MINISTÉRIO DE MINAS E ENERGIA / SECRETARIA DE GEOLOGIA, MINERAÇÃO E TRANSFORMAÇÃO MINERAL / SERVIÇO GEOLÓGICO DO BRASIL – CPRM	**POLÍTICA**	
Assunto: **Política de Segurança da Informação (POSIN)**	Aprovação: **ATA CA nº 333, de 8 de julho de 2024.**	Vigência: **08/07/2024**

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - POSIN

DA COMPANHIA DE PESQUISA DE RECURSOS MINERAIS - CPRM

1. OBJETIVO

Art. 1º Esta Política de Segurança da Informação (POSIN) tem o objetivo de estabelecer diretrizes estratégicas, responsabilidades, competências, além de regulamentar a elaboração de normas e procedimentos de uso, visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados, informações, sistemas, documentos, correspondências e publicações, bem como seus repositórios ou meios de armazenamento, que se constituem em ativos reconhecidamente necessários ao desempenho das atribuições da Companhia de Pesquisa de Recursos Minerais (CPRM), contra as ameaças que possam comprometer tais ativos, ou a sua própria imagem institucional.

§ 1º As diretrizes estabelecidas nesta Política são alinhadas ao Planejamento Estratégico Institucional (PEI) e ao Plano Diretor de Tecnologia da Informação (PDTI).

§ 2º Integram também a POSIN as normas e os procedimentos complementares derivados desta Política destinados à proteção da informação e à disciplina de sua utilização.

§ 3º A POSIN trata das diretrizes gerais acerca do uso e compartilhamento de ativos de informação durante todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte), visando à continuidade dos processos vitais da CPRM, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, bem como os valores éticos e as melhores práticas de Segurança da Informação (SI).

2. ALCANCE

Art. 2º Estão submetidos a esta Política todos os Agentes Públicos à serviço da CPRM, incluídos todos aqueles que, de alguma forma, exerçam atividades no âmbito da CPRM, bem como qualquer pessoa, física ou jurídica, que venha a ter acesso a qualquer Informação da CPRM.

Art. 3º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pela CPRM deverão incluir dispositivos de forma a viabilizar ou facilitar a implementação do disposto nesta POSIN.

3. CONCEITUAÇÃO

Art. 4º Para os fins dispostos nesta Política de Segurança da Informação (POSIN), aplica-se a seguinte conceituação técnica:

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 no âmbito da CPRM.

II - AMEAÇA: conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização.

III - ANÁLISE DE RISCOS: uso sistemático de informações para identificar fontes e estimar o risco.

IV - AVALIAÇÃO DE RISCOS: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

V - ATIVIDADE CRÍTICA: atividade que deve ser executada visando garantir a consecução de produtos e serviços fundamentais do órgão ou entidade, de forma a atingir os objetivos mais importantes e sensíveis ao tempo.

VI - 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.

VII - 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.

VIII - CLASSIFICAÇÃO DA INFORMAÇÃO: processo focado em garantir um nível adequado de proteção da informação conforme à sua sensibilidade.

IX - 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.

X - 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.

XI - INCIDENTE: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

XII - INCIDENTE DE SEGURANÇA: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

XIII - INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

XIV - INTEGRIDADE: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

XV - PLANO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO: documentação dos procedimentos e das informações necessárias para que os órgãos ou entidades da administração pública federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local

alternativo, em um nível previamente definido, em caso de incidente.

XVI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: documento aprovado pela autoridade responsável pelo órgão ou entidade da administração pública federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação. Este termo substituiu o termo Política de Segurança da Informação e Comunicação.

XVII - POSIC: sigla de Política de Segurança da Informação e Comunicação. Substituído pela sigla POSIN.

XVIII - POSIN: sigla de Política de Segurança da Informação. Substituiu a sigla POSIC.

XIX - SEGURANÇA DA INFORMAÇÃO: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

XX - 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.

XXI - VULNERABILIDADE: condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha.

4. BASE LEGAL E NORMATIVA

Art. 5º A Política de Segurança da Informação foi elaborada em consonância com a seguinte base legal e normativa:

I - ABNT NBR ISO/IEC 27001.

II - ABNT NBR ISO/IEC 27002.

III - Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

IV - Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação (LAI).

V - Decreto nº 9.637, de 26 de dezembro de 2018 - Política Nacional de Segurança da Informação.

VI - Instrução Normativa - IN/GSI/PR nº 1, de 27 de maio de 2020 - Estrutura de Gestão da Segurança da Informação.

