PORTARIA Nº 424

Institui a Política de Segurança da Informação - PSI, no âmbito da SEMA.

O SECRETÁRIO DE ESTADO DE MEIO AMBIENTE no uso de suas atribuições legais que lhe confere o art. 71, inciso IV e VIII, da Constituição Estadual c/c a Lei Complementar nº 214, de 23 de junho de 2005, que cria a Secretaria de Estado de Meio Ambiente;

Considerando as competências atribuições ao Assessor Chefe I na Portaria n.º 387, de 03 de maio de 2016;

Art. 1º O presente documento tem por objetivo instituir a Política de Segurança da Informação - PSI no âmbito da Secretaria do Meio Ambiente - SEMA do Estado do Mato Grosso - MT, em complemento a Política estabelecidas pelo COSINT - Conselho Superior do Sistema Estadual de Informação e Tecnologia da Informação - instituídas pela resolução nº 003/2010.

Capítulo I

ESCOPO

Seção I

Objetivo da Política de Segurança da Informação

Art. 2º A PSI objetiva garantir a confidencialidade, integridade, disponibilidade e autenticidade - CIDA das informações produzidas ou custodiadas pela SEMA.

Art. 3º A SEMA deve observar as diretrizes, normas, procedimentos, mecanismos, competências e responsabilidades estabelecidas nesta PSI.

Art. 4º Integram também a PSI as normas e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

Art. 5º As diretrizes de Segurança da Informação - SI devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e estrutura da SEMA.

Seção II

Abrangência

Art. 6º As diretrizes, normas complementares e manuais de procedimentos da PSI da SEMA aplicam-se a servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, execute atividades vinculadas a esta Secretaria.

Parágrafo único. Todos são responsáveis e devem estar comprometidos com a segurança da informação.

Art. 7º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pela SEMA devem atender a esta PSI.

Art. 8º Esta política também se aplica, no que couber, ao relacionamento da SEMA com outros órgãos e entidades públicos ou privados.

Capítulo II

CONCEITOS E DEFINIÇÕES

Art. 9º No âmbito da PSI considera-se:

I - ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

II - ativos de informação: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

III - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

IV - capacitação em SI: Desenvolvimento de aptidões, habilidades e conhecimentos mínimos em SI para o desempenho de suas funções.

V - classificação da informação Identificação, pelo gerador da informação, do seu nível de classificação para uso dos controles de proteção necessários.

VI - Comitê de Segurança da Informação - CSI: colegiado de caráter deliberativo e multidisciplinar responsável pela normatização e supervisão da segurança da informação no âmbito da SEMA. Em caso de não existência, o CSI deverá ser estabelecido no prazo de 90 dias à partir da data de publicação da PSI;

VII - confidencialidade: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada e credenciada;

VIII - conscientização em SI: saber o que é segurança da informação e aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema;

IX - controle de acesso: conjunto de normas, procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

X - custodiante do ativo de informação: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que lhe pertencem ou não, mas que estão sob sua custódia;

XI - disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade;

XII - gestão de ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

XIII - gestão de continuidade dos negócios: processo de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem.

XIV - gerenciamento de operações: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporta, satisfazendo os acordos de níveis de serviço;

XV - gestor dos ativos de informação: responsável por gerenciar determinado ativo de SI;

XVI - incidente de SI: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XVII - informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XVIII - infraestrutura de TI: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica;

XIX - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XX - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

XXI - recursos criptográficos: sistemas, programas, processos e equipamento isolado ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

XXII - risco de SI: 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;

XXIII - segurança física e do ambiente: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;

XXIV - sensibilização em SI: disponibilizar conhecimento em SI para capacitar os envolvidos em tomar decisões ou reagir em SI; - sistema estruturante: conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente;

XXV - terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos a SEMA;

XXVI - tratamento de incidentes: é a atividade de receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança;

XXVII - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição,

armazenamento, eliminação e controle da informação, inclusive as sigilosas; e,

XXVIII - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Capítulo III

PRINCÍPIOS

Art. 10. A PSI deve obedecer aos princípios constitucionais, administrativos e do arcabouço legal vigente que regem a Administração Pública Federal, Estadual e Municipal.

