JAZIDA

RESOLUÇÃO Nº 53, DE 13 DE JANEIRO DE 2021

Informamos que no Diário Oficial da União do dia 14 de janeiro 2021, o Diretor-Geral institui a Política de Segurança da Informação e Comunicações - POSIC, que fornece as diretrizes e critérios e define o suporte administrativo para o tratamento a ser dado às informações produzidas, processadas, transmitidas e armazenadas no ambiente convencional ou tecnológico no âmbito da Agência Nacional de Mineração.

AGÊNCIA NACIONAL DE MINERAÇÃO

RESOLUÇÃO Nº 53, DE 13 DE JANEIRO DE 2021

Institui a Política de Segurança da Informação e Comunicações (POSIC) da Agência Nacional de Mineração.

A DIRETORIA COLEGIADA DA AGÊNCIA NACIONAL DE MINERAÇÃO, no uso das atribuições que lhe confere o art. 11, § 1o, inciso I, da Lei no 13.575, de 26 de dezembro de 2017, o art. 9o, inciso I, do Anexo I da Estrutura Regimental da Agência Nacional de Mineração, aprovada pelo Decreto no 9.587, de 27 de novembro de 2018, e no art. 10, inciso I, do Anexo II da Resolução no 2, de 12 de dezembro de 2018, e

CONSIDERANDO a Instrução Normativa no 1 GSI/PR, de 13 de junho de 2008, e suas respectivas Normas Complementares, que disciplinam a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

CONSIDERANDO o Decreto no 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação, resolve:

Art. 1o Instituir a Política de Segurança da Informação e Comunicações - POSIC, que fornece as diretrizes e critérios e define o suporte administrativo para o tratamento a ser dado às informações produzidas, processadas, transmitidas e armazenadas no ambiente convencional ou tecnológico no âmbito da Agência Nacional de Mineração.

CAPÍTULO I

DO ESCOPO

Art. 2o O escopo da POSIC abrange os servidores, colaboradores, consultores

externos e demais agentes públicos ou particulares que, por força de convênios, protocolos, acordos de cooperação e instrumentos congêneres, executem atividades vinculadas à ANM.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3o Para fins desta Resolução, entende-se por:

I - POSIC: sigla utilizada para o documento aprovado pela autoridade

responsável da ANM, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações na Autarquia;

II - Segurança da informação e comunicações: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação ou divulgação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento, com a implementação de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

III - Comunicação: conjunto de recursos tecnológicos destinados a transmitir ou replicar informações;

IV - Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou

entidade; V - Integridade: propriedade de que a informação não foi modificada, inclusive quanto à origem e ao destino, ou destruída de maneira não autorizada ou acidental;

VI - Confidencialidade: propriedade de que a informação classificada quanto ao grau de sigilo, ou de acesso restrito, não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

VII - Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por determinada pessoa física, ou por determinado sistema, órgão ou entidade;

VIII - Gestão de segurança da informação e comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais, não se limitando, portanto, à tecnologia da informação e comunicações;

IX - Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive das classificadas quanto ao grau de sigilo;

X - Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações; e

XI - Ativos de informação: compreende os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios e os recursos humanos que a eles têm acesso.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 4o As ações relacionadas com a Segurança da Informação e Comunicações na ANM serão norteadas pelos seguintes princípios:

I - Responsabilidade: todos mencionados no art. 2o são responsáveis pelo tratamento da informação e pelo cumprimento das normas de segurança da informação e comunicações;

II - Conhecimento: os servidores, os colaboradores, os consultores externos, os estagiários e os prestadores de serviço na ANM tomarão ciência de todas as normas de segurança da informação e comunicações, para o pleno desempenho de suas atribuições;III - Legalidade: as ações de segurança da informação e comunicações levarão em consideração as leis, as políticas e as normas organizacionais, administrativas, técnicas e operacionais da ANM, formalmente estabelecidas;

IV - Proporcionalidade: o nível, a complexidade e os custos das ações de segurança da informação e comunicações na ANM serão adequados ao entendimento administrativo e ao valor do ativo a proteger; e

V - Proatividade: todas as unidades da ANM devem manter processo de gestão de continuidade das suas atividades e serviços, evitando a interrupção em caso de incidente de segurança, ou devido a caso fortuito ou de força maior, e assegurar a sua retomada em tempo hábil, quando for o caso.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 5o A alta direção da ANM deve manter postura exemplar em relação à segurança da informação e comunicação, bem como propiciar os recursos necessários para divulgações, capacitações e cumprimentos das normas e procedimentos.

