

RESOLUÇÃO Nº 931/2025.

**Institui a Política de Segurança da
Informação no âmbito da Câmara Municipal
de Ouro Preto e dá outras providências.**

A Mesa da Câmara Municipal de Ouro Preto, no uso de suas atribuições legais, faz saber que a Câmara Municipal aprovou e ela, em seu nome, promulga a seguinte RESOLUÇÃO:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança da Informação da Câmara Municipal de Ouro Preto – PSI-CMOP, que compreende princípios, objetivos, diretrizes, requisitos e define atribuições e instrumentos para a gestão da segurança da informação no âmbito desta Câmara.

Parágrafo único. A PSI-CMOP está alinhada aos normativos federais e estaduais vigentes e à família das normas ABNT ISO 27000 e demais normas correlatas.

Art. 2º Esta Política é de cumprimento obrigatório e aplica-se a todos os agentes públicos da Câmara Municipal de Ouro Preto, incluindo vereadores, servidores efetivos e comissionados, estagiários, prestadores de serviço e qualquer outro colaborador que, por vínculo funcional ou contratual, tenha acesso a informações sob responsabilidade da Câmara.

Art. 3º Para os fins desta Resolução, considera-se:

I - Autenticação: processo pelo qual o usuário apresenta sua identificação ao recurso computacional para obtenção de acesso válido, por meio de senha, dispositivo de segurança, biometria, entre outros;

II - Ciclo de vida dos conteúdos informacionais: compreende as etapas de criação, formalização, captura, aquisição, tratamento, armazenamento, preservação, recuperação, acesso, uso, disseminação, avaliação e destinação do conteúdo informacional da Câmara Municipal de Ouro Preto;

III - Confidencialidade: assegura que os dados sejam acessíveis somente por pessoas autorizadas, impedindo o acesso indevido, com observância das normas de sigilo e proteção de dados pessoais;

IV - Conteúdo informacional: toda informação registrada, produzida, recebida, adquirida, capturada ou colecionada pela Câmara Municipal de Ouro Preto, no desempenho de sua missão institucional;

V - Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais;

VI - Disponibilidade: assegura que as informações e os sistemas estejam acessíveis e utilizáveis sob demanda, por pessoas autorizadas;

VII - Incidente de segurança da informação: qualquer ocorrência que comprometa ou possa comprometer a confidencialidade, integridade ou disponibilidade da informação;

VIII - Informação: dados organizados que produzem significado e têm valor para a instituição;

IX - Integridade: garantia que a informação não foi alterada de forma não autorizada, preservando sua exatidão e completude;

X - Registros de segurança: registros contendo atividades dos usuários, exceções e outros eventos de segurança da informação;

XI - Risco: efeito da incerteza nos objetivos;

XII - Segurança da Informação: conjunto de medidas destinadas à proteção da informação contra acessos não autorizados, alterações indevidas, indisponibilidades e perdas acidentais ou intencionais;

XIII - Sistema de Gestão da Segurança da Informação (SGSI): conjunto que compreende estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos, pessoas e demais recursos que a organização utiliza para, de modo coordenado e com base na abordagem de riscos, tratar os temas da segurança da informação;

XIV - Usuário: toda pessoa que acessa, manipula ou trata informações institucionais ou utiliza ativos de tecnologia da informação da Câmara Municipal.

Parágrafo único. Em complementaridade, o Anexo desta Resolução contém glossário, com conceitos aplicáveis à PSI-CMOP.

CAPÍTULO II

DOS PRINCÍPIOS E DOS OBJETIVOS

Art. 4º A PSI-CMOP observará os seguintes princípios:

- I - visão abrangente e sistêmica da segurança da informação;
- II - orientação à gestão de riscos e à gestão da segurança da informação;
- III - prevenção e tratamento de incidentes de segurança da informação;
- IV - articulação entre as ações de segurança cibernética, de defesa cibernética e de proteção de dados e ativos da informação;
- V – confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas devidamente autorizadas;
- VI – integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la contra alterações indevidas, intencionais ou acidentais;
- VII - disponibilidade: garantia de acesso à informação e aos ativos correspondentes sempre que necessário;
- VIII - autenticidade: atributos que permitem atestar a proveniência, a veracidade e a fidedignidade dos conteúdos informacionais;
- IX - legalidade: garantia de que ações sejam realizadas em conformidade com os preceitos legais vigentes e que seus produtos tenham validade jurídica;
- X - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- XI - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- XII - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- XIII - livre acesso: garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- XIV - qualidade dos dados: garantia aos titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- XV - respeito aos legítimos interesses dos usuários no acesso e uso da informação;
- XVI - observância da publicidade como regra e do sigilo como exceção.

