DIÁRIO OFICIAL
DAS CÂMARAS MUNICIPAIS DO ESTADO DO RIO GRANDE DO NORTE
DIARIOOFICIAL.FECAMRN.COM.BR
RIO GRANDE DO NORTE, QUINTA-FEIRA, 07 DE NOVEMBRO DE 2024 - ANO: VI - EDIÇÂO Nº: 2025

Câmara Municipal de Currais Novos
(CNPJ: 08.470.502/0001-98)

Ato da Mesa Diretora nº 007, de 05 de novembro de 2024

Institui a Política de Segurança da Informação no âmbito da Câmara Municipal de Currais Novos

A MESA DIRETORA DA CÂMARA MUNICIPAL DE CURRAIS NOVOS, no uso das atribuições conferidas pelos incisos IV e V do art. 9º do Regimento Interno da Câmara Municipal de Currais Novos, RESOLVE:

Art. 1º - Instituir a Política de Segurança da Informação (PSI) no âmbito da Câmara Municipal de Currais Novos.

Parágrafo único. A PSI estabelece diretrizes, responsabilidades e ações para a gestão da segurança da informação e tem por objetivo assegurar:

I - a segurança cibernética;

II - a segurança física e a proteção de dados organizacionais; e

III - a disponibilidade, a integridade, a confidencialidade, a autenticidade da informação e a proteção de dados pessoais.

Art. 2º - Para os efeitos deste Ato da Mesa aplicam-se as seguintes definições:

I - auditoria: processo sistemático, independente e documentado para obter evidências de auditoria e avaliá-las objetivamente para determinar em que medida os critérios de auditoria são atendidos;

II - confidencialidade: propriedade de que as informações não são disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados;

III - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

IV - disponibilidade: propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada;

V - integridade: propriedade de precisão e completude;

VI - recurso de tecnologia de informação: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, instalações físicas que os abriguem;

VII - segurança da Informação: conjunto de ações, controles e medidas para assegurar a preservação da confidencialidade, disponibilidade e integridade da informação; e

VIII - usuários: vereadores e servidores públicos ocupantes de cargo efetivo ou em comissão, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados e outras pessoas que se encontrem a serviço da Câmara Municipal

de Currais Novos, utilizando em caráter temporário os recursos tecnológicos daquele órgão.

Art. 3º - As disposições deste Ato da Mesa aplicam-se a todos os usuários de recursos de tecnologia da informação da Câmara Municipal de Currais Novos.

Parágrafo único. Os contratos, os convênios e outros instrumentos de cooperação e/ou colaboração de interesse público firmados pela Câmara Municipal de Currais Novos que envolvam a utilização de recursos de tecnologia da informação devem observar as disposições deste Ato da Mesa.

Art. 4º - O uso adequado dos recursos de tecnologia da informação visa a contribuir para a efetividade e a continuidade das funções legislativas e administrativas exercidas pela Câmara Municipal de Currais Novos.

Parágrafo único. Os recursos de tecnologia da informação pertencentes à Câmara Municipal de Currais Novos, disponíveis para o usuário, serão utilizados em atividades relacionadas às suas funções institucionais.

Art. 5º - A utilização dos recursos de tecnologia da informação será monitorada, com a finalidade de detectar a ocorrência de eventos de segurança cibernética suspeitos e divergências entre as normas que integram a Política de Segurança da Informação e os registros de eventos monitorados, fornecendo evidências nos casos de incidentes de segurança.

§1º Serão realizadas auditorias ordinárias periódicas, cujos relatórios serão encaminhados ao Comitê Gestor de Segurança da Informação.

§ 2º As auditorias extraordinárias serão realizadas com o intuito de apurar eventos que deponham contra a segurança e as boas práticas no uso dos recursos de tecnologia da informação.

Art. 6º As informações, sistemas e métodos tratados pelos usuários, no exercício de suas funções, independentemente da forma de tratamento, são propriedade da Câmara Municipal de Currais Novos e serão utilizadas exclusivamente para fins relacionados às atividades a ele afetas.

Parágrafo único. Quando as informações, sistemas e métodos forem tratados por terceiros para uso exclusivo da Câmara Municipal de Currais Novos, ficam os criadores obrigados ao sigilo permanente de tais produtos, sendo vedada a sua reutilização em projetos para outrem.

Art. 7º Incumbe à chefia imediata e superior do usuário verificar a observância da Política de Segurança no âmbito de sua unidade, comunicando, de imediato, ao Comitê Gestor de Segurança da Informação, as irregularidades constatadas, para as providências cabíveis.

Câmara Municipal de Currais Novos
(CNPJ: 08.470.502/0001-98)

Art. 8º - O descumprimento das normas referentes à Política de Segurança da Informação da Câmara Municipal de Currais Novos poderá acarretar, isolada ou cumulativamente, nos termos da legislação vigente, sanções administrativas, civis e penais.

Art. 9º. - As normas complementares às diretrizes gerais definidas na Política de Segurança da Informação serão editadas sob a forma de Anexos, que integrarão o presente Ato da Mesa.

Art. 10. - O presente Ato entra em vigor a partir da data de sua publicação

Plenário da Câmara Municipal de Currais Novos/RN, em 05 de novembro de 2024.

YCLEYBER TRAJANO DA SILVA
Presidente

JORIAN PEREIRA DO SANTOS
Vice-Presidente

RAYSSA ALINE BATISTA DE ARAÚJO
1ª Secretária

JOÃO GUSTAVO COELHO GOMES GUIMARÃES
2º Secretário

Rua Vivaldo Pereira de Araújo, n.º 161, Centro – Telefone: (84) 3412–1567
59.380-000 Currais Novos/RN – E-mail: camaracurraisnovos@hotmail.com

Câmara Municipal de Currais Novos
(CNPJ: 08.470.502/0001-98)

ANEXO I

NSI001 - Controle de Acesso à Internet

1. **Objetivos**

1.1. Estabelecer diretrizes e padrões para o acesso à internet no âmbito da Câmara Municipal de Currais Novos.

2. **Motivações**

2.1. Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

2.2. Proteção do ambiente tecnológico da Câmara Municipal de Currais Novos.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos para prover o serviço de acesso à internet.

3. **Referências normativas**

3.1. Norma Técnica ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação;

3.2. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles de segurança da informação.

4. **Conceitos e definições**

4.1. Arquivo de registro de mensagens (*logs*): registro de eventos, utilizados para restaurar um sistema, diagnosticar problemas ou realizar auditorias.

4.2. Código malicioso: também conhecido por *malware*, termo comumente utilizado para genericamente se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, *worm*, *bot*, *spyware*, *backdoor*, cavalo de troia, *ransomware* e *rootkit*.

4.3. *Proxy web*: também conhecido por filtro de conteúdo, é o servidor responsável por intermediar o acesso à internet, aplicando regras de controle de acesso e mecanismos de proteção contra códigos maliciosos, previamente configurados, e por controlar a alocação de recursos de rede.

4.4. *Proxy web* externo: são servidores não administrados da Câmara Municipal de Currais Novos, responsáveis por intermediar o acesso à internet, que não aplicam as regras de controle de acesso e mecanismos de proteção da mesma forma que o *proxy* administrado da Câmara Municipal de Currais Novos.

4.5. Serviço: produto disponibilizado na internet, como mídia *streaming*, por exemplo, cujo acesso se dá por meio de navegador *web* ou por aplicativo (conhecidos também como *app*);

4.6. Sítio: é um conjunto de páginas *web* organizadas a partir de um URL básico, onde fica a página principal, e geralmente são armazenadas numa única pasta ou subpastas relacionadas no mesmo diretório de um servidor.

4.7. Situação de contingência: estado ou condição na qual exista a ocorrência de falha/problema, em um ou mais recursos tecnológicos, que reduzam a capacidade dos sistemas e serviços que suportam a atividade da organização.

5. **Diretrizes**

5.1. O acesso à internet no ambiente tecnológico da Câmara Municipal de Currais Novos dar-se-á, exclusivamente, pelos meios autorizados, configurados por servidor público designado pela Diretoria Executiva.

5.1.1. É expressamente proibido o uso de *proxies* externos ou similares.

5.2. O acesso à internet nas dependências da Câmara Municipal de Currais Novos é disponibilizado para uso nas atividades relacionadas ao trabalho, observado o disposto nesta norma.

5.2.1. Equipamentos da Câmara Municipal de Currais Novos que estão fora das dependências (ex.: teletrabalho, *home-office* etc.) da Câmara Municipal de Currais Novos poderão ser configurados para utilizar os mecanismos de controle de acesso à internet.

