PORTARIA MME Nº 887, DE 15 DE DEZEMBRO DE 2025

Aprova a Política de Segurança da Informação do Ministério de Minas e Energia - POSIN-MME.

O MINISTRO DE ESTADO DE MINAS E ENERGIA, no uso das atribuições que lhe confere o art. 87, parágrafo único, incisos II e IV, da Constituição, tendo em vista o disposto no art. 10 do Decreto nº 12.572, de 4 de agosto de 2025, no art. 9º da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, e considerando o que consta no Processo nº 48330.000156/2024-61, resolve:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Fica aprovada a Política de Segurança da Informação do Ministério de Minas e Energia, nos termos desta Portaria.

Do objetivo

Art. 2º A Política de Segurança da Informação do Ministério de Minas e Energia - POSIN-MME tem por objetivo estabelecer e difundir diretrizes, princípios, responsabilidades e competências de Segurança da Informação - SI, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Ministério, preservando sua disponibilidade, integridade, confidencialidade e autenticidade.

Do escopo e abrangência

Art. 3º A POSIN-MME e as normas complementares a ela associadas se aplicam a todas as unidades da estrutura organizacional do Ministério de Minas e Energia e aos agentes públicos que têm vínculo direto e/ou indireto com o Ministério, seja em ambientes virtuais ou físicos, abrangendo:

I - a defesa cibernética;

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

III - as ações destinadas a assegurar a disponibilidade, a integridade e a autenticidade da informação, bem como sua confidencialidade, quando exigível.

Art. 4º A POSIN-MME alinha as ações de segurança da informação às estratégias de planejamento organizacional do Ministério e contribui para o cumprimento da Lei Geral de Proteção de Dados Pessoais - LGPD e de outras normas vigentes sobre o tema.

Art. 5º A POSIN-MME orienta o tratamento da informação no âmbito do Ministério, em todo o seu ciclo de vida (criação, coleta, manuseio, divulgação, armazenamento, retenção, processamento, compartilhamento e eliminação), considerando a privacidade e a segurança desde a concepção da informação, visando à continuidade das atividades críticas, em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de SI.

Art. 6º Para o alcance dos seus objetivos, a POSIN-MME estabelece:

I - diretrizes, no que se refere a comportamentos, procedimentos e normas de segurança da informação, comunicação e proteção de dados;

II - estrutura de gestão de segurança da informação, comunicação e proteção de dados adequada às diretrizes institucionais, considerando um conjunto de papéis, responsabilidades e instrumentos normativos e organizacionais; e

III - orientações gerais de segurança da informação, comunicação e proteção de dados em harmonia com a legislação vigente, as boas práticas e a gestão eficiente dos riscos associados.

Art. 7º As diretrizes e orientações previstas nesta Política, nas demais normas específicas associadas e suas eventuais metodologias, manuais, procedimentos e documentos correlatos são aplicadas a todos os servidores, demais colaboradores e a terceiros do Ministério de Minas e Energia que tenham acesso às informações, aos dados e aos recursos de Tecnologia da Informação e Comunicação - TIC.

Dos conceitos e definições

Art. 8º Para os efeitos da POSIN-MME, os termos utilizados seguem as definições do Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República e, no que couber, as do art. 5º da Lei Geral de Proteção de Dados, em especial:

I - agente público: todo aquele que exerce, ainda que transitoriamente ou sem 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 federal, direta e indireta;

II - ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

III - auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas e em conformidade à consecução dos objetivos;

IV - autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

V - confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

VI - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Geralmente, requer procedimentos de autenticação;

VII - defesa cibernética: ações realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente;

VIII - disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

IX - gestão de continuidade de negócios em segurança da informação: processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

X - integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XI - 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; e

XII - usuário de informação (ou usuário): pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 9º A POSIN-MME é orientada pelos princípios estabelecidos na Política Nacional de Segurança da Informação e pelos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal, bem como os seguintes princípios orientadores:

I - alinhamento estratégico e sistêmico: necessidade desta política de alinhamento com o planejamento estratégico institucional, com o modelo de governança e com a Política de Gestão de Riscos do Ministério de Minas e Energia;