VII - PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021.

5. DOS PRINCÍPIOS

Art. 6º As ações relacionadas à Segurança da Informação (SI) na CPRM são norteadas pelos seguintes princípios:

I - Legalidade: a POSIN levará em consideração o disposto na legislação, bem como as normativas internas emanadas pela própria CPRM e, naquilo em que for aplicável, as normas, as instruções, as melhores práticas e as políticas administrativas, organizacionais, técnicas e operacionais formalmente estabelecidas.

II - Impessoalidade: a POSIN visará ao interesse público no tratamento das informações, buscando evitar que estas sejam utilizadas para finalidades particulares ou para a obtenção de benefícios pessoais.

III - Moralidade: a elaboração da POSIN, bem como sua posterior aplicação, deverá observar os preceitos da boa administração pública, pautando-se pela atuação ética e nos ideais de honestidade e justiça.

IV - Publicidade: as diretrizes, normas e procedimentos da POSIN definidos pela CPRM devem ser publicados e amplamente divulgados para o balizamento dos agentes públicos no pleno desempenho de suas atribuições.

V - Responsabilidade: a POSIN deverá ser seguida pelos agentes públicos no exercício de suas atividades, pautando-se por atitudes e comportamentos condizentes com as diretrizes, normas e procedimentos de SI.

VI - Proporcionalidade: a aplicação da POSIN, no que abrange o nível, a complexidade e o custo das ações deverá ser adequada aos valores dos ativos a serem protegidos.

VII - Privacidade: os dados pessoais de pessoas naturais, quando tratados pela CPRM no âmbito de suas atividades, devem estar consoantes com o interesse público ou com o consentimento do titular para assegurar-lhe a inviolabilidade da intimidade, da honra e da imagem.

VIII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

IX - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

6. DA ESTRUTURA E GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 7º A POSIN é proposta pelo Gestor de Segurança da Informação (GSIN) e aprovada pelo Comitê de Segurança da Informação (CSI).

§ 1º Por iniciativa do GSIN, grupos de trabalho podem ser formados para conceber, planejar ou realizar atividades específicas de Segurança da Informação.

§ 2º A recepção, a análise e o tratamento de eventos de SI serão realizados pela Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

7. DAS DIRETRIZES

Art. 8º As Diretrizes a seguir devem nortear a atuação dos Agentes Públicos da CPRM, definidos no artigo 2º desta Política, com relação à Segurança da Informação e à utilização dos recursos de Tecnologia da Informação (TI).

7.1. Do uso das Informações de TI

Art. 9º As informações tratadas referentes à CPRM são patrimônio da Empresa, excluindo dados de terceiros que façam referência à CPRM. As informações são classificadas, quanto ao nível de sigilo, e manipuladas de acordo com normas e legislação específica em vigor, mantendo a segurança durante todo o seu ciclo de vida.

Parágrafo único. O uso das informações deverá ser feito apenas para o desempenho das atividades profissionais.

Art. 10. Todos os contratos celebrados pela CPRM com prestadores de serviços devem conter cláusulas que determinem a observância da POSIN e seus respectivos documentos, bem como a manutenção do sigilo de suas informações durante e após sua vigência.

Art. 11. Os prestadores de serviços sob contrato com a CPRM serão obrigados a assinar Termo de Aceitação, em obediência ao estabelecido na POSIN.

7.2. Do uso de Recursos de TI

Art. 12. Os recursos de tecnologia da informação vinculados às unidades da CPRM, colocados à disposição para uso como ferramenta de trabalho, devem ser utilizados em atividades primordialmente relacionadas às funções institucionais desempenhadas pela empresa.

Parágrafo único. É vedado o uso de recursos computacionais para armazenar ou transmitir conteúdo ilegal, difamatório, invasivo à privacidade, obsceno ou injurioso.

Art. 13. É vedada a utilização dos recursos de tecnologia da informação com o objetivo de praticar ações prejudiciais ao funcionamento e à utilização de quaisquer recursos da rede de computadores da CPRM ou redes externas.

Parágrafo único. Caberá a CPRM identificar as vulnerabilidades e mensurar os riscos, adotando as medidas preventivas cabíveis junto as áreas responsáveis a fim de evitar quaisquer efeitos danosos ou impactos indesejáveis ao ambiente computacional e ao trabalho dos usuários.

Art. 14. O uso dos recursos computacionais pelos colaboradores da rede da CPRM está sujeito à monitoração, respeitando-se os princípios constitucionais e legais aplicáveis.