5.2.1.1. A eventual ausência de mecanismos de controle de acesso à internet em equipamentos fora das dependências da Câmara Municipal de Currais Novos não exime o usuário do dispositivo tecnológico de observar as regras e boas práticas definidas nesta norma.

5.3. Constitui acesso indevido à *internet* qualquer das seguintes ações:

5.3.1. Acessar conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais tais como: pornografia, pedofilia, racismo, jogos e páginas de distribuição e de compartilhamento de *software*.

5.3.1.1. A restrição de que trata o item 5.3.1 pode ser flexibilizada: por razão de trabalho, desde que, previamente, autorizada pela Diretoria Executiva.

5.3.2. Utilizar *softwares* para troca de conteúdo via rede ponto-a-ponto (*peerto-peer*) e/ou realizar o *download* de *softwares* e arquivos piratas, exceto programas homologados pela Câmara Municipal de Currais Novos.

5.3.3. Utilizar programas e/ou acessar sítios/serviços de áudio e vídeo em tempo real ou sob demanda, exceto aqueles homologados pela Câmara Municipal de Currais Novos.

5.3.4. Acessar sítios ou serviços que possam comprometer de alguma forma a confidencialidade, integridade ou disponibilidade do ambiente tecnológico e informações da Câmara Municipal de Currais Novos.

5.3.5. Acessar ou fazer *download* de arquivos não relacionados ao trabalho, em especial músicas, imagens, vídeos, jogos e programas de qualquer tipo.

5.4. Todo tráfego de internet será controlado, de forma automática, e poderá ser inspecionado, pela ferramenta de *proxy web* (filtro de conteúdo), configurada de acordo com os limites estabelecidos por esta norma ou definidos em norma específica pelo Comitê Gestor de Segurança da Informação.

5.4.1. A liberação de acesso a sítios e serviços bloqueados, mas necessários ao desempenho das atribuições funcionais do usuário, dependerá de solicitação, devidamente justificada, à Diretoria Executiva, que a submeterá, quando for o caso, ao Comitê Gestor de Segurança da Informação, para deliberação.

5.5. Cabe ao chefia imediata da unidade orientar os usuários sob sua responsabilidade a respeito do uso adequado do recurso de *internet*, conforme as regras estabelecidas nesta norma, bem como reportar ao Comitê Gestor de Segurança da Informação o seu descumprimento.

5.6. A critério da Mesa Diretoria, poderão ser adotadas medidas visando a manutenção da disponibilidade e da qualidade do acesso à internet, seja em situações normais de funcionamento, seja em situações de contingência, tais como:

5.6.1. Bloqueios totais ou parciais e/ou priorização de acessos a determinados sítios e serviços; e

5.6.2. Limitação de banda de tráfego de dados.

6. **Monitoramento e Auditorias**

6.1. Por motivos de segurança, todo acesso à internet será monitorado, e os registros serão mantidos pela Câmara Municipal de Currais Novos.

6.2. Em caso de indícios de descumprimento das diretrizes previstas nesta norma, a chefia imediata ou superior solicitará, justificadamente, ao Comitê Gestor de Segurança da a realização de auditoria extraordinária.

7. **Atualização da Norma**

7.1. O disposto na presente norma será atualizado sempre que alterados os procedimentos de controle de acesso à internet, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

Câmara Municipal de Currais Novos
(CNPJ: 08.470.502/0001-98)

ANEXO II

NSI002 – Do Serviço de Correio Eletrônico Institucional

1. **Objetivo**

1.1. Esta norma estabelece regras e padrões para a utilização do serviço de correio eletrônico no âmbito da Câmara Municipal de Currais Novos.

2. **Motivação**

2.1. Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

2.2. Proteção do ambiente tecnológico da Câmara Municipal de Currais Novos.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos para prover e controlar o serviço de correio eletrônico.

3. **Conceitos e definições**

3.1. Serviço de correio eletrônico institucional: serviço de envio e recebimento de mensagens eletrônicas (também conhecidas por “e-mails”) no âmbito da Câmara Municipal de Currais Novos;

3.2. Caixa postal: conta de correio eletrônico onde são armazenadas as mensagens recebidas e/ou enviadas;

3.2.1. Caixa postal institucional pessoal: conta de correio eletrônico de um único usuário (servidor público, vereador etc.);

3.2.2. Caixa postal institucional da unidade: conta de correio eletrônico de uma unidade administrativa, constante da estrutura organizacional da Câmara Municipal de Currais Novos;

3.2.3. Caixa postal de sistema: conta de correio eletrônico de um sistema informatizado que necessite esse recurso para o seu funcionamento;

3.3. Endereço eletrônico: conjunto de caracteres que individualiza e identifica o remetente e o destinatário da mensagem eletrônica. É formado por um identificador e por um domínio, separados pelo símbolo arroba (@);

3.4. Identificador: parte inicial do endereço eletrônico, localizada antes do símbolo arroba (@), que o diferencia das demais caixas postais e identifica seu usuário, órgão ou finalidade;

3.5. Domínio: parte final do endereço eletrônico, localizada após o símbolo arroba (@);

3.6. Arquivo de registro de mensagens (logs): registro de eventos, utilizados para restaurar um sistema, diagnosticar problemas ou realizar auditorias;

3.7. Usuário de correio eletrônico: vereador ou servidor público que utiliza alguma caixa postal eletrônica;

3.8. *Spam*: mensagem enviada a um grande número de endereços eletrônicos, que não possua caráter institucional e/ou cujo objeto não seja inerente à atividade funcional do usuário ou da unidade;

3.9. *Phishing:* fraude eletrônica, caracterizada pela tentativa de obtenção de dados e informações pessoais com o uso de meios técnicos e de engenharia social;

3.10. *Malware*: programas indesejados, desenvolvidos com a finalidade de executar ações danosas e atividades maliciosas em um computador ou sistema (ex.: *worm*, *bot*, *spyware*, *backdoor*, cavalo de tróia, *ransomware* e *rootkit*);

3.11. Material criptografado: dados e/ou informações codificadas por meio de técnicas que impossibilitam o seu entendimento/leitura, cuja reversão ocorre somente com a utilização de uma senha previamente conhecida e/ou dispositivo criptográfico (ex.: *token*, *smart card*);

3.12. *Hoax*: mensagem eletrônica encaminhada a muitos destinatários, de conteúdo geralmente alarmante e com pouca ou nenhuma veracidade, cujo objetivo é a propagação de boatos e informações distorcidas;

3.13. Alias: endereço eletrônico alternativo para uma conta de correio eletrônico. Pode ser usado para exibir um endereço genérico ou temporário para o público.

4. **Referências Normativas**

4.1. Norma Técnica ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação;

4.2. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles de segurança da informação.

5. **Caixas postais de correio eletrônico (criação, alteração e exclusão)**

5.1. As caixas postais são identificadas unicamente por meio de seu endereço eletrônico.

5.2. No âmbito da Câmara Municipal de Currais Novos, o domínio do endereço eletrônico é “curraisnovos.rn.leg.br”.

5.3. Somente será criada caixa postal institucional pessoal, caixa postal institucional da unidade ou caixa postal de sistema.

5.4. As solicitações de criação, alteração e exclusão de caixas postais devem ser encaminhadas à Diretoria Legislativa.

5.6. No caso de alteração de endereço eletrônico, o endereço antigo será mantido na forma de alias pelo período de até 12 (doze) meses, a contar da alteração, ou permanentemente, em casos excepcionais e devidamente justificados.

5.7. Caixa Postal Institucional Pessoal

5.7.1. Vereadores e Servidores

5.7.1.1. Todo vereador e servidor terá uma caixa postal institucional pessoal.

5.7.1.2. A criação de caixa postal institucional pessoal de servidor ou vereador será feita pela Diretoria Legislativa.

5.7.1.3. O identificador do endereço de correio eletrônico será formado pelo primeiro nome e pelo último sobrenome do servidor, separados pelo sinal de ponto.

5.7.1.4. O identificador do endereço de correio eletrônico será o nome parlamentar adotado pelo vereador.

5.7.1.5. Em situações justificadas, o identificador dos endereços de correio eletrônico poderá ser formado segundo outra ordem ou abreviação do nome do usuário.

5.7.1.5. A adequação dos endereços de correio eletrônico que não correspondam ao padrão estabelecido nesta norma será solicitada à Diretoria Legislativa pelo usuário interessado.