II - transparência: obrigação fundamental de prestar informações confiáveis, relevantes e tempestivas à sociedade, visando à participação social na proposição e no monitoramento da execução das políticas públicas geridas pelo Ministério de Minas e Energia. É também refletida no dever institucional e dos agentes públicos de garantir o sigilo das informações e dos dados imprescindíveis à segurança da sociedade e do Estado e à inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas;

III - corresponsabilidade: constituída pelo dever de todas as partes envolvidas em conhecer e respeitar a Política e as normas específicas a ela associadas;

IV - clareza: as responsabilidades pela segurança dos ativos do Ministério de Minas e Energia e pelo cumprimento de processos de segurança devem ser claramente definidas;

V - ética: todos os direitos e interesses legítimos dos usuários devem ser respeitados sem comprometimento da segurança;

VI - menor privilégio: restringir o acesso às informações, ao estritamente necessário ao exercício das funções;

VII - continuidade dos processos e serviços críticos: caráter de essencialidade ao funcionamento do Ministério de Minas e Energia e ao cumprimento de sua missão institucional, protegendo sua disponibilidade e segurança e definindo uma estratégia adequada de prevenção, gestão e recuperação de incidentes, visando à continuidade do negócio e à redução dos impactos em ocorrências de interrupção causadas por desastres e/ou falhas;

VIII - educação, treinamento, conscientização, comunicação e cooperação: para fomento e aprimoramento das práticas de promoção da cultura em segurança da informação;

IX - conformidade das normas e das ações de segurança da informação com a legislação regulamentos aplicáveis; e

X - respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade.

CAPÍTULO III
das DIRETRIZES

Seção I
Dos pressupostos básicos

Art. 10. A gestão de segurança da informação deve ser suportada por ações e métodos que visem à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento das informações e dos dados, à conformidade, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional dos processos institucionais estratégicos, operacionais e táticos, considerando, sob caráter geral, o seguinte:

I - informações e dados como ativos: toda e qualquer informação e dado gerados, custodiados, manipulados, utilizados ou armazenados no Ministério de Minas e Energia compõem um ativo de informação relevante para as suas atividades e devem ser protegidos e tratados com vistas à preservação dos princípios de disponibilidade, integridade, confidencialidade e autenticidade, bem como à proteção de dados pessoais e à privacidade, conforme as normas em vigor estabelecidas;

II - classificação da informação como requisito: todo ativo de informação deve ser classificado e tratado segundo sua classificação de segurança da informação, de maneira a proteger adequadamente as informações e os dados na sua criação, coleta, utilização, custódia e no descarte;

III - segregação de funções: sempre que processualmente viável, devem ser segregadas funções ou áreas de responsabilidade conflitantes, para que ninguém detenha controle de um processo crítico na sua totalidade, visando a reduzir os riscos de mau uso, acidental ou deliberado, dos ativos de informação;

IV - estabelecer controles adequados à relevância e ao risco: as medidas e os controles de segurança devem ser estabelecidos considerando a relevância dos ativos de informação e os níveis de risco associados - considerando o ambiente, o valor e a criticidade das informações e dos dados - de forma proporcional e balanceada, visando sempre à prevenção da ocorrência de incidentes;

V - menor privilégio e mínimo acesso: pessoas e aplicações devem ter o menor privilégio e o mínimo de acesso aos recursos necessários para realizar uma determinada tarefa, tendo como condição a ciência expressa dos termos desta Política, as responsabilidades e os compromissos decorridos deste acesso e o conhecimento das penalidades cabíveis pela inobservância das regras previstas;

VI - responsabilização individual: todos os usuários são responsáveis pela segurança dos ativos de informação que estejam sob sua custódia, pelo uso e pela guarda de suas credenciais de acesso, sendo vedada a exploração de eventuais vulnerabilidades - que, assim que identificadas, devem ser imediatamente comunicadas às instâncias superiores;

VII - corresponsabilidade de terceiros: todos os contratos de prestação de serviços, firmados pelo Ministério de Minas e Energia deverão conter cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta Política, incluindo a assinatura de Termo de Responsabilidade pelas empresas contratadas e de Termo de Ciência pelos colaboradores diretamente envolvidas na execução dos serviços contratados;