Capítulo IV

DIRETRIZES GERAIS

Art. 11. O cumprimento desta política de segurança e de suas normas complementares deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente constituído pelo Comitê de Segurança da Informação - CSI, buscando a certificação do cumprimento dos requisitos de segurança da informação;

Art. 12. Cabe ao Comitê de Segurança da Informação - CSI, convocar as reuniões de deliberação da PSI, instituir programas permanentes e regulares de conscientização, sensibilização e capacitação em SI, buscando também parcerias com outros órgãos e entidades.

Art. 13. Os órgãos e entidades da Secretaria de Meio Ambiente devem adotar ou utilizar esta PSI e suas normas complementares como modelos de referência para elaboração dos seus documentos.

Art. 14. As unidades administrativas da SEMA devem elaborar as normas peculiares de SI conforme suas atividades e submetê-la ao CSI;

Art. 15. Todo e qualquer incidente de SI ocorrido no âmbito da SEMA e demais órgão correlatos, devem ser formalmente comunicados ao Presidente do CSI.

Art. 16. Os membros da estrutura do CSI devem elaborar e gerenciar o plano de capacitação especializada nas disciplinas relacionadas à SI.

Art. 17. O CSI deve auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias da Secretaria e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

Art. 18. O CSI, com auxílio da CTI, deve planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança de tecnologia da informação.

Art. 19. A SEMA, além das diretrizes estabelecidas nesta PSI, deve também se orientar pelas melhores práticas e procedimentos de SI recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 20. É vetado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas ou custodiadas pela SEMA.

Parágrafo Único. O CSI deverá elaborar norma de descarte de informações.

Art. 21. O custodiante do ativo de informação deve ser formalmente designado pelo gestor do ativo de informação.

Parágrafo único. A não designação pressupõe que o gestor é o próprio custodiante.

Art. 22. Os contratos firmados pela SEMA devem conter cláusulas que determinem a observância da PSI e suas normas respectivas.

Art. 23. O CSI deverá propor à Direção da SEMA normas para regulamentação da computação em nuvem, ouvida a CTI.

Capítulo V

DIRETRIZES ESPECÍFICAS

Art. 24. Para cada uma das diretrizes constantes das seções deste capítulo devem ser elaboradas normas específicas, manuais e procedimentos conforme especialização de cada área da SEMA.

Seção I

Da Gestão de Ativos da Informação

Art. 25. Os ativos de informação devem:

I - ser inventariados e protegidos;

II - ter identificados os seus proprietários e custodiantes;

III - ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

IV - ter a sua entrada e saída nas dependências da SEMA autorizadas e registradas por autoridade competente;

V - ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de meios que permitam a rastreabilidade do uso desses ativos;

VI - ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 26. O CSI, ou comitê especialmente designado, deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 27. Os recursos tecnológicos, instalações de infraestrutura e os sistemas de informação da SEMA devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 28. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite a termo de sigilo e responsabilidade.

Seção II

Da Segurança em Recursos Humanos

Art. 29. Os usuários devem ter ciência:

I - das ameaças e preocupações relativas à SI; e

II - de suas responsabilidades e obrigações no âmbito desta PSI.

Art. 30. Todos os usuários devem difundir e exigir o cumprimento da PSI, das normas de segurança e da legislação vigente acerca do tema.

Art. 31. Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os usuários da SEMA e que apoie esta PSI de acordo com suas competências funcionais.

Art. 32. Do controle de acesso às informações de pessoal:

I - é de responsabilidade do titular da Coordenadoria de Gestão de Pessoas a proposição de normas de acesso a informações de pessoal da SEMA; e

II - deve estabelecer controles de perfis, permissões e procedimentos necessários para a salvaguarda da SI.

Seção III

Da Gestão de Operações

Art. 33. O CSI, com apoio da CTI, deve estabelecer normas adequadas, relacionados à SI de tecnologia da informação para a disponibilização dos serviços, sistemas e infraestrutura de TI que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais da SEMA.

Seção IV

Dos Controles de Acessos

Art. 34. Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.

Art. 35. Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 36. Os usuários da SEMA são responsáveis por todos os atos praticados com suas identificações, sejam digitais ou físicas.

Art. 37. A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

Art. 38. A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela informação.

Art. 39. Todos os sistemas de informação da SEMA, automatizados ou não, devem ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações.

Art. 40. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento da SEMA.