5.7.1.6. A caixa postal institucional pessoal de vereadores e/ou servidores será excluída definitivamente nos casos de falecimento, exoneração, demissão, redistribuição, aposentadoria, remoção, permuta, vacância por posse em outro cargo inacumulável, cessão permanente a outro órgão ou retorno à origem e fim do mandato.

5.7.1.6.1. Não ocorrerá a exclusão da caixa postal institucional pessoal nos casos de licenças.

5.7.1.7. Ocorridos os fatos descritos no item anterior, incumbe à Diretoria Executiva, no prazo de até 5 (cinco) dias da publicação do ato respectivo, exceto nos casos de demissão, quando a comunicação deverá ocorrer de imediato à ciência do afastamento, solicitar à Diretoria Legislativa a exclusão da caixa postal.

5.7.1.8. Nos casos de demissão haverá suspensão imediata da caixa postal institucional.

5.7.1.8.1. A exclusão da caixa postal será realizada somente após a decisão administrativa definitiva da qual não caiba mais recurso.

5.7.1.9. Nos demais casos de que trata o item 5.7.1.7, incumbe à Diretoria Legislativa:

a) no prazo de 5 (cinco) dias, informar ao vereador e ao servidor a data da exclusão definitiva da respectiva caixa postal;

b) no prazo de 20 (vinte) dias, excluir definitivamente a caixa postal.

5.8. Caixa Postal Institucional da Unidade

5.8.1. As unidades administrativas previstas na estrutura organizacional da Câmara Municipal de Currais Novos poderão ter caixa postal institucional da unidade.

5.8.2. O gestor da unidade será também o gestor da respectiva caixa postal, competindo-lhe:

a) solicitar a criação, a alteração e a exclusão da caixa postal institucional da unidade;

b) autorizar o acesso de outros servidores, mediante delegação no sistema de correio eletrônico, bem como excluir esse acesso.

5.8.3. A caixa postal institucional da unidade terá um único endereço de correio eletrônico, cujo identificador será formado pela denominação da unidade ou por sigla que permita a sua identificação, precedida pela sigla da unidade a qual pertence. (ex.: dileg@curraisnovos.rn.leg.br, dileg.rh@curraisnovos.rn.leg.br etc.).

5.8.4. Em casos excepcionais, devidamente justificados, e a critério da Presidência, poderão ser criadas caixas postais institucionais a fim de atender comissões, grupos de trabalho ou núcleos formalmente constituídos, bem como demandas de trabalho específicas e eventos temporários.

5.8.4.1. Nessa hipótese, quando da solicitação de criação da caixa postal, deverão ser indicados o vereador, servidor ou unidade que será responsável pelo respectivo gerenciamento, bem como, se for o caso, o período em que a caixa postal deverá ser mantida.

5.8.4.2. Findada a necessidade para a qual a caixa postal institucional da unidade foi criada, o responsável pelo gerenciamento deverá informar à Diretoria Legislativa para a exclusão da caixa postal.

5.9. Caixa Postal de Sistema

5.9.1. A caixa postal de sistema será criada quando houver essa necessidade para o funcionamento de um sistema informatizado.

5.9.2. O gestor da unidade responsável pelo desenvolvimento ou manutenção do sistema informatizado será também o gestor da respectiva caixa postal, competindo-lhe:

a) solicitar a criação, alteração e exclusão da caixa postal de sistema;

b) autorizar o acesso de outros servidores, mediante delegação no sistema de correio eletrônico, bem como excluir esse acesso.

5.9.3. O identificador do endereço de correio eletrônico será formado pela denominação ou sigla que permita a identificação do respectivo sistema informatizado.

6. **Utilização dos recursos do sistema de correio eletrônico**

6.1. O uso do correio eletrônico institucional restringe-se à mensagem cujo objeto seja, necessariamente, inerente à atividade funcional do usuário ou da unidade, sendo vedado o uso para fins particulares.

6.2. O acesso ao correio eletrônico a partir de estações de trabalho fornecidas pela Câmara Municipal de Currais Novos será feito apenas a partir do navegador de internet.

6.3. É vedada a tentativa de acesso a caixas postais às quais o usuário não tenha autorização de acesso.

6.4. É de responsabilidade do usuário:

a) eliminar periodicamente as mensagens eletrônicas contidas nas caixas postais;

b) manter exclusivo o acesso à sua caixa postal institucional pessoal, não compartilhando a respectiva senha e/ou delegando o acesso a terceiros.

6.7. É vedado aos usuários o envio de qualquer mensagem eletrônica contendo:

a) informações privilegiadas, confidenciais e/ou de propriedade da Câmara Municipal de Currais Novos para destinatários não autorizados;

b) materiais obscenos, ilegais ou antiéticos;

c) materiais preconceituosos ou discriminatórios;

d) materiais caluniosos ou difamatórios;

e) propaganda com objetivo comercial;

f) listagem com endereços eletrônicos institucionais, exceto nos casos em que a atividade funcional demande tal ação;

g) *malwares*;

h) material protegido por lei de propriedade intelectual;

i) entretenimentos e “correntes”;

j) assuntos ofensivos;

l) músicas, vídeos ou animações que não sejam de interesse específico do trabalho;

m) *spam*, *phishing* e *hoax*;

n) materiais criptografados, exceto nos casos em que as informações da mensagem necessitem proteção quanto ao sigilo;

o) dados pessoais, sensíveis ou não, que não estejam vinculados às atividades de trabalho e devidamente adequados às legislações vigentes.

7. **Monitoramento e Auditoria**

7.1. O uso do correio eletrônico será monitorado por meio de ferramentas com o intuito de impedir o recebimento de *spam*, *hoax*, *phishing*, mensagens contendo vírus e outros arquivos que coloquem em risco a segurança do ambiente tecnológico da Câmara Municipal de Currais Novos ou que contenham conteúdo impróprio.

7.2. As auditorias ordinárias ou extraordinárias serão coordenadas pela Diretoria Executiva e os relatórios serão encaminhados ao Comitê Gestor de Segurança da Informação.

7.3. Os arquivos de registro de mensagens eletrônicas (logs) serão mantidos pelo prazo de 30 dias, exceto nos casos de auditoria ou notificação administrativa ou judicial, em que serão devidamente armazenados, a fim de salvaguardar os dados respectivos.

8. **Atualização da Norma**

8.1. O disposto na presente norma será atualizado sempre que houver alterações significantes na arquitetura e/ou tecnologia referente ao serviço de correio eletrônico, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

ANEXO III

NSI003 – Uso de Recursos de Tecnologia da Informação e Controle de Acesso

1. **Objetivos**

1.1. Estabelecer diretrizes e padrões para a utilização dos recursos de tecnologia da informação e para o controle de acesso, no âmbito da Câmara Municipal de Currais Novos.

2. **Motivações**

2.1. Alinhamento às normas, regulamentações e melhores práticas, relacionadas à matéria.

2.2. Garantia de que os acessos aos recursos tecnológicos sejam feitos de forma segura e controlada.

2.3. Necessidade de um processo sistemático para gerenciar o uso de recursos de tecnologia da informação, visando garantir a segurança e continuidade das atividades da Câmara Municipal de Currais Novos.

3. **Referências normativas**

3.1. Norma Técnica ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação;

3.2. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles de segurança da informação.

4. **Conceitos e definições**

4.1. Arquivo de registro de mensagens (logs): registro de eventos relevantes, utilizados para restaurar um sistema, diagnosticar problemas ou realizar auditorias;

4.2. Controle de acesso: métodos para garantir que o acesso aos ativos seja autorizado e restrito com base no negócio e em segurança;

4.3. Dispositivo móvel: equipamento portátil dotado de capacidade computacional que permite conexão à rede cabeada ou à rede sem-fio, podendo acessar recursos de rede e internet, dos quais são exemplos: smartphones, notebooks e tablets, dentre outros;

4.4. *Malwares*: programas indesejados, desenvolvidos com a finalidade de executar ações danosas e atividades maliciosas em um computador ou sistema (ex.: *worm*, *bot*, *spyware*, *backdoor*, cavalo de troia, *ransomware* e *rootkit*);

4.5. Proprietário do ativo de informação: pessoa ou outra entidade que tem a responsabilidade (aprovada pela Administração) para qualificar o ciclo de vida de um ativo;

4.6. Rede cabeada: corresponde ao acesso aos recursos tecnológicos e à transmissão de dados através da utilização de meios físicos (ativos de distribuição de dados, cabos e pontos de rede);

4.7. Rede lógica: é a rede de dados utilizada pela Câmara Municipal de Currais Novos, abrangendo serviços e sistemas de tecnologia da informação, rede cabeada, rede sem-fio, ativos de distribuição de dados e equipamentos conectados nessa rede;