VIII - restrição de uso dos ativos de informação: o acesso e uso das informações e dados que não sejam de domínio público e dos ativos de informação do Ministério de Minas e Energia são controlados e limitados às atribuições necessárias para cumprimento das atividades dos solicitantes e usuários devidamente autorizados e utilizados no estrito interesse do custodiante, apenas para as finalidades profissionais, lícitas, éticas, administrativamente aprovadas e devidamente autorizadas. Qualquer outra forma de acesso e uso necessitará de prévia autorização do proprietário do ativo de informação;

IX - uso seguro dos ativos de informação: apenas os ativos de informação homologados e autorizados pelo Ministério de Minas e Energia devem ter uso permitido, desde que sejam identificados de forma individual, inventariados, protegidos e tenham um proprietário do ativo de informação responsável. Os ativos de informação devem ter documentação atualizada, riscos mapeados, capacidade e contingência adequadas e sua operação deve estar de acordo com as normas, cláusulas contratuais e a legislação em vigor; e

X - divulgação desta política e suas atualizações, bem como normas específicas de segurança da informação do Ministério: devem ser divulgadas amplamente a todos os usuários de Informação, que devem ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

Art. 11. Essas diretrizes gerais constituem os pilares da gestão de segurança da informação e proteção de dados do Ministério de Minas e Energia e norteiam a construção de ações, planos e normas associados que objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Seção II
Do tratamento da informação

Art. 12. Toda informação e dado criados manuseados, armazenados, transportados, descartados ou custodiados pelo Ministério de Minas e Energia são de sua responsabilidade e devem ser protegidos, classificados e tratados adequadamente, quanto aos aspectos de confidencialidade, integridade, autenticidade e disponibilidade, bem como à proteção de dados pessoais e à privacidade, segundo as diretrizes descritas e demais regulamentações em vigor.

Art. 13. Toda informação e dado institucionais, se eletrônicos, serão armazenados nos servidores de arquivos (físicos, virtuais ou em nuvem) e bases de dados sob gestão e administração da Subsecretaria de Tecnologia e Inovação e, se não eletrônicos, mantidos em local físico adequado.

Art. 14. Toda informação e dado institucionais sob a forma eletrônica deverão estar salvaguardados por meio de cópia de segurança (backup) em solução que garanta sua preservação e recuperação, quando necessária, conforme disposto em normas e procedimentos específicos sob responsabilidade da Subsecretaria de Tecnologia e Inovação.

Art. 15. É expressamente proibido o acesso, a guarda ou o encaminhamento de material discriminatório, malicioso, não ético, obsceno ou ilegal por intermédio de quaisquer meios e recursos de tecnologia da informação disponibilizados pelo Ministério de Minas e Energia.

Art. 16. As informações e os dados classificados, considerando a legislação vigente, que sejam produzidos, armazenados e/ou transportados em meio eletrônico utilizarão criptografia compatível com o respectivo grau de sigilo, em especial as informações de autenticação de usuários das aplicações geridas pelo Ministério de Minas e Energia.

Art. 17. No tratamento das informações, deve-se respeitar a classificação segundo o grau de sigilo, a criticidade e a proteção de dados pessoais, conforme normas internas e legislação específica em vigor.

Art. 18. A manipulação e a eliminação de informações classificadas em qualquer grau de sigilo devem seguir as normas internas e a legislação em vigor.

Art. 19. Os responsáveis pelos ativos de informação devem manter registros e procedimentos que assegurem o rastreamento, o acompanhamento, o controle e a verificação de acesso, em especial aos sistemas corporativos e às redes computacionais.

