

INSTRUÇÃO NORMATIVA N.º 002/2022

A Diretoria Executiva da Empro Tecnologia e Informação, no uso de suas atribuições legais previstas no Estatuto Social da empresa, especialmente no seu artigo 23, inciso X, dispõe sobre a Classificação de Informações da EMPRO, nos termos dos arts. 25 e seguintes da Lei Federal n.º 12.527/2011 e dá outras providências.

CONSIDERANDO:

- A Lei de Acesso à Informação (LAI), Lei nº 12.527, de 18 de novembro de 2011, garante ao cidadão o acesso às informações produzidas ou custodiadas pela Administração Pública, estabelecendo procedimentos que visam garantir que estas informações estejam disponíveis de maneira ampla à sociedade;
- Por princípio, a divulgação é a regra e o sigilo, a exceção. Portanto, na excepcionalidade, a LAI vem proteger as informações que, em situações especiais, não poderão ser divulgadas ou não poderão estar acessíveis por prazos estabelecidos;
- Da cadeia de valores da **EMPRO** destacamos a Transparência como um dos pilares da gestão responsável onde se busca disponibilizar informações e comunicar ações e decisões, observadas as restrições legais ou estratégicas, de modo a permitir que a sociedade acompanhe a atuação da empresa;
- Em linha, portanto, as ações e os resultados institucionais devem se pautar na preocupação e no zelo com a avaliação, o tratamento e a divulgação de informações, tanto na proteção correta daquelas classificadas em grau de sigilo, como na promoção do direito de acesso àquelas consideradas públicas.
- A necessidade de regulamentar o procedimento de classificação de Informações da EMPRO, nos termos dos artigos 25 e seguintes da Lei nº 12.527/2011.

RESOLVE:

1. DEFINIÇÕES

- ❖ **Agente público** – todo aquele que exerce, ainda que transitoriamente ou sem

Empro Tecnologia e Informação

Endereço: Av. Romeu Strazzi, 199, Vila Sinibaldi - CEP 15084-010 - São José do Rio Preto-SP
Telefone: (17) 3201 1200 Home Page: www.empro.com.br E-mail: falecomaempro@empro.com.br

remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública;

❖ **Autenticidade** – qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

❖ **Ciclo de vida da informação** – ciclo formado pelas fases da produção e recepção, organização, uso, disseminação e destinação;

❖ **Classificação da informação** – atribuição de grau de sigilo às informações nos termos da Lei nº 12.527/2011, Lei de Acesso à Informação (LAI);

❖ **Confidencialidade** – garantia de que a informação é acessível somente por usuários autorizados;

❖ **Dados processados** – dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;

❖ **Desclassificação** – cancelamento da classificação atual de uma informação pela autoridade competente ou por transcurso de prazo;

❖ **Disponibilidade** – qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

❖ **Documento** – unidade de registro de informações, qualquer que seja o suporte ou formato, ou seja, todo registro físico (papéis, etc.), virtual (prints, telas, imagens, etc.) ou eletrônico (programas, códigos fonte, etc.), sujeito ou não à classificação de sigilo;

❖ **Documento preparatório** – documento formal utilizado como fundamento da tomada de decisão ou de ato administrativo, a exemplo de pareceres e notas técnicas;

❖ **Informação** – dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

❖ **Informação ostensiva** – em oposição à informação sigilosa, é qualquer informação não submetida à restrição de acesso público;

❖ **Informação pessoal** – informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;

❖ **Informação restrita** – informações classificadas como sigilosas (reservada, secreta ou ultrassecreta) ou consideradas de acesso restrito nos termos da Lei de Acesso à Informação ou protegidas pelas demais hipóteses legais de sigilo e restrição.

❖ **Informação sigilosa** – informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

❖ **Integridade** – qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;

❖ **Marcação** – ação de inscrever, no documento ou repositório, o grau de sigilo associado à informação sigilosa, classificada ou não;

❖ **Primariedade** – qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações;

❖ **Tratamento da informação** – conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

❖ **Reclassificação** – alteração da classificação da informação pela autoridade classificadora;

❖ **Termo de Classificação de Informação (TCI)** – formulário que formaliza a decisão de classificação, desclassificação, reclassificação ou alteração do prazo de sigilo de informação classificada em qualquer grau; expediente interno dirigido à Presidência propondo a classificação de sigilo de determinado documento;

❖ **Termo de Confidencialidade** – termo pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei.

