DECRETO MUNICIPAL Nº 120, DE 15 DE AGOSTO DE 2024.

"INSTITUI A PLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO PODER EXECUTIVO MUNICIPAL DE CARACOL/MS E DÁ OUTRAS PROVIDÊNCIAS".

O **PREFEITO MUNICIPAL DE CARACOL, ESTADO DE MATO GROSSO DO SUL**, no uso de suas atribuições que lhe confere a Lei Orgânica Municipal, e

CONSIDERANDO, as disposições contidas na Lei Federal 13.709, de 14 de agosto de 2018;

CONSIDERANDO o disposto no Decreto 106/2024 que aprova o Plano de Ação/ROADMAP;

DECRETA:

Art. 1º. Fica instituída a Política de Segurança da Informação – PSI, no âmbito do Poder Executivo Municipal de Caracol/MS, conforme Diretrizes e Normas constante no anexo único deste Decreto.

Art. 2º. Este Decreto entra em vigor na data de sua publicação.

Caracol/MS, 15 de agosto de 2024.

Carlos Humberto Pagliosa
Prefeito Municipal de Caracol/MS

Anexo único ao Decreto Municipal nº 120/2024

POLITICA DE SEGURANÇA DA INFORMAÇÃO – PSI

Caracol/MS

SUMÁRIO

Glossário

- **Backup:** Cópia de segurança de dados para evitar perdas.
- **Cloud Backup:** Backup realizado em nuvem, através de um provedor externo.
- **Controlador:** Pessoa ou organização que determina as finalidades e os meios de tratamento de dados pessoais.
- **Encarregado:** Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- **LGPD:** Lei Geral de Proteção de Dados, que regula o tratamento de dados pessoais no Brasil.
- **Operador:** Pessoa ou organização que realiza o tratamento de dados pessoais em nome do controlador.
- **PSI:** Política de Segurança da Informação, documento que estabelece diretrizes e normas para proteger as informações de uma organização.
- **TI:** Tecnologia da Informação, conjunto de recursos tecnológicos utilizados para armazenar, processar e transmitir informações.

1. INTRODUÇÃO

A *Política de Segurança da Informação* abrange tanto dados **lógicos** quanto **físicos**. Ela é um conjunto de diretrizes e práticas que visam proteger todas as formas de informação dentro de uma organização. Aqui estão os principais aspectos que são estão cobertos por esta *Política de Segurança da Informação:*

Dados Lógicos

- **Dados Digitais:** Informações armazenadas em sistemas computacionais, incluindo bancos de dados, arquivos eletrônicos, e-mails, e qualquer tipo de informação que é manipulada digitalmente.
- **Redes e Comunicação:** Segurança das redes internas e externas, comunicação via internet, VPNs, e todos os tipos de transmissão de dados digitais.
- **Acesso e Autenticação:** Controle de acesso a sistemas e dados através de senhas, autenticação multifator, permissões de usuário e políticas de uso.
- **Software e Aplicações:** Segurança do software utilizado pela organização, incluindo sistemas operacionais, aplicativos de negócios, e softwares de segurança como antivírus e firewalls.

Dados Físicos

- **Infraestrutura Física:** Proteção das instalações físicas onde os dados são armazenados e processados, como data centers, salas de servidores e escritórios.
- **Equipamentos e Dispositivos:** Segurança de hardware como servidores, computadores, laptops, dispositivos móveis e outros equipamentos eletrônicos.
- **Documentos e Mídias:** Proteção de documentos físicos, mídia removível (como CDs, DVDs, pen drives) e backups físicos.
- Controle de Acesso Físico: Medidas de segurança para controlar o acesso físico às instalações, como crachás, biometria, vigilância por câmeras e guardas de segurança.
- **Gestão de Descarte:** Procedimentos seguros para o descarte de equipamentos, mídias e documentos físicos, garantindo que dados sensíveis não sejam recuperados.

Objetivos Gerais da *Política de Segurança da Informação*:

- **Confidencialidade:** Garantir que a informação seja acessível apenas por pessoas autorizadas.
- **Integridade:** Assegurar que a informação seja precisa e confiável, e não tenha sido alterada de forma não autorizada.
- **Disponibilidade:** Garantir que a informação esteja disponível quando necessária para os processos de negócios.

A atual *Política de Segurança de Informação* adotada pelo município de Caracol-MS contempla um conjunto de normas e procedimentos, delineando de forma clara os métodos de uso dos recursos de tecnologias e o cuidados com a segurança da informação.

O conceito adotado de *Segurança da Informação* é a imperativa preservação e valorização da informação, focando na necessidade de permitir que apenas pessoas autorizadas tenham acesso a essas informações.

A normatização possui objetivo de conduzir de forma eficiente as ações diárias de servidores municipais que utilizam os recursos de tecnologia de Informação (TI), ou outros meios, disponibilizados pelo município como ferramenta de trabalho, para melhor servir aos interesses públicos.

Secundariamente ao efetuar o regramento, busca-se uniformizar padrões de utilização da rede e recursos de TI, permitindo o perfeito discernimento da separação da "coisa pública", muitas vezes indevidamente utilizadas.

Desta forma, torna-se vital a ampla comunicação e adesão dos servidores, conselheiros, bem como, dos prestadores de serviço com acesso a informações do munícipio.

2- LEI GERAL DA PROTEÇÃO DE DADOS – LGPD Lei nº 13.709/2018.

Em resumo: Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por **pessoa jurídica de direito público** ou

privado, com o objetivo de proteger os direitos fundamentais de **liberdade e de privacidade** e o livre desenvolvimento da personalidade da pessoa natural.

2.1 Controlador

Art. 5º, VI: "O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais."

2.2 Operador

Art. 5º, VII: "O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador."

2.3 Encarregado

Art. 5º, VIII: "O encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)."

2.4 Resumo das Atribuições e Responsabilidades

a. Controlador

O controlador é responsável por:

- Determinar as finalidades e os meios de tratamento dos dados pessoais.
- Garantir que o tratamento de dados esteja de acordo com a legislação.
- Assegurar a transparência no tratamento de dados pessoais, informando aos titulares dos dados sobre como suas informações são usadas.
- Adotar medidas de segurança apropriadas para proteger os dados pessoais.
- Notificar a ANPD e os titulares sobre incidentes de segurança que possam acarretar risco ou dano relevante aos titulares dos dados.

b. Operador

O operador é responsável por:

- Realizar o tratamento de dados pessoais conforme as instruções do controlador.

- Garantir a segurança dos dados pessoais durante o tratamento.
- Cooperar com a ANPD e com o controlador na execução de suas funções.
- Não usar os dados pessoais para finalidades diferentes daquelas definidas pelo controlador.

c. Encarregado

O encarregado é responsável por:

- Ser o ponto de contato entre o controlador, os titulares dos dados e a ANPD.
- Orientar os funcionários e os contratados da entidade a respeito das práticas de proteção de dados pessoais.
- Receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.
- Receber comunicações da ANPD e adotar providências.
- Realizar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Na prática, o "tratamento de dados" são operações com dados pessoais, incluídos desde o recolhimento, registro e organização de dados até a consulta e divulgação destas informações.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei.