Art. 15. É vedado aos colaboradores não autorizados alterar, física ou logicamente, as estações de trabalho disponibilizadas pela empresa.

Art. 16. O uso de recursos criptográficos deverá ser considerado no trânsito e no armazenamento das informações, de acordo com a classificação quanto ao nível de sigilo.

Art. 17. O uso dos recursos tecnológicos, postos à disposição do Agente Público a serviço da CPRM, em sua estação de trabalho, devem ser pautados pelo resguardo dos equipamentos e das informações neles produzidos, estejam eles fisicamente na mesa de trabalho, ou digitalmente, na tela do computador, sobretudo, quando o colaborador estiver ausente de sua estação de trabalho, de forma a evitar a sua subtração ou seu uso indevido por terceiros.

7.3. Da gestão de ativos de informação

Art. 18. As informações e dados produzidos ou recebidos pela CPRM serão considerados públicos, ressalvadas as exceções previstas na legislação aplicável.

Art. 19. 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 CPRM 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 mecanismos que permitam a rastreabilidade do uso desses ativos;

VI - ser regulamentados por norma específica quanto a sua utilização; e

VII - 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. 20. Para realização das atividades, uso de sistemas e acesso a redes corporativas, devem ser utilizados estritamente ativos de informação, sendo vedado o uso de dispositivos pessoais, excetuando-se ocasiões previamente definidas pela CPRM ou para uso de redes formalmente estabelecidas para acesso de visitantes.

Art. 21. Os Agentes Públicos contratados pela CPRM devem utilizar apenas recursos tecnológicos (*softwares e hardwares*) formalmente definidos pela DIINFO como apropriados para determinada atividade, independentemente do regime de trabalho adotado.

Art. 22. Cada ativo de informação da CPRM deverá ter um gestor designado pelo CSI.

Art. 23. A definição do custodiante do ativo de informação, deve ser feita formalmente pelo gestor do ativo de informação.

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

Art. 24. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 25. Durante todo o ciclo de vida de um ativo de informação, sua manipulação e uso observarão medidas especiais de segurança compatíveis com seu grau de sigilo e em conformidade com a legislação vigente e normas complementares adotadas pela CPRM.

Art. 26. O acesso dos Agentes Públicos contratados pela CPRM aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite do Termo de Sigilo e Responsabilidade.

7.4. **Do tratamento de incidentes de segurança**

Art. 27. Nos contratos de serviços relacionados ao provimento, gerenciamento e suporte da infraestrutura computacional de TI, deverá constar cláusula que exija a existência de estrutura de tratamento de incidentes de Segurança da Informação (SI) por parte do prestador.

Parágrafo único. Em relação aos contratos mencionados no *caput*, cabe à Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) comunicar os incidentes de segurança ao Encarregado pela Proteção de Dados da CPRM, bem como supervisionar o tratamento desses para o fiel cumprimento das suas atribuições.

7.5. **Da gestão de risco**

Art. 28. A gestão de riscos corporativos em SI constitui um processo contínuo de planejamento, execução, verificação e revisão das ações que visem manter em níveis aceitáveis os riscos de SI a que estão sujeitos os ativos de informação da CPRM.

Parágrafo único. A gestão de riscos de SI deve contemplar a execução

desta Política de Segurança da Informação e privacidade dos dados, bem como identificar e avaliar os eventos que podem prejudicar para este atingimento.

Art. 29. O processo de gestão de riscos corporativos em SI deverá observar a metodologia estabelecida na Política de Gestão de Riscos Corporativos da CPRM, contemplando as etapas de estabelecimento do contexto, identificação, análise, tratamento, monitoramento e comunicação dos riscos, de forma a proteger os ativos de informação da Empresa.

§ 1º Nas etapas de identificação, análise e tratamento dos riscos de SI deverão ser levantados e definidos os eventos, causas, impactos e responsáveis pelos riscos, contendo definição dos atributos de impacto e probabilidade, para elaboração do Mapa de Riscos, de forma a dar suporte para priorização de esforços e minimização dos principais riscos, de acordo com a Declaração de Apetite a Riscos da CPRM.

§ 2º Na etapa de monitoramento dos riscos de SI, deverá ser supervisionada a implementação e manutenção dos respectivos planos de ações e iniciativas previstas na etapa de tratamento dos riscos, e o alcance das metas estabelecidas, por meio de atividades gerenciais contínuas e/ou avaliações independentes pela área responsável.