2. DIRETRIZES GERAIS

2.1. Além dos princípios básicos que regem a Administração Pública, os procedimentos apresentados nesta Norma devem ser executados em conformidade com as seguintes diretrizes:

- Observância da publicidade como preceito geral e do sigilo como exceção;
- Toda informação institucional da **EMPRO**, em quaisquer suportes, materiais, áreas, comunicações e sistemas de informação institucionais, é patrimônio da empresa e deve ser tratada segundo os preceitos descritos nesta Norma e nos termos da legislação pertinente em vigor;
- O tratamento da informação sigilosa deve ser realizado de modo ético e responsável pelos agentes públicos;
- O tratamento da informação sigilosa deve ser feito assegurando-se os requisitos da disponibilidade, integridade, confidencialidade e autenticidade da informação;

- É dever do agente público salvaguardar a informação sigilosa e a informação pessoal, bem como assegurar a publicidade da informação ostensiva, utilizando-as, exclusivamente, para o exercício das atribuições de cargo, emprego ou função pública, sob pena de responsabilização administrativa, civil e penal;
- As medidas e os procedimentos relacionados ao tratamento da informação a serem realizados com apoio de empresa terceirizada devem ser estabelecidos contratualmente para que se assegure o cumprimento das diretrizes previstas nesta Norma, bem como em legislações vigentes; e
- A **EMPRO** promoverá ações para conscientização dos seus agentes públicos visando à disseminação das diretrizes de tratamento da informação sigilosa.

3. TRATAMENTO E CICLO DE VIDA DA INFORMAÇÃO

3.1. O tratamento da informação sigilosa na **EMPRO** abrangerá as políticas, os processos, as práticas e os instrumentos utilizados para lidar com a informação ao longo de cada fase de seu ciclo de vida.

3.2. O ciclo de vida da informação é composto pelas seguintes fases:

- Produção e Recepção – Fase inicial do ciclo de vida. Compreende a produção, recepção ou custódia e classificação da informação;
- Organização – Refere-se ao armazenamento, arquivamento e controle da informação;
- Uso e Disseminação – Refere-se à utilização, acesso, reprodução, transporte, transmissão e distribuição da informação; e
- Destinação – Fase final do ou eliminação ciclo de vida da informação, que compreende a avaliação e a destinação da informação.

3.3. Esta Norma busca esclarecer os aspectos legais e operacionais de cada uma dessas fases no que se refere a documentos sigilosos.

4. PRODUÇÃO E RECEBIMENTO DE INFORMAÇÕES SIGILOSAS NO ÂMBITO DA EMPRO

4.1. Os documentos e informações produzidos ou custodiados no âmbito da **EMPRO** deverão ser avaliados com vistas à eventual necessidade de classificação em grau de sigilo.

4.2. Da mesma forma, os documentos que forem recebidos na **EMPRO**, com indicativo de restrição de acesso, deverão receber o mesmo tratamento e cuidado para terem o sigilo resguardado.

4.3. Estão sujeitas à classificação em grau de sigilo:

- Informações classificadas como reservadas, secretas ou ultrassecretas, nos termos dos artigos 23 e 24 da LAI.

4.4. Estão sujeitas à restrição de acesso:

- Informações pessoais - art. 31 da LAI;
- Documentos preparatórios que embasem decisões de política de segurança da informação;
- Documentos contendo Códigos Fonte;
- Informações sigilosas protegidas por legislação específica;
- Informações cuja divulgação possa representar vantagem competitiva a outros agentes de tecnologia da informação e comunicação (TIC);

5. INFORMAÇÕES PESSOAIS

5.1. As informações pessoais relativas à intimidade, à vida privada, à honra e à imagem terão acesso restrito a agentes públicos legalmente autorizados e à pessoa a que se referirem, independentemente da classificação de sigilo, pelo prazo máximo de cem anos a contar da data de sua produção.

