Política Administrativa

Assunto: Segurança da Informação.	**Feixe:** Administrativo.
Identificação: POL-0007-G / Versão: 06.	**Uso:** Público.
Deliberação: DDE 017/2025.	**Emissão em:** 17/02/2025.
Responsável: Diretoria de Tecnologia e Inovação.	**Revisão até:** 17/02/2030.

1. Diretrizes Gerais

A Vale está comprometida em atuar na segurança das informações e dos Recursos Tecnológicos baseada nos quatro pilares da segurança da informação na Companhia:

Confidencialidade: a Informação só pode ser conhecida por quem possui autorização prévia.

Integridade: a Informação deve estar íntegra e só pode sofrer alteração por pessoas ou processos autorizados.

Disponibilidade: a Informação deve estar disponível para as pessoas autorizadas sempre que necessário.

Autenticidade: o serviço de autenticidade serve para provar quem realizou a operação e garantir que sua origem seja confiável e legítima.

Desta forma, é dever de todos[1] proteger as Informações e os Recursos Tecnológicos sob sua responsabilidade, de acordo com a classificação da Informação (Uso Interno, Público, Confidencial e Restrito), devendo observar as diretrizes para a segurança da informação estabelecidas a seguir, de modo a evitar que informações sejam divulgadas, compartilhadas ou utilizadas de forma inadequada podendo ou não causar potenciais impactos à Vale, Pessoal-Chave da Administração, Empregados, Fornecedores, Parceiros, Partes Interessadas e Clientes.

- Toda a aquisição de Recursos Tecnológicos no ambiente Vale deve respeitar os padrões e processos da segurança da informação.
- O acesso às informações e aos Recursos Tecnológicos da Vale deve seguir os princípios de segregação de função e gestão de acesso e deve ser controlado e restrito àqueles que tenham a legítima necessidade de conhecimento e utilização de acordo com a função que lhes é atribuída.
- Toda Informação e Recursos Tecnológicos produzidos ou adquiridos pela Vale e suas controladas, bem como as Informações produzidas por fornecedores ou parceiros para a Vale são considerados parte do patrimônio da Vale, nos casos e na extensão previstos nos respectivos contratos, devendo ser adequadamente protegidos e estar em conformidade com a legislação e os demais requisitos legais vigentes.
- Os Recursos Tecnológicos, de uso individual, de propriedade da Vale e/ou disponibilizados pela Vale, não devem ser utilizados como meios de armazenamento de cunho pessoal, não sendo de responsabilidade da Vale a proteção dessas Informações. Credenciais de empregados, como crachá e contas de acesso, são únicas, individuais e intransferíveis.

2. Abrangência

Esta Política aplica-se à Vale e às suas controladas[2], observando sempre o Estatuto Social, os respectivos documentos constitutivos e a legislação aplicável, devendo ser observada pelos Empregados e pelo Pessoal-Chave da Administração.

Espera-se que Clientes, Fornecedores e Parceiros da Vale e de suas controladas conheçam esta Política e pautem sua conduta em linha com as melhores práticas de segurança da informação, bem como com as diretrizes aqui estabelecidas.

[1] Qualquer pessoa que tenha acesso às informações relacionadas ao Sistema Vale, podendo ser empregados , Pessoal-Chave da Administração, em ambiente próprio ou terceirizado, localizado dentro ou fora das instalações da empresa.
[2] Para saber mais sobre a classificação das controladas, consulte a POL-0043-G - Política de Gestão de Empresas e Entidades do Grupo Vale.

3. Referências

- POL-0001-G - Código de Conduta.
- POL-0009-G - Política de Gestão de Riscos.
- POL-0034-G - Política de Proteção e Privacidade de Dados Pessoais.
- POL-0041-G - Gestão de Desvios de Conduta.

4. Definições:

Clientes: qualquer cliente, inclusive seus intermediários, de produtos ou serviços da Vale ou de suas controladas.

Empregados: qualquer empregado Vale e/ou de suas controladas integrais, permanentes ou temporários, estagiários, jovens aprendizes e/ou trainees.

Fornecedores: qualquer fornecedor de bens ou prestador de serviços, incluindo consultores, agentes, representantes comerciais, despachantes, intermediários, entre outros.

Informação: entende-se por Informação todo e qualquer conteúdo, digital ou não, que trate de assuntos relacionados à Vale e as empresas e entidades do Sistema Vale ou que estejam circulando em ambiente, físico ou digital, controlado pela Companhia.