4.8. Rede sem-fio: também conhecida como rede *wireless* ou *wi-fi*, corresponde ao acesso aos recursos tecnológicos e à transmissão de dados sem a utilização de meios físicos (cabeamento), através da utilização de pontos de acesso sem-fio;

4.9. Remoção de acesso: processo que tem por finalidade remover/excluir definitivamente ou parcialmente determinado(s) acesso(s);

4.10. Solução baseada em nuvem: modelo computacional que permite acesso por demanda e independente da localização a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

4.11. Usuários: vereadores e servidores públicos ocupantes de cargo efetivo ou em comissão, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados e outras pessoas que se encontrem a serviço da Câmara Municipal de Currais Novos, utilizando em caráter temporário os recursos tecnológicos daquele órgão;

4.12. Acesso privilegiado: nível de acesso restrito onde uma pessoa tem permissão para gerenciar um sistema e/ou serviço;

4.13. Fator de autenticação: é um componente utilizado pelo usuário para se autenticar na rede, sistema e/ou aplicação. Pode ser algo que se sabe (senha), algo que se tem (*token*, *certificado*, etc.) ou algo que se é (biometria); e

4.14. Autenticação de multifator: é quando mais de um fator é utilizado em conjunto para autenticação do usuário. Por exemplo: senha e certificado.

Rua Vivaldo Pereira de Araújo, n.º 161, Centro – Telefone: (84) 3412–1567
59.380-000 Currais Novos/RN – E-mail: camaracurraisnovos@hotmail.com

Câmara Municipal de Currais Novos
(CNPJ: 08.470.502/0001-98)

5. **Uso de Recursos de Tecnologia da Informação**

5.1. **Diretrizes gerais**

5.1.1. O uso adequado dos recursos de tecnologia da informação visa a contribuir para a efetividade e a continuidade das atividades desenvolvidas pela Câmara Municipal de Currais Novos.

5.1.2. Os recursos de tecnologia da informação disponibilizados pela Câmara Municipal de Currais Novos aos usuários serão utilizados em atividades relacionadas às funções institucionais, e abrangem os seguintes elementos:

a) os computadores servidores, os computadores para uso individual ou coletivo, de qualquer porte, os equipamentos de armazenamento e distribuição de dados, os dispositivos móveis, as impressoras, as copiadoras e os equipamentos multifuncionais, assim como os respectivos suprimentos, periféricos e acessórios;

b) a rede lógica da Câmara Municipal de Currais Novos e os respectivos canais e pontos de distribuição;

c) as contas de acesso dos usuários, assim como os certificados digitais;

d) os sistemas e serviços tecnológicos contratados de terceiros, sob licença ou na forma de *software* livre ou aberto, incluídas as soluções baseadas em nuvem.

5.1.3.O usuário é responsável por:

a) zelar pelos recursos que lhe sejam destinados para o exercício de suas atribuições, especialmente os de utilização pessoal, tais como computadores, impressoras, dispositivos móveis e demais equipamentos;

b) preservar o sigilo de sua senha ou outro mecanismo de autenticação que venha a ser utilizado para acesso aos recursos tecnológicos disponibilizados;

c) preservar o sigilo das informações a que tiver acesso, sendo vedada sua revelação a usuários ou terceiros não autorizados;

d) atos praticados e acessos realizados aos recursos de tecnologia por meio de sua credencial de acesso.

5.1.4. Os procedimentos de instalação, configuração e manutenção de equipamentos e *softwares* serão realizados por servidor público designado pela Diretoria Executiva, que verificará a adequação do serviço realizado ao atendimento das atividades desenvolvidas pela unidade.

5.1.5. Não será fornecido suporte a equipamentos particulares (por exemplo: computadores, notebooks, smartphones e tablets), seja quanto à instalação e configuração de sistemas ou aplicativos, seja quanto às questões relacionadas à conexão à rede sem-fio.

5.1.6. Os equipamentos servidores e os computadores para uso individual ou coletivo, de qualquer porte, serão dotados de mecanismos de proteção contra *malwares*.

5.2. **Da Rede Lógica**

5.2.1. Todos os equipamentos e dispositivos móveis conectados à rede lógica de dados da Câmara Municipal de Currais Novos terão seus acessos monitorados por questões de segurança e para fins de auditoria.

5.2.2. A cada ponto de acesso à rede de dados da Câmara Municipal de Currais Novos poderá ser conectado apenas um equipamento, vedada a utilização de dispositivos multiplicadores de acesso, salvo mediante expressa autorização da Diretoria Executiva.

5.2.4. A Câmara Municipal de Currais Novos disponibilizará acesso à rede sem-fio para usuários internos e externos.

5.2.5.1. O acesso à internet por meio das redes sem-fio observará as regras dispostas no Anexo I - Controle de Acesso à Internet, da Política de Segurança da Informação.

5.2.5.2. Poderão ser bloqueados os acessos à rede sem-fio, temporariamente ou por tempo indeterminado, de dispositivos móveis identificados durante o monitoramento como fonte de ações maliciosas, intencionais ou não, ou em que detectadas vulnerabilidades ou problemas de segurança tecnológica.

5.2.6. Cada unidade da Câmara Municipal de Currais Novos terá disponível área de armazenamento em rede para salvaguardar os arquivos relacionados ao trabalho desenvolvido, com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança.

5.2.6.1. Os dados armazenados nas estações de trabalho dos usuários não estão contemplados pelas garantias mencionadas nesse item, cabendo aos usuários providenciar eventual cópia de segurança e a eliminação periódica dos arquivos armazenados nos discos rígidos locais.

5.2.6.2. É proibido o armazenamento, em qualquer diretório na rede da Câmara Municipal de Currais Novos ou nas soluções baseadas em nuvem, sob pena de serem excluídos por servidor público designado pela Diretoria Executiva, sem anuência do usuário, de arquivos não relacionados ao trabalho, tais como:

a) fotos, músicas e filmes de qualquer formato;

b) programas não homologados ou não licenciados; e

c)programas de conteúdo prejudicial à segurança do parque computacional da Câmara Municipal de Currais Novos.

5.3. **Nuvem corporativa**

5.3.1.Ao armazenamento de arquivos na nuvem corporativa aplicam-se as regras previstas no item 5.2.6.2.

5.4. **Licenças de *software***

5.4.1. As licenças de *softwares*, de qualquer natureza, contratadas ou adquiridas pela Câmara Municipal de Currais Novos são de uso institucional, privativo deste órgão.

5.4.2. A Câmara Municipal de Currais Novos utilizará, preferencialmente, em suas atividades, *Software* Livre ou de Código Aberto.

5.4.3. É proibida a instalação de *softwares* não licenciados ou não homologados pela Câmara Municipal de Currais Novos nos equipamentos conectados à rede da Câmara Municipal de Currais Novos.

5.4.3.1. A instalação de *softwares* não homologados poderá ser autorizada excepcionalmente pela Diretoria Executiva, desde que demonstrada a necessidade de sua utilização para o desempenho das atribuições funcionais do usuário, observadas as condições de segurança e proteção estabelecidas, bem como a compatibilidade e adequação aos recursos computacionais disponibilizados pela Câmara Municipal de Currais Novos.

5.4.3.2. As unidades organizacionais da Câmara Municipal de Currais Novos poderão encaminhar à Diretoria Executiva pedido de homologação de *softwares*, para o uso em suas atividades.

6. **Do controle do acesso**

6.1. Do gerenciamento de acessos

6.1.1. Os acessos à rede, serviços e aos sistemas computacionais disponibilizados pela Câmara Municipal de Currais Novos serão solicitados à Diretoria Executiva, por meio do sistema de atendimento, em que definidos os níveis de acesso adequados às atividades desenvolvidas.

6.1.2.Incumbe à chefia imediata solicitar à Diretoria Executiva:

a) os acessos necessários ao desenvolvimento das atividades dos servidores e terceirizados vinculados a sua unidade.

b) a alteração dos níveis de acesso ou a remoção do acesso a sistemas concedidos a servidor ou terceirizado da unidade, sempre que necessária sua adequação às atividades desenvolvidas.

c) a remoção dos acessos concedidos ao servidor ou terceirizado, imediatamente após o afastamento ou desligamento da unidade.

d) a inclusão, alteração ou remoção de acessos decorrentes da alteração do regime de trabalho (presencial ou teletrabalho).

6.1.2.1. Não solicitada a alteração ou exclusão no momento oportuno, a chefia poderá ser responsabilizada pelo acesso indevido do servidor/terceirizado a informações da unidade.