5.2. Desta forma, estas informações sofrerão restrição de acesso sem a necessidade de receber o tratamento dado às informações classificadas em grau de sigilo (elaboração de Termo de Classificação de Informação e demais procedimentos previstos em lei).

5.3. Caso o titular das informações pessoais esteja morto ou ausente, o direito assistirá ao cônjuge ou companheiro, aos descendentes ou ascendentes, conforme o disposto no parágrafo único do art. 20 da Lei nº 10.406/2002.

5.4. As informações pessoais devem ser tratadas de forma transparente e com respeito às liberdades e garantias individuais e o seu acesso deve observar o prescrito nos artigos 55 a 62 do Decreto nº 7.724/2012, garantindo, entre outros, os seguintes aspectos:

- Restrição de acesso a agentes públicos autorizados;
- Acesso limitado a terceiros mediante autorização prévia do titular;
- Observância do direito de acesso ao cônjuge, ascendentes e descendentes;
- Respeito aos direitos fundamentais de privacidade, intimidade e proteção à imagem;
- Inexistência de restrição de acesso em caso de apuração de irregularidades ou levantamento de fatos históricos;
- Devido processo legal; e
- Responsabilidade do agente público.

5.5. Exemplos de informações consideradas pessoais:

- Número de documentos de identificação pessoal (rg, cpf, título de eleitor);
- endereço pessoal;
- Número de telefone pessoal;
- Informações referentes a alimentandos, dependentes ou pensões;
- Informações médicas;
- Orientação sexual, filiação sindical, partidária ou a organizações de caráter religioso, filosófico ou político.

6. DOCUMENTO PREPARATÓRIO PARA EMBASAR DECISÕES

6.1. Os documentos preparatórios são aqueles que fundamentam a tomada de decisão ou a elaboração de ato administrativo e seu acesso é restrito somente às pessoas que tenham a necessidade funcional de conhecer seu conteúdo.

6.2. Caracterizam-se por conter informações que, se divulgadas antes do ato administrativo, podem gerar impactos negativos.

6.3. As tipologias recomendadas na **EMPRO** são a nota técnica e o parecer. Porém não há restrição a outros tipos documentais desde que contenham informações necessárias ao embasamento do ato decisório ou administrativo.

7. VANTAGEM COMPETITIVA A OUTROS AGENTES

7.1. Ficarão sujeitos à restrição de acesso, embora não sejam objeto de classificação, os documentos e as informações cuja divulgação possa representar vantagem competitiva a outros agentes de tecnologia da informação e comunicação (TIC).

8. CLASSIFICAÇÃO COM BASE EM LEGISLAÇÃO ESPECÍFICA

8.1. Toda informação classificada em grau de sigilo é, também, sigilosa, porém nem toda informação sigilosa será classificada em grau de sigilo, uma vez que esta contém informações com acesso restringido em virtude de uma legislação específica.

8.2. É fundamental esclarecer os conceitos “informação sigilosa” e “informação classificada em grau de sigilo” e o que as diferencia. Ambos os termos estão em oposição à informação ostensiva, ou seja, aquela que deve ser mantida acessível ao cidadão.

8.2.1. INFORMAÇÃO SIGILOSA:

É a informação que, por algum motivo previsto em lei, deverá ter o seu acesso restrito.

8.2.2. INFORMAÇÃO CLASSIFICADA EM GRAU DE SIGILO:

8.2.2.1. Refere-se a um tipo específico de informação sigilosa que tem sua restrição amparada pelos art. 23 e 24 da Lei de Acesso à Informação – LAI e para estas deverá ser elaborado o termo de classificação de informação – TCI.

8.2.2.2. São consideradas sigilosas as informações protegidas em legislação específica. A exemplo das informações pessoais, terão também restrição de acesso sem a necessidade de receber o tratamento dado às informações classificadas em grau de sigilo, como a elaboração de Termo de Classificação de Informação - TCI e demais procedimentos previstos em lei.