§ 3º Na etapa de comunicação dos riscos identificados, deverão ser apresentadas informações confiáveis, íntegras e tempestivas, de forma contínua e interativa, permeando todo o processo de Gestão de Riscos Corporativos no âmbito da CPRM.

7.6. Da continuidade de negócios

Art. 30. A Gestão de Continuidade de Negócios compreenderá um conjunto de normas e procedimentos que visem assegurar o funcionamento contínuo ou recuperação antecipada da CPRM quando da ocorrência de indisponibilidade de recursos de infraestrutura, de tecnologia ou de recursos humanos, isolada ou simultaneamente.

Art. 31. O Plano de Continuidade de Negócios da CPRM, baseado em metodologias e boas práticas e aprovado pelo Comitê de Segurança da Informação (CSI), deverá ser desenvolvido, implementado e testado periodicamente para garantir a continuidade dos serviços críticos.

Art. 32. O Plano de Continuidade de Negócios deve ser amparado por um processo de *backups* (físico e lógico) dos dados organizacionais com redundâncias e retenções adequáveis em conformidade com a política de *backup* institucional.

7.7. Da auditoria e conformidade

Art. 33. A CPRM manterá registros e procedimentos, como trilhas de auditoria e outros, que assegurem o rastreamento, acompanhamento, controle e verificação de acessos aos seus ativos de informação, considerando sua criticidade.

Art. 34. Os processos de negócio, em todas as áreas da CPRM, deverão ser auditados em conformidade com as normas de Segurança da Informação e a legislação pertinente em vigor.

Art. 35. É vedado ao prestador de serviços a responsabilidade de executar a verificação de qualquer conformidade de seus serviços.

Art. 36. A verificação da conformidade será realizada pela área competente, de forma planejada, mediante calendário de ações proposto pelo Gestor de Segurança da Informação (GSIN) e aprovado pelo Comitê de Segurança da Informação (CSI).

Parágrafo único. Os resultados de cada ação de verificação de conformidade, em segurança da informação, serão documentados em relatório de avaliação de conformidade, pela área competente, o qual será encaminhado pelo Gestor de Segurança da Informação (GSIN) ao Comitê de Segurança da Informação (CSI), devendo ser elaborado um plano de ação para a tomada das ações cabíveis.

Art. 37. Verificar se as atividades relacionadas ao tratamento de dados estão em consonância com as exigências da Lei Geral de Proteção de Dados Pessoais (LGPD).

7.8. Dos controles de acesso

Art. 38. As instalações, equipamentos, redes e sistemas de computadores, exceto os sistemas destinados a atendimento ao público, deverão possuir mecanismos adequados de controle de acesso físico e/ou lógico, que possibilitem a identificação do usuário.

Art. 39. O controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa.

Art. 40. Para utilização dos recursos de TI da CPRM será sempre necessária a autenticação de todo colaborador ou visitante, mediante credencial de acesso.

§ 1º As responsabilidades pela segurança da informação devem ser definidas nas descrições de cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimento sobre a CPRM.

§ 2º As credenciais de acesso deverão delegar a seu portador somente os níveis de privilégio mínimos ao exercício de sua função.

Art. 41. Os equipamentos e softwares utilizados na administração dos recursos de TI deverão ser protegidos por senha, que será de conhecimento exclusivo dos técnicos da Central de Serviços e/ou terceiros responsáveis pela administração destes recursos.

Parágrafo único. Os administradores dos recursos de TI da CPRM são responsáveis pelo uso adequado dos recursos sob sua responsabilidade, devendo zelar pela integridade, disponibilidade e confidencialidade dos sistemas e dos dados sob seus cuidados.

Art. 42. Na ocorrência de afastamento, mudança de responsabilidades e de lotação ou atribuições dentro da empresa, os direitos de acesso e uso dos ativos deverão ser atualizados, com a revogação de todos os acessos e posterior autorização dos novos acessos necessários.

§ 1º Em casos de afastamentos por férias, licença por saúde ou cessão a outro órgão, os acessos do colaborador serão temporariamente suspensos, enquanto durar o referido afastamento.

§ 2º Na efetivação do desligamento do usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos de informação a ele atribuídos.

Art. 43. A senha de acesso é de uso pessoal e intransferível e sua divulgação é vedada sob qualquer hipótese, devendo ser alterada pelo próprio colaborador, a qualquer tempo, ou por determinação da DIINFO, especialmente quando houver suspeita de sua violação.