6.1.7. Nos casos de casos de falecimento, exoneração, demissão, redistribuição, aposentadoria, remoção e cessão a outro órgão, retorno à origem, ou encerramento do mandato, servidor designado pela Diretoria Executiva efetuara a remoção dos acessos concedidos aos usuários.

6.1.8. O privilégio de administrador na estação de trabalho é restrito a servidor público designado pela Diretoria Executiva que necessite de acesso privilegiado para o desempenho das atividades funcionais.

6.1.9. Os acessos privilegiados aos sistemas e serviços de TIC serão concedidos a servidor público designado pela Diretoria Executiva, sempre que necessários ao desempenho das atividades funcionais, de modo a permitir a gestão e configuração do ambiente tecnológico.

6.1.9.1. É responsabilidade da chefia imediata solicitar a concessão, a alteração e a remoção dos acessos privilegiados dos seus subordinados.

6.1.10. As solicitações de acessos de prestadores de serviço aos recursos tecnológicos da terceirizado terão caráter temporário e deverão ser acompanhadas da respectiva justificativa, bem como do prazo previsto para a realização das atividades.

6.1.10.1. No caso do prestador de serviço necessitar de acesso privilegiado, as regras observarão o disposto no item 6.1.9.

6.2. Da conta de rede e respectiva senha para utilização

6.2.1. Para ter acesso aos recursos de tecnologia da informação disponibilizados pela Câmara Municipal de Currais Novos é necessário que o usuário possua uma conta de rede.

6.2.2. A identificação de usuário será composta pela primeira letra do prenome e o último sobrenome do servidor ou vereador.

6.2.3. Em situações justificadas, poderá ser utilizado outro prenome ou sobrenome para a composição da identificação.

6.2.4. A cada conta de acesso será associada uma senha, de uso pessoal e intransferível.

6.2.5. Na utilização das credenciais de acesso, compete ao usuário observar os procedimentos a seguir indicados, bem como adotar outras medidas de segurança de caráter pessoal, com vista a impedir o uso não autorizado dos recursos de tecnologia da informação a partir de sua conta de acesso:

a) não compartilhar a senha com outras pessoas;

b) não armazenar senhas em local acessível por terceiros;

c) não utilizar senhas de fácil dedução como as que contêm nomes próprios e de familiares, datas festivas e sequências numéricas;

d) ao ausentar-se de sua estação de trabalho, ainda que temporariamente, o usuário deverá encerrar ou bloquear a sessão.

6.2.6. Em caso de suspeita de comprometimento da senha ou de outro recurso de autenticação, o usuário comunicará imediatamente à Diretoria Executiva, que poderá, como medida preventiva, suspender temporariamente o acesso.

7. **Registros (log) de Eventos**

7.1. Serão mantidos, por um período mínimo de 03 (três) meses, os registros dos acessos dos usuários e dos acessos privilegiados aos recursos tecnológicos disponibilizados pela Câmara Municipal de Currais Novos, inclusive para fins de apuração e comprovação de incidentes de segurança.

7.2. Serão registrados os seguintes dados:

a) identificação de usuário de quem efetuou o acesso;

b) data e hora de entrada e saída do sistema;

c) origem do acesso;

d) erros ou falhas de conexão e acesso;

e) troca de senhas de Serviços de Infraestrutura de TI;

f) outras informações que venham a ser necessárias para os controles de segurança.

8. **Atualização da Norma**

8.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de uso de recursos de tecnologia da informação e de controle de acesso, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

ANEXO IV

NSI004 - Procedimentos de *backup* e recuperação de dados

1. **Objetivo**

1.1. Estabelecer diretrizes e padrões para os procedimentos de *backup*, testes e recuperação de dados realizados pela Câmara Municipal de Currais Novos.

2. **Motivações**

2.1. Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

2.2. Garantia de que a salvaguarda das informações seja realizada de forma otimizada, atendendo às necessidades da Câmara Municipal de Currais Novos.

2.3. Alinhar expectativas no processo de salvaguarda e *restore* dos dados armazenados em *backup*, visto que tal procedimento é uma das ações do processo de restauração/restabelecimento do ambiente.

3. **Conceitos e definições**

3.1. *Backup* tipo "*archive*": é o utilizado pelos *backups* mensais e anuais, tem retenção maior, mas só contém a versão do arquivo no momento do *archive*;

3.2. *Backup* tipo "*backup*": é o ordinário, utilizado no *backup* diário, com retenção menor, mas que contém versão diária dos arquivos (possibilita o *backup* de várias versões e a navegação por estas versões);

3.3. *Backup* completo: são copiados todos os arquivos existentes no momento do *backup*;

3.4. *Backup* em fita: mídia magnética. Pode ser movida para cofre resistente a fogo;

3.5. *Backup* incremental: somente os arquivos novos ou modificados desde o último *backup* são transmitidos;

3.6. Disco rígido: dispositivo de armazenamento local de dados utilizados pelos computadores;

3.7. Equipamento servidor: computador com alta capacidade de armazenamento e processamento, destinado ao provimento de serviços e sistemas de TIC;

3.8. Produto, sistema ou serviço: soluções tecnológicas que demandam a salvaguarda de dados por ele utilizados;

3.9. RPO (*Recovery-Point Objective*): o quanto é necessário voltar no tempo para encontrar um *backup* dos dados, ou seja, o tempo máximo de perda de dados, o que indica o volume de dados perdidos em caso de tempo de inatividade do serviço;

3.10. RTO (*Recovery-Time Objective*): define o período de tempo desejado necessário para realizar todas as tarefas de recuperação antes que um aplicativo ou serviço possa executar solicitações normalmente novamente;

3.11. Versão ativa: é a última versão do arquivo no *backup*;

3.12. Versão de arquivos: sempre que um arquivo for criado/alterado/apagado, é criada uma nova versão deste arquivo no *backup*;

3.13. Versão(ões) inativa(s): versão(ões) anterior(es) à última versão do arquivo no *backup*; e

3.14. *Virtual Tape Library* (VTL): tecnologia que emula fitas magnéticas em disco, o que garante gravação e restauração em alta velocidade.

4. **Referências Normativas**

Câmara Municipal de Currais Novos
(CNPJ: 08.470.502/0001-98)

4.1. Norma Técnica ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação; e

4.2. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles de segurança da informação.

5. **Procedimentos de *backup***

5.1. Os procedimentos de *backup* realizados pelo servidor público designado pela Diretoria Executiva serão executados por soluções automatizadas, em conformidade com a presente política, abrangendo os dados armazenados no ambiente tecnológico disponibilizado pela Câmara Municipal de Currais Novos.

5.2. Os dados armazenados no disco rígido de estações de trabalho ou de *notebooks* não serão objeto de *backup* de dados, o que não garante a sua recuperação não em casos de indisponibilidade causados por erros de *hardware* no disco rígido, apagamentos acidentais ou intencionais, falhas no sistema operacional, ação de códigos maliciosos, dentre outros.

5.3. Os dados objeto de *backup* tipo "*archive*" serão armazenados, ao final do processo, em dois locais: uma cópia no conjunto de fitas primárias, disponíveis para restaurações, e a outra cópia no conjunto de fitas secundárias.

5.4. A periodicidade, o tempo de retenção, o RPO e o RTO dos *backups* observarão as seguintes regras:

Tipos de backup	Dias e horários	Retenção
Backup diário (tipo *backup*)	Todos os dias, às 10h.	05 (cinco) últimas versões do arquivo, desde que as versões inativas estejam dentro de um prazo de 30 (trinta). No caso de arquivos deletados, a última versão será mantida pelo prazo de 60 (sessenta) dias.
Backup mensal (tipo *archive*)	Terceira sexta-feira de cada mês.	A versão do arquivos objeto de *backup* será retida pelo período de 06 (seis) meses.
Backup anual (tipo *archive*)	Durante o recesso legislativo ao fim de cada sessão legislativa.	A versão objeto do *backup* será retida pelo período de 05 (cinco) anos.

RPO (tempo máximo de perda dos dados)	24 horas	
RTO (tempo estimado para restauração)	Imediato para restaurações pontuais e 30 (trinta) horas para restauração completa.	

5.5. No caso de serviços armazenados em nuvem, a responsabilidade pelo *backup* será da prestadora de serviços, assegurado um prazo de retenção de, no mínimo, 30 (trinta) dias.

5.6. As mídias de *backup*, quando transportadas, deverão ser protegidas de extravio e de eventos que possam causar dano físico.

5.6.1.A movimentação de mídias de backup deverá ser realizada por servidor designado, com registro, no mínimo, da identificação da mídia e a data e hora da movimentação.