Art. 5º São objetivos da PSI-CMOP:

- I - estabelecer diretrizes e responsabilidades para a segurança da informação no âmbito institucional;
- II - implementar a governança da segurança da informação;
- III - incorporar a segurança como requisito essencial dos sistemas de informação, informatizados ou não;
- IV - minimizar riscos associados à perda, vazamento ou uso indevido de informações;
- V - assegurar o uso ético, legal e transparente das informações públicas;
- VI - promover uma cultura de segurança da informação entre todos os usuários;
- VII - fomentar a participação dos usuários na prevenção, detecção e resposta aos incidentes de segurança da informação.

CAPÍTULO III DAS DIRETRIZES

Art. 6º A implementação da segurança da informação obedecerá às seguintes diretrizes:

- I - aplicação de controles de acesso a informações e sistemas, conforme o perfil de cada usuário;
- II - classificação das informações de acordo com seu grau de sensibilidade e criticidade;
- III - registro e auditoria das atividades relacionadas ao tratamento de informações;
- IV - promoção de ações de capacitação e conscientização dos usuários;
- V - utilização de ferramentas e tecnologias atualizadas e seguras para proteção de dados e sistemas.

Art. 7º As informações geradas ou custodiadas pela Câmara Municipal de Ouro Preto serão utilizadas com finalidade institucional, vedado o uso para atender a interesses pessoais ou de terceiros.

CAPÍTULO IV DAS HIPÓTESES DE APLICAÇÃO

Seção I

Disposições Preliminares

Art. 8º São objeto de tutela da Política de Segurança da Informação, no âmbito da Câmara Municipal de Ouro Preto, dentre outros:

- I - o acesso lógico à rede corporativa;
- II - a concessão de acesso remoto à rede corporativa;
- III - a utilização de senhas dos sistemas e serviços;
- IV - o armazenamento de informações;
- V - a utilização de dispositivos móveis;
- VI - a utilização do correio eletrônico;
- VII - a utilização de estações de trabalho;
- VIII - a utilização da Internet.

Seção II

Do acesso à rede corporativa e das senhas

Art. 9º O acesso lógico, local ou remoto, aos sistemas, aplicações e serviços disponibilizados pela CMOP será feito por meio de autenticação empregando login e senha, certificado digital ou outra forma determinada pelo setor responsável pela segurança da informação.

Art. 10 É responsabilidade do usuário manter o sigilo de todas as suas senhas, que são de uso pessoal e intransferível, bem como cuidar do certificado digital, se fornecido pela CMOP.

Art. 11 Sempre que possível, será habilitado o duplo ou terceiro fator de autenticação para acesso aos sistemas, aplicações e serviços disponíveis.

Art. 12 A concessão, alteração, bloqueio de acesso lógico ao diretório Active Directory (AD) e aos sistemas e aplicações da CMOP, bem como a cessação e o cancelamento de acesso com perfil de administrador na rede corporativa e nas estações de trabalho serão realizados mediante autorização do Departamento de Tecnologia da Informação.

Art. 13 As permissões de acesso dos usuários aos sistemas da CMOP e de terceiros, quando o fato for informado ao Departamento de Tecnologia da Informação, serão:

- I - bloqueadas para os usuários em licença ou afastamento;
- II - revogadas para os aposentados, falecidos, transferidos ou desligados.

Art. 14 As conexões realizadas e os serviços disponibilizados na rede corporativa serão limitados, controlados e autorizados pela área responsável pela segurança da informação.

Art. 15 A definição das permissões de acesso dos usuários será feita exclusivamente com base na solicitação formal da chefia imediata ou da área demandante,

observando-se o princípio da necessidade e a compatibilidade com as atribuições do cargo ou da função desempenhada.

Parágrafo único. O Departamento de Tecnologia da Informação é responsável por operacionalizar os acessos conforme a solicitação recebida, não lhe competindo decidir de forma autônoma sobre o conteúdo ou abrangência dos acessos.