Parágrafo único. Qualquer utilização dos sistemas e demais recursos de informática da CPRM é de responsabilidade do colaborador ao qual estejam

associadas as credenciais de acesso utilizadas.

Art. 44. A senha de rede valerá por prazo determinado, em normatização complementar estabelecida pela Divisão de Informática (DIINFO).

Parágrafo único. A Divisão de Informática (DIINFO) divulgará as regras a serem seguidas na definição da senha de rede dos colaboradores, além de recomendações que visem assegurar a maior privacidade possível da senha.

Art. 45. Deverão ser implementados controles de acesso físico para o acesso às dependências da CPRM, com a disponibilização de credenciais que permitam o acesso de todos os Agentes Públicos às instalações da empresa, respeitando o mínimo privilégio ao exercício de sua função.

Art. 46. Deverão ser disponibilizadas credenciais de acesso físico também aos visitantes, que permitirão o acesso destes às instalações da CPRM, sempre mediante autorização de Agente Público da área visitada.

§ 1º Os visitantes não poderão possuir credenciais de acesso a redes e sistemas de computadores da CPRM, exceto nos casos de redes destinadas para tais pessoas, mediante autorização expressa da Divisão de Informática (DIINFO) e casos previstos em lei.

§ 2º Nos casos de invalidação temporária ou definitiva das credenciais de acesso de colaboradores, o acesso aos ativos de informação da empresa dar-se-á mediante as condições estabelecidas para os visitantes.

7.9. Do desenvolvimento de sistemas

Art. 47. O Comitê de Segurança da Informação (CSI) deverá estabelecer critérios de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção.

Art. 48. Os desenvolvimentos e aquisições de sistemas e aplicações corporativas devem atender a requisitos de segurança previstos em norma específica.

8. PENALIDADES

Art. 49. As ações que violem as diretrizes desta Política de Segurança da Informação (POSIN), normas e procedimentos ou que quebrem os controles de Segurança da Informação (SI), identificados pelo Comitê de Segurança da Informação, deverão ser comunicadas ao Gestor de Segurança da Informação, que deverá avaliar as situações que serão encaminhadas à Corregedoria, para apuração de responsabilidades e aplicação das respectivas penalidades.

9. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO DA CPRM

Art. 50. Esta POSIN é alinhada com os objetivos estratégicos institucionais e com as normas pertinentes, respeitadas as restrições orçamentárias, por meio das seguintes iniciativas que visam a:

I - garantir a difusão da Segurança da Informação dentro da CPRM;

II - promover a melhoria da segurança das informações institucionais de forma contínua;

III - promover a capacitação e conscientização relativas à Segurança da Informação; e

IV - regulamentar e operacionalizar as diretrizes estabelecidas nas normas relativas à Segurança da Informação.

10. DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 51. Compete à Divisão de Informática (DIINFO):

I - implantar ações técnicas para os controles de segurança dos ativos de informação;

II - encaminhar solicitação dos recursos necessários para implantação desta POSIN, no limite de suas atribuições, à Diretoria Executiva, para as providências cabíveis;

III - prestar assessoria técnica aos gestores de ativos e ao Comitê de Segurança da Informação, nos temas relacionados à TI;

IV - informar ao Comitê de Segurança da Informação situações que eventualmente comprometam a Segurança da Informação;

V - operacionalizar a Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) no âmbito de suas atribuições;

VI - monitorar o uso dos recursos computacionais; e

VII - promover o aperfeiçoamento constante de seu corpo técnico quanto às boas práticas e tecnologias de Segurança da Informação.

Art. 52. Compete à Diretoria de Administração e Finanças (DAF):

I - notificar a Diretoria de Infraestrutura Geocientífica (DIG) sobre qualquer alteração de cargo, função ou lotação dos empregados ou dos usuários indicados no artigo 2º desta Política, bem como sobre afastamentos destes por períodos superiores a 30 (trinta) dias; e

II - promover a capacitação dos usuários indicados no artigo 2º desta Política, nas normas de Segurança da Informação e nos procedimentos complementares derivados desta Política destinados à proteção da informação e à disciplina de sua utilização.