8.2.2.3. Com base na LAI, a informação pública somente poderá ser classificada como sigilosa quando for considerada imprescindível à segurança da sociedade (à vida, segurança, saúde da população) ou do Estado (soberania nacional, relações internacionais, atividades de inteligência). Como a divulgação é a regra e o sigilo, a exceção, a Lei só abre espaço para classificação da informação cuja divulgação ou acesso irrestrito possa:

- Pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
- Prejudicar ou pôr em risco a condução de negociações ou as relações do País, do Estado ou do Município;
- Prejudicar ou pôr em risco informações fornecidas em caráter sigiloso por outras entidades privadas ou órgãos públicos;
- Pôr em risco a vida, a segurança ou a saúde da população;
- Oferecer elevado risco à segurança da informação do município;

8.3. Exemplos de informações sigilosas protegidas por legislação específica:

- Segredo de justiça – código de processo civil, código de processo penal e outros;
- Sigilo decorrente de direitos autorais – lei 9.610/98;
- Sigilo empresarial: sigilo das sociedades anônimas (lei 6.404/76) e sigilo decorrente de risco à governança empresarial (decreto 7.724/12).
- Processo administrativo disciplinar em curso.
- Prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional, estadual ou municipal;
- Pôr em risco a segurança de instituições ou de autoridades e seus familiares;
- Comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

9. PRAZOS DE RESTRIÇÃO DE ACESSO À INFORMAÇÃO

9.1. O prazo da restrição de acesso à informação começará a contar a partir da data de

produção do documento/processo e não da data de sua classificação.

9.2. A LAI prevê:

PRAZOS MÁXIMOS DE RESTRIÇÃO DE ACESSO À INFORMAÇÃO:

- **INFORMAÇÃO CLASSIFICADA EM GRAU ULTRASSECRETO** – vinte e cinco anos, podendo ser prorrogada por mais vinte e cinco anos;
- **INFORMAÇÃO CLASSIFICADA EM GRAU SECRETO** – quinze anos, sem possibilidade de prorrogação; e
- **INFORMAÇÃO CLASSIFICADA EM GRAU RESERVADO** – cinco anos, sem possibilidade de prorrogação.

9.3. Alternativamente aos prazos citados, poderá ser estabelecida, como termo final de restrição de acesso, a ocorrência de determinado evento, observados, sempre, os prazos máximos de classificação. É o que acontece, por exemplo, com os documentos preparatórios, os quais perdem o grau de sigilo no instante da edição do ato ao qual deram fundamento.

10. CLASSIFICAÇÃO DE SIGILO NO ÂMBITO DA EMPRO

10.1. São competentes para indicar o nível de classificação de informações com grau de sigilo os gerentes de área.

10.2. São competentes para decidir sobre a classificação de informações com grau de sigilo os servidores ocupantes dos seguintes cargos:

- No mínimo 02 Diretores em conjunto, vedada a classificação individual.

10.3. A autoridade que classificar um documento ou uma informação possui competência para desclassificar ou reduzir o prazo de sigilo, mediante provocação ou de ofício.

10.4. Ao desclassificar, reclassificar ou reduzir prazo de sigilo, deve ser dada ciência a todos os órgãos e entidades pelas quais a informação tenha tramitado.

10.5. Os documentos ou informações a serem classificados como secreto ou ultrassecreto deverão ser encaminhados pelo titular da Secretaria, acompanhados do despacho fundamentado e do Interno com titulação "Termo de Classificação de Informação (TCI)" preenchido, em papel, ao Diretor Presidente da **Empro**.

10.6. A classificação do documento será colocada à apreciação na próxima Reunião Ordinária de Diretoria Executiva, com registro em Ata.

11. OPORTUNIDADE DA CLASSIFICAÇÃO

11.1. Quando uma informação já circular por outro órgão e, eventualmente, pela internet, deve-se avaliar cuidadosamente a efetividade da imposição de sigilo.

