



SISTEMA DE CONTROLO INTERNO

MCI 12 - SISTEMAS DE INFORMAÇÃO

Índice

Abreviaturas e Acrónimos	3
Objetivo.....	4
Contexto Normativo e Requisitos Gerais.....	5
Gestão de Acessos	7
Segurança das Redes e Sistemas de Informação	8
Regras de Utilização dos Recursos Tecnológicos.....	10
Utilização da Internet.....	11
Utilização do correio eletrónico (e-mail).....	13
Tratamento da Informação Digital.....	14

Abreviaturas e Acrónimos

MCI – Manual de Controlo Interno

Objetivo

O objetivo deste Manual de Controlo Interno – MCI.12 – Sistemas de Informação é estabelecer princípios e procedimentos de controlo que garantam o adequado cumprimento das condições de gestão dos ambientes informáticos do Município de Celorico da Beira, de modo a garantir o funcionamento adequado e o desenvolvimento contínuo dos sistemas de informação e das infraestruturas tecnológicas, atendendo às necessidades identificadas e proporcionando suporte eficiente aos processos e serviços do Município.

Contexto Normativo e Requisitos Gerais

- i. Este Manual de Controlo Interno (MCI) está em conformidade com a Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço e que estipula:
 - a) A definição dos requisitos de segurança para a Administração Pública, incluindo a implementação e o cumprimento de medidas técnicas e organizativas adequadas e proporcionais aos riscos que afetam as redes e sistemas de informação utilizados;
 - b) O estabelecimento de procedimentos para a notificação de incidentes, impondo que qualquer incidente com impacto significativo na segurança das redes e sistemas de informação seja comunicado ao Centro Nacional de Cibersegurança dentro dos prazos estabelecidos neste diploma;
 - c) Para avaliar a relevância do impacto de um incidente, devem ser considerados os seguintes fatores:
 1. O número de utilizadores afetados;
 2. A duração do incidente;
 3. A extensão geográfica da área afetada pelo incidente.
- ii. O Decreto-Lei n.º 65/2021, de 30 de junho, regulamenta o Regime Jurídico da Segurança do Ciberespaço e estabelece as obrigações relativas à certificação em Cibersegurança, em cumprimento do Regulamento (EU) 2019/881 do Parlamento Europeu, de 17 de abril de 2019;
- iii. Foi publicado no Diário da República, 2.ª série, o Regulamento n.º 183/2022, de 21 de fevereiro, que especifica os procedimentos técnicos para a comunicação e reporte de informações sobre os pontos de contacto permanentes, responsáveis pela segurança, inventário de ativos, relatórios anuais e notificações de incidentes;
- iv. O serviço responsável pelos sistemas de informação tem a incumbência de identificar as necessidades do Município e, com base nisso, elaborar planos para o desenvolvimento dos sistemas de gestão e informação;
- v. No seguimento do ponto anterior, o serviço responsável pelos sistemas de informação também deve garantir o acompanhamento e controlo da execução dos planos de desenvolvimento mencionados;

- vi. Deve ser assegurada a proteção dos dados pessoais e conformidade das aplicações informáticas do Município, bem como das bases de dados utilizadas, de acordo com a legislação em vigor sobre a proteção de dados.

Gestão de Acessos

- i. O serviço responsável pela gestão de recursos humanos deve, sempre que possível, comunicar ao serviço responsável pelos sistemas de informação, com antecedência de 5 dias úteis, sobre a entrada de um novo colaborador;
- ii. O acesso aos recursos do Município será concedido aos colaboradores com a disponibilização dos meios necessários, como computadores, ligações em rede, áreas de armazenamento, periféricos, aplicações e credenciais de acesso (login e password) reconhecidas pelos sistemas em uso, após a atribuição do número mecanográfico pelo serviço responsável pela gestão de recursos humanos;
- iii. O responsável por cada serviço municipal deve indicar ao serviço responsável pelos sistemas de informação quais os acessos necessários para cada colaborador, conforme as seguintes diretrizes:
 - a) Cada colaborador terá acesso apenas às aplicações informáticas necessárias para o desempenho das suas funções;
 - b) O tipo de utilizador será determinado conforme as funções desempenhadas pelo trabalhador e as operações informáticas mais comuns no exercício dessas funções;
 - c) Cada colaborador deve criar uma password única, composta por letras maiúsculas, minúsculas, números e caracteres especiais, com pelo menos oito caracteres, não podendo ser o mesmo nome do login. A password não poderá ser repetida por um período de 12 meses, deve ser escolhida pelo trabalhador e deve ser do seu exclusivo conhecimento.
- iv. Após a validação da proposta de acesso, o serviço responsável pelos sistemas de informação realizará o registo do perfil de utilizador nas aplicações, anotando a data da operação na proposta;
- v. Deverá ser implementado um processo de alteração periódica de password, a fim de prevenir o uso indevido dos acessos;
- vi. Quando houver necessidade de alteração de utilizador, o processo seguirá o mesmo procedimento que foi utilizado para a definição inicial do acesso;