Art. 16 As informações dos usuários cadastrados e seus acessos à rede corporativa serão documentados, observado o tratamento dos dados pessoais estritamente necessários.

Seção III

Do armazenamento de dados e informações

Art. 17 Os servidores de arquivos disponibilizados na rede corporativa da Câmara serão utilizados exclusivamente para armazenamento de arquivos que contenham dados e informações relacionadas aos processos e negócios da Câmara Municipal.

Art. 18 A utilização do espaço nos servidores de arquivos da Câmara Municipal deve ser limitada, controlada e monitorada.

Art. 19 O armazenamento das informações corporativas será feito em diretórios disponibilizados nos servidores da rede da Câmara, com acesso restrito ao grupo de usuários que as utilizam.

Art. 20 A Câmara poderá adotar, como boa prática, o serviço de armazenamento em nuvem para dados corporativos.

Art. 21 O armazenamento de dados e informações de trabalho deverá ser preferencialmente realizado nos diretórios da rede corporativa ou nos serviços de nuvem institucionalmente autorizados, a fim de garantir a segurança, integridade e disponibilidade das informações.

§1º O armazenamento local em disco poderá ocorrer em caráter transitório ou quando tecnicamente necessário, sendo de responsabilidade do usuário garantir a posterior migração dos dados para os repositórios institucionais adequados.

§2º Cabe ao Departamento de Tecnologia da Informação orientar os usuários quanto ao uso adequado do armazenamento local, bem como adotar medidas para mitigar riscos relacionados à perda, acesso indevido ou vazamento de informações armazenadas fora dos repositórios institucionais.

Art. 22 O Departamento de Tecnologia da Informação poderá auditar a utilização do espaço disponibilizado, para identificar arquivos em desacordo com as determinações desta norma e adotar as providências cabíveis, no que lhe competir.

Seção IV

Dos dispositivos móveis

Art. 23 Os dispositivos móveis disponibilizados aos usuários, de propriedade da Câmara, são de uso restrito às atividades profissionais.

Art. 24 O Departamento de Tecnologia da Informação poderá realizar auditorias de conformidade em todos os dispositivos móveis de propriedade da Câmara, no âmbito de sua competência.

Art. 25. Recomenda-se a não utilização de dispositivos particulares na rede corporativa da Câmara.

Parágrafo único. O uso de dispositivos particulares poderá ocorrer, excepcionalmente, nos acessos realizados por meio de redes sem fio segregadas e gerenciadas pelo Departamento de Tecnologia da Informação, ou mediante uso de *Virtual Private Network – VPN*, conforme política e orientações da área de segurança da informação.

Art. 26 É de inteira responsabilidade do usuário a configuração e manutenção do dispositivo particular, bem como uso de softwares e instalações de hardwares, conforme as regras de segurança da informação definidas pela Câmara.

Art. 27 Em caso de perda, furto, roubo ou comprometimento do dispositivo que contenha informações institucionais, o usuário deverá comunicar imediatamente ao Departamento de Tecnologia da Informação, para que sejam adotadas as providências técnicas e administrativas cabíveis.

Seção V

Do Correio eletrônico

Art. 28 O serviço de correio eletrônico de caráter institucional disponibilizado aos usuários é de propriedade da Câmara, sendo seu uso obrigatório e restrito às atividades profissionais.

Art. 29 É vedada a utilização do correio eletrônico institucional para fins pessoais, atividades ilícitas, compartilhamento de conteúdos inapropriados ou alheios ao interesse público.

Art. 30 O Departamento de Tecnologia da Informação poderá monitorar o uso dos serviços de correio eletrônico institucional, como também o correio eletrônico particular, quando houver indícios de utilização com finalidade institucional.

Art. 31 Constatado o uso indevido do correio eletrônico institucional, o Departamento de Tecnologia da Informação adotará providências, como:

I – bloqueio temporário ou definitivo do acesso à conta de e-mail;

II – retenção ou exclusão de mensagens e arquivos que comprometam a segurança ou a legalidade das operações institucionais;

III – encaminhamento do caso à autoridade competente para providências disciplinares, quando necessário.

Seção VI

Da Estação de trabalho

Art. 32 O uso dos computadores das estações de trabalho disponibilizadas aos usuários deve ser restrito às atividades profissionais pertinentes aos processos e negócios da Câmara.

