1. DEFINIÇÕES

TERMO	ACRÔNIMO	DEFINIÇÃO
Usuário	-	Agente que usa qualquer equipamento ou sistema de tecnologia da informação coberto pelos termos desta Política, seja um funcionário direto ou prestador de serviços;
Descarte	-	Eliminação de documentos físicos ou digitais vencidos, obsoletos e/ou duplicados. De preferência, os documentos físicos devem ser destruídos por meio de processos que permitam a reciclagem do papel e impossibilitem a leitura dos documentos.
Documento		Unidade composta de informações e seu suporte, produzida ou recebida como resultado da realização de uma atividade, preservada para servir como prova, testemunho e pesquisa.
Backup	-	Uma cópia de backup dos seus dados de um dispositivo ou sistema de armazenamento que pode ser acessado em caso de necessidade de recuperação.
Tabela de gerenciamento de informações	IMT	Um instrumento que estabelece o período de armazenamento da documentação da empresa em suas fases de arquivamento, considerando seu valor e a responsabilidade por esse armazenamento, identifica seus registros vitais e planos de contingência.
Taxonomia	-	Estrutura utilizada para classificar e armazenar todos os documentos gerados ou recebidos pela Brazilian Nickel S/A durante a execução de suas atividades.
Matriz de responsabilidade	-	Instrumento que estabelece quem é responsável por realizar e apoiar a gestão de documentos em cada área/programa, a fim de garantir a implementação e a manutenção do processo documental.
Informações confidenciais	-	Informações de natureza confidencial, destinadas a pessoas específicas, cuja divulgação não autorizada poderia causar danos e/ou riscos às finanças, à imagem ou à execução de projetos da empresa, que só podem ser acessadas por funcionários específicos.
Informações restritas	-	Informações que podem ser acessadas por funcionários de um setor ou grupo de trabalho específico.
Informações internas	-	Informações que podem ser acessadas e divulgadas internamente.
Informações ao público	-	Informações que podem ser acessadas e divulgadas dentro e fora das empresas do Grupo Brazilian Nickel S/A
Sistema de gerenciamento de informações	GED	Tecnologia que facilita o controle, o armazenamento, o compartilhamento e a recuperação de informações existentes. Pode ser um sistema de Gerenciamento Eletrônico de Documentos (GED) como SharePoint ou um sistema de Gerenciamento de Conteúdo (ECM).
Produtos e serviços de gerenciamento de informações	-	Qualquer iniciativa que vise armazenar, catalogar e gerenciar o conteúdo corporativo do Brazilian Nickel S/A, tais como: bibliotecas virtuais, bases de conhecimento, planos de ação, lições aprendidas, clippings, portais corporativos, catálogos on-line, entre outros.
Grupo	-	Todas as empresas são controladas direta ou indiretamente pelas empresas. O termo "subsidiária" e/ou "empresas controladas" é aquele definido pela Lei das Sociedades Anônimas (6.404/76).
Ativos da Informação	-	Patrimônio tangível e intangível da Brazilian Nickel S/A, que compreende tanto as informações propriamente ditas (de qualquer natureza), como os equipamentos de tecnologia da informação, hardwares, dados pessoais, sistemas e softwares, além de técnicas, know-how, e qualquer outra informação relacionada à Brazilian Nickel S/A e suas atividades.
Incidente de Segurança	-	Qualquer evento confirmado ou sob suspeita que comprometa ou possa comprometer a confidencialidade, integridade, disponibilidade ou autenticidade dos Ativos de Informação da Companhia. Isso inclui acessos não autorizados, perda, vazamento, destruição, alteração indevida, indisponibilidade, falhas operacionais, comportamentos anômalos, uso indevido de credenciais, ataques cibernéticos, malware, ou qualquer situação que represente risco à continuidade das operações, aos dados pessoais, às informações corporativas ou aos ativos críticos da organização.
Inteligência Artificial	IA	Qualquer sistema, modelo ou tecnologia capaz de realizar tarefas que normalmente exigiriam inteligência humana, utilizando métodos computacionais, tais como aprendizado de máquina, processamento de linguagem natural, visão computacional ou modelos preditivos, para analisar dados, identificar padrões, gerar