- vii. Quando um colaborador perder o vínculo com a Câmara Municipal ou for transferido para outro serviço, o serviço responsável pela gestão de recursos humanos deve informar o serviço responsável pelos sistemas de informação com 5 dias úteis de antecedência. Com essa informação, deverão ser realizados os seguintes procedimentos:
- a) Será realizada uma cópia de segurança de todos os arquivos armazenados no computador do colaborador, após a sua autorização para o acesso;
 - b) O acesso ao e-mail (se aplicável) será removido, tornando-o inativo em caso de término de vínculo;
 - c) O login de utilizador será desativado, e as permissões de acesso aos diferentes subsistemas de informação municipal serão revogadas;
 - d) A conta de acesso à rede interna ficará inativa por um período de três meses, sendo apagada após esse prazo, caso o vínculo do colaborador termine.

Segurança das Redes e Sistemas de Informação

- i. Os sistemas informáticos devem incluir procedimentos de segurança e controlo adequados, garantindo que o registo automático das operações seja realizado de maneira correta e dentro do prazo estabelecido;
- ii. Para cada aplicação, deve ser designado um responsável pela criação das cópias de segurança, bem como pela definição da periodicidade dessas cópias;
- iii. No que se refere à gestão da rede, deverá ser nomeado um responsável máximo pelos sistemas de informação, único e sem restrições no acesso e controlo de todas as aplicações;
- iv. A proteção da integridade e confidencialidade dos dados informáticos deve ser garantida adequadamente;
- v. Os colaboradores do Município de Celorico da Beira devem manter a confidencialidade sobre as instalações e equipamentos informáticos da

autarquia, salvo quando houver autorização específica para a divulgação, e não devem partilhar tais informações com entidades externas;

- vi. A cada utilizador de computador será atribuído um nome de utilizador e password únicos, que não devem ser partilhados, sendo ainda obrigatória a alteração periódica da password;
- vii. O nome de utilizador e a password são pessoais e intransmissíveis, sendo responsabilidade de cada colaborador garantir a sua proteção;
- viii. Sempre que um colaborador se ausentar do seu local de trabalho, não deve deixar o computador ligado à rede com a password já inserida. A sessão de trabalho deve ser bloqueada ou o computador deve ser desligado;
- ix. Apenas o serviço responsável pelos sistemas de informação, ou outro serviço autorizado, pode realizar configurações ou modificações nos equipamentos informáticos;
- x. O serviço responsável pelos sistemas de informação, ou outro responsável autorizado, deverá realizar verificações, em datas aleatórias, nos subsistemas informáticos que possam gerar ou que estejam a gerar outputs, com o objetivo de identificar possíveis erros no sistema;
- xi. Caso sejam identificadas irregularidades, o serviço responsável pelos sistemas de informação deve corrigir os problemas com os respetivos serviços envolvidos;
- xii. Em casos de má utilização, danos intencionais, furtos ou acessos não autorizados a dados ou equipamentos, sejam realizados pelo próprio utilizador ou por terceiros, o serviço responsável pelos sistemas de informação deve tomar as medidas necessárias para assegurar a integridade da infraestrutura informática do Município e reportar os incidentes superiormente;
- xiii. Para proteger os dados informáticos, todos os computadores são equipados com programas antivírus que são atualizados regularmente através de uma plataforma centralizada na cloud.