Art. 33 Os usuários só poderão utilizar aplicativos desktops desde que previamente homologados pelo Departamento de Tecnologia da Informação.

Art. 34 A concessão de perfil de administrador nas estações de trabalho é restrita, devendo o pedido ser formalizado pelo responsável pelo Departamento de Tecnologia da Informação.

Art. 35 O Departamento de Tecnologia da Informação poderá realizar verificação de logs e averiguar registros de conformidade nas estações de trabalho da Câmara.

Art. 36 A execução ou supervisão dos serviços de expansão, substituição ou manutenção das estações de trabalho competirá ao Departamento de Tecnologia da Informação.

Art. 37 É vedado aos usuários a aquisição e instalação de qualquer hardware ou periférico nas estações de trabalho, salvo se autorizado pelo Departamento de Tecnologia da Informação.

Seção VII

Do uso da internet

Art. 38 O serviço de internet é disponibilizado pela Câmara para execução das atividades profissionais dos usuários.

Art. 39 A Câmara poderá monitorar o uso da internet disponibilizada aos usuários, implantando recursos e programas de computador que registrem o acesso à internet e à rede corporativa.

Art. 40 Os usuários devem zelar pelo bom uso da internet, respeitando direitos autorais, regras de licenciamento de software, direitos de propriedade, privacidade e proteção de dados pessoais e de propriedade intelectual.

Art. 41 O acesso à internet pela rede corporativa deverá ser efetuado somente por dispositivos autorizados.

Art. 42 A Câmara poderá bloquear o acesso a arquivos e sites não autorizados que comprometam o uso de banda da rede ou que exponham a rede à riscos de segurança.

Art. 43 Mediante solicitação justificada do usuário, a área de Segurança da Informação poderá autorizar a utilização de outras conexões, desde que não haja comprometimento da segurança da rede da Câmara.

CAPÍTULO V

DAS RECOMENDAÇÕES E DAS RESPONSABILIDADES

Art. 44 Fica recomendado ao usuário a adoção de boas práticas de segurança da informação, tais como:

I - trocar a senha quando exigido pelo sistema ou em caso de indício de comprometimento do sistema, do serviço ou da própria senha;

II - configurar, quando disponível, o duplo fator de autenticação (DFA) no acesso aos serviços, sistemas e aplicações disponibilizados pela CMOP;

III - não utilizar a senha de acesso aos sistemas, serviços e aplicações da CMOP em ambientes externos;

IV - evitar o acesso remoto à rede corporativa da CMOP em locais públicos;

V - utilizar o crachá de identificação somente no exercício das atividades funcionais;

VI - manter a mesa de trabalho sempre limpa, sem papéis e mídias exposta;

VII - evitar discutir assuntos relacionados às atividades profissionais em locais públicos;

VIII - não abrir mensagens de correio eletrônico cujo assunto, remetente ou conteúdo sejam de origem desconhecida ou contendo links e arquivos suspeitos;

IX - não divulgar o endereço eletrônico institucional fornecido pela Câmara para recebimento de mensagens particulares, alheias aos interesses do órgão;

X - não deixar os equipamentos móveis sob sua responsabilidade desprotegidos;

XI - não armazenar arquivos que contenham informações da CMOP em equipamentos e mídias particulares;

XII - evitar alimentar-se, fumar ou ingerir líquidos próximo às estações de trabalho ou equipamentos eletrônicos de propriedade ou posse da CMOP;

XIII - evitar utilizar outro serviço de correio eletrônico que não seja o institucional nos equipamentos conectados à rede corporativa;

XIV - compartilhar assuntos de trabalho, em qualquer local, dentro ou fora do ambiente corporativo, a partir de qualquer tipo de canal, mídia, ferramenta ou tecnologia, respeitando a ética, a legislação vigente e cumprindo com seu dever de sigilo profissional, aplicando a melhor técnica disponível para garantir a segurança da informação no nível exigido pela relevância dela;

XV - tratar dados pessoais observadas as regras da Lei Federal nº 13.709, de 2018, e das normas da CMOP atinentes ao tema.