		conteúdo, apoiar decisões ou executar ações de forma autônoma ou semiautônoma
Enterprise Resource Planning (Planejamento de Recursos Empresariais)	ERP	Sistema integrado de gestão empresarial que centraliza e automatiza o processamento e consolidação dos dados e processos operacionais da organização, incluindo áreas como finanças, contabilidade, compras, estoque, recursos humanos e operações.
Antivírus	-	Sistema de proteção contra vírus de computador.
Malware	-	Arquivo malicioso projetado para danificar ou explorar dispositivos e/ou serviços de TI.
Enterprise Content Management (Gestão de Conteúdo Empresarial)	ECM	Conjunto de sistemas e práticas destinados à gestão do ciclo de vida das informações não estruturadas e documentos corporativos, desde sua criação ou captura até seu arquivamento ou descarte.
Honeypots	-	Redes usadas para testar ataques de segurança cibernética, projetadas para pesquisa e coleta de dados de invasores
Unidade de Processamento Gráfico	GPU	Componente de hardware projetado para processar e acelerar operações relacionadas a gráficos e renderização de imagens em computadores e dispositivos móveis.
Lei Geral de Proteção de Dados	LGPD	A Lei nº 13.709/2018 é a legislação brasileira que regulamenta as atividades de processamento de dados e tem como foco a criação de um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a proteção dos dados pessoais de todos os cidadãos.
Lei de Proteção de Informações Pessoais e Documentos Eletrônicos do Canadá	PIPEDA	Lei federal de privacidade do Canadá, de 13 de abril de 2000, voltada para organizações do setor privado. Ela estabelece regras sobre como as empresas devem lidar com dados pessoais no curso de suas atividades.
Regulamento Geral sobre a Proteção de Dados da União Europeia	GDPR	O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho da União Europeia é a legislação de proteção de dados e privacidade da União Europeia. Ele estabelece as regras fundamentais sobre como organizações devem tratar os dados pessoais de indivíduos no contexto de suas atividades.
Lei de Proteção de Dados do Reino Unido	UK GDPR / DUAA	O conjunto normativo britânico de proteção de dados é composto pelo UK GDPR, pela Data Protection Act 2018 e pela Data (Use and Access) Act 2025, que juntos regulam o tratamento de dados pessoais por organizações públicas e privadas no Reino Unido. O regime estabelece bases legais para o tratamento de dados, direitos dos titulares, obrigações de segurança e transferências internacionais, sendo aplicável a toda organização que processe dados de indivíduos localizados no território britânico.
Leis de Proteção de Dados Aplicáveis	-	Leis de proteção de dados aplicáveis conforme a operação do Grupo Brazilian Nickel S/A, incluindo a LGPD, GDPR, PIPEDA, UK GDPR / DUAA, bem como quaisquer outras normas, regulamentos ou orientações de autoridades supervisoras relevantes em matéria de proteção de dados pessoais vigentes nas jurisdições em que a Companhia opera, podendo variar conforme o país de atuação.
Regulamento de Inteligência Artificial da União Europeia	EU AI Act	O Regulamento (UE) 2024/1689 é a legislação da União Europeia que regula o desenvolvimento, a comercialização e o uso de sistemas de inteligência artificial, classificando-os conforme o nível de risco e estabelecendo obrigações proporcionais para fornecedores e operadores que atuem ou impactem o território europeu.
Leis de Inteligência Artificial Aplicáveis	-	Leis que regulam o desenvolvimento, a implementação e o uso de sistemas de inteligência artificial conforme a operação da Brazilian Nickel S/A, incluindo o EU AI Act, bem como demais normas, regulamentos e orientações de autoridades competentes em matéria de inteligência artificial vigentes em cada jurisdição em que a Companhia opera, podendo variar conforme o país de atuação.

2. OBJETIVOS

I. O objetivo desta política é definir os princípios, as diretrizes e as ações relacionadas à governança de dados, documentos e informações corporativas de todas as empresas do Grupo Brazilian Nickel S/A, bem como garantir o uso correto e adequado da Internet, Intranet, extranet (acesso controlado para fornecedores, parceiros, clientes ou prestadores de serviço), ativos de TI e Recursos de Computação e Comunicação, com vistas a garantir a segurança, a conformidade, a integridade, a publicação e a disponibilidade de todos os recursos de informação necessários à execução dos processos do Grupo.

II. A presente política visa ainda descrever o uso aceitável de sistemas e equipamentos de computador na empresa, bem como de todos os seus Ativos da Informação. Essas regras existem para proteger o funcionário, a empresa, seus clientes e fornecedores. O uso inadequado de sistemas e equipamentos de computador expõe a empresa a riscos, incluindo ataques de vírus, comprometimento de

sistemas e serviços de rede e questões legais.

III. Por fim, o presente regulamento visa ainda estabelecer as especificações de hardware para desktops, laptops e dispositivos complementares para uso no ambiente operacional Brazilian Nickel S/A no qual a tecnologia está fornecendo suporte.

3. APLICAÇÃO

IV. O escopo desta política aplica-se a todos os funcionários, prestadores de serviços e demais usuários envolvidos, direta ou indiretamente, na geração, recebimento, guarda, processamento, consulta, organização e arquivamento de documentos e informações gerados ou recebidos por qualquer setor, unidade ou empresa do Grupo Brazilian Nickel S/A, no Brasil ou no exterior.