Art. 41. Os sistemas estruturantes devem possuir normas específicas, no âmbito de sua atuação, que requerem o controle de acesso quanto:

I - ao acesso às suas bases de dados;

II - à extração, carga e transformação de dados; e,

III - aos serviços acessíveis via linguagem de programação.

Art. 42. Os sistemas estruturantes devem possuir mecanismos automáticos para:

I - revogar as concessões e desativar as contas de acesso do servidor nos casos de exoneração, demissão, aposentadoria e falecimento do servidor;

II - criação automática de “log” de acessos, com informações suficientes para inequívoca identificação de qual usuário fez o acesso, quais transações realizou;

III - bloquear as contas de acesso do servidor nos casos de férias, licença, afastamento - mesmo que temporário, cessão e disponibilidade; e

IV - tratar os casos de remoção e redistribuição do servidor, segundo as definições constantes na norma de controle de acesso ao sistema.

Art. 43. É responsabilidade do Coordenador de Gestão de Pessoas disponibilizar, de imediato, os registros de todas as movimentações de pessoal referenciadas no art. 51 na forma definida por norma complementar elaborada pela Coordenadoria de Gestão de Pessoas.

Parágrafo Único. O CSI deverá prover recursos específicos para a elaboração de um sistema para cadastro, alteração ou exclusão de servidores dos acessos à informação, em até 180 (cento e oitenta dias) da publicação desta PSI.

Seção V

Da Criptografia

Art. 44. O uso de recursos criptográficos interfere na Confidencialidade, Integridade, Disponibilidade e Autenticidade das informações, sendo, portanto, responsabilidade do CSI a implementação dos procedimentos relativos ao seu uso, no âmbito das informações produzidas e custodiadas na SEMA, em conformidade com as orientações contidas em norma específica.

Art. 45. O usuário é responsável pelo recurso criptográfico que receber, devendo assinar Termo de Responsabilidade e Confidencialidade pelo seu uso.

Seção VI

Da Aquisição, do Desenvolvimento e da Manutenção de Sistemas

Art. 46. A estrutura da CTI deve estabelecer critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção, em até 180 dias.

Art. 47. O processo de aquisição de sistemas e aplicações corporativas deve atender requisitos de segurança previstos em norma específica

Seção VII

Da Conformidade

Art. 48. Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de SI da SEMA e de suas unidades administrativas com esta PSI e suas normas e procedimentos complementares, bem como com a legislação específica de SI.

§ 1º: É de responsabilidade do CSI essa verificação, sendo responsável pela alocação de recursos, mesmo que externos, para a execução desta atividade;

§ 2º: O CSI estabelecerá o escopo da análise de risco e conformidade para o período determinado;

Art. 49. A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com a SEMA.

Art. 50. A verificação da conformidade da SI de tecnologia da informação será realizada de forma planejada, mediante calendário de ações proposto pela CTI e aprovado pelo CSI.

Art. 51. O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos identificados ou percebidos.

Art. 52. Nenhuma unidade administrativa poderá permanecer sem verificação de conformidade de suas práticas de SI por período superior a 2 (dois) anos.

Art. 53. A execução da verificação de conformidade será realizada pelo CSI e com o apoio da CTI para o escopo de tecnologia da informação podendo, com a prévia aprovação do CSI, ser subcontratada no todo ou em parte.

Art. 54. É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

Art. 55. A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

Art. 56. Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo Gestor de SI ao Gestor da unidade administrativa verificada, para ciência, ficando a cargo deste as iniciativas para tratamento das vulnerabilidades eventualmente apresentadas.

Seção VIII

Do Plano de Investimentos em SI da SEMA

Art. 57 Os investimentos em SI serão realizados anualmente, de forma planejada e consolidados em um plano de investimentos.

Art. 58 O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco.

Art. 59. Os investimentos em SI constituirão ação orçamentária específica e permanente na Lei Orçamentária Anual, distinta das outras ações orçamentárias;

Art. 60. O plano de investimentos, assim como a correspondente proposta orçamentária, será aprovado pelo CSI, mediante recomendação elaborada pela CTI no escopo de tecnologia da informação.

Seção IX

Da Propriedade Intelectual

Art. 61. As informações produzidas por servidores, colaboradores e prestadores de serviços, no exercício de suas funções, são patrimônio intelectual da SEMA, sujeitas à política de classificação da informação e não cabe a seus criadores qualquer forma de direito autoral.