Regras de Utilização dos Recursos Tecnológicos

- i. O Município de Celorico da Beira disponibiliza aos seus colaboradores diversos equipamentos, máquinas e aplicações informáticas para a realização das suas atividades profissionais. O uso desses recursos é, em regra, restrito a fins relacionados com as funções atribuídas a cada trabalhador;
- ii. As aplicações ou sistemas que não sejam de uso livre (freeware) estão devidamente licenciados para uso interno, através de contratos de licenciamento ou licenças avulsas. É proibido o uso de qualquer software que não tenha sido instalado pelo serviço responsável pelos sistemas de informação, que é encarregue da gestão das licenças e instalações das aplicações;
- iii. Não é permitida a instalação de qualquer software que não esteja devidamente licenciado pelo Município de Celorico da Beira;
- iv. Os utilizadores estão proibidos de copiar, adaptar, atualizar ou modificar qualquer software instalado no seu posto de trabalho, e serão responsabilizados por qualquer alteração realizada. Caso, devido a uma vulnerabilidade no sistema ou outro motivo, o utilizador infrinja esta norma, poderá ser responsabilizado pelas penalidades que o Município de Celorico da Beira venha a enfrentar, em decorrência de ações legais movidas pelos detentores dos direitos autorais dos programas não autorizados ou de outras obras intelectuais protegidas;
- v. O uso de equipamentos que não sejam propriedade do Município de Celorico da Beira para se conectar à sua infraestrutura informática, como computadores portáteis, tablets, smartphones, entre outros, pode comprometer a Segurança da Informação. Portanto, o trabalhador deve solicitar autorização ao serviço responsável pelos sistemas de informação, que avaliará a possibilidade de permitir essa conexão;
- vi. Durante o uso dos computadores e periféricos pertencentes ao Município de Celorico da Beira, caso o utilizador enfrente dúvidas ou problemas com os equipamentos ou aplicações informáticas, deve entrar em contacto com o serviço responsável pelos sistemas de informação;
- vii. A cedência temporária de equipamentos será realizada com base na disponibilidade e mediante solicitação ao serviço responsável pelos

sistemas de informação, que formalizará o processo com um auto de entrega, conforme o modelo a ser definido;

- viii. Em relação ao uso do correio eletrónico, devem ser seguidos procedimentos específicos para garantir a segurança do sistema, incluindo:
- a) O uso do endereço do e-mail institucional para fins pessoais é proibido;
 - b) Não é permitido o uso de contas de e-mail pessoais nos clientes de e-mail instalados nos computadores do Município;
 - c) Todos os anexos recebidos por e-mail devem ser analisados por uma ferramenta antivírus antes de serem abertos;
 - d) Caso seja recebido um e-mail com um link para ser aberto, os colaboradores devem evitar clicar diretamente no link. Em vez disso, devem copiar o endereço URL do link e colá-lo no navegador de internet ou, preferencialmente, digitar o endereço diretamente no navegador;
 - e) As intervenções técnicas nos sistemas serão, sempre que possível, realizadas remotamente, exceto em situações que exijam uma intervenção presencial.

Utilização da Internet

- i. O acesso a redes externas, incluindo a Internet, é essencial para o desenvolvimento de várias atividades relacionadas com as competências de cada serviço do Município. Assim, o uso da Internet deve ser direcionado para consultar informações ou plataformas relevantes para essas atividades;
- ii. O acesso à Internet (páginas, sites e portais) na infraestrutura informática do Município de Celorico da Beira está sujeito a monitorização e filtragem;

- iii. O objetivo da monitorização e filtragem do tráfego é garantir que os utilizadores sigam as regras estabelecidas neste regulamento, além de proteger a infraestrutura contra ameaças à segurança da informação;
- iv. A navegação em sites não diretamente relacionados com a atividade profissional do utilizador não é proibida, mas deve ser feita de maneira equilibrada e responsável, garantindo a segurança e a boa performance no trabalho;
- v. No entanto, é estritamente proibido aceder a conteúdos inadequados, como por exemplo:
 - a) Conteúdos com imagens sexualmente explícitas ou material relacionado;
 - b) Conteúdos que promovam atividades ilegais;
 - c) Conteúdos que incentivem intolerância ou discriminação contra outros.
- vi. O serviço responsável pelos sistemas de informação é o encarregado de gerir as redes Wi-Fi do Município;
- vii. Os utilizadores não devem publicar na Internet ou na Intranet qualquer material que possa ser considerado impróprio, ofensivo ou desrespeitoso para outras pessoas, ou que de alguma forma possa prejudicar a imagem do Município;
- viii. Não é permitido executar programas de fontes duvidosas ou desconhecidas;
- ix. Ao realizar downloads ou uploads de materiais na Internet, deve-se garantir que a propriedade intelectual ou os direitos autorais do material sejam respeitados;
- x. É expressamente proibido:
 - a) Aceder sites com conteúdos pornográficos, pedófilos, violentos, xenófobos, racistas, discriminatórios, jogos de azar ou qualquer conteúdo ilegal ou ofensivo;
 - b) Distribuir software pirata ou dados não autorizados, ou partilhar materiais sujeitos a direitos autorais sem a devida permissão;
 - c) Utilizar a Internet para espalhar vírus, "worms", "cavalos de Troia" ou qualquer outro código malicioso;
 - d) Usar o acesso à Internet para vender produtos ou serviços;

- xi. O serviço responsável pelos sistemas de informação deve realizar operações de monitorização do uso da Internet, com o objetivo de obter uma visão quantitativa e qualitativa do tráfego gerado, além de identificar situações de uso inadequado ou abusivo da Internet.