Seção III
Da segurança física e do ambiente

Art. 20. As ações de segurança física e ambiental, no que se referem aos aspectos de segurança da informação, deverão prover normas e procedimentos que abordem, no mínimo, os seguintes aspectos:

I - controle e monitoramento de acesso físico: compreendem as necessidades de controle e monitoramento de acesso às instalações e aos ambientes físicos do Órgão, estabelecimento dos

perímetros de segurança, regras de controle de acesso da gestão de autorizações e manutenção de registros de acesso de pessoal autorizado e de visitantes;

II - controles ambientais: compreendem provisão e manutenção dos controles ambientais necessários, com base em uma avaliação de requisitos, que inclui, mas não se limita, a energia de reserva para facilitar um processo de desligamento ordenado (no mínimo), a detecção e supressão de incêndios, os controles de temperatura e umidade e a detecção e mitigação de danos ambientais; e

III - descarte seguro de equipamentos: compreende a provisão e manutenção de controles para identificação e remoção permanente de quaisquer dados sensíveis e softwares licenciados em equipamentos antes do descarte.

Seção IV
Da gestão de incidentes em segurança da informação

Art. 21. O Ministério de Minas e Energia deverá prover e manter normas e procedimentos de resposta a incidentes consistentes com as leis e políticas governamentais aplicáveis, incluindo, mas não se limitando, a identificação de papéis e responsabilidades, a investigação, os procedimentos de contenção e escalonamento, a documentação e preservação de evidências, os protocolos de comunicação e as lições aprendidas.

Art. 22. O processo de gestão de incidentes deverá envolver também procedimentos adequados de comunicação de incidentes incluindo, mas não se limitando, a treinamento de servidores, demais colaboradores e terceiros para identificar e comunicar rapidamente incidentes e preparação e apresentação de relatórios de acompanhamento.

Art. 23. Os incidentes que afetem dados pessoais deverão ser imediatamente comunicados ao Encarregado pelo Tratamento de Dados Pessoais, que orientará as práticas a serem adotadas.

Art. 24. Caberá à Subsecretaria de Tecnologia e Inovação a responsabilidade pela infraestrutura necessária para fins de registro e resposta aos incidentes de segurança da informação no âmbito da rede corporativa do Ministério de Minas e Energia.

Seção V
Da gestão de ativos

Art. 25. O Ministério de Minas e Energia manterá um processo de inventário e mapeamento dos ativos de informação objetivando a segurança das infraestruturas críticas que garantem suas informações e dados. O processo de inventário e mapeamento de ativos de informação subsidiará o conhecimento, a valoração, a proteção, a auditoria e a manutenção de seus ativos de informação e deverá ser dinâmico, periódico e estruturado, para manter a base de dados de ativos de informação atualizada.

Seção VI
Da gestão do uso dos recursos operacionais e de comunicações

Comunicações

Art. 26. Todos os sistemas de comunicação eletrônica, quer seja de origem externa, quer seja interna, são recursos de Tecnologia da Informação e Comunicação disponibilizados pelo Ministério de Minas e Energia a seus servidores, demais colaboradores e terceiros.

Parágrafo único. Esses sistemas deverão ser utilizados precipuamente no exercício das funções institucionais, em conexão com a finalidade do Órgão e de forma aderente a esta Política e à legislação vigente, podendo ser concedidos ou revogados a qualquer tempo, em caráter total ou parcial, de acordo com os interesses do Ministério.

Art. 27. Ao Ministério de Minas e Energia se reserva o direito de monitorar, acessar e revisar quaisquer aspectos de seus recursos de informação eletrônica e sistemas de comunicação, incluindo,

entre outros, o uso da Internet, sistemas de comunicação eletrônica como e-mail, sistemas de telefonia, tráfego da rede e revisar ativos armazenados em qualquer sistema de comunicação.

Parágrafo único. O consentimento para tais registros e monitoramento é presumido por parte dos usuários, não cabendo qualquer contestação ou alegação de desconhecimento dessa regra.

Art. 28. As comunicações eletrônicas são comunicações formais e espera-se que os usuários exerçam cuidado e profissionalismo na aplicação desses recursos, assim como o faria com qualquer outro expediente de comunicação formal emitido em nome do Ministério de Minas e Energia.

Parágrafo único. O uso dos recursos de comunicação eletrônica deverá ser disciplinado em regramento próprio, associado a esta Política.