Parceiros: para fins desta Política, quaisquer sociedades ou entidades (associações, instituições, organizações etc.) com a qual a Vale (ou suas controladas) realize algum tipo de parceria comercial, técnica, social, institucional, entre outras, que não se configuram como Cliente ou Fornecedor.

Partes Interessadas: comunidades, investidores e terceiros.

Pessoal-Chave da Administração: Para os fins da presente Política, são os membros do Conselho de Administração, do Comitê Executivo, dos Comitês de Assessoramento ao Conselho de Administração, Conselho Fiscal, os executivos que se reportem diretamente ao Conselho de Administração da Companhia e ao Presidente e os Vice-Presidentes Executivos não estatutários que se reportam diretamente ao Presidente.

Recursos Tecnológicos: são os equipamentos (computadores, tablets, celulares), softwares, aplicativos, incluindo aqueles que contenham funcionalidades de inteligência artificial, *drivers* de rede ou da nuvem e outros.

5. Governança

Segundo a Norma e a Política de Gestão de Riscos, os riscos da Companhia, incluindo os cibernéticos, são identificados, monitorados, reportados e revisados pelos cargos gerenciais apropriados até o nível do Conselho de Administração, sendo que o Comitê Executivo conta com o apoio dos Comitês Executivos de Riscos, conforme área de atuação.

6. Responsabilidades

Comitê Executivo da Vale:

- Aprovar a presente Política e suas alterações.

Vice-Presidência Executiva de Assuntos Corporativos e Institucionais:

- Avaliar esta Política e qualquer alteração proposta, orientando todas as instâncias envolvidas sobre aspectos legais aplicáveis.

Vice-Presidência de Finanças e Relações com Investidores:

- Monitorar a execução das ações de disseminação relacionadas a esta Política.

Diretoria de Tecnologia e Inovação:

- Definir e operar uma arquitetura tecnológica moderna, ágil, que atenda aos requisitos de negócio, utilizando as melhores práticas de segurança da informação.
- Desenvolver sistemas e ferramentas utilizando as melhores práticas de segurança da informação e de acordo com os padrões definidos pela área de arquitetura e de segurança da informação.
- Capacitar o público-alvo adequado, para que protejam as informações da Companhia.

- Monitorar os Recursos Tecnológicos de propriedade da Vale e/ou utilizados pelos Empregados, Pessoal-Chave da Administração ou qualquer pessoa que utilize tais recursos, sem prévia notificação, desde que restrita à identificação de potenciais ameaças cibernéticas[1].
- Reportar imediatamente para a Diretoria de Auditoria e Conformidade, caso seja identificada qualquer situação que enseje no descumprimento das Políticas e Normas da Vale, mesmo que não associadas ao risco cibernético.

Diretoria de Auditoria e Conformidade:

- Avaliar a efetividade das ações de disseminação relacionadas a esta Política.
- Acessar as informações e os Dados Pessoais disponíveis nos sistemas corporativos para fins de apuração do Canal de Denúncias, em conformidade com legislação aplicável e de acordo com as diretrizes desta Política.
- Acessar e auditar eventualmente ou de forma contínua, sem qualquer prévia notificação, Recursos Tecnológicos, sob responsabilidade da Vale e Informações que neles são processadas ou armazenadas de qualquer Empregado, Pessoal-Chave da Administração ou qualquer pessoa que utilize tais recursos.
- Disponibilizar, quando necessário, Recursos Tecnológicos e Informações para análise das áreas de apoio à apuração.

Gestores de Empregados próprios e de contratos:

- Difundir os princípios dessa Política e incentivar a participação dos profissionais em campanhas e treinamentos de segurança da informação.

Áreas custodiantes de sistemas e/ou informações digitais:

- Garantir o atendimento dos requisitos de disponibilidade, tempos e pontos de recuperação dos sistemas e/ou informações digitais, de acordo com o que foi determinado pelas demais áreas da Vale em seus planos de continuidade.

Todas as áreas da Vale:

- Identificar a dependência de sistemas e/ou informações digitais na elaboração do seu plano de continuidade.
- Determinar para a área custodiante dos sistemas e/ou informações digitais sua necessidade de disponibilidade, tempos e pontos de recuperação.

7. Divulgação e Disseminação

Esta Política será arquivada e publicada pela Vice-Presidência Executiva de Finanças e Relações com Investidores nos repositórios oficiais da Vale em atendimento ao público interno e externo, conforme aplicável, cabendo à Diretoria de Tecnologia e Inovação promover ações necessárias para disseminação desta Política.