6. **Recuperação de dados**

6.1. A recuperação de dados e arquivos, sempre que não puder ser realizada pelo próprio usuário, será solicitada ao servidor público designado pela Diretoria Executiva.

7. **Atualização da Norma**

8.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de backup, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

Anexo V

NSI005 - Gestão de Riscos de Tecnologia da Informação e Comunicações

1. **Objetivos**

1.1. Estabelecer as diretrizes da gestão de riscos relacionada ao ambiente tecnológico no âmbito da Câmara Municipal de Currais Novos e aos processos de Tecnologia da Informação e Comunicações (TIC) e definir o processo de Gerenciamento de Riscos de Segurança da Informação e Comunicações daquele órgão.

2. **Aplicabilidade**

2.1. Este documento aplica-se a todas aos órgãos responsáveis à gestão da tecnologia da informação da Câmara Municipal de Currais Novos.

3. **Motivações**

3.1. Necessidade de um processo sistemático para gerenciar riscos referentes à Segurança da Informação e Comunicações (SIC) e processos de TIC (Tecnologia da

Informação e Comunicações), provendo insumos para aumentar a proteção contra eventos indesejados.

3.2. Correto direcionamento de esforços e investimentos financeiros, tecnológicos e humanos.

3.3. Conformidade com normatizações e regulamentações relacionadas ao assunto.

4. **Referências normativas**

4.1. Norma Técnica ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação;

4.2. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles de segurança da informação.

4.3. Norma Técnica ABNT NBR ISO/IEC 27005:2019, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação.

4.4. Norma Técnica ABNT NBR ISO 31000:2018, que fornece princípios e diretrizes genéricas para a gestão de riscos.

5. **Conceitos e definições**

5.1. Ameaça: causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização;

5.2. Análise de riscos: processo para compreender a natureza do risco e determinar o nível de risco;

5.3. Avaliação de riscos: processo de comparação dos resultados da análise de risco com critérios de risco para determinar se o risco e/ou sua magnitude são aceitáveis ou toleráveis;

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

5.5. Comunicação do risco: conjunto de processos contínuos e iterativos que uma organização realiza para fornecer, compartilhar ou obter informações e para dialogar com as partes interessadas sobre o gerenciamento de riscos;

5.6. Estimativa de riscos: processo utilizado para atribuir valores à probabilidade e às consequências de um risco;

5.7. Evitar risco: forma de tratamento de risco pela qual se decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;

5.8. Evento adverso: ocorrência ou alteração negativa de um conjunto de circunstâncias;

5.9. Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC): conjunto de atividades que permitem identificar e implementar as medidas de proteção necessárias

Rua Vivaldo Pereira de Araújo, n.º 161, Centro – Telefone: (84) 3412–1567
59.380-000 Currais Novos/RN – E-mail: camaracurraisnovos@hotmail.com

para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

5.10. Gestão de Riscos em Processos de TIC: conjunto de atividades, estabelecidas de acordo com as peculiaridades ou normatividades que regem cada processo, que visam a identificar e minimizar ou eliminar os riscos;

5.12. Identificação de riscos: processo para localizar, listar e caracterizar elementos do risco;

5.13. Impacto: é a medida do dano ocasionado caso o evento adverso concretize-se;

5.14. Probabilidade: é a possibilidade de algum evento adverso ocorrer;

5.15. Reduzir risco: forma de tratamento de risco pela qual se decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;

5.16. Reter risco: forma de tratamento de risco pela qual se decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;

5.17. Riscos de Segurança da Informação e Comunicações: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

5.18. Transferir risco: uma forma de tratamento de risco pela qual se decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

5.19. Tratamento dos riscos: processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco; e

5.20. Vulnerabilidade: fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

6. **Escopo**

6.1. A Gestão de Riscos, definida por esta norma, tem seu escopo limitado às medidas protetivas dos ativos de informação e dos processos relacionados à área de TIC, que suportam os principais processos da Câmara Municipal de Currais Novos.

7. **Diretrizes**

7.1. A Gestão de Riscos leva em consideração as definições do Planejamento Estratégico Institucional e está alinhada à Política de Segurança da Informação da Câmara Municipal de Currais Novos.

7.2. A Gestão de Riscos é abordada de forma sistemática, com o objetivo de manter os riscos em níveis aceitáveis para cada projeto, processo e/ou serviço analisado.

7.3. Os riscos são analisados e avaliados em função de sua relevância para os principais processos de negócio da Câmara Municipal de Currais Novos e são tratados de forma a assegurar respostas tempestivas e efetivas.

8. **Gestão de riscos em processos de TIC**

8.1. A gestão e comunicação de riscos em processos de TIC são definidas na especificação de cada processo e visam à identificação e ao controle dos eventos que possam comprometer seus objetivos, contribuindo para sua melhoria.

8.2. As atividades inerentes à gestão de riscos nos processos de TIC devem observar as diretrizes desta norma e outras específicas relacionadas ao processo.

10. **Gestão de riscos em Segurança da Informação e Comunicações (GRSIC)**

10.1. O processo de GRSIC é contínuo, fornecendo subsídios e integrando-se à implantação e operação do Sistema de Gestão de Segurança da Informação.

10.2. O processo de GRSIC está baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27005:2019 e ABNT NBR ISO/IEC 31000:2018.

10.3. Os riscos serão avaliados a partir da:

a) probabilidade: é a possibilidade de algum evento adverso ocorrer e acarretar impactos negativos, cuja escala tem quatro níveis (raro, possível, provável ou iminente);

b) impacto: é a medida do dano ocasionado caso o evento adverso concretize-se, com quatro níveis de análise (perceptível, moderado, crítico ou catastrófico).

10.3.1. O produto das variáveis de análise de risco, probabilidade e impacto, determina o nível do risco, conforme mapa a seguir:

	1 - Raro	**2 - Possível**	**3 - Provável**	**4 - Iminente**
1 - Perceptível	1	2	3	4
2 - Moderado	2	4	6	8
3 - Crítico	3	6	9	12
4 - Catastrófico	4	8	12	6

Classificação do Risco	**Valores do Risco**
Muito baixo	1 a 2
Baixo	3 a 4
Médio	6 a 8

Alto	9 a 12
Muito alto	16

10.4. O tratamento dos riscos será definido de acordo com as necessidades levantadas pelas partes interessadas, regulamentações e legislações vigentes, avaliação técnica e análise custo/benefício.

10.5. O processo de GRSIC é composto pelas etapas descritas a seguir:

a) contextualização: compreende a definição e aprovação do contexto da análise e avaliação de riscos a ser realizada, com a identificação de seu propósito, escopo, limites e partes interessadas;

b) análise e avaliação dos riscos: compreende o mapeamento dos ativos, identificação, análise e avaliação dos riscos, bem como a elaboração e aprovação do Plano de Tratamento dos Riscos;

c) tratamento dos riscos: compreende a implementação das ações do Plano de Tratamento de Riscos; e

d) melhoria contínua: compreende a realização da análise crítica pela Câmara Municipal de Currais Novos, com avaliação dos resultados e das propostas de melhoria apresentadas.

10.6. O desenho do processo de Gestão de Riscos de Segurança da Informação, a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos no processo, bem como demais documentos relacionados, serão publicados no Portal de Transparência, após aprovação pela Presidência.

10.7. O processo será revisto anualmente ou em menor prazo, quando necessário, e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência, objeto de imediata divulgação na forma do item anterior.

11. **Atualização da Norma**

11.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de Gestão de Riscos de TIC, observada a periodicidade prevista para a Política de Segurança da Informação.

Câmara Municipal de Currais Novos
(CNPJ: 08.470.502/0001-98)

ANEXO VI

NSI006 - Tratamento e Resposta a Incidentes de Segurança da Informação

1. **Objetivos**

1.1. Estabelecer as diretrizes para o funcionamento da atividade de Tratamento e Resposta a Incidentes de Segurança da Informação da Câmara Municipal de Currais Novos.

2. **Motivações**

2.1. Alinhamento às normas, regulamentações e melhores práticas, relacionadas à matéria.

2.2. Necessidade de formalização da atividade de Tratamento e Resposta a Incidentes de Segurança da Informação (TIR) e seu funcionamento.

2.3. Proteção do ambiente tecnológico da Câmara Municipal de Currais Novos.

3. **Referências Normativas**

3.1. Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições relacionados às normas de segurança da informação.

3.2. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles genéricos de segurança da informação.