V. Esta política considera o uso de todos os sistemas, aplicativos, dispositivos e equipamentos de TI gerenciados pelo Grupo ou por terceiros e que armazenam, processam ou transmitem dados e informações, independentemente do formato em que são apresentados. Isso inclui redes de computadores, hardware, software e aplicativos, dispositivos móveis e sistemas de telecomunicações. Inclui também informações processadas por outras organizações em suas relações comerciais com a empresa, como clientes, fornecedores, prestadores de serviços e parceiros institucionais.

4. DEVERES E RESPONSABILIDADES

VI. Todos os funcionários, prestadores de serviços e demais usuários dos dados e informações do Grupo devem estar cientes de que as informações geradas e manipuladas a partir dos sistemas são de propriedade da Brazilian Nickel S/A.

VII. Todos os funcionários, prestadores de serviços e outros usuários dos sistemas, dados e informações do Grupo devem estar cientes das diretrizes expressas nesta Política, especialmente das regras que os afetam direta e especificamente.

VIII. A segurança eficaz dos ativos da Brazilian Nickel S/A é um esforço coletivo de toda a equipe e envolve a participação e o apoio de todos os funcionários da empresa.

IX. Além disso, há várias partes responsáveis pelo uso e gerenciamento aceitáveis de dados e informações. Isso inclui responsabilidades específicas da Brazilian Nickel S/A, dos Funcionários em Geral, dos Gestores, da área de Tecnologia da Informação, da área Jurídica e de terceiros prestadores de serviços. Cada uma delas está descrita nesta política:

4.1. Títulos institucionais da Brazilian Nickel S/A

- Garantir que todos os dados, documentos e informações sejam mantidos em ambientes seguros.
- Assumir a responsabilidade de fornecer ferramentas de segurança e gerenciamento de dados.
- Garantir a vigilância e a proteção de dados por meio de normas, políticas e diretrizes das Leis de Proteção de Dados Aplicáveis a cada país onde a Companhia opera;
- Agir em tempo hábil no caso de um risco à segurança dos dados, tomando as medidas legalmente adequadas.
- Direcionar sanções e medidas disciplinares no caso de violações de dados e violações desta política.

4.2. Obrigações da área jurídica

- Prestar assessoria jurídica a gerentes, funcionários, terceiros, diretoria e área de TI no que diz respeito ao cumprimento das Leis de Proteção de Dados Aplicáveis, conforme país de atuação.
- Orientar o procedimento correto em casos de sanções e medidas disciplinares para violações de dados e violações desta política.
- Estudar e fornecer consultoria jurídica em caso de litígio ou violação dos dados ou informações do Grupo.
- Apontar os riscos legais que envolvem a segurança e a governança dos dados, documentos e informações da Brazilian Nickel S/A.

4.3. Obrigações dos gerentes

- Certificar-se de que esse padrão seja aplicado e, em caso de dúvida, peça ao departamento de Tecnologia da Informação para validar o procedimento correto a ser seguido.
- Orientar os funcionários e prestadores de serviços sobre os procedimentos corretos de uso e gerenciamento de Ativos da Informação, bem como sobre a correta conformidade com as diretrizes estabelecidas por esta política.
- Identificar violações desta política, comunicá-las à área de Tecnologia da Informação e aplicar as medidas disciplinares apropriadas, conforme orientação das áreas de Recursos Humanos e Jurídica.
- Especificar quem pode acessar os documentos e as informações sob sua responsabilidade.
- Garantir que todos os registros formais recebidos sejam armazenados de acordo com os padrões estabelecidos pela Política de Segurança e Governança de Dados.

4.4. Obrigações dos funcionários

- Informar imediatamente a TI sobre qualquer vazamento ou roubo de dados e informações detectado.
- Conhecer e agir de acordo com a Política de Segurança e Governança de Dados, protegendo as informações de propriedade da Brazilian Nickel S/A, enviadas ou armazenadas em qualquer meio físico (papel ou eletrônico);
- Cuidar das informações relevantes e dos dados pessoais processados, usando as informações somente para os fins adequados às suas funções e atividades.
- Ser responsável pela preservação, segurança e confiabilidade das informações da Brazilian Nickel S/A.
- Garantir que todos os documentos e informações sob sua responsabilidade sejam tratados conforme definido nas regras e procedimentos de gerenciamento de documentos e informações.
- Solicitar atualizações das ferramentas de gerenciamento de documentos e informações à área de tecnologia da informação sempre que necessário.
- Proteger e controlar as informações armazenadas em mídias removíveis e estações de trabalho.
- Devolver, em perfeita integridade física, todos os ativos de informação em seu poder pertencentes à Brazilian Nickel S/A, mediante solicitação ou após o encerramento de suas atividades.
- Usar as informações e/ou dados pessoais somente pelo período necessário para cumprir sua finalidade e/ou de acordo com o período de retenção da legislação em vigor.
- Tomar as precauções necessárias ao divulgar informações sobre o Grupo, independentemente do meio (telefones fixos, e-mail, telefones celulares, comunicações por rádio, entre outros).
- Verificar se os terceiros ou contratados assinaram o acordo de confidencialidade apropriado com a Brazilian Nickel S/A antes de encaminhar documentos e informações da instituição.