Art. 6o Cada colaborador ou servidor ativo na ANM deverá manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de Segurança da Informação e Comunicações da ANM, tomando as ações necessárias para cumprir tal responsabilidade.

Art. 7o Para uma efetiva implementação da POSIC deverão ser previstas ações de divulgação, conscientização e educação quanto ao conteúdo do normativo, entre todos os colaboradores e servidores da ANM.

Art. 8o São valores e diretrizes gerais da POSIC:

I - Segurança focada na instituição: garantir segurança tanto aos sistemas no ambiente de computação quanto aos meios convencionais de processamento, comunicação e armazenamento em papel;

II - Informação é patrimônio: considerar que toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela ANM é patrimônio da instituição e deve ser protegida quanto aos aspectos de confidencialidade, autenticidade, integridade e disponibilidade;

III - Proteção compatível com riscos: dimensionar e aplicar os investimentos necessários em medidas de segurança, segundo o valor do ativo que está sendo protegido e de acordo com a identificação de risco de potenciais prejuízos e de impacto na reputação para o negócio, a atividade fim e os objetivos institucionais;

IV - Tratamento conforme classificação: tratar todas as informações a partir da classificação de segurança, aplicada de maneira a serem adequadamente protegidas quanto ao seu acesso e uso;

V - Responsabilização baseada na credencial: responsabilizar, com base no uso da credencial, que se caracteriza por ser pessoal e intransferível, qualificando aquele que se encontra formalmente associado a ela como responsável por todas as atividades desenvolvidas em seu uso, sendo pré-requisito para a liberação da credencial o preenchimento de um termo de responsabilidade;

VI - Utilização restrita às atividades: administrar o acesso e o uso da informação e dos ativos de informação de acordo com as atribuições necessárias para o cumprimento das atividades institucionais. Qualquer outra forma de uso necessitará de prévia autorização

VII - Utilização orientada à segurança: permitir somente o uso de ativos de informação homologados e autorizados pela ANM, desde que sejam identificados de forma individual, protegidos, inventariados, com documentação atualizada e estando de acordo com a legislação em vigor;

VIII - Autorização definida pelos gestores: definir acessos e cancelar acessos aos recursos e aos locais restritos com base na solicitação do gestor de cada Unidade Organizacional - UORG, que também é responsável pelos ativos disponibilizados para uso;

IX - Segregação de funções: segregar a administração e execução de funções ou áreas de responsabilidade críticas para o negócio, evitando o controle de um processo na sua totalidade, visando à redução do risco de mau uso acidental ou deliberado;

X - Educação: promover continuamente ações educativas sobre segurança da informação e comunicações aos servidores e colaboradores para que realizem suas atividades na instituição de forma segura, utilizando procedimentos que minimizem os riscos e que possibilitem o uso correto dos ativos e ferramentas de informação, com destaque para os serviços de correio eletrônico e acesso à internet;

XI - Auditoria: monitorar e auditar, pela área competente da ANM, a implementação e o cumprimento da Política de Segurança da Informação e Comunicações. Consultorias externas especializadas poderão ser utilizadas para avaliação da POSIC e de seu cumprimento;

XII - Continuidade aplicada aos serviços: planejar e definir estratégias para reduzir a um nível aceitável a possibilidade de interrupção causada por desastres ou falhas nos recursos que suportam os processos de trabalho. O resultado desse planejamento deve ser documentado, testado e revisado conforme a necessidade, assegurados os recursos necessários à sua implementação;

XIII - Notificação imediata de incidentes: notificar o incidente imediatamente ao superior hierárquico que, sem prejuízo dos encaminhamentos necessários à apuração de responsabilidades, dará ciência do fato à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR;

XIV - Monitoramento contínuo de segurança: a infraestrutura de TI e os sistemas aplicativos serão monitorados continuamente quanto a atividades suspeitas e possíveis violações de segurança; e

XV - Uso apropriado: todos os usuários da infraestrutura e dos sistemas da ANM estarão sujeitos às políticas e requisitos de uso apropriados da informação e seus

ativos.