8

Empro Tecnologia e Informação

Endereço: Av. Romeu Strazzi, 199, Vila Sinibaldi - CEP 15084-010 - São José do Rio Preto-SP
Telefone: (17) 3201 1200 Home Page: www.empro.com.br E-mail: falecomaempro@empro.com.br

11.2. Desta forma, a restrição de acesso deve ser imposta tão logo o documento seja criado.

11.3. Se necessário, e como exceção, a classificação poderá ser realizada em momento posterior. Nesse caso, será dada ciência a todos os órgãos e entidades pelos quais a informação tenha tramitado.

12. OUVIDORIA DA EMPRO

12.1. Nas demandas dirigidas à Ouvidoria ou a outro mecanismo de contato com a sociedade, os documentos e as informações deverão ser avaliados para efeito de eventual classificação, sem prejuízo da observância dos prazos e procedimentos de resposta a demandas dessa natureza, estabelecidos pela LAI.

13. FLUXO PARA CRIAR DOCUMENTO CLASSIFICADO

13.1. O critério para classificação de uma informação produzida pela **EMPRO** deve restringir-se ao indispensável, considerando que é adotado como preceito geral a publicidade, restando ao sigilo o papel de exceção.

13.2. Serão classificados como sigilosos:

- As Informações amparadas nos termos dos art. 23 e 24 da Lei nº 12.574/2011 – LAI, e
- Documentos preparatórios que contenham decisões de segurança da informação ou projetos de TIC essenciais a qualquer órgão público municipal.

13.3. Em ambos os casos, é obrigatória a indicação da justificativa para classificação de sigilo.

13.4. A relação de informações classificadas deverá ser elaborada por cada Gerência da empresa em modelo padrão próprio de planilha e encaminhada para sua Diretoria, que se responsabilizará pela apresentação na reunião subsequente de Diretoria Executiva.

13.5. A aprovação da classificação deverá constar de Ata de Reunião da Diretoria Executiva, bastando a aprovação por, no mínimo, 02 (dois) diretores.

13.4. Após a aprovação pela Diretoria Executiva, a planilha será encaminhada para o setor de Administração da empresa, que se encarregará de sua guarda, manutenção e atualização nos mesmos moldes do realizado com o sistema de patrimônio.

Modelo de planilha/extrato de classificação de informações:

EXTRATO DE CLASSIFICAÇÃO DE INFORMAÇÕES									
GRAU DE SIGILO									
RESERVADO:	cinco anos, sem possibilidade de prorrogação								
SECRETO:	quinze anos, sem possibilidade de prorrogação								
ULTRA SECRETO:	vinte e cinco anos, podendo ser prorrogada por mais vinte e cinco anos								
TIPO DE SIGILO									
CLASSIFICAÇÃO:	estabelecer Grau de Sigilo								
RECLASSIFICAÇÃO:	revisar Grau de Sigilo								
DESCLASSIFICAÇÃO:	retirar sigilo								
CATEGORIA									
ADMINISTRATIVA:	documento de cunho administrativo								
TÉCNICA:	documento de cunho técnico								
Gerência:	_____								
ANO:	202...								
Nº DE ORDEM - CÓDIGO	Nº DA ATA DE DIRETORIA	DATA DA ATA	TÍTULO DA INFORMAÇÃO	CATEGORIA	GRAU DE SIGILO	TIPO DE SIGILO	PRAZO EM ANOS	DATA INÍCIO	FUNDAMENTO DA DECISÃO - DISPOSITIVO LEGAL
001/202									
002/202									
003/202									
004/202									
Diretor Presidente		Diretor Administrativo			Diretor de Desenvolvimento				

13.5. O sistema de controle de classificação de informações também poderá ser realizado através de sistema informatizado próprio, à critério da Diretoria Executiva, também nos mesmos moldes do sistema de patrimônio.

13.6. O Interno TCI (Termo de Classificação de Informação) sempre acompanhará o documento principal (planilha física) e deverá conter o histórico dos eventos e justificativas relativos à classificação, ratificação, desclassificação ou reavaliação do grau de sigilo da informação.

13.7. No processo classificado como sigiloso, todos os documentos que o compõem serão sigilosos independentemente de serem classificados.

14. CREDENCIAIS DE ACESSO A DOCUMENTO/PROCESSO SIGILOSO

14.1. O documento/processo classificado como sigiloso estará disponível somente àqueles que possuírem credencial/autoridade de acesso.