3- CONTROLE DE ACESSO

3.1 Acesso físico

Para a área de recepção dos orgãos públicos municipais, haverá livre acesso ao público, porém, para acesso as demais dependências dos orgãos públicos municipais,

deve haver a perfeita identificação do visitante, o motivo de sua visita, a área que será visitada e a aprovação do responsável pela área. A saída do visitante deverá se "liberada" pela área visitada;

3.2 Acesso a rede lógica

O acesso a rede lógica do MUNICÍPIO será efetuado apenas por servidores dos orgãos públicos deste municipios , servidores da área de Tecnologia de Informação da Prefeitura de Itapoá designados para tal função, ou, por serviço técnico devidamente contratado para tal finalidade. Quando da realização de serviço, o mesmo deverá ser integralmente acompanhado e, a saída do prestador de serviço deverá se "liberada" pela área que acompanhou a realização do serviço.

4- DOS RECURSOS DE TECNOLOGIA DE INFORMAÇÃO (TI) DISPONIBILIZADOS.

Os recursos de Tecnologia da Informação (TI) disponibilizados aos operadores englobam todos os equipamentos, periféricos, suprimentos e qualquer outro serviço e/ou dispositivo correlato disponibilizados aos servidores e ou prestadores de serviço para a realização de atividades diversas, dentre os quais estão incluídos impressoras e suprimentos, dispositivos de armazenamento, computadores, tablets, celulares, smartphones, contas de acesso (internet, correio eletrônico e demais sistemas), escâneres, rede local, câmeras digitais, etc.

5- PADRÃO DE CONFIGURAÇÃO DE TI DISPONIBILIZADO.

Todos os dispositivos de Tecnologia da Informação (TI) fornecidos aos operadores (computadores, notebooks, tablets, etc.) deverão seguir o padrão de configuração definido pelo setor de TI. Este padrão visa garantir o melhor desempenho dos dispositivos e a proteção dos dados pessoais.

Qualquer alteração na configuração, troca interna ou externa de equipamentos ou periféricos deverá ser **autorizada previamente** pelo setor de TI, por meio de solicitação formal e justificativa da necessidade da alteração. Alterações não autorizadas podem comprometer a segurança dos dados pessoais e a integridade dos sistemas.

Em caso de identificação de alterações não autorizadas, o usuário responsável

será notificado e as configurações originais serão restauradas. Além disso, serão tomadas as medidas cabíveis para investigar o ocorrido e garantir a segurança dos dados pessoais, incluindo a apuração de responsabilidades e a aplicação de sanções administrativas, se necessário.

6- DA INSTALAÇÃO DE SISTEMAS/SOFTWARES.

Para garantir a proteção de dados pessoais e a segurança da informação, a instalação de qualquer software em equipamentos utilizados para o tratamento de dados pessoais (computadores, notebooks, tablets, etc.) deverá ser realizada **somente após análise e aprovação prévia** da equipe responsável pela segurança da informação, em conformidade com a Política de Segurança da Informação e com a LGPD.

A instalação de softwares não autorizados ou sem a devida análise pode comprometer a segurança dos dados pessoais, expondo-os a riscos como acesso não autorizado, perda, alteração, destruição ou vazamento. Além disso, a utilização de softwares sem licença ou de origem duvidosa pode configurar crime de violação de direitos autorais.

Em caso de identificação de softwares não autorizados instalados em equipamentos utilizados para o tratamento de dados pessoais, **o usuário responsável será notificado e o software será removido imediatamente**. Adicionalmente, serão tomadas as medidas cabíveis para investigar o ocorrido e garantir a segurança dos dados pessoais, incluindo a apuração de responsabilidades e a aplicação de sanções administrativas, se necessário.

É fundamental que todos os usuários que lidam com dados pessoais estejam cientes da importância de seguir as políticas e procedimentos de segurança da informação, contribuindo para a proteção dos dados pessoais e para a conformidade com a LGPD. A equipe responsável pela segurança da informação está à disposição para esclarecer dúvidas e fornecer orientações sobre a instalação de softwares.

7- ACESSOS DO USUÁRIO.

Cada operador receberá "acessos aos recursos de TI", conforme solicitado pela sua chefia, se estiverem em acordo com a PSI.

Por "acessos aos recursos de TI", entende-se o fornecimento de determinado tipo de permissão através de login/senha com configurações de acesso pré-determinadas.

As senhas de acesso são de uso pessoal e intransferível.

Ao ausentar-se de ponto de acesso (microcomputador, notebook), o operador deverá efetuar o logout ou bloqueio de tela.

8- USO CORRETO DO E-MAIL.

Cada usuário é diretamente responsável pelo uso de seu e-mail e suas consequências.

As senhas de acesso são de uso pessoal e intransferível.

O e-mail corporativo é uma ferramenta de trabalho disponibilizada pelo MUNICÍPIO ao servidor, portanto, pode ser monitorado/auditado a qualquer momento pelo setor de TI, com ou sem o consentimento do usuário;

9 - USO CORRETO DA INTERNET.

O acesso à internet no ambiente de trabalho é fornecido para fins profissionais e, portanto, está sujeito a monitoramento, em conformidade com a legislação trabalhista e a LGPD.

Visando garantir a segurança da informação e a proteção de dados pessoais, o acesso a determinados sites e conteúdo online pode ser restringido ou bloqueado, especialmente aqueles que representam riscos à segurança da rede, como:

- **Sites com conteúdo malicioso:** Páginas conhecidas por conter malware, vírus ou outros softwares nocivos.
- **Sites de phishing:** Páginas que tentam enganar os usuários para obter informações confidenciais, como senhas e dados bancários.
- **Sites com conteúdo inadequado:** Páginas com conteúdo impróprio, ofensivo ou discriminatório, que podem gerar um ambiente de trabalho hostil.
- **Sites que consomem banda larga excessiva:** Páginas com vídeos, jogos ou outros conteúdos que podem prejudicar o desempenho da rede e afetar a produtividade.

O setor de TI é responsável por buscar sempre o equilíbrio entre a necessidade de acesso à informação e a proteção dos dados pessoais e da segurança da rede.

É importante que todos os usuários estejam cientes das políticas de uso da internet e das restrições de acesso, utilizando a rede de forma responsável e ética. O descumprimento das políticas pode resultar em sanções administrativas e outras medidas disciplinares cabíveis.

10- PLANO DE CONTINGÊNCIA.

Plano de Contingência para Proteção de Dados Pessoais do Município de Caracol/MS

10.1 Objetivo

O presente Plano de Contingência tem como objetivo estabelecer diretrizes e procedimentos para a prevenção, detecção e resposta a incidentes de segurança que possam comprometer a disponibilidade, integridade e confidencialidade dos dados pessoais tratados pelo Município de Caracol/MS, em conformidade com a Lei Geral de Proteção de Dados (LGPD).

10. 2. Escopo

Este plano abrange todos os órgãos e entidades da administração pública municipal, direta e indireta, que realizam o tratamento de dados pessoais.