Art. 62. É vedada a utilização de informações produzidas por terceiros para uso exclusivo da SEMA em quaisquer outros projetos ou atividades de uso diverso do estabelecido pela Secretaria, salvo autorização específica e formal pelos titulares das unidades administrativas, nos processos e documentos de sua competência, ou pelo Secretário de Estado do Meio Ambiente, nos demais casos.

Seção X

Dos Contratos, Convênios, Acordos e Instrumentos Congêneres.

Art. 63. Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Art. 64. Os acordos com terceiros devem envolver todas as partes envolvidas.

Parágrafo único. Os acordos que concedam o acesso a terceiros podem incluir, quando necessário e justificado, permissão para designação de outras partes autorizadas e condições para os seus acessos desde que expressamente autorizadas pela SEMA.

Art. 65. Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta PSI.

Art. 66. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta PSI e suas normas complementares aos seus empregados e prepostos envolvidos em atividades na SEMA.

Art. 67. Todo contrato, convênio, acordos ou instrumentos congêneres deverão prever um plano de contingência para caso de uma das partes desejar o seu encerramento antes dos prazos acordados;

Capítulo VI

PENALIDADES

Art. 68. Ações que violem a PSI ou quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SI serão devidamente apuradas por processo administrativo e aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor.

Capítulo VII

COMPETÊNCIAS E RESPONSABILIDADES

Art. 69. Cabe ao CSI:

I - promover cultura de segurança da informação;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - propor recursos necessários às ações de SI;

IV - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SI;

V - propor, sempre que necessário, alterações na PSI e nas normas vigentes;

VI - propor, anualmente revisões na PSI e normas vigentes;

VII - normatizar e supervisionar a SI no âmbito da SEMA;

VIII - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SI;

IX - solicitar apurações quando da suspeita de ocorrências de quebras de SI;

X - avaliar, revisar e analisar criticamente a PSI e suas normas complementares, visando a sua aderência aos objetivos institucionais da SEMA e às legislações vigentes;

XI - dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PSI da SEMA;

XII - constituir grupo de trabalho para realizar verificações de conformidade;

XIII - aprovar o plano de investimentos em SI da SEMA;

XIV - monitorar e avaliar periodicamente o plano de SI de que trata o parágrafo único do art. 15, assim como determinar os ajustes cabíveis; e,

XV - definir e atualizar seu Regimento Interno.

Parágrafo único. É de competência privativa do CSI propor normas e procedimentos complementares a esta PSI ao Sr. Secretário de Estado de Meio Ambiente.

Art. 70. Cabe ao titular da unidade administrativa:

I - conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SI;

II - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SI;

III - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SI por parte dos usuários sob sua supervisão;

IV- informar à Coordenadoria de Gestão de Pessoas a movimentação de pessoal de sua unidade;

V - realizar o tratamento e a classificação da informação conforme plano de classificação da informação da SEMA;

VI - manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores.

Art. 71. Cabe aos terceiros e fornecedores, conforme previsto em contrato:

I - observar, no exercício de suas atividades, a íntegra desta PSI;

II - tomar conhecimento desta PSI;

IIII - fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e

IV - fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

Art. 72. Cabe aos usuários:

I - conhecer e cumprir todas as políticas, normas e procedimentos relacionados à SI; e

II - comunicar, via central de serviços, os incidentes que afetam a segurança dos ativos de informação ao CSI.

Capítulo VIII

PROCEDIMENTOS DE ATUALIZAÇÃO E TRANSIÇÃO

Art. 73. Esta PSI, bem como os documentos gerados a partir dela, deverão ser revisados anualmente, ou por deliberação do CSI.

Parágrafo primeiro. O CSI formalizará a proposta de revisão da PSI por meio de Resolução, a qual deve ser, sucessivamente, apreciada pelo Secretário Adjunto de Gestão Sistêmica e aprovada pelo Secretário de Estado do Meio Ambiente.

Art. 74. As Coordenações e Superintendências deverão elaborar e propor as suas normas e procedimento de SI ao CSI em até 180 (cento e vinte) dias após a publicação desta PSI.

Art. 75. - Esta Portaria entra em vigor na data de sua publicação.

Registre-se, publique-se e cumpra-se.

Cuiabá-MT, 05 de Junho de 2017.

Rodrigo Quintana Fernandes

Assessor Chefe I

Portaria nº 387/2016