4.5. Obrigações de terceiros e prestadores de serviços em geral

- Conhecer e agir de acordo com a presente política, protegendo as informações de propriedade da Brazilian Nickel S/A, enviadas ou armazenadas em qualquer meio físico ou digital (papel ou eletrônico);
- Assegurar a confidencialidade das informações relevantes às quais têm acesso e não as usar para obter vantagens para si ou para outros, protegendo-as de acesso indevido.
- Usar os dados e as informações estritamente para o escopo definido contratualmente e em conformidade com a legislação de proteção de dados.
- Manter a confidencialidade das informações às quais têm acesso como resultado da prestação de seus serviços.
- Garantir que todos os documentos e informações sob sua responsabilidade sejam tratados de acordo com as regras e os procedimentos relacionados ao Gerenciamento de Documentos e Informações.
- Devolver, em perfeita integridade física, todos os ativos de informação em seu poder pertencentes à Brazilian Nickel S/A, mediante solicitação, ou após o encerramento de suas atividades.

4.6. Obrigações da área de tecnologia da informação, dos analistas de segurança da informação e dos administradores de sistemas

- Garantir que todos os equipamentos e sistemas sejam mantidos atualizados e totalmente funcionais durante todo o ciclo de vida para atingir os objetivos da empresa.
- Garantir que softwares e aplicativos não aprovados pela organização não sejam instalados em hardware ou outros equipamentos pertencentes à empresa.
- Instalar aplicativos antivírus/anti-malware e todos os aplicativos de linha de negócios considerados necessários para que os usuários desempenhem suas funções.
- Realizar o monitoramento e a proteção dos dados por meio das normas e diretrizes expressas nesta política e nas Leis Gerais de Proteção de Dados Aplicáveis.
- Identificar riscos de segurança para dados e/ou equipamentos de tecnologia.
- Elaborar, manter e disseminar políticas, padrões, procedimentos e instrumentos relacionados ao gerenciamento de informações e à governança de dados.
- Orientar os funcionários e prestadores de serviços sobre os procedimentos corretos de gerenciamento de informações e governança de dados, bem como sobre a correta conformidade com as diretrizes estabelecidas por esta política.
- Fornecer suporte técnico e validar os procedimentos operacionais elaborados pelas áreas do Grupo.
- Coordenar as ações de Gerenciamento de Informações e Governança de Dados, visando à conformidade e à padronização do processo documental.
- Realizar auditorias, sempre que necessário, para verificar o armazenamento correto de documentos e informações.
- Apoiar a definição, o desenvolvimento e a parametrização de ferramentas de suporte ao gerenciamento de documentos e informações.
- Treinar e apoiar os funcionários do Grupo na metodologia e nas tecnologias de gerenciamento de informações e governança de dados.
- Selecionar, aprovar e solicitar a contratação de fornecedores, parceiros e prestadores de serviços relacionados à governança e segurança de dados.

- Assumir a responsabilidade pela elaboração e atualização de instrumentos de segurança e gerenciamento de dados, como procedimentos, fluxogramas e padrões.
- Fornecer o material adequado para armazenar a coleção, bem como pessoal treinado para realizar a atividade.
- Assegurar o cumprimento e a ampla divulgação desta Política e dos demais regulamentos dela decorrentes.
- Realizar manutenção preventiva, preditiva e corretiva em sistemas, software, aplicativos, programas, dispositivos e equipamentos de TI gerenciados pela empresa.
- Estabelecer procedimento de tratamento adequado para a redução ou destruição/descarte de mídias e equipamentos.
- Administrar, proteger e testar as cópias de segurança das informações e dados críticos para o negócio.
- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro Ativo da Informação a um responsável identificável.
- Implementar processo contínuo para gestão de vulnerabilidades com foco em monitoramento, correção, erradicação e defesa.
- Criar e implementar processos para gestão de acessos aos ambientes restritos de TI, como datacenters, salas de rack, ambientes com equipamentos sensíveis etc.
- Elaborar um Plano de Recuperação de Desastres ("DRP") para restauração ágil e eficaz dos dados informações perdidas em decorrência de um desastre.
- Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.
- Quando da entrega de algum equipamento para os colaboradores, garantir que eles assinem o Termo de Responsabilidade pela Guarda e Uso de Equipamentos; bem como garantir a devolução dos ativos, quando do desligamento do colaborador.