4. **Conceitos e definições**

4.1. Artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

4.2. Comunidade ou público alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas pelo responsável pelo Tratamento e Resposta a Incidentes de Segurança da Informação;

4.3. Responsável pelo Tratamento e Resposta a Incidentes de Segurança da Informação: servidor público com competências relacionadas à recepção, análise e resposta às notificações e atividades relacionadas a incidentes de segurança da informação;

4.4. Incidente de segurança da informação: um único ou uma série de eventos indesejados ou inesperados de segurança da informação que têm uma probabilidade significativa de colocar em perigo as operações da instituição e ameaçar a segurança da informação;

4.5. Tratamento de Incidentes de Segurança da Informação: conjunto de processos para detectar, relatar, avaliar, responder, lidar e aprender com incidentes de segurança da informação;

4.6. Usuários: vereadores e servidores públicos ocupantes de cargo efetivo ou em comissão, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados e outras pessoas que se encontrem a serviço da Câmara Municipal de Currais Novos, utilizando em caráter temporário os recursos tecnológicos daquele órgão;

4.7. Vulnerabilidade: fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

5. **Objetivo da atividade de Tratamento e Resposta a Incidentes de Segurança da Informação**

5.1. Prover capacidade adequada para prevenção, resposta e tratamento de incidentes de segurança da informação e de dados pessoais no âmbito da Câmara Municipal de Currais Novos.

6. **Público-alvo**

6.1. O público-alvo da atividade de Tratamento e Resposta a Incidentes de Segurança da Informação é formado por todos os usuários do ambiente tecnológico da Câmara Municipal de Currais Novos.

7. **Modelo de Implementação**

7.1. A atividade de Tratamento e Resposta a Incidentes de Segurança da Informação será realizada por servidor público designado pela Diretoria Executiva que, além de suas funções regulares, desempenharão as atividades relacionadas à prevenção, ao tratamento e à resposta a incidentes de segurança da informação e de dados pessoais.

8. **Atribuições**

8.1. Planejar, em conjunto com outras áreas, ações para a prevenção de incidentes cibernéticos e de dados pessoais;

8.2. Responder e tratar os incidentes de segurança da informação e de dados pessoais no âmbito da Câmara Municipal de Currais Novos.

8.3. Receber e analisar as informações sobre vulnerabilidades, artefatos maliciosos e tentativas de intrusão, com definição de estratégias e ações para sua detecção ou correção;

8.4. Fornecer informações, aos envolvidos, sobre a ocorrência e, ao público interno, orientações de prevenção de incidentes de segurança da informação.

8.5. Manter os registros dos incidentes de segurança da informação e de dados pessoais no âmbito da Câmara Municipal de Currais Novos.

8.6. Divulgar alertas ou advertências diante da ocorrência de um incidente de segurança da informação ou de dados pessoais ou, de forma proativa, em face de vulnerabilidades e incidentes conhecidos e que possam gerar impactos nas atividades dos usuários.

8.7. Interagir com outras equipes e órgãos relacionados ao tratamento de incidentes de segurança, participação em fóruns e redes nacionais e internacionais.

9. **Atualização da Norma**

9.1. O disposto na presente norma será atualizado sempre que alterados os procedimentos de controle de acesso à internet, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

ANEXO VII

NSI007 - Gestão de Incidentes de Segurança da Informação

1. **Objetivos**

1.1. Estabelecer as diretrizes e definir o processo de Gestão de Incidentes de Segurança da Informação no âmbito da Câmara Municipal de Currais Novos.

2. **Motivações**

2.1. Alinhamento às normas, regulamentações e melhores práticas, relacionadas à matéria.

2.2. Necessidade de tratar os incidentes de segurança da informação com resposta rápida e eficiente.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos e humanos para prover uma Gestão de Incidentes de Segurança da Informação com menor custo e maior qualidade.

2.4. Formalização de um processo para gerenciamento dos incidentes de segurança da informação, provendo insumos para minimizar e/ou evitar eventos adversos futuros.

3. **Referências normativas**

3.1. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles genéricos de segurança da informação; e

3.2. Norma ABNT NBR ISO/IEC 27035-3:2021 que fornece diretrizes para operações de resposta a incidentes de TIC.

4. **Conceitos e definições**

4.1. Artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

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

4.3. Usuários: vereadores e servidores públicos ocupantes de cargo efetivo ou em comissão, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados e outras pessoas que se encontrem a serviço da Câmara Municipal de Currais Novos, utilizando em caráter temporário os recursos tecnológicos daquele órgão;

4.4. Responsável pelo Tratamento e Resposta a Incidentes de Segurança da Informação: servidor público com competências relacionadas à recepção, análise e resposta às notificações e atividades relacionadas a incidentes de segurança da informação;

4.5. Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

4.6. Incidente de segurança da informação: é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

4.7. Medida de contenção: controle e/ou ação tomada para evitar que danos causados por um determinado incidente continuem aumentando com o passar do tempo, bem como restabelecer do sistema/serviço afetado, mesmo eu não seja em sua capacidade total;

4.8. Medida de erradicação: controle e/ou ação tomada para sanar vulnerabilidades e problemas que sejam a causa-raiz de um ou mais incidentes de segurança da informação;

4.9. Medidas de recuperação: conjunto de ações para restabelecer o ambiente ao estado normal, situação na qual se encontrava antes do incidente, contemplando medidas de melhoria observadas no tratamento do evento adverso;

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

4.11. Vulnerabilidade: fragilidade de um ativo ou controle que pode ser explorado por uma ameaça; e

5. **Escopo**

5.1. A Gestão de Incidentes de Segurança da Informação, definida nesta norma, tem seu escopo limitado às situações relacionadas ao ambiente, ativos e processos de TIC.

6. **Diretrizes**

6.1. A Gestão de Incidentes de Segurança da Informação tem como principal objetivo assegurar que incidentes de segurança da informação sejam identificados, registrados e avaliados em tempo hábil, com a tomada de medidas de contenção, erradicação e recuperação adequadas.

6.2. Estão abrangidos por esta norma os eventos, confirmados ou suspeitos, relacionados à segurança de sistemas ou redes computacionais, que comprometam o ambiente tecnológico da Câmara Municipal de Currais Novos, seus ativos, informações e processos de negócio, bem como aqueles que contrariem a Política de Segurança da Informação deste órgão, e dos quais decorram interrupção, parcial ou total, de serviço essencial ao desempenho das atividades, vulnerabilidades de segurança, divulgação, alteração ou destruição de informações e/ou prática de ato definido como crime ou infração administrativa.

6.3. A Câmara Municipal de Currais Novos providenciará dispositivos de monitoramento, ferramentas de segurança e detecção de intrusão, a fim de subsidiar a Gestão de Incidentes de Segurança da Informação.

7. **O processo de Gestão de Incidentes de Segurança da Informação**

7.1. O processo de Gestão de Incidentes de Segurança da Informação é composto pelas seguintes etapas:

a) preparação: consiste no conjunto de atividades proativas, para mapeamento e proteção do ambiente tecnológico, como implantação de mecanismos para auxílio à detecção de incidentes, elaboração de planos de resposta a incidentes, dentre outros;

b) detecção e análise: compreende a detecção ou recebimento de informação sobre eventos maliciosos suspeitos, a investigação do ocorrido, para determinar se de fato é um incidente, avaliação da extensão e do impacto do incidente e a comunicação do evento.

c) contenção, erradicação e recuperação: compreende o conjunto de atividades necessárias para a contenção e erradicação de um incidente, bem como as ações necessárias à recuperação do ambiente tecnológico à operação normal; e

d) atividades pós-incidente: consistem nas tarefas relacionadas realizadas após o encerramento do incidente, que visam ao aperfeiçoamento na deteção e resposta dadas, além dos processos realizados durante todo o tratamento.

7.3. Os incidentes, notificados ou detectados, devem ser objeto de registro, com a finalidade de assegurar a manutenção do histórico e auxiliar na geração de indicadores.

7.4. A notificação de incidente, suspeito ou confirmado, poderá ser feita por qualquer usuário, sem necessidade de prévia autorização do gestor, através de requerimento ao responsável pela atividade de Tratamento e Resposta a Incidentes de Segurança da Informação.

7.5. Os usuários devem notificar, o mais breve possível, os incidentes de segurança da informação e vulnerabilidades de que tenham conhecimento (observada ou suspeita).

7.6. Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos usuários, sob o risco de violar a política de segurança da informação e/ou provocar danos aos serviços ou recursos tecnológicos.

7.7. O tratamento da informação deve ser realizado de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, com retorno das operações à normalidade no menor prazo possível, bem como evitar futuras ocorrências, com a proposição de ações de solução, quando existentes.