Art. 45 São responsabilidades dos usuários:

I - conhecer e cumprir integralmente todas as diretrizes e regras da Política de Segurança da Informação da Câmara, bem como os procedimentos, regulamentos e instruções de trabalho;

II - responder pelo uso de sistemas, serviços por meio de sua identificação;

III - responder pelo uso do equipamento móvel sob sua responsabilidade;

IV - utilizar obrigatoriamente os sistemas disponibilizados pela Câmara ou sistemas obrigatórios por lei comunicação institucional, vedada a finalidade privada;

V - avisar formalmente à chefia sobre:

a) a perda, o furto ou o desaparecimento de ativos da CMOP;

b) a presença de pessoas desconhecidas e sem identificação nas dependências da CMOP;

c) os incidentes de segurança da informação, registrando-os no momento da constatação do fato;

VI - apresentar à área responsável da CMOP, em caso de furto, roubo ou extravio de dispositivos móveis, o Boletim de Ocorrência Policial, no prazo máximo de 48 (quarenta e oito) horas do fato ocorrido;

VII - conscientizar o público externo acerca da importância da segurança das informações e do cumprimento do disposto nesta política;

VIII - sugerir medidas que possam elevar os níveis de segurança das instalações na sua área de atuação;

IX - devolver o crachá à área de recursos humanos ao término do contrato de trabalho, nos casos de exoneração de cargo público, término de mandato, aposentadoria ou outra hipótese de desligamento da Câmara;

X - utilizar adequadamente os recursos institucionais;

XI - guardar documentos físicos que contenham informações sigilosas ou dados pessoais de forma segura e em locais adequados;

XII - imprimir documentos, caso sejam sigilosos ou que contenham dados pessoais, utilizando impressoras com proteção por meio de senhas ou permanecer próximo à impressora, no momento de sua emissão;

XIII - zelar pela guarda do dispositivo de armazenamento do certificado digital e pela senha de acesso ao dispositivo.

CAPÍTULO VI DAS VEDAÇÕES

Art. 46 - É vedado aos usuários:

I - instalar qualquer hardware ou software em estações de trabalho e dispositivos móveis da CMOP sem a autorização formal do Departamento de Tecnologia da Informação da Câmara;

II - efetuar comodato de dispositivo móvel corporativo a terceiros;

III - divulgar dados de configuração de acesso da rede corporativa da Câmara;

IV - armazenar e acessar dados ou informações não ligados às atividades profissionais;

V - acessar, propagar ou armazenar qualquer tipo de conteúdo malicioso, malware, vírus, worms, cavalos de Troia ou programas de controle de outros computadores;

VI - tratar assuntos relacionados ao trabalho em outros softwares de comunicação instantânea, mensageiros instantâneos ou programas de computador que permitam a comunicação imediata e direta entre usuários e grupos de usuários por meio da internet, em dispositivos pessoais e na rede corporativa, exceto quando não for possível a comunicação por meio da ferramenta institucional de comunicação;

VII - fazer download de softwares não autorizadas e de mídias não ligadas às atividades profissionais;

VIII - utilizar programas de computador, utilitários ou ferramentas para burlar os mecanismos de segurança estabelecidos pela CMOP;

IX - registrar senha em meios físicos ou em qualquer outro meio que coloque em risco a sua confidencialidade;

X - fornecer a senha de acesso a qualquer sistema ou serviço da CMOP para outro usuário, autorizado ou não;

XI - acessar qualquer sistema ou serviço da CMOP por meio da identificação de outro usuário;

XII - tentar obter acesso não autorizado, como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta de acesso;

XIII - utilizar senhas compartilhadas para acesso a qualquer recurso computacional da CMOP, exceto nos casos em que seja impossível a implantação de senha individual e devidamente autorizado pela área responsável;

XIV - tentar interferir nos serviços de qualquer outro usuário, servidor ou rede, inclusive ataques do tipo negação de serviço - DoS e DDoS, provocar congestionamento em redes, tentativas deliberadas de sobrecarregar ou invadir um servidor;

XV - conectar equipamentos particulares à rede corporativa sem prévia autorização da área de segurança da informação;

XVI - acessar as estações de trabalho sem autorização do responsável pela unidade;

XVII - movimentar as estações de trabalho, periféricos e ou equipamentos de rede sem autorização do Departamento de Tecnologia da Informação;

XVIII - incluir senhas em processos automáticos, exceto se autorizado pelo Departamento de Tecnologia da Informação e desde que, comprovadamente, não haja comprometimento à segurança da informação;

XIX - armazenar informações corporativas da CMOP em diretórios públicos;

XX - utilizar serviços de nuvem pública não corporativos para armazenar informações institucionais;

XXI - desativar o antivírus instalado nos equipamentos da CMOP ou realizar qualquer alteração nas configurações da ferramenta;

XXII – realizar o compartilhamento externo de qualquer software sem a autorização expressa ou de dados sob custódia da CMOP sem a autorização do responsável competente.