4.7. Obrigações do Encarregado de Proteção de Dados ou figura equivalente, conforme designado nas Leis de Proteção de Dados Aplicáveis

- Apoiar a Equipe de Tecnologia da Informação nos procedimentos de análise, apuração e proposição de soluções nas questões que envolvam dados pessoais.
- Conforme as Leis de Proteção de Dados Aplicáveis, orientar a realização de Avaliações de Impacto sobre a Proteção de Dados (DPIA ou PIA) para operações de tratamento de alto risco.
- Quando necessário conforme a Lei de Proteção de Dados Aplicável, comunicar à autoridade nacional responsável (e.g., Agência Nacional de Proteção de Dados – ANPD, Information Commissioner's Office – ICO, Office of the Privacy Commissioner of Canada – OPC) e ao(s) titular(es) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, em conformidade com demais políticas e normas da Brazilian Nickel S/A e os prazos legais de notificação.

5. DIRETRIZES

5.1. Diretrizes gerais

X. As diretrizes aqui previstas têm como objetivo estabelecer um padrão a ser adotado aos destinatários da presente Política, a fim de garantir a segurança dos Ativos da Informação, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação. Todas as exceções deverão ser aprovadas pela equipe de TI e o Gestor responsável.

XI. Os dados da empresa só devem ser armazenados em dispositivos oficiais da empresa que tenham sido submetidos a backup e aprovados pela equipe de TI.

XII. Caberá à Área de Tecnologia da Informação, em conjunto com o DPO e CFO da Brazilian Nickel S/A, elaborar a matriz de responsabilidades para designar os responsáveis pelo suporte à gestão de documentos em cada área da empresa.

XIII. O compartilhamento só é permitido por meio de plataformas como SharePoint e Teams, quando licenciadas e aprovadas pela Brazilian Nickel S/A. Isso garante a segurança da transferência e os princípios de finalidade, adequação e necessidade do destinatário das informações/dados.

XIV. As atualizações da política, das normas ou dos procedimentos associados à Governança e Gestão da Informação somente poderão ser divulgadas oficialmente quando forem elaboradas ou validadas pela Área de Tecnologia da Informação.

XV. A presente política deve ser atualizada anualmente pela Área de Tecnologia da Informação, ou sempre que houver necessidade.

XVI. Para processar os documentos gerados ou recebidos, as ferramentas de gerenciamento de documentos e informações precisam ser homologadas e validadas pela área de tecnologia da informação em conjunto com as áreas que geram a documentação.

XVII. É proibida a contratação de produtos e serviços associados à Gestão de Documentos e Informações por qualquer uma das áreas ou do Grupo sem a devida aprovação da área de Tecnologia da Informação, sob pena de aplicação das medidas disciplinadas cabíveis.

XVIII. Qualquer exceção a esta Política deve ser aprovada com antecedência pela equipe de TI, através do formulário de solicitação: Corporate Financial Portal, disponibilizado na Intranet.

XIX. Qualquer solicitação de alteração desta política deve ser avaliada e aprovada pelo departamento de Tecnologia da Informação, através do Change Management (Corporate Financial Portal), revisada em conjunto com o DPO e CFO da Brazilian Nickel S/A.

XX. As informações da Brazilian Nickel S/A deverão ser tratadas em estrita observância à Política de Guarda e Descarte de Dados, garantindo que sua retenção, armazenamento e eliminação ocorram conforme os prazos, critérios e requisitos nela estabelecidos, de modo a assegurar a conformidade legal, a proteção de dados pessoais e a mitigação de riscos relacionados ao uso indevido ou à manutenção indevida de registros.

XXI. Aos Usuários foram estabelecidos direitos e deveres de apoio e fiscalização de cumprimento da presente Política, cabendo a todos o reporte de qualquer descumprimento, risco ou incidente de segurança da informação à área de Tecnologia da Informação pelo e-mail suporte.ti@brnickel.com e ou itsupport@brnickel.com, conforme aplicável.

5.2. Uso geral e propriedade dos Ativos da Informação

XXII. Os sistemas e equipamentos disponibilizados pela empresa (incluindo servidores, desktops, notebooks, tablets, equipamentos de rede, telefones, smartphones, projetores, softwares, aplicativos, sistemas de negócios, bancos de dados, mídias de armazenamento e quaisquer outros bens materiais ou imateriais disponibilizados pela área de Tecnologia da Informação), ainda que cedidos a funcionários, são de propriedade e responsabilidade da Brazilian Nickel S/A. O manejo destes ativos representa apenas detenção provisória, e não a posse ou propriedade, sendo proibida qualquer reprodução ou retenção pelos usuários.

XXIII. Os sistemas e equipamentos devem ser utilizados livremente apenas para atividades profissionais destinadas a atender aos interesses da Brazilian Nickel S/A.

XXIV. O uso de equipamentos da empresa para realização de atividades e armazenamento de arquivos pessoais não é permitido aos Usuários. Entretanto, o uso pessoal para fins não corporativos só é permitido com a permissão da empresa, através do formulário de solicitação (Corporate Financial Portal) e email suporte.ti@brnickel.com e ou itsupport@brnickel.com. Além disso, a prática só deve ser realizada durante intervalos apropriados que não afetem a produtividade no trabalho. Respeitar as políticas da empresa, priorizar as tarefas profissionais e estabelecer limites de tempo para as atividades pessoais também são práticas importantes.