10.3. Definições

- **Incidente de segurança:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos dados pessoais, como acesso não autorizado, destruição, perda, alteração, vazamento ou qualquer outra forma de tratamento inadequado.
- **Dados pessoais:** qualquer informação relacionada a pessoa natural identificada ou identificável.
- **Backup:** cópia de segurança dos dados pessoais, realizada periodicamente para garantir sua recuperação em caso de incidente de segurança.
- **Restauração:** processo de recuperação dos dados pessoais a partir de um backup.

10.4. Prevenção de Incidentes de Segurança

- **Medidas de segurança:** Implementação de medidas de segurança adequadas ao risco de cada tratamento de dados, como criptografia, controle de acesso, firewalls, antivírus e sistemas de detecção de intrusão.
- **Treinamento e conscientização:** Realização de treinamentos periódicos para os servidores e colaboradores sobre a importância da proteção de dados pessoais e as medidas de segurança a serem adotadas.
- **Atualização de softwares:** Manutenção dos softwares e sistemas atualizados, com a aplicação de patches de segurança sempre que disponíveis.
- **Política de segurança da informação:** Elaboração e divulgação de uma política de segurança da informação que estabeleça diretrizes e responsabilidades para a proteção de dados pessoais.

10.5. Detecção de Incidentes de Segurança

- **Monitoramento:** Monitoramento contínuo dos sistemas e logs para identificar atividades suspeitas ou tentativas de acesso não autorizado.
- **Canais de comunicação:** Criação de canais de comunicação para que os servidores e colaboradores possam reportar incidentes de segurança ou suspeitas de violação de dados pessoais.
- **Análise de riscos:** Realização periódica de análises de riscos para identificar vulnerabilidades e ameaças aos dados pessoais.

10.6. Resposta a Incidentes de Segurança

- **Equipe de resposta a incidentes:** Criação de uma equipe de resposta a incidentes, composta por profissionais de diferentes áreas, responsável por coordenar as ações de resposta a incidentes de segurança.
- **Plano de comunicação:**

Público-alvo:

- ***Titulares de dados:*** *Indivíduos cujos dados pessoais foram afetados pelo incidente.*

- ***Autoridade Nacional de Proteção de Dados (ANPD):*** *Órgão responsável pela fiscalização e aplicação da LGPD.*
- ***Outros órgãos competentes:*** *Outros órgãos que possam ter interesse no incidente, como o Ministério Público ou a Polícia Civil, dependendo da natureza do incidente.*
- ***Público interno:*** *Servidores e colaboradores do Município de Caracol/MS.*

Canais de Comunicação:

- ***Titulares de dados:***
  - ***Individual:*** *Contato direto por e-mail, telefone ou carta, dependendo da gravidade do incidente e do número de titulares afetados.*
  - ***Coletivo:*** *Divulgação de comunicado no site oficial do Município, redes sociais e outros meios de comunicação relevantes.*
- ***ANPD:***
  - *Comunicação formal por meio do sistema de notificação de incidentes da ANPD, dentro do prazo legal estabelecido.*
- ***Outros órgãos competentes:***
  - *Comunicação formal por meio de ofício ou outros meios adequados, conforme a natureza do incidente e as exigências legais.*
- ***Público interno:***
  - ***Comunicado interno:*** *Divulgação de comunicado por e-mail, intranet ou outros canais internos de comunicação.*

Conteúdo da Comunicação:

- ***Descrição clara e objetiva do incidente:*** *O que aconteceu, quando e como ocorreu, quais dados pessoais foram afetados.*
- ***Medidas adotadas:*** *Informar sobre as medidas já tomadas para conter o incidente e minimizar os danos, como a investigação das causas, a notificação dos titulares de dados e a adoção de medidas de segurança adicionais.*
- ***Recomendações aos titulares de dados:*** *Orientações sobre como os titulares de dados podem se proteger, como alterar senhas, monitorar extratos bancários e ficar atentos a mensagens fraudulentas.*
- ***Informações de contato:*** *Disponibilizar canais de contato para que os titulares de*

dados possam obter mais informações ou esclarecer dúvidas.

Responsabilidades:

- ***Encarregado pelo Tratamento de Dados (DPO):*** *Responsável por coordenar o processo de comunicação, garantir a conformidade com a LGPD e manter contato com a ANPD e outros órgãos competentes.*
- ***Equipe de resposta a incidentes:*** *Responsável por fornecer informações técnicas sobre o incidente e auxiliar na elaboração das comunicações.*
- ***Assessoria de Comunicação:*** *Responsável pela elaboração e divulgação dos comunicados ao público externo e interno.*
- **Investigação:** Realização de investigação para identificar as causas do incidente, avaliar os danos causados e adotar medidas para evitar que o incidente se repita.
- **Contenção:** Isolamento dos sistemas afetados e adoção de medidas para conter o incidente e minimizar os danos.
- **Recuperação:** Restauração dos dados pessoais a partir de backups e adoção de medidas para garantir a continuidade das atividades.

10.7. Procedimentos de Backup

- **Frequência:** Realização de backups periódicos, com frequência definida de acordo com a criticidade dos dados e o risco de perda ou alteração.
- **Tipos de backup:** Realização de backups completos e incrementais, para garantir a recuperação dos dados em diferentes momentos.
- **Armazenamento:** Armazenamento dos backups em locais seguros, como dispositivos externos criptografados ou servidores redundantes em locais geograficamente distintos.
- **Testes de restauração:** Realização periódica de testes de restauração para verificar a integridade dos backups e a capacidade de recuperar os dados em caso de necessidade.

10.8. Responsabilidades

- **Secretaria Municipal de Administração:** Responsável pela coordenação e

implementação do Plano de Contingência, bem como pela definição das políticas e procedimentos de segurança da informação.

- **Encarregado pelo Tratamento de Dados Pessoais (DPO):** Responsável por orientar e supervisionar a execução do Plano de Contingência, além de atuar como canal de comunicação entre o controlador, os titulares de dados e a ANPD.
- **Setor de Tecnologia da Informação (TI):** Responsável pela implementação e manutenção das medidas de segurança, pela realização dos backups e pela recuperação dos dados em caso de incidente.
- **Servidores e colaboradores:** Responsáveis por seguir as políticas e procedimentos de segurança da informação, reportar incidentes de segurança e colaborar com as ações de resposta a incidentes.

10.9. Revisão e Atualização

Este Plano de Contingência deverá ser revisado e atualizado periodicamente, sempre que houver mudanças significativas nos sistemas, nos processos ou nas tecnologias utilizadas pelo Município, ou em caso de alterações na legislação de proteção de dados.

11- VEDAÇÕES

11.1- Uso de equipamentos particulares

É vedado trazer/conectar equipamentos/periféricos particulares na rede de sistemas e comunicações sem autorização prévia do responsável pelo orgão público.

11.2- uso de equipamentos públicos para fins particulares

É terminantemente vedado o uso de equipamentos/recursos de TI para fins particulares como:

- Utilizar a impressora para impressões de material de cunho particular.
- Utilizar a internet (wifi) para downloads de material diverso ao desempenho de seu cargo.
- Armazenar músicas, vídeos, fotos e/ou qualquer material de interesse ou uso pessoal.

- Acessar e-mails particulares utilizando computadores/conexão de internet disponibilizada pelo Município.