14.2. A credencial de acesso é automaticamente concedida ao autor do documento, à Diretoria Executiva, ao Encarregado de Dados/Compliance, ao Controlador Geral Interno e aos Advogados da empresa. O autor do documento ou autoridade com acesso poderão conceder credencial de acesso a outro servidor para que este possa acessar o documento/processo.

14.3. Em qualquer tempo, a credencial de acesso poderá ser revogada por quem a concedeu ou o servidor credenciado poderá renunciá-la.

14.4. Não é possível a disponibilização de acesso externo a processos categorizados como sigilosos, e estes não ficarão disponíveis para consulta pública.

15. LEMBRETES: DOCUMENTO/PROCESSO RESTRITO:

15.1. Não há necessidade do processo ser tarjado de vermelho para ser classificado como restrito.

15.2. É obrigatória a indicação da hipótese legal.

15.3. No processo classificado como restrito, todos os documentos que o compõem serão restritos independentemente de serem classificados.

15.4. O documento/processo classificado como restrito ficará disponível a todos os servidores com autoridade de acesso.

16. EXPEDIÇÃO DE DOCUMENTOS SIGILOSOS

16.1. Para a expedição de documentos sigilosos devem ser observados os seguintes procedimentos especiais que visam proteger a informação ou o documento classificado:

- Acondicionar os documentos em envelopes duplos (um envelope dentro de outro envelope);
- Informar, no envelope externo, os dados do destinatário: nome completo, cargo e endereço completo. Neste envelope não deve ter qualquer informação relacionada ao sigilo do documento;
- Informar, no envelope interno, de forma legível e destacada, a indicação de "Documento Sigiloso", incluindo o grau de sigilo (quando classificado). Este envelope deve trazer novamente todas as informações que identifiquem o destinatário, como no envelope externo;
- Nos casos de documento de interesse exclusivo do destinatário, no envelope interno deve haver a indicação da palavra "PESSOAL"; e
- O envelope interno deverá ser fechado e expedido mediante recibo onde constará o remetente, o destinatário e número que identifique o documento.

16.2. Já os envelopes internos contendo a marca "PESSOAL" somente poderão ser abertos pelo destinatário.

16.3. A tramitação de documento classificado em grau de sigilo deve ser realizada pessoalmente e entregue em mãos ao destinatário.

17. TRAMITAÇÃO E COMUNICAÇÃO DE DOCUMENTOS SIGILOSOS

17.1. Na tramitação de um documento com informação classificada, seja por expediente ou correspondência, o responsável pelo atendimento (protocolo) deverá cumprir alguns procedimentos especiais:

- Verificar a integridade do meio de recebimento e conferir os dados do destinatário;
- Abrir o envelope externo, conferir os dados do remetente no envelope interno, bem como a identificação de “documento sigiloso”;
- Providenciar a entrega, em mãos, ao destinatário citado no envelope, com registro de entrega; e
- Se for observado indício de violação ou de irregularidade, o responsável pelo atendimento deve registrar o fato e comunicar o chefe imediato e o destinatário, que deverão informar imediatamente ao remetente.

17.2. O destinatário, ao receber a informação, deverá informar ao remetente o recebimento do expediente, no prazo mais curto possível.

17.3. O envelope interno somente será aberto pelo destinatário, seu representante autorizado ou autoridade hierarquicamente superior.

18. ACESSO, USO E DISSEMINAÇÃO DE INFORMAÇÕES SIGILOSAS

18.1. Ao se tornar sigilosa, a informação precisa estar revestida de cuidados no seu manuseio. Quanto menos pessoas tiverem acesso ao seu conteúdo, mais fácil será garantir o sigilo.

18.2. Dessa forma, é importante limitar a geração, o acesso, a divulgação e o tratamento dessa informação, classificada ou não, às pessoas que tenham necessidade de conhecê-la por dever de ofício e que sejam devidamente autorizadas pelo titular da unidade organizacional responsável por sua guarda e manipulação.