8. Gestão de Consequências

O Canal de Denúncias da Vale pode ser utilizado por qualquer pessoa, dentro ou fora da empresa, que queira reportar um caso de suspeita ou violação ao nosso Código de Conduta e às diretrizes desta Política.

São exemplos de desvios de conduta relacionados à segurança da informação: a divulgação não autorizada de informações, tratamento e manipulação inadequados de dados e informações não respeitando a classificação da Informação, a violação ou uso de credenciais de outros usuários que não o próprio, dano, perda ou roubo de Informação, compartilhamento de senhas de acesso ou qualquer outra violação a esta Política.

O descumprimento desta Política estará sujeito aos termos da Política de Gestão de Desvio de Conduta, “POL-0041-G”.

9. Prazo de Revisão

Esta Política deve ser revisada no prazo máximo de 5 (cinco) anos, ou sempre que necessário, de forma a manter o seu conteúdo atualizado.

[1] Caso a ameaça cibernética se concretize, uma investigação de dispositivos tecnológicos pode ser necessária, desde que garanta minimamente a rastreabilidade das atividades realizadas.

10. Disposições Finais

Em caso de conflito entre esta Política e o Estatuto Social da Vale, este último prevalecerá, e a presente Política deverá ser alterada na medida do necessário.

Esta Política entra em vigor na data de sua aprovação pelo Comitê Executivo da Vale.

11. Aprovações

Áreas:	**Descrição:**
Diretoria de Tecnologia e Inovação.	Elaboração.
Vice-Presidência Executiva de Finanças e Relações com Investidores.	Revisão / Recomendação.
Vice-Presidência Executiva de Assuntos Corporativos e Institucionais.	Revisão / Recomendação.
Diretoria de Auditoria e Conformidade.	Revisão / Recomendação.
Comitê Executivo – **DDE 017/2025.**	Aprovação.

Administrative Policy

Subject: Information Security.	**Cluster:** Administrative
Identification: POL-0007-G / Version: 06.	**Use:** Public.
Deliberation: DDE 017/2025.	**Issued in:** 02/17/2025.
Responsible: Technology and Innovation Department.	**Review up to:** 02/17/2030.

1. General Guidelines

Vale is committed to securing information and technological resources based on four pillars of information security:

Confidentiality: Information can only be accessed by authorized individuals.

Integrity: Information must be complete and can only be altered by authorized individuals or processes.

Availability: the Information must be available to authorized individuals whenever needed.

Authenticity: Verifies the identity of the person performing the operation and ensures the origin is reliable and legitimate.

Everyone[1] is responsible for protecting information and technological resources according to their classification (Internal Use, Public, Confidential, and Restricted). Follow the guidelines below to prevent inappropriate disclosure, sharing, or use, which could impact Vale, key management personnel, employees, suppliers, partners, stakeholders, and customers.

- All acquisition of Technological Resources in the Vale environment must comply with information security standards and processes.
- Access to Vale's information and technological resources must follow principles of function segregation and access management and be restricted to those with a legitimate need based on their role.
- All information and technological resources produced or acquired by Vale and its subsidiaries, as well as those produced by suppliers or partners for Vale, are considered Vale's assets. They must be adequately protected and comply with legislation and current legal requirements.
- Technological Resources, for individual use, owned by Vale and/or made available by Vale, must not be used as means of personal storage, and it is not Vale's responsibility to protect this Information. Employee credentials, such as badges and access accounts, are unique, individual, and non-transferable.

2. Applicability

This Policy applies to Vale and its subsidiaries[2], always observing the social status, the respective constitutive documents and applicable legislation, and must be observed by employees and key management personnel. Customers, suppliers, and partners of Vale and its subsidiaries are expected to be aware of this policy and to align their conduct with the best information security practices and the guidelines established here.

3. References

- POL-0001-G - Code of Conduct.
- POL-0009-G - Risk Management Policy.
- POL-0034-G - Privacy and Personal Data Protection Policy.
- POL-0041-G - Management of Misconduct Policy.

[1] Anyone who has access to information related to the Vale System, which may be employees, Key Administration Personnel, in their own or outsourced environment, located inside or outside the company's facilities.

[2] To find out more about the classification of subsidiaries, see POL-0043-G - Vale Group Company and Entity Management Policy.

4. Definitions

Clients: any client, including its intermediaries, of products or services from Vale or its subsidiaries.

Employees: any employee of Vale and/or its wholly owned subsidiaries, permanent or temporary, interns, young apprentices and/or trainees.