XXV. Qualquer uso de recursos tecnológicos deve ser responsável, evitar a sobrecarga do equipamento e manter a segurança e a confidencialidade dos dados da empresa.

XXVI. É essencial que os funcionários estejam cientes das políticas específicas da organização sobre esse assunto e que assumam a responsabilidade pessoal por quaisquer danos ou problemas causados aos equipamentos da empresa.

XXVII. Em caso de furto, roubo ou perda de qualquer equipamento ou dispositivo, o funcionário detentor da concessão deve registrar imediatamente perante a autoridade policial do respectivo estado e país em que se encontra. Em seguida, deverá apresentar o relatório ao departamento de Tecnologia da Informação, relatando o ocorrido.

XXVIII. Para a proteção, integridade e adequada manutenção dos Ativos da Informação, compete à área de Tecnologia da Informação realizar o monitoramento contínuo de equipamentos, sistemas e do tráfego de rede, por meio de ferramentas especializadas e plataformas corporativas de gestão e segurança da informação (tais como soluções de monitoramento, registro e correlação de eventos), em consonância com as normas e diretrizes de Segurança da Informação estabelecidas pela organização.

XXIX. Os Usuários não devem usar os sistemas e equipamentos da empresa para fins ilegais, antiéticos, prejudiciais à empresa ou improdutivos, pois isso coloca a organização em risco. Em nenhuma circunstância um funcionário da empresa está autorizado a usar os sistemas e equipamentos da Brazilian Nickel S/A para qualquer atividade ilegal, de acordo com as leis locais, estaduais e federais.

XXX. A instalação de sistemas nos equipamentos do Grupo somente será permitida se expressamente autorizada, através do formulário de solicitação (Corporate Financial Portal), disponibilizado na Intranet. Nesses casos, o funcionário deve se certificar de que não se trata de software ou aplicativo pirata, bem como garantir que o sistema seja de uso exclusivo em atividades inerentes às rotinas de trabalho de sua área. Para equipamentos de computação portáteis, incluindo laptops, tablets e smartphones, o usuário do equipamento também deve considerar o acesso aos dados armazenados no dispositivo e as redes que podem estar disponíveis para o dispositivo se conectar.

XXXI. Todos os colaboradores que utilizam ativos de TI (desktops, notebooks, telefones, telefone móvel, datashow, servidores, rede sem fio, monitores, nobreaks, e-mails, salas de conferência virtual (Teams®, Zoom®, Skype®, Google Meet®, etc.), sistemas de intranet, e demais ferramentas tecnológicas) devem estar cientes de que seu uso deve ocorrer de forma responsável, ética e alinhada às diretrizes internas, garantindo a proteção das informações, a integridade dos equipamentos e a observância das políticas corporativas aplicáveis.

I. Exemplos de atividades inaceitáveis relacionadas ao uso de sistemas e redes:

a) Violações dos direitos de qualquer pessoa ou empresa protegida por direitos autorais, segredo comercial, patente ou outra propriedade intelectual, ou leis ou regulamentos semelhantes, incluindo, entre outros, a instalação ou distribuição de produtos "pirateados" ou outros produtos de software que não estejam devidamente licenciados para uso pela empresa;

b) Fazer cópias não autorizadas de material protegido por direitos autorais, incluindo, entre outros, digitalizar e distribuir fotografias de revistas, livros ou outras fontes protegidas por direitos autorais, músicas protegidas por direitos autorais e instalar qualquer software protegido por direitos autorais para o qual a empresa ou o usuário final não tenha uma licença ativa;

c) Acessar dados, servidores ou contas para qualquer finalidade que não seja a condução dos negócios da empresa, mesmo que você tenha acesso autorizado;

d) Exportação de software, informações técnicas e tecnologias em geral;

e) Introduzir programas maliciosos na rede ou no servidor (por exemplo, vírus, worms, cavalos de troia, phishing e spam de e-mail, etc.)

f) Revelar a senha de sua conta a terceiros ou permitir que terceiros usem sua conta. Isso inclui familiares e outros membros da família quando o trabalho estiver sendo realizado em casa;

g) Usar equipamentos de informática de propriedade da empresa para participar ativamente da aquisição ou transmissão de material que envolva bullying, assédio sexual, violência, ódio, racismo, xenofobia, preconceito, pornografia ou pornografia infantil;

h) Usar equipamentos e sistemas da empresa para fazer ofertas fraudulentas de produtos, itens ou serviços;

i) Fazer declarações, explícitas ou implícitas, sobre garantias de produtos ou serviços, exceto como parte das funções normais do trabalho;