- Acessar através de computadores/conexão de internet disponibilizada pelo Município, páginas com conteúdo impróprio como pornografia, pirataria etc.

- Acessar, alterar, ou remover pastas, arquivos ou qualquer recurso de sistema disponibilizado.

12- SANÇÕES.

Não poderá o operador e/ou prestador de serviços alegar o desconhecimento dessa PSI (Politica de Segurança da Informação) e, a infração as normas aqui descritas poderá causar sanções, de acordo com a LGPD (Lei 13.709 de 2018).

Além das sanções administrativas, a LGPD também prevê a possibilidade de reparação por danos materiais e morais causados pelas violações à lei imputando responsábilidades também a pessoas físicas que realizem o tratamento de dados pessoais em desacordo com a lei.

13- CAPACITAÇÃO EM LGPD PARA SERVIDORES MUNICIPAIS

Em conformidade com a Lei Geral de Proteção de Dados (LGPD), a Prefeitura Municipal de Caracol-MS se compromete a fornecer um programa abrangente de capacitação para todos os servidores que lidam com dados pessoais. Este programa tem como objetivo garantir que todos os funcionários compreendam a importância da proteção de dados e estejam aptos a aplicar as melhores práticas em seu trabalho diário.

Conteúdo do Programa de Capacitação:

- **Noções Básicas de LGPD:** Apresentação dos principais conceitos da LGPD, como dados pessoais, tratamento de dados, direitos dos titulares, consentimento e bases legais para o tratamento.
- **Boas Práticas em Proteção de Dados:** Orientações sobre como coletar, armazenar, processar, compartilhar e descartar dados pessoais de forma segura e em conformidade com a LGPD.
- **Segurança da Informação:** Medidas de segurança técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, perda, alteração, divulgação

ou destruição.

- **Gerenciamento de Incidentes de Segurança:** Procedimentos a serem adotados em caso de incidentes de segurança que envolvam dados pessoais, incluindo notificação aos titulares e à Autoridade Nacional de Proteção de Dados (ANPD).
- **Estudos de Caso:** Análise de casos práticos para ilustrar a aplicação da LGPD em diferentes situações do dia a dia da administração pública.

Frequência e Formato da Capacitação:

O programa de capacitação será oferecido periodicamente, com atualizações sempre que houver mudanças relevantes na legislação ou nas práticas de proteção de dados. A capacitação poderá ser realizada em diferentes formatos, como palestras, workshops, cursos online e materiais informativos.

Avaliação e Monitoramento:

A efetividade do programa de capacitação será avaliada por meio de questionários, testes e outras ferramentas de avaliação. Os resultados serão utilizados para aprimorar o programa e garantir que os servidores estejam sempre atualizados sobre as melhores práticas em proteção de dados.

Responsabilidades:

- **Controlador:** A Prefeitura Municipal de Caracol-MS, como controladora de dados, é responsável por implementar e manter o programa de capacitação.
- **Encarregado de Dados:** O Encarregado de Dados da Prefeitura será responsável por coordenar o programa de capacitação, monitorar sua efetividade e garantir que todos os servidores recebam a formação adequada.
- **Servidores:** Os servidores municipais têm a responsabilidade de participar ativamente do programa de capacitação e aplicar os conhecimentos adquiridos em suas atividades profissionais.

A Prefeitura Municipal de Caracol-MS reafirma seu compromisso com a proteção de dados pessoais e a privacidade dos cidadãos, e acredita que a capacitação contínua de seus servidores é fundamental para garantir o cumprimento da LGPD e a construção de uma cultura de proteção de dados na administração pública.

14- DISPOSIÇÕES FINAIS

A presente Política de Segurança da Informação (PSI) tem como objetivo

principal estabelecer um conjunto de normas, diretrizes e procedimentos que nortearão o uso responsável e seguro dos recursos de Tecnologia da Informação (TI) e demais informações sensíveis do Município de Caracol-MS. Buscamos, com isso, garantir a confidencialidade, integridade e disponibilidade das informações, protegendo-as contra acessos não autorizados, perdas, alterações indevidas ou qualquer tipo de uso que possa prejudicar a administração pública e os cidadãos.

A efetiva implementação desta PSI depende do comprometimento e colaboração de todos os servidores, colaboradores, prestadores de serviço e demais pessoas que tenham acesso às informações do Município. É fundamental que cada um compreenda a importância da segurança da informação e siga rigorosamente as normas e procedimentos aqui estabelecidos.

A PSI não se esgota neste documento. Ela é um processo contínuo de aprimoramento e adaptação às novas tecnologias e ameaças. Sendo assim, esta política poderá ser revisada e atualizada periodicamente, sempre que necessário, para garantir sua adequação às necessidades do Município e às mudanças no cenário da segurança da informação.

Quaisquer dúvidas ou sugestões relacionadas à PSI devem ser encaminhadas ao Encarregado de Dados do Município, que estará à disposição para prestar esclarecimentos e orientações.

A Prefeitura Municipal de Caracol-MS reafirma seu compromisso com a segurança da informação e a proteção de dados, e conta com a colaboração de todos para garantir a efetividade desta política.

Caracol/MS, 14 de agosto de 2024.

Elaborado por:
Mariane Benites Godoy
Assessora adjunta da Procuradoria Municipal

Adriano Maciel Gonçalves
Secretaria Municipal de Saúde

Aprovado por:

Gesiene Martins Moreno – Procuradora Municipal

Luiz Fernando Bernardino Gouvêa (Secretaria Municipal de Direitos Humanos, Assistência Social, Trabalho e Habitação)

Carlos Júnior Godoy (Secretaria Municipal de Agricultura, Pecuária e Meio Ambiente)

Antonio Carlos dos Santos Gouvêa (Secretaria Municipal de Educação, Cultura, Esporte e Lazer)

Ibrain Araujo Garcia (Secretaria Municipal de Obras e Serviços Públicos)

Carlos Antonio dos Santos Gouvêa (Secretaria Municipal de Planejamento)

Modesto Vaz Filho (Secretaria Municipal de Administração)

José Roberto Pissurno (Secretaria Municipal de Finanças)

PREFEITURA MUNICIPAL DE CARACOL

DEPARTAMENTO DE RECURSOS HUMANOS

DECRETO MUNICIPAL N° 120, DE 15 DE AGOSTO DE 2024.

" INSTITUI A PLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO PODER EXECUTIVO MUNICIPAL DE CARACOL/MS E DÁ OUTRAS PROVIDÊNCIAS ".

O **PREFEITO MUNICIPAL DE CARACOL, ESTADO DE MATO GROSSO DO SUL**, no uso de suas atribuições que lhe confere a Lei Orgânica Municipal, e

CONSIDERANDO , as disposições contidas na Lei Federal 13.709, de 14 de agosto de 2018;

CONSIDERANDO o disposto no Decreto 106/2024 que aprova o Plano de Ação/ROADMAP;

DECRETA:

Art. 1º. Fica instituída a Política de Segurança da Informação – PSI, no âmbito do Poder Executivo Municipal de Caracol/MS, conforme Diretrizes e Normas constante no anexo único deste Decreto.