Suppliers: any supplier of goods or service provider, including consultants, agents, commercial representatives, dispatchers, intermediaries, among others.

Information: Information means all content, digital or not, that deals with matters related to Vale and the companies and entities of the Vale System or that are circulating in an environment, physical or digital, controlled by the Company.

Partners: for the purposes of this Policy, any companies or entities (associations, institutions, organizations, etc.) with which Vale (or its subsidiaries) enters into any type of commercial, technical, social, institutional partnership, among others, that are not configured as a client or supplier.

Interested Parties: communities, investors and third parties.

Key Administration Personnel: for the purposes of this Policy, these are the members of the Board of Directors, Executive Committee, the Advisory Committees to the Board of Directors, the Fiscal Council, the executives who report directly to the Company's Board of Directors and the President and the non-statutory Executive VicePresidents who report directly to the President.

Technological Resources: equipment (computers, tablets, cell phones), software, apps, including those that contain artificial intelligence functionalities, network or cloud drivers and others.

5. Governance

According to the Risk Management Standard and Policy, the company's risks, including cyber risks, are identified, monitored, reported, and reviewed by appropriate management positions up to the level of the Board of Directors, with the Executive Committee having the support of the Executive Risk Committees, depending on the area of activity.

6. Responsibilities

Executive Committee:

- Approve this Policy and its amendments.

Executive Vice Presidency of Corporate and Institutional Affairs:

- Evaluate this Policy and any proposed changes, advising all instances involved on applicable legal aspects.

Executive Vice Presidency of Finance and Investor Relations:

- Monitor the execution of dissemination actions related to this Policy.

Technology and Innovation Department:

- Define and operate a technological, modern, and agile architecture that meets business requirements, using the best information security practices.
- Develop systems and tools using the best information security practices and in accordance with the standards defined by the architecture and information security area.
- Train the appropriate target audience to protect the Company's information.
- Monitor technological resources owned by Vale and/or used by Employees, key management personnel or anyone using such resources, without prior notification, if they are restricted to identifying potential cyber threats[1].

[1] If the cyber threat materializes, an investigation of technological devices may be necessary, as long as it minimally guarantees the traceability of the activities carried out.

- Report immediately to the Audit and Compliance Department if any situation is identified that leads to non-compliance with Vale's policies and standards, even if not associated with cyber risk.

Audit and Compliance Department:

- Make available, when necessary, technological resources and information for analysis of areas to support the investigation.

Managers of own Employees and contractors:

- Disseminate the principles of this policy and encourage the participation of professionals in information security campaigns and training.

Custodian areas of systems and/or digital information:

- Ensure compliance with availability requirements, times, and recovery points for systems and/or digital information, in accordance with what was determined by other areas of Vale in their continuity plans.

All areas of Vale:

- Identify the dependency on systems and/or digital information when developing your continuity plan.
- Determine the need for availability, times, and recovery points for the custodian area of the systems and/or digital information.

7. Disclosure and Dissemination

This policy will be archived and published by the Executive Vice-Presidency of Finance and Investor Relations in Vale's official repositories for internal and external audiences. The Technology and Innovation Department will be responsible for promoting the necessary actions to disseminate this Policy.

8. Consequence Management

Vale's Whistleblowing Channel can be used by anyone, inside or outside the company, who wants to report a case of suspicion or violation of our code of conduct and the guidelines of this Policy.

Examples of misconduct related to information security are the unauthorized disclosure of information, inappropriate treatment and manipulation of data and information without respecting the Information classification, the violation or use of credentials of users other than himself, damage, loss or theft of Information, sharing of access passwords or any other violation of this Policy.

Failure to comply with this policy will be subject to the terms of the Misconduct Management Policy, “POL-0041-G”.

9. Review Deadline

This Policy must be revised within a maximum period of 5 (five) years, or whenever necessary, in order to keep its content updated.

10. Final Provisions

In case of conflict between this Policy and Vale's By Laws, the latter will prevail, and this Policy must be changed as necessary.

This policy comes into effect on the date of its approval by Vale's Executive Committee.

11. Approvals

Areas:	**Description:**
Technology and Innovation Department.	Elaboration.
Executive Vice Presidency of Finance and Investor Relations.	Review / Recommendation.
Executive Vice Presidency of Corporate and Institutional Affairs.	Review / Recommendation.
Audit and Compliance Department.	Review / Recommendation.
Executive Committee – **DDE 017 /2025.**	Approval.