Acesso à Internet

Art. 29. O acesso à Internet no ambiente de trabalho do Ministério de Minas e Energia está condicionado às necessidades dos agentes públicos no exercício de suas atribuições e será regido por norma específica, em conformidade com esta Política e demais orientações governamentais e legislação em vigor.

Art. 30. Cada usuário de informação é responsável por tomar todas as medidas razoáveis para utilizar os recursos de Internet de forma responsável e segura, tendo em vista que credenciais de acesso são pessoais e intransferíveis, sendo que o usuário é individualmente responsável por todas as atividades exercidas a partir de sua credencial.

Art. 31. O uso da Internet no Ministério de Minas e Energia será monitorado e os acessos serão registrados em dispositivo ou sistema computacional que assegure a possibilidade de rastreio e apuração de responsabilidades em caso de incidentes cibernéticos, incidentes de segurança e outras violações a esta Política.

Art. 32. Para apuração das quebras de segurança relativas ao uso da Internet, os ativos de informação fornecidos pelo Ministério de Minas e Energia poderão ser analisados, a qualquer tempo, pela Equipe de Prevenção e Tratamento e Resposta a Incidentes Cibernéticos deste Ministério.

Art. 33. No que se refere ao acesso à Internet, cada usuário deverá:

I - utilizar os recursos de forma a proteger a organização de qualquer risco legal, regulatório, operacional ou de reputação;

II - não compartilhar suas credenciais de acesso;

III - não acessar websites ou objetos com conteúdo inadequado ou ilegal; e

IV - estar ciente de suas responsabilidades pelo uso apropriado da Internet e de que o uso dela está sujeito a registro e pode ser monitorado de acordo com as exigências das leis e dos regulamentos aplicáveis.

Computação em Nuvem

Art. 34. O uso de aplicativos e a contratação de serviços em nuvem deverá assegurar que toda a cadeia de suprimentos de TIC, baseada em provedores de serviços no ambiente de computação em nuvem, seja avaliada por todos os aspectos de segurança para proteger dados, metadados, informações e conhecimentos produzidos ou custodiados pelo Ministério de Minas e Energia, incluindo o cumprimento da legislação e regulamentação nacional e estrangeira, o gerenciamento de identidades, o monitoramento e auditoria regulares e as restrições de localizações geográficas.

Mídias Sociais

Art. 35. Os critérios, limitações e responsabilidades no uso institucional das mídias sociais, será regido por norma específica, em conformidade com esta Política e demais orientações governamentais e legislação em vigor.

Seção VII
Dos controles de acesso

Art. 36. Todo usuário de informação que faça uso dos recursos de Tecnologia da Informação e Comunicação do Ministério de Minas e Energia deverá possuir uma conta de acesso único e intransferível, que permita seu reconhecimento individual de maneira inequívoca, e cujos concessão e gerenciamento serão regulamentados em norma específica associada.

Art. 37. A concessão e a revogação dos privilégios de acesso às informações ficam atribuídas ao agente responsável pelo tratamento dos dados sob a sua tutela, considerando sempre o princípio do menor privilégio.

Art. 38. O controle de acesso aos ativos de informação e às áreas e instalações deve ser implantado nos níveis físico e lógico, conforme procedimentos estabelecidos pelas áreas competentes.

Seção VIII
Da gestão de riscos

Art. 39. A gestão de riscos em segurança da informação e proteção de dados deverá observar a legislação em vigor, e no que couber, as disposições da Política de Gestão de Riscos do Ministério de Minas e Energia.

Art. 40. O processo de gestão de riscos em segurança da informação deverá fornecer uma estrutura consistente de gerenciamento por meio da qual os riscos relacionados às funções, ativos da informação e aos processos críticos possam ser identificados, avaliados, monitorados e tratados mediante sistemas de revisão, controle e garantia.

Seção IX
Da gestão de continuidade

Art. 41. O Ministério de Minas e Energia deve estabelecer um Programa de Gestão de Continuidade de Negócio - PGCN, em Segurança da Informação e Proteção de Dados visando a reduzir a possibilidade de interrupção causada por desastres ou falhas nos recursos de Tecnologia da Informação e Comunicação que suportam as operações do Ministério.