Art. 2º. Este Decreto entra em vigor na data de sua publicação.

Caracol/MS, 15 de agosto de 2024.

Carlos Humberto Pagliosa

Prefeito Municipal de Caracol/MS

Anexo único ao Decreto Municipal nº 120/2024

POLITICA DE SEGURANÇA DA INFORMAÇÃO – PSI

Caracol/MS

SUMÁRIO

Glossário

Backup: Cópia de segurança de dados para evitar perdas.

Cloud Backup: Backup realizado em nuvem, através de um provedor externo.

Controlador: Pessoa ou organização que determina as finalidades e os meios de tratamento de dados pessoais.

Encarregado: Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

LGPD: Lei Geral de Proteção de Dados, que regula o tratamento de dados pessoais no Brasil.

Operador: Pessoa ou organização que realiza o tratamento de dados pessoais em nome do controlador.

PSI: Política de Segurança da Informação, documento que estabelece diretrizes e normas para proteger as informações de uma organização.

TI: Tecnologia da Informação, conjunto de recursos tecnológicos utilizados para armazenar, processar e transmitir informações.

INTRODUÇÃO

A Política de Segurança da Informação abrange tanto dados **lógicos** quanto **físicos** . Ela é um conjunto de diretrizes e práticas que visam proteger todas as formas de informação dentro de uma organização. Aqui estão os principais aspectos que são estão cobertos por esta Política de Segurança da Informação:

Dados Lógicos

Dados Digitais: Informações armazenadas em sistemas computacionais, incluindo bancos de dados, arquivos eletrônicos, e-mails, e qualquer tipo de informação que é manipulada digitalmente.

Redes e Comunicação: Segurança das redes internas e externas, comunicação via internet, VPNs, e todos os tipos de transmissão de dados digitais.

Acesso e Autenticação: Controle de acesso a sistemas e dados através de senhas, autenticação multifator,

permissões de usuário e políticas de uso.

Software e Aplicações: Segurança do software utilizado pela organização, incluindo sistemas operacionais, aplicativos de negócios, e softwares de segurança como antivírus e firewalls.

Dados Físicos

Infraestrutura Física: Proteção das instalações físicas onde os dados são armazenados e processados, como data centers, salas de servidores e escritórios.

Equipamentos e Dispositivos: Segurança de hardware como servidores, computadores, laptops, dispositivos móveis e outros equipamentos eletrônicos.

Documentos e Mídias: Proteção de documentos físicos, mídia removível (como CDs, DVDs, pen drives) e backups físicos.

Controle de Acesso Físico: Medidas de segurança para controlar o acesso físico às instalações, como crachás, biometria, vigilância por câmeras e guardas de segurança.

Gestão de Descarte: Procedimentos seguros para o descarte de equipamentos, mídias e documentos físicos, garantindo que dados sensíveis não sejam recuperados.

Objetivos Gerais da Política de Segurança da Informação:

Confidencialidade: Garantir que a informação seja acessível apenas por pessoas autorizadas.

Integridade: Assegurar que a informação seja precisa e confiável, e não tenha sido alterada de forma não autorizada.

Disponibilidade: Garantir que a informação esteja disponível quando necessária para os processos de negócios.

A atual Política de Segurança de Informação adotada pelo município de Caracol-MS contempla um conjunto de normas e procedimentos, delineando de forma clara os métodos de uso dos recursos de tecnologias e o cuidados com a segurança da informação.

O conceito adotado de Segurança da Informação é a imperativa preservação e valorização da informação, focando na necessidade de permitir que apenas pessoas autorizadas tenham acesso a essas informações.

A normatização possui objetivo de conduzir de forma eficiente as ações diárias de servidores municipais que utilizam os recursos de tecnologia de Informação (TI), ou outros meios, disponibilizados pelo município como ferramenta de trabalho, para melhor servir aos interesses públicos.

Secundariamente ao efetuar o regramento, busca-se uniformizar padrões de utilização da rede e recursos de TI, permitindo o perfeito discernimento da separação da "coisa pública", muitas vezes indevidamente utilizadas.

Desta forma, torna-se vital a ampla comunicação e adesão dos servidores, conselheiros, bem como, dos prestadores de serviço com acesso a informações do munícipio.

2- LEI GERAL DA PROTEÇÃO DE DADOS – LGPD Lei nº 13.709/2018.

Em resumo: Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por **pessoa jurídica de direito público** ou privado, com o objetivo de proteger os direitos fundamentais de **liberdade e de privacidade** e o livre desenvolvimento da personalidade da pessoa natural.

2.1 Controlador

Art. 5º, VI: "O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais."

2.2 Operador

Art. 5º, VII: "O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador."

2.3 Encarregado

Art. 5º, VIII: "O encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)."

2.4 Resumo das Atribuições e Responsabilidades

a. Controlador

O controlador é responsável por:

Determinar as finalidades e os meios de tratamento dos dados pessoais.

Garantir que o tratamento de dados esteja de acordo com a legislação.

Assegurar a transparência no tratamento de dados pessoais, informando aos titulares dos dados sobre como suas informações são usadas.

Adotar medidas de segurança apropriadas para proteger os dados pessoais.

Notificar a ANPD e os titulares sobre incidentes de segurança que possam acarretar risco ou dano relevante aos titulares dos dados.

b. Operador

O operador é responsável por:

Realizar o tratamento de dados pessoais conforme as instruções do controlador.

Garantir a segurança dos dados pessoais durante o tratamento.

Cooperar com a ANPD e com o controlador na execução de suas funções.

Não usar os dados pessoais para finalidades diferentes daquelas definidas pelo controlador.

c. Encarregado

O encarregado é responsável por:

Ser o ponto de contato entre o controlador, os titulares dos dados e a ANPD.

Orientar os funcionários e os contratados da entidade a respeito das práticas de proteção de dados pessoais.

Receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.

Receber comunicações da ANPD e adotar providências.

Realizar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Na prática, o "tratamento de dados" são operações com dados pessoais, incluídos desde o recolhimento, registro e organização de dados até a consulta e divulgação destas informações.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

- mediante o fornecimento de consentimento pelo titular;

- para o cumprimento de obrigação legal ou regulatória pelo controlador;

- pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei.

CONTROLE DE ACESSO

Acesso físico

Para a área de recepção dos orgãos públicos municipais, haverá livre acesso ao público, porém, para acesso as demais dependências dos orgãos públicos municipais, deve haver a perfeita identificação do visitante, o motivo de sua visita, a área que será visitada e a aprovação do responsável pela área. A saída do visitante deverá se "liberada" pela área visitada;

Acesso a rede lógica

O acesso a rede lógica do MUNICÍPIO será efetuado apenas por servidores dos orgãos públicos deste municipios , servidores da área de Tecnologia de Informação da Prefeitura de Itapoá designados para tal função, ou, por serviço técnico devidamente contratado para tal finalidade. Quando da realização de serviço, o mesmo deverá ser integralmente acompanhado e, a saída do prestador de serviço deverá se "liberada" pela área que acompanhou a realização do serviço.

DOS RECURSOS DE TECNOLOGIA DE INFORMAÇÃO (TI) DISPONIBILIZADOS.