Utilização do correio eletrónico (e-mail)

- i. O correio eletrónico é disponibilizado a todos os utilizadores e deve ser utilizado de maneira responsável e adequada, dentro do contexto das funções desempenhadas pelos colaboradores do Município de Celorico da Beira;
- ii. Todos os e-mails enviados pelos utilizadores do Município de Celorico da Beira devem incluir, no final da mensagem, uma assinatura padrão, conforme as Normas de Gestão Documental aprovadas, as quais estão disponíveis na intranet do Município;
- iii. Em seguida, estabelece-se a política referente ao uso do correio eletrónico:
 - a) Todos os e-mails enviados para destinatários externos, relacionados com assuntos oficiais do Município, devem ser enviados a partir dos endereços institucionais (seja o endereço de e-mail geral ou o endereço de e-mail do serviço específico);
 - b) Em casos excecionais e quando solicitado ou necessário por algum serviço, poderão ser criadas contas de e-mail partilhadas no serviço, que poderão ser acedidas por vários utilizadores, mas devem seguir as regras vigentes para o uso de contas institucionais;
 - c) O utilizador está ciente de que não existe uma expectativa de privacidade ao utilizar a sua conta de e-mail corporativa, e que o uso da mesma está sujeito a monitorização e filtragem de conteúdo, tanto nas mensagens recebidas e enviadas quanto na navegação pela Internet;

- d) Fica proibido o envio de qualquer e-mail que possa ser considerado impróprio, ofensivo ou desrespeitoso, ou que possa prejudicar a imagem do Município, além de mensagens que possam interferir no trabalho de outros, gerar tráfego excessivo na rede ou sobrecarregar a infraestrutura tecnológica;
 - e) A conta de e-mail corporativa não pode ser utilizada para enviar ou disseminar informações que violem a legislação em vigor, como ameaças, difamação, calúnia, injúria, racismo, pornografia infantil, entre outros conteúdos ilegais;
- iv. As mensagens de e-mail na infraestrutura informática do Município de Celorico da Beira estão sujeitas a monitorização e filtragem. Esta monitorização será realizada de forma automática e a qualquer momento, utilizando sistemas informáticos disponíveis na infraestrutura tecnológica do Município;
 - v. Como parte do processo de monitorização e filtragem, as mensagens enviadas para os endereços de e-mail do Município de Celorico da Beira poderão ser redirecionadas para outros e-mails internos, caso haja suspeita de conter conteúdo malicioso que possa comprometer a segurança da informação. Isto ocorrerá sem aviso prévio, e tanto o remetente quanto o destinatário da mensagem não serão informados sobre este redirecionamento.

Tratamento da Informação Digital

- i. Todos os documentos eletrónicos, dados e informações digitais gerados no âmbito das atividades desempenhadas pelos trabalhadores do Município de Celorico da Beira devem ser armazenados nos servidores de rede;
- ii. É proibido armazenar dados e documentos pessoais dos utilizadores (ou seja, aqueles que não são de interesse ou propriedade do Município de Celorico da Beira) nos postos de trabalho ou nos servidores de rede;
- iii. Os dados armazenados nas bases de dados usadas pelos sistemas informáticos do Município, sendo propriedade do Município, devem ser

- mantidos íntegros e invioláveis. O serviço responsável pelos sistemas de informação é o encarregado de gerir e proteger esses dados;
- iv. Todos os documentos armazenados nos servidores ou nos postos de trabalho são propriedade do Município de Celorico da Beira, e o serviço responsável pelos sistemas de informação pode monitorizá-los para controlar e otimizar o uso dos recursos de armazenamento;
 - v. O serviço responsável pelos sistemas de informação só dará suporte para recuperar dados armazenados nos servidores de rede. Não se responsabiliza pela informação armazenada nos discos dos computadores dos utilizadores, que permanece sob a responsabilidade exclusiva destes.