XIII - utilizar redes privadas virtuais (VPNs) não autorizadas para acesso à internet ou aos sistemas da CMOP;

XXVI - realizar conexões a serviços remotos sem autorização expressa e controle técnico do Departamento de Tecnologia da Informação;

XXVII - realizar espelhamento de tela (*screen sharing*) ou transmissão de imagem de sistemas e documentos institucionais em plataformas externas sem autorização prévia.

CAPÍTULO VII

DOS AGENTES ATIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Seção I

Da Mesa Diretora, do Departamento de Tecnologia da Informação e demais unidades administrativas

Art. 47 Compete à Mesa Diretora:

- I - aprovar a Política;
- II - garantir os recursos necessários à sua execução;
- III - designar os membros do Comitê de Segurança da Informação.

Art. 48 Compete ao Departamento de Tecnologia da Informação:

- I - propor normas complementares à PSI-CMOP;
- II - implantar mecanismos de controle e proteção de ativos de informação;
- III - monitorar os acessos e registrar incidentes de segurança;
- IV - promover ações de conscientização, capacitação e orientação contínua dos usuários sobre boas práticas de segurança da informação e proteção de dados pessoais, preservadas as atribuições do Encarregado de Dados Pessoais da CMOP;
- V - avaliar tecnicamente a aquisição, o desenvolvimento e a implementação de soluções de TI, garantindo sua conformidade com a PSI-CMOP e com a LGPD;
- VI - apoiar a alta administração e as unidades organizacionais na gestão de riscos relacionados à informação e à continuidade dos serviços tecnológicos;
- VII - controlar o acesso lógico aos sistemas, redes e aplicações, garantindo o princípio do menor privilégio e a rastreabilidade das ações dos usuários;
- VIII - zelar pelo inventário, classificação e tratamento adequado dos ativos de informação sob sua responsabilidade;
- IX - elaborar relatórios e fornecer subsídios técnicos para auditorias, sindicâncias e apurações administrativas relacionadas à segurança da informação;
- X - adotar e manter ferramentas de segurança, como antivírus, *firewall*, autenticação multifator, criptografia e outras medidas que garantam a confidencialidade, integridade, disponibilidade e autenticidade das informações.

Art. 49 Compete a todas as unidades administrativas da Câmara:

- I - cumprir e fazer cumprir as diretrizes estabelecidas nesta Resolução;
- II - participar da implantação e da execução da PSI-CMOP;
- III - participar da definição dos requisitos e funcionalidades de segurança da informação dos aplicativos e sistemas de informação vinculados aos seus processos de trabalho, validando-os;
- IV - reportar incidentes ou vulnerabilidades ao Departamento de Tecnologia da Informação;
- V - zelar pela proteção das informações no âmbito dos processos de trabalho e atividades sob sua responsabilidade.

Seção II

Do Comitê de Segurança da Informação

Art. 50 Fica instituído o Comitê de Segurança da Informação - CSI, composto por representantes das seguintes unidades administrativas:

I - Presidência;

II - Diretoria-Geral;

III - Departamento de Tecnologia da Informação;

IV - Procuradoria.

§1º Os membros do Comitê serão designados por portaria.

§2º O CSI terá caráter consultivo e será responsável por propor melhorias, revisar a Política e acompanhar sua implementação.

CAPÍTULO VIII

DAS SANÇÕES E DISPOSIÇÕES FINAIS

Art. 51 O descumprimento das disposições desta Resolução sujeitará o responsável à suspensão temporária do acesso aos recursos informacionais e de comunicação da CMOP, bem como às penalidades previstas na legislação vigente e no Regimento Interno da Câmara Municipal de Ouro Preto.

Art. 52 A PSI-CMOP deverá ser revista no prazo máximo de 02 (dois) anos ou, em prazo inferior, por recomendação do Comitê de Segurança da Informação ou por deliberação da Mesa Diretora.

Art. 53 A Câmara poderá editar normas complementares para fiel execução da sua Política de Segurança da Informação.