Os recursos de Tecnologia da Informação (TI) disponibilizados aos operadores englobam todos os equipamentos, periféricos, suprimentos e qualquer outro serviço e/ou dispositivo correlato disponibilizados aos servidores e ou prestadores de serviço para a realização de atividades diversas, dentre os quais estão incluídos impressoras e suprimentos, dispositivos de armazenamento, computadores, tablets, celulares, smartphones, contas de acesso (internet, correio eletrônico e demais sistemas), escâneres, rede local, câmeras digitais, etc.

PADRÃO DE CONFIGURAÇÃO DE TI DISPONIBILIZADO.

Todos os dispositivos de Tecnologia da Informação (TI) fornecidos aos operadores (computadores, notebooks, tablets, etc.) deverão seguir o padrão de configuração definido pelo setor de TI. Este padrão visa garantir o melhor desempenho dos dispositivos e a proteção dos dados pessoais.

Qualquer alteração na configuração, troca interna ou externa de equipamentos ou periféricos deverá ser **autorizada previamente** pelo setor de TI, por meio de solicitação formal e justificativa da necessidade da alteração. Alterações não autorizadas podem comprometer a segurança dos dados pessoais e a integridade dos sistemas.

Em caso de identificação de alterações não autorizadas, o usuário responsável será notificado e as configurações originais serão restauradas. Além disso, serão tomadas as medidas cabíveis para investigar o ocorrido e garantir a segurança dos dados pessoais, incluindo a apuração de responsabilidades e a aplicação de sanções administrativas, se necessário.

DA INSTALAÇÃO DE SISTEMAS/SOFTWARES.

Para garantir a proteção de dados pessoais e a segurança da informação, a instalação de qualquer software em equipamentos utilizados para o tratamento de dados pessoais (computadores, notebooks, tablets, etc.) deverá ser realizada **somente após análise e aprovação prévia** da equipe responsável pela segurança da informação, em conformidade com a Política de Segurança da Informação e com a LGPD.

A instalação de softwares não autorizados ou sem a devida análise pode comprometer a segurança dos dados pessoais, expondo-os a riscos como acesso não autorizado, perda, alteração, destruição ou vazamento. Além disso, a utilização de softwares sem licença ou de origem duvidosa pode configurar crime de violação de direitos autorais.

Em caso de identificação de softwares não autorizados instalados em equipamentos utilizados para o tratamento de dados pessoais, **o usuário responsável será notificado e o software será removido imediatamente**. Adicionalmente, serão tomadas as medidas cabíveis para investigar o ocorrido e garantir a segurança dos dados pessoais, incluindo a apuração de responsabilidades e a aplicação de sanções administrativas, se necessário.

É fundamental que todos os usuários que lidam com dados pessoais estejam cientes da importância de seguir as políticas e procedimentos de segurança da informação, contribuindo para a proteção dos dados pessoais e para a conformidade com a LGPD. A equipe responsável pela segurança da informação está à disposição para esclarecer dúvidas e fornecer orientações sobre a instalação de softwares.

ACESSOS DO USUÁRIO.

Cada operador receberá "acessos aos recursos de TI", conforme solicitado pela sua chefia, se estiverem em acordo com a PSI.

Por "acessos aos recursos de TI", entende-se o fornecimento de determinado tipo de permissão através de login/senha com configurações de acesso pré-determinadas.

As senhas de acesso são de uso pessoal e intransferível.

Ao ausentar-se de ponto de acesso (microcomputador, notebook), o operador deverá efetuar o logout ou bloqueio de tela.

USO CORRETO DO E-MAIL.

Cada usuário é diretamente responsável pelo uso de seu e-mail e suas consequências.

As senhas de acesso são de uso pessoal e intransferível.

O e-mail corporativo é uma ferramenta de trabalho disponibilizada pelo MUNICÍPIO ao servidor, portanto, pode ser monitorado/auditado a qualquer momento pelo setor de TI, com ou sem o consentimento do usuário;

9 - USO CORRETO DA INTERNET.

O acesso à internet no ambiente de trabalho é fornecido para fins profissionais e, portanto, está sujeito a monitoramento, em conformidade com a legislação trabalhista e a LGPD.

Visando garantir a segurança da informação e a proteção de dados pessoais, o acesso a determinados sites e conteúdo online pode ser restringido ou bloqueado, especialmente aqueles que representam riscos à segurança da rede, como:

Sites com conteúdo malicioso: Páginas conhecidas por conter malware, vírus ou outros softwares nocivos.

Sites de phishing: Páginas que tentam enganar os usuários para obter informações confidenciais, como senhas e dados bancários.

Sites com conteúdo inadequado: Páginas com conteúdo impróprio, ofensivo ou discriminatório, que podem gerar um ambiente de trabalho hostil.

Sites que consomem banda larga excessiva: Páginas com vídeos, jogos ou outros conteúdos que podem prejudicar o desempenho da rede e afetar a produtividade.

O setor de TI é responsável por buscar sempre o equilíbrio entre a necessidade de acesso à informação e a proteção dos dados pessoais e da segurança da rede.

É importante que todos os usuários estejam cientes das políticas de uso da internet e das restrições de acesso, utilizando a rede de forma responsável e ética. O descumprimento das políticas pode resultar em sanções administrativas e outras medidas disciplinares cabíveis.

10- PLANO DE CONTINGÊNCIA.

Plano de Contingência para Proteção de Dados Pessoais do Município de Caracol/MS

10.1 Objetivo

O presente Plano de Contingência tem como objetivo estabelecer diretrizes e procedimentos para a prevenção, detecção e resposta a incidentes de segurança que possam comprometer a disponibilidade, integridade e confidencialidade dos dados pessoais tratados pelo Município de Caracol/MS, em conformidade com a Lei Geral de Proteção de Dados (LGPD).

10. 2. Escopo

Este plano abrange todos os órgãos e entidades da administração pública municipal, direta e indireta, que realizam o tratamento de dados pessoais.

10.3. Definições

Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos dados pessoais, como acesso não autorizado, destruição, perda, alteração, vazamento ou qualquer outra forma de tratamento inadequado.

Dados pessoais: qualquer informação relacionada a pessoa natural identificada ou identificável.

Backup: cópia de segurança dos dados pessoais, realizada periodicamente para garantir sua recuperação em caso de incidente de segurança.

Restauração: processo de recuperação dos dados pessoais a partir de um backup.

10.4. Prevenção de Incidentes de Segurança

Medidas de segurança: Implementação de medidas de segurança adequadas ao risco de cada tratamento de dados, como criptografia, controle de acesso, firewalls, antivírus e sistemas de detecção de intrusão.

Treinamento e conscientização: Realização de treinamentos periódicos para os servidores e colaboradores sobre a importância da proteção de dados pessoais e as medidas de segurança a serem adotadas.

Atualização de softwares: Manutenção dos softwares e sistemas atualizados, com a aplicação de patches de segurança sempre que disponíveis.

Política de segurança da informação: Elaboração e divulgação de uma política de segurança da informação que estabeleça diretrizes e responsabilidades para a proteção de dados pessoais.