18.3. Os cuidados devem ser tomados, inclusive, nas reuniões em que são produzidas ou manipuladas as informações sigilosas. Aqui, deverão ser adotados controles de segurança para o acesso ao ambiente, aos documentos, às anotações, às mídias e aos demais recursos utilizados.

18.4. Cuidados adicionais deverão ser tomados com os arquivos temporários, manuscritos e anotações que forem gerados durante o processo de produção da informação sigilosa. Estes devem ser eliminados ao final da reunião.

18.5. MESMO SENDO AUTORIZADO O ACESSO, AO TOMAR CONHECIMENTO DE INFORMAÇÃO SIGILOSA, O SERVIDOR CRIA PARA SI A OBRIGAÇÃO DE RESGUARDAR O SIGILO, PODENDO SER RESPONSABILIZADO EM CASO DE USO INDEVIDO OU VAZAMENTO.

18.6. Nos casos em que pessoa física ou entidade privada precisarem executar atividade de tratamento de informação sigilosa mantida pela **EMPRO** deverão ser adotadas todas as providências necessárias para que seus empregados, contratados, prepostos ou representantes observem as condições de sigilo.

18.7. Para tanto, deve ser assinado um Termo de Confidencialidade, no qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei.

19. DISSEMINAÇÃO E REPRODUÇÃO DE INFORMAÇÃO SIGILOSA

19.1. A reprodução total ou parcial de informação sigilosa deve ser precedida de autorização expressa ou da autoridade que a classificou ou de autoridade hierarquicamente superior com igual prerrogativa.

19.2. Ressalta-se que a reprodução terá o mesmo grau de sigilo do documento original.

19.3. O responsável pela reprodução deverá ser agente credenciado ou ter assinado o Termo de Confidencialidade e deve manter o sigilo da operação, providenciando a eliminação de notas manuscritas, carbonos, provas ou qualquer outro recurso, que possam dar origem a cópia não-autorizada do todo ou parte.

19.4. Por fim, caso a preparação, a impressão ou a reprodução de informação classificada em qualquer grau de sigilo seja efetuada em tipografia, impressora, oficina gráfica ou similar, a operação deverá ser acompanhada por servidor oficialmente designado, ou agente que tenha assinado o Termo de Confidencialidade, tornando-se responsável pela garantia do sigilo durante a confecção do documento.

20. CELEBRAÇÃO DE CONTRATOS

20.1. O Decreto nº 7.845/2012 traz observações sobre a celebração de contrato, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção, cujo objeto contenha informação sigilosa ou cuja execução envolva informação sigilosa. Explicita ainda que tal ato estará condicionado à assinatura do Termo de Confidencialidade e ao estabelecimento de cláusulas contratuais que prevejam os seguintes requisitos:

- Obrigação de manter sigilo relativo ao objeto e a sua execução;
- Possibilidade de alteração do objeto para inclusão ou alteração de cláusula de segurança não estipulada previamente;
- Obrigação de adotar procedimentos de segurança adequados, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto;
- Identificação, para fins de concessão de credencial de segurança e assinatura do Termo de Confidencialidade, das pessoas que poderão ter acesso a informação classificada em qualquer grau de sigilo e material de acesso restrito;

- Obrigação de receber inspeções para habilitação de segurança e manutenção;
- e
- Responsabilidade em relação aos procedimentos de segurança, relativa à subcontratação, no todo ou em parte.

21. CICLO DE VIDA DA INFORMAÇÃO SIGILOSA

21.1. A fase final do ciclo de vida da informação engloba sua avaliação e destinação.

22. DESCLASSIFICAÇÃO, REAVALIAÇÃO E REVISÃO DE INFORMAÇÃO SIGILOSAS

22.1. Existem três possibilidades de uma informação classificada como sigilosa deixar de sê-la:

- Por decurso do prazo indicado no ato da classificação. Nesses casos, a desclassificação é automática e não carece de comando de qualquer autoridade.
- Por consumação do evento que definiu o seu termo final. Por exemplo, se um documento for classificado como sigiloso por servir como fundamento de uma política de TIC, tão logo a política econômica torne-se pública, automaticamente o documento sigiloso será desclassificado.