j) Praticar violações de segurança ou interrupções na comunicação da rede (as violações de segurança incluem, entre outros, acessar dados dos quais o funcionário não é o destinatário pretendido ou fazer login em um servidor ou conta que o funcionário não esteja expressamente autorizado a acessar, a menos que essas funções estejam dentro do escopo de suas atribuições regulares);

k) Realizar varreduras de portas ou varreduras de segurança/vulnerabilidade sem autorização expressa da empresa;

l) Realizar qualquer forma de monitoramento de rede que intercepte dados não destinados ao host do funcionário, a menos que essa atividade faça parte das funções do funcionário;

m) Contornar a autenticação do usuário ou a segurança de qualquer host, rede ou conta;

n) Introduzir honeypots, honeynets ou tecnologia semelhante na rede da empresa;

o) Interferir ou negar serviço a qualquer usuário que não seja o host do funcionário (por exemplo, ataque de negação de serviço).

p) Usar qualquer programa, script ou comando, ou enviar mensagens de qualquer tipo, com a intenção de interferir ou desativar a sessão de terminal de um usuário, por qualquer meio, localmente ou pela Internet/Intranet;

q) Tentativa de acessar ou obter dados pessoais de funcionários, clientes, fornecedores e parceiros de negócios, a menos que essa atividade faça parte de seus deveres ou tarefas.

II. Caso seja comprovado, por meio de sindicância interna, a má utilização dos Ativos da Informação, o Usuário que tiver agido com dolo ou culpa será responsabilizado, podendo ser penalizado conforme medidas disciplinares estabelecidas no Regimento Interno da Companhia ou de acordo com as penalidades previstas em contrato, conforme aplicável.

5.3. Ferramentas de gerenciamento de documentos e informações

5.3.1. Fluxo de documentos

XXXII. Para que os documentos de cada área sejam tratados de acordo com as melhores práticas de gerenciamento de documentos, o fluxo de informações precisa ser devidamente mapeado, padronizado, redesenhado e automatizado, seja executado pela equipe de TI em conjunto com fornecedor especializado contratado, se necessário.

XXXIII. O levantamento do fluxo documental consiste em identificar, analisar, descrever e registrar o processo documental em cada área da Brazilian Nickel S/A, com o objetivo de padronizar o funcionamento desses processos e identificar ações para sua melhoria contínua.

XXXIV. Caberá à área de Tecnologia da Informação disponibilizar os recursos necessários, bem como equipe qualificada, em conjunto com fornecedor especializado contratado, para mapear e redesenhar o fluxo de documentos, considerando as prioridades definidas pela Brazilian Nickel S/A.

XXXV. A parametrização, a criação de fluxos de trabalho e/ou a automação de fluxos de documentos devem ser realizadas com a concordância da área de Tecnologia da Informação, que será responsável pela aprovação da solução.

5.3.2. Taxonomia corporativa

XXXVI. A taxonomia tem o objetivo de organizar, categorizar e classificar as informações geradas em cada um dos processos do Grupo. Essa taxonomia será configurada em tecnologias de gerenciamento de informações para armazenar os documentos, com o objetivo de facilitar sua busca e recuperação.

XXXVII. A taxonomia de cada unidade deve ser estruturada hierarquicamente, considerando os processos, subprocessos e atividades da empresa, a fim de garantir uma visão sistêmica de todas as informações geradas pela instituição para a realização de suas atividades.

XXXVIII. Os termos usados para estruturar a taxonomia são classificados do tópico geral para o específico ou do todo para as partes, a fim de facilitar a navegação lógica dos assuntos no documento.

XXXIX. Os elementos que compõem a estrutura taxonômica devem, preferencialmente, ser descritos no formato em língua inglesa, adotando-se o seguinte padrão: aaaammdd_BRN_Assunto.

XL. Caberá à área de Tecnologia da Informação disponibilizar os recursos necessários, bem como equipe qualificada, em conjunto com o fornecedor especializado contratado, para a elaboração e a atualização da taxonomia de cada área, sempre que necessário, em consonância com as prioridades estabelecidas pela Brazilian Nickel S/A.

XLI. As áreas devem avaliar periodicamente a necessidade de atualizar a taxonomia e informar a área de Tecnologia da Informação para que tome as medidas necessárias.

XLII. As áreas do Grupo poderão fazer sugestões de alterações na estrutura, sempre que julgarem necessário, a fim de garantir a aderência entre a taxonomia e as necessidades dos usuários das informações.

5.3.3. Tabela de gerenciamento de informações

XLIII. Toda área responsável pela geração ou recebimento de documentos físicos ou digitais necessários à execução dos processos da Brazilian Nickel S/A deve ter uma tabela de gestão da informação elaborada, de acordo com a metodologia de Gestão de Documentos e Informações.

XLIV. A TABELA DE GERENCIAMENTO INFORMACIONAL deve conter, no mínimo, as informações sobre como cada documento da Brazilian Nickel S/A é tratado, sua classificação de confidencialidade e por quanto tempo é mantido.