7.8. O responsável pela atividade de Tratamento e Resposta a Incidentes de Segurança da Informação deve conduzir investigação do incidente e de artefatos maliciosos, propondo e implementando as ações de contenção, erradicação e recuperação, comunicando as áreas afetadas e coletando os dados necessários.

7.9. A coleta de evidência dos incidentes de segurança da Informação deve ser realizada responsável pela atividade de Tratamento e Resposta a Incidentes de Segurança da Informação.

7.10. Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação, será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

7.11. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, o Comitê Gestor de Segurança da Informação de Dados e o Presidente da Câmara Municipal de Currais Novos deverão ser comunicados, para avaliação das providências cabíveis.

7.12. A avaliação do processo de gestão de incidentes de segurança da informação ocorrerá por meio do histórico de incidentes, com verificação das oportunidades de melhoria.

8. **Atualização da norma**

8.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos da Gestão de Incidentes de Segurança da Informação, observada a periodicidade prevista para a revisão da Política de Segurança da Informação.

ANEXO VIII

NSI008 - Gestão de Continuidade de TIC

1. **Objetivos**

Câmara Municipal de Currais Novos
(CNPJ: 08.470.502/0001-98)

1.1. Estabelecer as diretrizes e definir o processo de Gestão de Continuidade de Tecnologia da Informação e Comunicações, aplicáveis ao ambiente tecnológico da Câmara Municipal de Currais Novos.

2. **Motivações**

2.1. Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

2.2. Correto direcionamento e dimensionamento de recursos tecnológicos para prover a Gestão de Continuidade de TIC.

2.3. Manutenção de um nível adequado de resiliência dos serviços e sistemas de TIC críticos frente a eventos que possam causar sua interrupção, contribuindo para contínua melhoria das atividades legislativas e administrativas desempenhadas pela Câmara Municipal de Currais Novos.

2.4. Estabelecer procedimentos de gestão para assegurar a continuidade das operações de TIC.

3. **Referências normativas**

3.1. Norma ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão da Segurança da Informação;

3.2. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles genéricos de segurança da informação;

3.3. Norma Técnica ABNT NBR ISO/IEC 22301:2020, que normatiza o sistema de gestão de continuidade de negócios e especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se proteger, reduzir a possibilidade de ocorrência, preparar-se, responder e recuperar-se de incidentes de interrupção quando estes ocorrerem.

4. **Conceitos e definições**

4.1. Atividades críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade, de forma que permitam atingir os objetivos mais importantes e sensíveis ao tempo;

4.2. Análise de Impacto nos Negócios (AIN): estimativa dos impactos resultantes da interrupção de atividades e de cenários de desastres que possam afetar as atividades da Câmara Municipal de Currais Novos, bem como técnicas para quantificar e qualificar esses impactos.

4.3. Continuidade de negócios: capacidade de um órgão ou entidade de, quando ocorrer algum incidente de interrupção, manter suas operações em um nível aceitável,

previamente definido, minimizando os impactos e recuperando perdas de ativos da informação das atividades críticas;

4.4. Desastre: incidente que tenha causado algum dano grave, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo superior ao aceito pela organização;

4.5. Estratégia de continuidade: abordagem de um órgão ou entidade que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior;

4.6. Gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem;

4.7. Plano de Continuidade: conjunto de procedimento documentados que orientam a organização, após a interrupção, em como responder, recuperar, retomar e restaurar para um nível predefinido de operação, composto por Plano de Continuidade Operacional e Plano de Recuperação de Desastres;

4.8. Plano de Continuidade Operacional (PCO): documento que descreve procedimentos operacionais e técnicos a serem realizados frente a determinados cenários de falha, para manutenção dos serviços, ainda que em um nível mínimo de operacionalidade;

4.9. Plano de Recuperação de Desastres (PRD): documento que descreve procedimentos técnicos, focado em ativos e serviços tecnológicos, a serem realizados frente a determinados cenários de falhas dos principais serviços de TIC, visando o retorno à normalidade;

4.10. Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;

4.11. RPO (*Recovery Point Objective*): ponto em que a informação usada por uma atividade deve ser restaurada para permitir a operação da atividade na retomada; e

4.12. RTO (*Recovery Time Objective*): tempo máximo para retorno operacional de um serviço ou processo de negócio após a ocorrência de um desastre.

5. **Diretrizes**

5.1. A gestão de continuidade de TIC visa a:

a) reduzir o risco de interrupções dos serviços e sistemas de TIC que suportam as atividades críticas da Câmara Municipal de Currais Novos, minimizando o impacto decorrente de tais eventos adversos;

b) manter os sistemas e serviços críticos de TIC em um nível minimamente operável e aceitável durante a ocorrência de um desastre, de forma a não interromper as atividades da Câmara Municipal de Currais Novos;

c) definir procedimentos para que as atividades críticas operem em nível de contingência quando da ocorrência de um desastre ou interrupção não programada, até que a situação retorne à normalidade.

5.2. A gestão de continuidade de TIC deve observar o resultado das análises de riscos de TIC e da análise de impacto de negócio realizadas, de forma a nortear as estratégias de continuidade.

5.3. Será elaborado o Plano de Continuidade de TIC, com vistas a documentar os procedimentos necessários à operação em nível de contingência e as comunicações necessárias, bem como o retorno à normalidade, quando da ocorrência de interrupções dos serviços e sistemas de TIC.

5.4. Devem ser fornecidos recursos humanos, tecnológicos e financeiros para a manutenção e melhoria contínua da gestão de continuidade de TIC.

6. **Processo de Gestão de Continuidade de TIC**

6.1. O processo de Gestão de Continuidade de TIC é composto pelas seguintes etapas:

a) planejamento: compreende a análise dos processos críticos para o negócio, a fim de estabelecer quais atividades da SETIC são essenciais para prestação dos serviços, quais deverão ser tratadas na Continuidade de TIC e quais estratégias serão utilizadas durante a ocorrência de um incidente;

b) execução: abrange a elaboração ou revisão dos planos pelas equipes técnicas, com a descrição dos cenários de falhas e os procedimentos técnicos para lidar com os problemas, a aprovação dos planos, seu armazenamento e divulgação;

c) verificação: abrange a realização de testes periódicos dos planos desenvolvidos e a análise dos incidentes críticos ocorridos (desastres) a fim de subsidiar a etapa de melhoria; e

d) melhoria: compreende a identificação das oportunidades de melhoria e seu encaminhamento à consideração superior, com vistas a dar início a novo ciclo do processo.

6.2. O processo será revisto anualmente ou em menor prazo, quando necessário, e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência, objeto de imediata divulgação na forma do item anterior.

7. **Plano de Continuidade de TIC**

7.1. O Plano de Continuidade de TIC é composto pelos Planos de Continuidade Operacional e Planos de Recuperação de Desastres.

7.2. O Plano de Continuidade de TIC deve ser periodicamente testado, de forma a garantir sua efetividade.

7.3. O Plano de Continuidade de TIC deve ser revisado no mínimo uma vez por ano ou, ainda, em função dos resultados de testes realizados ou após mudança significativa nos ativos de informação (infraestrutura tecnológica, processo, atividades etc.).

7.4. O Plano de Continuidade de TIC será acionado quando verificadas interrupções parciais ou totais que impactem nas atividades críticas da Câmara Municipal de Currais Novos.

7.5. Ocorrido o incidente, considerados os serviços, sistemas ou ativos afetados e a criticidade, as equipes técnicas responsáveis acionarão os Planos de Continuidade Operacional para a manutenção da continuidade das atividades, ainda que de forma contingencial, e os Planos de Recuperação de Desastre para retorno das atividades à normalidade.

7.6. A comunicação às partes interessadas observará as orientações contidas nos Planos de Continuidade Operacional.

7.7. Os ativos e serviços afetados pelo incidente serão monitorados pelas equipes responsáveis, a fim de subsidiar o fornecimento de informações à autoridade superior.

7.8. A ativação do Plano de Continuidade de TIC será encerrada quando da comunicação de retorno à normalidade dos serviços, sistemas ou ativos afetados.

8. **Atualização da Norma**

8.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de Gestão de Continuidade de TIC, observada a periodicidade prevista para a Política de Segurança da Informação.

Rua Vivaldo Pereira de Araújo, n.º 161, Centro – Telefone: (84) 3412–1567
59.380-000 Currais Novos/RN – E-mail: camaracurraisnovos@hotmail.com

Publicado por:
YCLEYBER TRAJANO DA SILVA
Código Identificador: 00528204