Art. 53. Compete aos Superintendentes Regionais e Chefes de Departamento:

I - indicar as necessidades de treinamento dos usuários indicados no artigo 2º desta Política, em cada unidade de lotação, pelas quais são responsáveis no que diz respeito às normas de Segurança da Informação adotadas pela CPRM;

II - indicar as necessidades de concessão/revogação de credenciais de acesso para os Agentes Públicos nos ativos de informação de sua responsabilidade;

III - classificar, respeitando a Lei nº 12.527, de 18 de novembro de 2011, (Lei de Acesso a Informação - LAI) e demais normativos pertinentes, os ativos de informação sob sua responsabilidade;

IV - determinar o nível de acesso dos seus subordinados e terceiros frente aos ativos de informação sob sua responsabilidade; e

V - solicitar o credenciamento e descredenciamento de Agentes Públicos associados a contratações sob sua responsabilidade.

Art. 54. Compete aos usuários indicados no artigo 2º desta Política:

I - conhecer e disseminar institucionalmente esta POSIN e as normas complementares de Segurança da Informação, propondo, inclusive, apresentar

sugestões de melhoria;

II - cumprir e fazer cumprir as normas e procedimentos relativos à segurança da informação da CPRM;

III - informar imediatamente à Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) e ao Encarregado pela Proteção de Dados da CPRM qualquer evento relacionado à Segurança da Informação;

IV - zelar pelo sigilo das suas credenciais de acesso aos ativos de informação da CPRM;

V - comunicar a perda ou o comprometimento das suas credenciais de acesso;

VI - responder pela quebra de segurança ocorrida com a utilização da sua credencial de acesso; e

VII - manter o nível de proteção da informação a que tem acesso.

Art. 55. As competências do Gestor de Segurança da Informação e do Comitê de Segurança da Informação deverão ser definidas em normativos específicos.

11. DISPOSIÇÕES FINAIS

Art. 56. Esta Política de Segurança da Informação será complementada por normas, procedimentos e outros documentos pertinentes, os quais serão considerados partes integrantes desta Política.

Art. 57. As propostas de alteração ou criação de instrumentos normativos internos sobre Segurança da Informação deverão ser encaminhadas ao Comitê de Segurança da Informação.

Art. 58. Após sua publicação, o Comitê de Segurança da Informação deverá dar ampla divulgação da Política de Segurança da Informação a todos os Agentes Públicos no âmbito da Empresa.

Art. 59. Os casos omissos e as dúvidas surgidas na aplicação desta Política serão dirimidos pelo Comitê de Segurança da Informação.

Art. 60. A Política de Segurança da Informação está atrelada aos objetivos estratégicos da CPRM e deve ser observada por toda sua estrutura organizacional: Conselho de Administração, Diretoria Executiva, Conselho Fiscal, Comitê de Auditoria, Comitê de Elegibilidade, Corregedoria, Ouvidoria, Comissão de Ética, órgão interno de Governança e Auditoria Interna, além de todos os Agentes Públicos usuários dos serviços de TI no âmbito da Empresa.

Art. 61. A presente Política, atribuída ao Processo SEI nº 48035.004800/2022-42, aprovada pelo Conselho de Administração em reunião realizada em 08/07/2024 (ATA CA nº 333), revoga e substitui a Política de Segurança da Informação - Tecnologia da Informação, bem como a Política Normativa - Tecnologia da Informação, vigentes até a data de publicação desta Política.

Art. 62. A Política de Segurança da Informação integra o Rol de Políticas da Empresa e vigerá pelo período de 2 (dois) anos, a partir da data de sua aprovação pelo Conselho de Administração.

Art. 63. A presente Política deverá ser revisada e/ou atualizada sempre que eventos ou mudanças significativas relativas ao tema assim o exigirem ou a cada período de 2 (dois) anos de vigência.

Art. 64. O Departamento de Informática (DEINF) é responsável pelo histórico, controle e atualização desta Política, cabendo à Área de Controles Internos da Governança, a sua compatibilização com os instrumentos normativos em vigor, bem como a sua publicação e divulgação no âmbito da Empresa.

Documento assinado eletronicamente

CONSELHO DE ADMINISTRAÇÃO

COMPANHIA DE PESQUISA DE RECURSOS MINERAIS – CPRM

Distribuição: Geral

Chancelas:

Análise Técnica:	Governança
Análise Jurídica:	Consultoria Jurídica

Documento assinado eletronicamente por **JULIANO DE SOUZA OLIVEIRA**, **Chefe da Governança**, em 15/07/2024, às 15:44, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Breno Zaban Carneiro**, **Membro do Conselho de Administração**, em 31/07/2024, às 09:25, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site sei.sgb.gov.br/autenticidade, informando o código verificador **2146082** e o código CRC **FDE342DF**.

Referência: Processo nº 48035.004800/2022-42 SEI nº 2146082