22.1. Após reavaliação feita pela autoridade classificadora ou por autoridade hierarquicamente superior, mediante provocação ou de ofício. Além da desclassificação, essa reavaliação poderá dar origem a uma redução de prazo ou até mesmo à sua prorrogação.

22.3. Na reavaliação, serão observados o prazo máximo de restrição de acesso à informação, conforme os termos da LAI, a permanência das razões da classificação e a possibilidade de danos decorrentes da divulgação ou acesso irrestrito da informação. O novo prazo de restrição manterá como termo inicial a data da produção da informação.

22.4. Quando da desclassificação, reclassificação ou alteração de prazo de sigilo da informação classificada, deve-se formalizar um novo Interno TCI (Termo de Classificação de Informação), que seguirá anexo ao termo que o precede, a fim de manter o histórico da classificação.

23. DESTINAÇÃO FINAL

23.1. O documento de guarda permanente com informação classificada em qualquer grau de sigilo deverá ser encaminhado, em caso de desclassificação, ao Arquivo Geral para fins de organização, preservação e acesso.

23.2. Na **EMPRO**, caberá à Diretoria Executiva a responsabilidade de propor o destino final das informações e documentos desclassificados.

23.3. **RESSALTA-SE QUE ENQUANTO OS DOCUMENTOS PERMANECEREM CLASSIFICADOS COM GRAU DE SIGILO NÃO DEVERÃO SER ELIMINADOS.**

24. ROL DE INFORMAÇÕES CLASSIFICADAS E DESCLASSIFICADAS

24.1. A **EMPRO** deve divulgar, anualmente, lista das informações classificadas e desclassificadas em grau de sigilo em seu sítio na internet, conforme estabelece o art. 45 do Decreto Nº 7.724/2012.

25. RESPONSABILIZAÇÃO

25.1. A legislação vigente prevê que o agente público poderá ser responsabilizado nos casos em que obstruir acesso à informação ostensiva e nos que divulgar informação sigilosa.

25.2. O art. 65 do Decreto nº 7.724/2012 elucida condutas que podem ser consideradas ilícitas e que ensejam responsabilidade do agente público, a saber:

- Recusar-se a fornecer informação requerida nos termos do Decreto, retardar deliberadamente o seu fornecimento ou fornecê-la intencionalmente de forma incorreta, incompleta ou imprecisa;
- Utilizar indevidamente, subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda, a que tenha acesso ou sobre que tenha conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública;
- Agir com dolo ou má-fé na análise dos pedidos de acesso à informação;
- Divulgar, permitir a divulgação, acessar ou permitir acesso indevido a informação classificada em grau de sigilo ou a informação pessoal;
- Impor sigilo à informação para obter proveito pessoal ou de terceiro, ou para fins de ocultação de ato ilegal cometido por si ou por outrem;
- Ocultar da revisão de autoridade superior competente informação classificada em grau de sigilo para beneficiar a si ou a outrem, ou em prejuízo de terceiros;
- Destruir ou subtrair, por qualquer meio, documentos concernentes a possíveis violações de direitos humanos por parte de agentes do Estado.

26. EXTRAVIO DE INFORMAÇÕES

26.1. Ao constatar extravio de documento ou informação sigilosa, é dever de qualquer agente público comunicar o ocorrido, com urgência, à chefia imediata ou ao responsável pela custódia do documento ou da informação.

26.2. Da mesma forma deverá agir o servidor que encontrar ou tiver conhecimento de documento ou informação sigilosa extraviado.

27. DÚVIDAS E CASOS NÃO TRATADOS

27.1. As dúvidas e os casos não abordados nesta Norma poderão ser encaminhados à Diretoria Executiva da **EMPRO**.

Esta Norma entrará em vigor após aprovação em ata da Diretoria Executiva da EMPRO e publicação por meio de sua interação na intranet e site da empresa, revogadas as disposições em contrário.

São José do Rio Preto (SP), 17 de outubro de 2022.



Angelo Bevilacqua Neto
Diretor-Presidente



João Pereira Curado Junior
Diretor Administrativo e Financeiro



Domingos Correa
Diretor de Desenvolvimento e Tecnologia