Art. 42. O PGCN deve prever a recuperação de perdas de ativos de informação em nível aceitável, por intermédio de ações de resposta a incidentes e recuperação de desastres.

Art. 43. O processo de gestão de continuidade de negócios deve se basear no PGCN, estruturado a partir da análise e avaliação dos riscos de Segurança da Informação identificados e da prioridade de recuperação dos processos de negócio.

Art. 44. Toda e qualquer solução, sistema, aplicação e/ou serviço crítico do Ministério de Minas e Energia deverá estar suportado pelo Programa de Gestão de Continuidade de Negócio.

Seção X
Da auditoria e conformidade

Art. 45. O uso dos recursos de Tecnologia da Informação e Comunicação disponibilizados pelo Ministério de Minas e Energia é passível de monitoramento e auditoria, incluindo a análise regular de registros de eventos [log] com aplicação, sempre que viável, de softwares utilitários específicos para monitoramento do uso de sistemas computacionais.

Art. 46. Sempre que possível, deverão ser implementados e mantidos mecanismos que permitam a rastreabilidade dos recursos de TIC por meio de estratégias como: trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para todos os sistemas corporativos e rede corporativa.

Art. 47. Como medida de preservação de evidências, sempre que tecnicamente possível, todo e qualquer ativo de informação deverá ser configurado para armazenar registros históricos de registros

de eventos (log) em formato que permita a completa identificação dos fluxos de dados e das operações de seus usuários e/ou administradores.

Parágrafo único. Esses registros devem ser armazenados pelo período mínimo de seis meses, sem prejuízo de outros prazos previstos em normativos específicos e os ativos de informação devem ser configurados de forma a armazenar seus registros de eventos [log] não apenas localmente, como também remotamente, por meio de tecnologia aplicável.

CAPÍTULO IV
DAS COMPETÊNCIAS E ESTRUTURA DE GESTÃO

Art. 48. A estrutura de Gestão de Segurança da Informação do Ministério de Minas e Energia possui a seguinte composição:

I - Alta administração: representada pela autoridade máxima do Ministério de Minas e Energia ou o seu substituto nomeado oficialmente, responsável por fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação e adotar as decisões acerca do tratamento das informações e dos dados vinculados à atuação institucional do Ministério;

II - Subsecretaria de Tecnologia e Inovação: unidade responsável pela gestão da informação e proteção de dados em meio eletrônico no âmbito do Ministério de Minas e Energia, apoia as unidades na definição de procedimentos para proteção de suas informações e seus dados, monitora e avalia as práticas de segurança da informação e coordena ações de conscientização e treinamento bem como de tratamento de incidentes de segurança da informação, promove ações para viabilizar a aderência do Ministério às normas, boas práticas e controles de segurança cibernética, aplicáveis a seus ativos de informação, considerando as suas competências institucionais previstas no Decreto nº 11.492, de 17 de abril de 2023;

III - Comitê de Governança Digital - CGD/MME: órgão colegiado de natureza consultiva e deliberativa e de caráter permanente, de cunho estratégico e executivo, instituído para deliberar sobre assuntos relativos à Governança Digital e às ações, aos programas, às políticas e aos projetos de Tecnologia da Informação e Comunicação no âmbito do Ministério de Minas e Energia, conforme competências estabelecidas na Portaria MME nº 784, de 6 de maio de 2024;

IV - Comitê de Segurança da Informação e da Comunicação - CSIC/MME: colegiado responsável por tratar de assuntos relacionados à segurança da informação nos ambientes convencionais e de TIC e a cibersegurança das infraestruturas críticas, no âmbito do Ministério de Minas e Energia, conforme competências estabelecidas na Portaria MME nº 784, de 6 de maio de 2024, considerado como estrutura equivalente àquela prevista no art. 20 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020;

V - Gestor de Segurança da Informação: servidor formalmente designado para exercer as competências definidas no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020;

VI - Dirigente de Unidade ou Subunidade: responsável por conscientizar servidores, demais colaboradores e terceiros em relação aos conceitos e às práticas de segurança da informação bem como incorporá-las aos processos de trabalho da unidade. Em caso de comprometimento da segurança da informação, devem tomar medidas administrativas para que sejam adotadas ações corretivas em tempo hábil;

VII - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR/MME: responsável por receber, analisar e responder às notificações e atividades relacionadas a incidentes cibernéticos no âmbito do Ministério de Minas e Energia, prevista no art. 22 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, e regulamentada pela Norma Complementar nº 05/IN01/DSIC/GSIPR; e

VIII - Servidores, demais Colaboradores e Terceiros: qualquer pessoa que tenha acesso a informações e dados do Ministério de Minas e Energia, responsável pela segurança da informação dos ativos a que tenha acesso.