10.5. Detecção de Incidentes de Segurança

Monitoramento: Monitoramento contínuo dos sistemas e logs para identificar atividades suspeitas ou tentativas de acesso não autorizado.

Canais de comunicação: Criação de canais de comunicação para que os servidores e colaboradores possam reportar incidentes de segurança ou suspeitas de violação de dados pessoais.

Análise de riscos: Realização periódica de análises de riscos para identificar vulnerabilidades e ameaças aos dados pessoais.

10.6. Resposta a Incidentes de Segurança

Equipe de resposta a incidentes: Criação de uma equipe de resposta a incidentes, composta por profissionais de diferentes áreas, responsável por coordenar as ações de resposta a incidentes de segurança.

Plano de comunicação:

Público-alvo:

Titulares de dados: Indivíduos cujos dados pessoais foram afetados pelo incidente.

Autoridade Nacional de Proteção de Dados (ANPD): Órgão responsável pela fiscalização e aplicação da LGPD.

Outros órgãos competentes: Outros órgãos que possam ter interesse no incidente, como o Ministério Público ou a Polícia Civil, dependendo da natureza do incidente.

Público interno: Servidores e colaboradores do Município de Caracol/MS.

Canais de Comunicação:

Titulares de dados:

Individual: Contato direto por e-mail, telefone ou carta, dependendo da gravidade do incidente e do número de titulares afetados.

Coletivo: Divulgação de comunicado no site oficial do Município, redes sociais e outros meios de comunicação relevantes.

ANPD:

Comunicação formal por meio do sistema de notificação de incidentes da ANPD, dentro do prazo legal estabelecido.

Outros órgãos competentes:

Comunicação formal por meio de ofício ou outros meios adequados, conforme a natureza do incidente e as exigências legais.

Público interno:

Comunicado interno: Divulgação de comunicado por e-mail, intranet ou outros canais internos de comunicação.

Conteúdo da Comunicação:

Descrição clara e objetiva do incidente: O que aconteceu, quando e como ocorreu, quais dados pessoais foram afetados.

Medidas adotadas: Informar sobre as medidas já tomadas para conter o incidente e minimizar os danos, como a investigação das causas, a notificação dos titulares de dados e a adoção de medidas de segurança adicionais.

Recomendações aos titulares de dados: Orientações sobre como os titulares de dados podem se proteger, como alterar senhas, monitorar extratos bancários e ficar atentos a mensagens fraudulentas.

Informações de contato: Disponibilizar canais de contato para que os titulares de dados possam obter mais informações ou esclarecer dúvidas.

Responsabilidades:

Encarregado pelo Tratamento de Dados (DPO): Responsável por coordenar o processo de comunicação, garantir a conformidade com a LGPD e manter contato com a ANPD e outros órgãos competentes.

Equipe de resposta a incidentes: Responsável por fornecer informações técnicas sobre o incidente e auxiliar na elaboração das comunicações.

Assessoria de Comunicação: Responsável pela elaboração e divulgação dos comunicados ao público externo e interno.

Investigação: Realização de investigação para identificar as causas do incidente, avaliar os danos causados e adotar medidas para evitar que o incidente se repita.

Contenção: Isolamento dos sistemas afetados e adoção de medidas para conter o incidente e minimizar os danos.

Recuperação: Restauração dos dados pessoais a partir de backups e adoção de medidas para garantir a continuidade das atividades.

10.7. Procedimentos de Backup

Frequência: Realização de backups periódicos, com frequência definida de acordo com a criticidade dos dados e o risco de perda ou alteração.

Tipos de backup: Realização de backups completos e incrementais, para garantir a recuperação dos dados em diferentes momentos.

Armazenamento: Armazenamento dos backups em locais seguros, como dispositivos externos criptografados ou servidores redundantes em locais geograficamente distintos.

Testes de restauração: Realização periódica de testes de restauração para verificar a integridade dos backups e a capacidade de recuperar os dados em caso de necessidade.

10.8. Responsabilidades

Secretaria Municipal de Administração: Responsável pela coordenação e implementação do Plano de Contingência, bem como pela definição das políticas e procedimentos de segurança da informação.

Encarregado pelo Tratamento de Dados Pessoais (DPO): Responsável por orientar e supervisionar a execução do Plano de Contingência, além de atuar como canal de comunicação entre o controlador, os titulares de dados e a ANPD.

Setor de Tecnologia da Informação (TI): Responsável pela implementação e manutenção das medidas de segurança, pela realização dos backups e pela recuperação dos dados em caso de incidente.

Servidores e colaboradores: Responsáveis por seguir as políticas e procedimentos de segurança da informação, reportar incidentes de segurança e colaborar com as ações de resposta a incidentes.

10.9. Revisão e Atualização

Este Plano de Contingência deverá ser revisado e atualizado periodicamente, sempre que houver mudanças significativas nos sistemas, nos processos ou nas tecnologias utilizadas pelo Município, ou em caso de alterações na legislação de proteção de dados.

11- VEDAÇÕES

11.1- Uso de equipamentos particulares

É vedado trazer/conectar equipamentos/periféricos particulares na rede de sistemas e comunicações sem autorização prévia do responsável pelo orgão público.

11.2- uso de equipamentos públicos para fins particulares

É terminantemente vedado o uso de equipamentos/recursos de TI para fins particulares como:

Utilizar a impressora para impressões de material de cunho particular.

- Utilizar a internet (wifi) para downloads de material diverso ao desempenho de seu cargo.

Armazenar músicas, vídeos, fotos e/ou qualquer material de interesse ou uso pessoal.

- Acessar e-mails particulares utilizando computadores/conexão de internet disponibilizada pelo Município.

Acessar através de computadores/conexão de internet disponibilizada pelo Município, páginas com conteúdo impróprio como pornografia, pirataria etc.

Acessar, alterar, ou remover pastas, arquivos ou qualquer recurso de sistema disponibilizado.

12- SANÇÕES.

Não poderá o operador e/ou prestador de serviços alegar o desconhecimento dessa PSI (Politica de Segurança da Informação) e, a infração as normas aqui descritas poderá causar sanções, de acordo com a LGPD (Lei 13.709 de 2018).

Além das sanções administrativas, a LGPD também prevê a possibilidade de reparação por danos materiais e morais causados pelas violações à lei imputando responsábilidades também a pessoas físicas que realizem o tratamento de dados pessoais em desacordo com a lei.

13- CAPACITAÇÃO EM LGPD PARA SERVIDORES MUNICIPAIS

Em conformidade com a Lei Geral de Proteção de Dados (LGPD), a Prefeitura Municipal de Caracol-MS se compromete a fornecer um programa abrangente de capacitação para todos os servidores que lidam com dados pessoais. Este programa tem como objetivo garantir que todos os funcionários compreendam a importância da proteção de dados e estejam aptos a aplicar as melhores práticas em seu trabalho diário.

Conteúdo do Programa de Capacitação:

Noções Básicas de LGPD: Apresentação dos principais conceitos da LGPD, como dados pessoais, tratamento de dados, direitos dos titulares, consentimento e bases legais para o tratamento.

Boas Práticas em Proteção de Dados: Orientações sobre como coletar, armazenar, processar, compartilhar e descartar dados pessoais de forma segura e em conformidade com a LGPD.