Art. 54 Esta Resolução entra em vigor na data de sua publicação.

Ouro Preto, Patrimônio Cultural da Humanidade, 18 de dezembro de 2025, trezentos e quatorze anos da Instalação da Câmara Municipal e quarenta e cinco anos do Tombamento.

Registrada e publicada nesta Secretaria em 18 de dezembro de 2025.

Vantuir Antônio da Silva
Presidente da Câmara Municipal de Ouro Preto

Renato Zoroastro
1º Secretário

Projeto de Resolução nº 980/25

Autoria: Mesa Diretora (Vantuir, Renato, Kuruzu e Alex)

ANEXO

(a que se refere o parágrafo único do art. 3º)

GLOSSÁRIO

1. Acesso lógico: acesso à rede, aos sistemas e às informações da Câmara;
2. Acesso remoto: conexão à distância entre um dispositivo isolado (terminal ou microcomputador) e uma rede;
3. Active Directory (AD): implementação de serviço de diretório (pasta) que armazena informações sobre objetos em rede de computadores e disponibiliza essas informações aos usuários e administradores desta rede;
4. Administrador de Sistemas: pessoa responsável pela gestão dos usuários das aplicações e sistemas, sejam eles desktops ou web;
5. Aplicativo de Desktop: software ou aplicação que precisa ser instalado ou acessado diretamente pelo sistema operacional independente da sua funcionalidade;
6. Antivírus: programa de segurança com a finalidade de prevenir, fazer a varredura, detectar e excluir vírus de um computador, com o objetivo de aumentar a segurança, para fornecer proteção em tempo real contra-ataques de vírus;
7. Auditoria de segurança da informação: procedimento que avalia a gestão da segurança da informação, o controle dos ativos e os riscos envolvidos, considerados de forma efetiva pela organização, abordando aspectos de confidencialidade, integridade e disponibilidade contidos nos conceitos de segurança lógica e física;
8. Backup ou cópia de segurança: procedimento de cópia de dados de um dispositivo de armazenamento para outra fonte segura que poderá ser utilizada futuramente;
9. Certificado digital: arquivo eletrônico que contém dados de uma pessoa física ou jurídica, assinado digitalmente por uma Autoridade Certificadora, utilizados para comprovar sua identidade, armazenado em mídia física, denominada token, dispositivo de hardware ou armazenamento em nuvem, possibilitando o acesso à

- assinatura digital por meio de computador ou dispositivo móvel com acesso à internet;
10. *Cloud computing* (computação em nuvem): Modelo de computação que permite acesso remoto, via internet, a recursos e serviços de tecnologia, como armazenamento, processamento e aplicações, hospedados em ambientes externos à organização;
 11. Compartilhamento de tela (*screen sharing*): Recurso tecnológico que permite transmitir, em tempo real, o conteúdo exibido na tela de um dispositivo para outro, podendo representar risco se feito sem autorização ou em ambientes inseguros;
 12. Dado pessoal: informação relacionada à pessoa natural identificada ou identificável;
 13. Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
 14. Desktop virtual: infraestrutura em nuvem composta por sistemas operacionais e aplicativos em que o ambiente de desktop é separado do dispositivo físico usado para acessá-lo, podendo ser acessados de forma remota, a partir de qualquer dispositivo com acesso à internet;
 15. Diretrizes: regras de alto nível que representam os princípios básicos incorporados na gestão de uma organização, conforme sua visão estratégica, e que orientam normas e procedimentos complementares;
 16. Disco local: disco rígido físico que armazena dados em um computador, sendo a unidade C, ou o disco local C, o disco primário ativo no sistema;
 17. Duplo fator de autenticação (DFA): componente de gestão de acesso que requer que os usuários provem a sua identidade utilizando pelo menos dois fatores de verificação diferentes antes de acessarem websites, aplicações móveis ou outros recursos online, protegendo com uma barreira adicional para romper antes de obter acesso à conta alvo, nos casos em que um fator é comprometido por um invasor;