CAPÍTULO V

DAS NORMAS E PROCEDIMENTOS ESPECÍFICOS

Art. 9o As normas e procedimentos específicos, necessários à implementação da POSIC, serão sugeridas pelo Comitê de Governança Digital - CGD da ANM (instituído pela Portaria no 8 de 03 de janeiro 2020), e posteriormente aprovadas pela Diretoria Colegiada da ANM.

Parágrafo único. Para cada um dos princípios e diretrizes relacionadas nesta política devem ser observadas a pertinência na elaboração de procedimentos, orientações e/ou manuais que disciplinem ou facilitem o entendimento da POSIC.

CAPÍTULO VI

DAS COMPETÊNCIAS E RESPONSABILIDADES

Seção I

Do Comitê de Governança Digital

Art. 10o O Comitê de Governança Digital (CGD/ANM), instituído pela PORTARIA

No 8, DE 03 DE JANEIRO DE 2020 da ANM, é o órgão de caráter consultivo e deliberativo vinculado à Diretoria Colegiada, de atuação permanente, que tem por objetivo o estabelecimento de políticas e diretrizes estratégicas transversais relativas à Governança de Tecnologia da Informação e Comunicação (TIC) e à Segurança da Informação e Comunicação (SIC).

Art. 11o São competências do CGD/ANM dentre outras:

I - aprovar, monitorar e manter a Política de Segurança da Informação (POSIC) da ANM e as normas internas de segurança da informação, observadas as disposições do art. 15 do Decreto no 9.637, de 26 de dezembro de 2018, e as normas de segurança da informação editadas pelo Gabinete de Segurança Institucional da Presidência da República;

ISSN 1677-7042 No 9, quinta-feira, 14 de janeiro de 2021

II - assessorar na implementação das ações de segurança da informação; e III - propor alterações na política de segurança da informação interna. Seção II

Do Gestor de Segurança da Informação e Comunicações

Art. 12o Compete ao Gestor de Segurança da Informação e Comunicações da ANM:

I - promover cultura de segurança da informação e comunicações;

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

III - realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na segurança da informação e comunicação da organização; e

IV - manter contato direto com o Departamento de Segurança da Informação e Comunicações (DSIC/GSI/PR) para o trato de assuntos relativos à segurança da informação e comunicações.

Art. 13o O Gestor de Segurança da Informação e Comunicações da ANM e o seu substituto serão designados em portaria ou resolução específica.

Seção III

Dos usuários

Art. 14o Compete aos usuários da ANM:

I - cumprir fielmente as políticas, normas, os procedimentos e as orientações de segurança da informação e comunicações da ANM;

II - buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

III - assinar o Termo de Responsabilidade, formalizando a ciência e o aceite da POSIC, bem como assumindo a responsabilidade por seu cumprimento;

IV - proteger as informações contra acesso, modificação, destruição ou divulgação não autorizadas pela ANM; e

V - assegurar que os recursos tecnológicos à sua disposição no local de trabalho sejam utilizados apenas para as finalidades da Agência. CAPÍTULO VII

DAS PENALIDADES

Art. 15o A não observância desta política e/ou de seus documentos complementares, bem como a quebra de controles de segurança da informação e comunicações, poderá acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

CAPÍTULO VIII

DA REVISÃO E ATUALIZAÇÃO

Art. 16o Esta política, bem como o conjunto de instrumentos normativos gerados a partir dela, serão revisados de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 02 (dois) anos.

Art. 17o Esta Resolução entra em vigor na data de sua publicação.

VICTOR HUGO FRONER BICCA
Diretor-Geral