Segurança da Informação: Medidas de segurança técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, perda, alteração, divulgação ou destruição.

Gerenciamento de Incidentes de Segurança: Procedimentos a serem adotados em caso de incidentes de segurança que envolvam dados pessoais, incluindo notificação aos titulares e à Autoridade Nacional de Proteção de Dados (ANPD).

Estudos de Caso: Análise de casos práticos para ilustrar a aplicação da LGPD em diferentes situações do dia a dia da administração pública.

Frequência e Formato da Capacitação:

O programa de capacitação será oferecido periodicamente, com atualizações sempre que houver mudanças relevantes na legislação ou nas práticas de proteção de dados. A capacitação poderá ser realizada em diferentes formatos, como palestras, workshops, cursos online e materiais informativos.

Avaliação e Monitoramento:

A efetividade do programa de capacitação será avaliada por meio de questionários, testes e outras ferramentas de avaliação. Os resultados serão utilizados para aprimorar o programa e garantir que os servidores estejam sempre atualizados sobre as melhores práticas em proteção de dados.

Responsabilidades:

Controlador: A Prefeitura Municipal de Caracol-MS, como controladora de dados, é responsável por implementar e manter o programa de capacitação.

Encarregado de Dados: O Encarregado de Dados da Prefeitura será responsável por coordenar o programa de capacitação, monitorar sua efetividade e garantir que todos os servidores recebam a formação adequada.

Servidores: Os servidores municipais têm a responsabilidade de participar ativamente do programa de capacitação e aplicar os conhecimentos adquiridos em suas atividades profissionais.

A Prefeitura Municipal de Caracol-MS reafirma seu compromisso com a proteção de dados pessoais e a privacidade dos cidadãos, e acredita que a capacitação contínua de seus servidores é fundamental para garantir o cumprimento da LGPD e a construção de uma cultura de proteção de dados na administração pública.

14- DISPOSIÇÕES FINAIS

A presente Política de Segurança da Informação (PSI) tem como objetivo principal estabelecer um conjunto de normas, diretrizes e procedimentos que nortearão o uso responsável e seguro dos recursos de Tecnologia da Informação (TI) e demais informações sensíveis do Município de Caracol-MS. Buscamos, com isso, garantir a confidencialidade, integridade e disponibilidade das informações, protegendo-as contra acessos não autorizados, perdas, alterações indevidas ou qualquer tipo de uso que possa prejudicar a administração pública e os cidadãos.

A efetiva implementação desta PSI depende do comprometimento e colaboração de todos os servidores, colaboradores, prestadores de serviço e demais pessoas que tenham acesso às informações do Município. É fundamental que cada um compreenda a importância da segurança da informação e siga rigorosamente as normas e procedimentos aqui estabelecidos.

A PSI não se esgota neste documento. Ela é um processo contínuo de aprimoramento e adaptação às novas tecnologias e ameaças. Sendo assim, esta política poderá ser revisada e atualizada periodicamente, sempre que necessário, para garantir sua adequação às necessidades do Município e às mudanças no cenário da segurança da informação.

Quaisquer dúvidas ou sugestões relacionadas à PSI devem ser encaminhadas ao Encarregado de Dados do Município, que estará à disposição para prestar esclarecimentos e orientações.

A Prefeitura Municipal de Caracol-MS reafirma seu compromisso com a segurança da informação e a proteção de dados, e conta com a colaboração de todos para garantir a efetividade desta política.

Caracol/MS, 14 de agosto de 2024.

Elaborado por:

Mariane Benites Godoy

Assessora adjunta da Procuradoria Municipal

Adriano Maciel Gonçalves

Secretaria Municipal de Saúde

Aprovado por:

Gesiene Martins Moreno – Procuradora Municipal

Luiz Fernando Bernardino Gouvêa (Secretaria Municipal de Direitos Humanos, Assistência Social, Trabalho e Habitação)

Carlos Júnior Godoy (Secretaria Municipal de Agricultura, Pecuária e Meio Ambiente)

Antonio Carlos dos Santos Gouvêa (Secretaria Municipal de Educação, Cultura, Esporte e Lazer)

Ibrain Araujo Garcia (Secretaria Municipal de Obras e Serviços Públicos)

Carlos Antonio dos Santos Gouvêa (Secretaria Municipal de Planejamento)

Modesto Vaz Filho (Secretaria Municipal de Administração)

José Roberto Pissurno (Secretaria Municipal de Finanç

Matéria enviada por MODESTO VAZ FILHO

DEPARTAMENTO DE RECURSOS HUMANOS

Republica-se por Incorreção

EXTRATO DO PRIMEIRO TERMO ADITIVO AO CONTRATO DE TRABALHO POR PRAZO DETERMINADO Nº 093/2024.

CONTRATANTE: Município de Caracol – MS.

CONTRATADO (A): Ingridi Leite Figueredo.

FUNDAMENTO: Cláusula Quarta do contrato de trabalho por prazo determinado n. 093/2024 bem como no inciso IX, do artigo 37 da Constituição Federal, e artigo 2º, §1º, inciso IV e V da Lei Municipal Nº 803/2019.

DO OBJETO: **Constitui objeto do presente termo aditivo alterar a carga horaria acrescentando 2 horas aulas e alteração de valor do contrato de trabalho por prazo determinado n. 093/2024.**

DA ALTERAÇÃO DE VALOR: Em razão da alteração salarial prevista na Lei Municipal n. 937/2024 e aumento de carga horaria de 2 horas aulas, o CONTRATADO passará a receber mensalmente, como retribuição pelo seu trabalho, valor equivalente ao vencimento fixado para o cargo efetivo de Professora de Artes, Classe A Nível PG2, nesta data equivalente a **R$ 4.214,11 (Quatro mil duzentos e quatorze reais e onze centavos).**

DOTAÇÃO: 05 .003.12.361.0600.2044 - 3.1.90.04.00.00.

DATA DE ASSINATURA: 15/08/2024.

VIGÊNCIA: 12/08/2024 a 20/12/2024.

ASSINAM: Thaiz Leite de Andrade (Secretária Municipal de Educação) **Ingridi Leite Figueredo..** (Contratado).

Matéria enviada por MODESTO VAZ FILHO

DEPARTAMENTO DE RECURSOS HUMANOS

EXTRATO DO PRIMEIRO TERMO ADITIVO AO CONTRATO DE TRABALHO POR PRAZO DETERMINADO Nº 072/2024.

CONTRATANTE: Município de Caracol – MS.

CONTRATADO (A): Miguel Joselio Leite Costa.

FUNDAMENTO: Cláusula Quarta do contrato de trabalho por prazo determinado n. 072/2024 bem como no inciso IX, do artigo 37 da Constituição Federal, e artigo 2º, §1º, inciso IV e V da Lei Municipal Nº 803/2019.

DO OBJETO: **Constitui objeto do presente termo aditivo alterar a carga horaria acrescentando 2 horas aulas e alteração de valor do contrato de trabalho por prazo determinado n. 072/2024.**

DA ALTERAÇÃO DE VALOR: Em razão da alteração salarial prevista na Lei Municipal n. 937/2024 e aumento de carga