizado diariamente, após encerrada a utilização do arquivo ou documento, promovendo a exclusão do histórico.

a) Computador e impressora: mediante a transferência do documento para o servidor e exclusão do mesmo da pasta vinculada à impressora na rede;

b) Celular institucional: Envio dos arquivos para o computador e depois para o servidor com consequente exclusão dos arquivos do aparelho.

As máquinas impressoras, *scanners* e computadores de propriedade do Município de Naviraí passarão por vistoria periódica com a finalidade de promover a verificação a respeito do cumprimento das medidas acima orientadas.

XIII) Antivírus e sistemas de detecção de invasões nas máquinas.

Os computadores institucionais passarão por varredura por antivírus, ficando estabelecida a adoção de um antivírus padrão para todas as máquinas do Município de Naviraí, que seja programado para este tipo de varredura, o que será validado e executado pelo Departamento de Tecnologia da Informação.

XIV) Da utilização de drives e armazenamento em nuvem

É vedada a utilização de serviços de armazenamento em nuvem, tais como drives e pastas de transferência, sem o conhecimento e liberação formal para a sua utilização pelo Núcleo de Tecnologia da Informação.

O Núcleo de Tecnologia da Informação, quando efetivar a liberação do uso de tais serviços, deve promover o registro do seu uso e de como o departamento está efetivando a utilização desse serviço, identificação qual empresa e serviço está sendo utilizado, além de quais são as medidas de segurança adotados para a segurança das informações que serão processadas nesse ambiente, tais como a realização de backup, gestão de acesso e análise do local do servidor deste serviço, especialmente se for estrangeiro. O e-mail a ser cadastrado, caso haja liberação para a utilização do serviço, deve sempre institucional com controle pelo Município.

XV) Do Monitoramento por Câmeras de Segurança - CFTV

De modo a garantir a confidencialidade, a integridade e a disponibilidade, bem como o acesso restrito à pessoas autorizadas, o manejo das informações provenientes do monitoramento de imagens por circuito fechado de televisão, deve observar as diretrizes e controles constantes na presente cláusula.

O acesso às imagens de monitoramento dever se restringir apenas ao pessoal autorizado e necessário, com base no princípio do mínimo privilégio, com revisão dos direitos de acesso periodicamente. Devem ser adotadas medidas de controle de acesso, tanto físico quanto lógico, aos dispositivos e servidores que armazenam as imagens, inclusive com implementação de sistemas de autenticação, com especial atenção às imagens que envolvam monitoramento de crianças e adolescentes.

Deverá o departamento responsável pela Central de Monitoramento promover monitoramento e auditoria dos sistemas de captação de imagens, de modo a registrar todas as atividades relacionadas às imagens, permitindo a detecção de atividades suspeitas, bem como definir política clara de retenção das imagens obtidas pelo monitoramento, garantindo que as imagens sejam retidas apenas pelo tempo necessário e em conformidade com as leis aplicáveis.

Caberá ao departamento e Tecnologia da Informação manter todos os sistemas de monitoramento e dispositivos relacionados atualizados com as última correções de segurança e patches do software. Observando ainda o dever de transparência no tratamento de dados, o Município deverá realizar a inclusão de informativo de monitoramento do ambiente por câmera, sempre que assim o for, visando resguardar o direito de conhecimento da existência de tratamento de dados do titular.

5. Encarregado de Dados

O Encarregado de Dados é o responsável pela implantação e manutenção das medidas e tecnologias de adequação a Lei Geral de Proteção de Dados. O Encarregado tem a responsabilidade de se atualizar sempre que houver uma nova perspectiva a respeito das exigências de adequação legal a proteção de dados e sempre buscar meios atuais e eficiente de prevenção e segurança para a rotina e os acessos tecnológicos da organização.

Caso seja registrada alguma solicitação de informação a respeito do tratamento dos dados feita pelo titular, é de responsabilidade do Encarregado respondê-la, assim como atender e enviar toda e qualquer informação solicitada pelo controlador ou autoridade competente em até no máximo 2 (dois) dias úteis, podendo este prazo ser inferior em casos justificados.

Caso seja identificada alguma falha ou invasão nos sistemas ou no servidor onde são armazenados os dados pessoais tratados pelas unidades do Município de Naviraí, o Encarregado deverá ser informado de maneira formal e imediata, em um prazo de até 24 horas, a fim de que, em conjunto com o Município e com o responsável pela Tecnologia da informação, investigue a natureza do vazamento, para que possa apresentar um relatório descritivo do motivo da falha e os procedimentos que serão adotados para evitar a sua recorrência.

Evidencias de vazamento, invasão ou qualquer outro incidente devem ser armazenados por até 3 anos da data do ocorrido ou da qual se tenha tomado conhecimento do fato, para nutrir material probatório em uma eventual ação judicial ou administrativa.

6. Disposições gerais

Este documento é a primeira edição da Política Corporativa de Segurança da Informação do Município de Naviraí, devendo ser atualizada, ao menos anualmente para manter conformidade com as exigências legais, sendo que, após toda atualização deve ser entregue aos servidores para ciência a respeito de seu conteúdo e atualizações promovidas.

CAMILA DOS SANTOS OLIVEIRA

Assinado de forma digital por CAMILA DOS SANTOS OLIVEIRA
Dados: 2025.01.22 13:10:20 -04'00'