18. Engenharia social: Conjunto de técnicas utilizadas por agentes mal intencionados para manipular pessoas a fim de obter informações confidenciais ou acesso indevido a sistemas e recursos.
19. Equipamento móvel: equipamento com capacidade de processamento e armazenamento de dados, passível de utilização por usuários em trânsito, como notebooks, tablets e telefones inteligentes (smartphones), bem como equipamentos similares;
20. Equipamento particular: todo dispositivo que não é fornecido institucionalmente para o desenvolvimento das atividades profissionais;
21. Estação de trabalho: equipamentos disponibilizados no ambiente de trabalho com a finalidade de execução das atividades profissionais em local fixo, com a capacidade de comunicação em rede, como desktops e equipamentos móveis;
22. Ferramenta de colaboração: solução digital pautada em tecnologias móveis, como a computação em nuvem, a telefonia e as *Application Programming Interfaces (APIs)*, com o objetivo principal de promover comunicação efetiva e integrada, seja entre membros de um time corporativo, entre colaboradores e clientes ou mesmo entre usuários de serviços;
23. *Firewall*: sistema de segurança de rede que monitora e controla o tráfego de entrada e de saída da rede com base em regras de segurança pré-determinadas, e que, geralmente, estabelece uma barreira de segurança entre uma rede interna confiável e outra rede externa, como a internet, que se assume não segura ou confiável;
24. Gestão de continuidade do negócio: conjunto de planos e procedimentos necessários para a recuperação efetiva de um incidente, minimizando ao máximo os impactos à organização;
25. Gestão de mudanças: processo que torna mais fácil para a organização distribuir solicitações de mudança em sua infraestrutura de tecnologia da informação – TI, apoiando a solicitação, priorização, autorização, aprovação, programação e implementação de quaisquer mudanças, sejam elas simples ou complexas, contribuindo para controlar os riscos e reduzir ao mínimo as interrupções nos serviços;

26. Gestão de riscos: conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos com o intuito de conferir razoável segurança quanto ao alcance dos objetivos institucionais;
27. Intranet: rede interna, de uso corporativo, que utiliza a mesma tecnologia da internet, para que os usuários possam acessar as informações das suas organizações;
28. Logs: registros contínuos que contém a data e a hora de determinado evento, além de mensagem criada automaticamente pelos softwares e sistemas de TI, com o objetivo de documentar as ações realizadas nos sistemas e possibilitar a rastreabilidade das ações realizadas;
29. Mecanismos de proteção: barreiras que impedem ou limitam o acesso à informação, propiciando um ambiente controlado, seguro e disponível, geralmente eletrônico, evitando que a informação esteja exposta à exclusão, divulgação, alteração ou acesso não autorizado por indivíduo mal-intencionado;
30. Política de segurança da informação: conjunto de definições, diretrizes, restrições e requisitos que servem para nortear o uso de boas práticas no trato com os ambientes, recursos e ativos computacionais, em aspectos físicos, lógicos e de pessoal, com a finalidade de proporcionar maior segurança às informações;
31. Perfil de administrador: permissão que possibilita modificar as configurações de um computador, inclusive as de segurança, instalar e remover softwares e acessar qualquer arquivo existente na máquina;
32. *Ransomware*: Tipo de software malicioso que restringe o acesso ao sistema infectado, geralmente criptografando os dados e exigindo um resgate para restaurar o acesso.
33. Rede corporativa: infraestrutura de tecnologia da informação projetada para facilitar a comunicação, o compartilhamento de recursos e informações, e a execução de operações administrativas dentro da entidade governamental, garantindo a segurança dos dados e o cumprimento das regulamentações governamentais;
34. Serviço de correio eletrônico: sistema de mensageria utilizado na internet, que tem a função de possibilitar o envio e o recebimento de mensagens entre usuários, grupos ou sistemas computacionais;

35. Teletrabalho: regime de trabalho no qual a atividade laboral é executada, no todo ou em parte, em local diverso daquele estabelecido para a realização do trabalho presencial, mediante a utilização de tecnologias de informação e de comunicação que permitam a execução remota das atribuições inerentes ao cargo, função ou atribuições desenvolvidas pela unidade de exercício do servidor;
36. Termo de responsabilidade: Documento formal assinado pelo usuário ou colaborador que atesta o conhecimento e o compromisso com as normas de segurança da informação da instituição, incluindo o uso adequado dos recursos tecnológicos.
37. *Virtual Private Network (VPN)*: forma de comunicação que permite que uma ou mais máquinas acessem uma rede privada, utilizando como infraestrutura as redes públicas, tais como a internet, nas quais os dados trafegam na rede de forma segura, utilizando encapsulamento, criptografia e autenticação.