Art. 49. Quanto à composição normativa, a gestão de segurança da informação do Ministério de Minas e Energia obedece à seguinte estrutura:

I - política (nível estratégico): documento que define objetivos, princípios e diretrizes de alto nível que traduzem a visão estratégica do órgão nessa temática e orientam a elaboração de normas, procedimentos e ações de segurança da informação e proteção de dados;

II - normas (nível tático): especificam, no plano tático, as regras, as escolhas tecnológicas e os controles que deverão ser implementados para execução dos objetivos e das diretrizes oriundas da Política de Segurança da Informação, dotando-a de instrumentos de implementação; e

III - procedimentos (nível operacional): instrumentalizam o disposto nas normas, orientando e direcionando sua aplicação.

CAPÍTULO V
DAS PENALIDADES

Art. 50. Ações que violem a Política Corporativa de Segurança da Informação do Ministério de Minas e Energia caracterizam infração funcional e poderão acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurado aos envolvidos o contraditório e a ampla defesa.

CAPÍTULO VI
DA ATUALIZAÇÃO E REVISÃO

Art. 51. A Política de Segurança da Informação do Ministério de Minas e Energia deverá ser revisada em função de alterações na legislação pertinente, das diretrizes superiores do Governo Federal, de alterações nos normativos internos, quando considerada necessária ou no prazo máximo de quatro anos, a contar da data de sua publicação, mediante proposição do Comitê de Segurança da Informação e Comunicações.

Art. 52. O Comitê de Segurança da Informação e Comunicações poderá expedir normas complementares associadas à POSIN-MME, no âmbito de sua competência regimental, visando a detalhar particularidades e procedimentos relativos à sua implementação no âmbito do Ministério de Minas e Energia.

Art. 53. Incumbe à Subsecretaria de Tecnologia e Inovação expedir e gerir os procedimentos de nível operacional que instrumentalizam o disposto nas normas complementares e nesta Política.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 54. Esta Política de Segurança da Informação e suas atualizações deverão ser divulgadas amplamente a todos os servidores, demais colaboradores e terceiros do Ministério de Minas e Energia, ainda que sua atuação no Órgão seja temporária, a fim de promover sua observância e seu conhecimento bem como a formação da cultura de segurança da informação.

Art. 55. É responsabilidade de todos os gestores do Ministério de Minas e Energia promover o conhecimento e a disseminação desta Política e demais normas associadas à segurança da informação aos servidores, demais colaboradores e terceiros sob a sua gestão.

Art. 56. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pelo Ministério para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.

Art. 57. São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pelo Ministério.

Art. 58. É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários.

Art. 59. É vedada a exploração de eventuais vulnerabilidades de processos e ativos digitais de informação, as quais devem ser comunicadas às instâncias superiores assim que identificadas.

Art. 60. As unidades organizacionais do Ministério de Minas e Energia devem promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

Parágrafo único. A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos colaboradores.

Art. 61. Os casos omissos e as dúvidas sobre a POSIN-MME e seus complementos devem ser submetidas ao Comitê de Segurança da Informação e das Comunicações do Ministério de Minas e Energia.

Art. 62. As referências normativas citadas neste documento devem ser consideradas em sua versão vigente, na data de publicação da Política. Caso venham a ser atualizadas ou substituídas, recomenda-se a adoção da versão mais recente, salvo disposição em contrário.

Art. 63. Fica revogada a Portaria MME nº 679, de 29 de dezembro de 2014.

Art. 64. Esta Portaria entra em vigor na data de sua publicação.

ALEXANDRE SILVEIRA