XLV. O período de retenção, além das leis e regulamentos em vigor, deve considerar o descarte de informações que já cumpriram sua finalidade, em conformidade com as Leis de Proteção de Dados Aplicáveis e regulamentos em vigor, e que as exceções devem ser documentadas, justificadas e aprovadas.

XLVI. O QUADRO DE GESTÃO INFORMATIVA de cada unidade/área deve ser aprovado pelo gerente de cada unidade em conjunto com e a Área Jurídica do Grupo.

XLVII. Caberá à área de Tecnologia da Informação disponibilizar a equipe necessária para a elaboração da Tabela de Gestão da Informação para cada unidade/área, considerando as prioridades definidas pelo Grupo.

5.3.4. Padrões operacionais

XLVIII. Consiste na descrição de como realizar um determinado trabalho, com o objetivo de regularizar e padronizar a forma como as tarefas são realizadas.

XLIX. Os procedimentos de gerenciamento de documentos e as instruções de trabalho relacionadas descrevem a metodologia para lidar com a coleção de documentos, detalhando as atividades para classificar, organizar, nomear, indexar, arquivar e mover documentos físicos e digitais em suas respectivas fases.

L. Caberá à área de Tecnologia da Informação disponibilizar a equipe para elaborar os procedimentos e instruções de trabalho necessários à implementação da gestão de documentos em cada área/programa, considerando as prioridades definidas pela Brazilian Nickel S/A.

LI. As áreas/programas do Grupo podem elaborar procedimentos técnicos específicos, sujeitos à aprovação da área de Tecnologia da Informação.

5.4. Requisitos de processamento de informações

Os requisitos operacionais específicos relacionados à forma como o Grupo lida com documentos e informações são definidos abaixo:

5.4.1. Classificação de informações

LII. Cabe aos gerentes, em suas respectivas áreas de atividade, especificarem quem pode acessar os documentos e as informações sob sua responsabilidade.

LIII. A classificação de todos os documentos necessários à execução dos processos do Brazilian Nickel S/A deve ser SEMPRE registrada no QUADRO DE GESTÃO INFORMACIONAL, de acordo com os critérios de classificação de confidencialidade.

LIV. **Classificação de informações confidenciais:**

a) A classificação confidencial é atribuída a documentos e informações destinados a pessoas específicas da Brazilian Nickel S/A. Essa classificação geralmente está associada a documentos cujo vazamento de informações pode representar um risco financeiro ou de imagem para o Grupo.

LV. **Classificação da confidencialidade de informações restritas:**

a) A classificação restrita ou reservada é atribuída a documentos e informações necessários à execução dos processos de negócios da Brazilian Nickel S/A, que são disseminados no âmbito de cada gerência que os produz.
b) As informações restritas podem ser disponibilizadas apenas para grupos internos de cada gerência ou entre gerências específicas.
c) Os documentos que contêm dados pessoais (com base nas Leis de Proteção de Dados Aplicáveis para cada país) devem ter acesso restrito, em conformidade com os princípios da lei.

LVI. **Classificação do sigilo de informações corporativas:**

a) A classificação corporativa é atribuída às informações que podem ser conhecidas por todos os funcionários do Grupo, pois não apresentam potencial de risco. As informações corporativas podem ser disponibilizadas no âmbito da Brazilian Nickel S/A, sem restrições de confidencialidade.

LVII. **Classificação de informações públicas:**

a) A classificação pública é dada às informações da Brazilian Nickel S/A que não apresentem potencial de risco e que sua divulgação ao público externo agregue valor à imagem da instituição. As informações públicas podem ser disponibilizadas ao público externo, que é o alvo da informação, de acordo com as competências estabelecidas nas políticas de comunicação e divulgação da Brazilian Nickel S/A.

LVIII. Todos os sistemas utilizados para armazenar dados e informações na Brazilian Nickel S/A devem ser configurados de acordo com os critérios de classificação de confidencialidade definidos pelas áreas, para evitar acessos indevidos.

LIX. A classificação adequada do documento na estrutura de taxonomia deve ser realizada para o registro e a evidência da execução dos processos, para facilitar o armazenamento eletrônico e garantir a rápida busca e recuperação de documentos e informações.

5.4.2. Produção, recebimento e circulação de documentos e informações

LX. Os documentos gerados ou recebidos pelas áreas ou programas devem ser publicados no momento de sua geração/recebimento nas tecnologias disponibilizadas pela Brazilian Nickel S/A para Gestão de Documentos e Informações. Somente ferramentas e aplicativos aprovados podem ser utilizados para manipular os dados.

LXI. Os documentos técnicos devem ser recebidos, identificados e codificados de acordo com os padrões relevantes. Quando aplicável, os fornecedores devem ser aconselhados a usar modelos de documentos ou identificação padrão de documentos do Grupo.

LXII. As áreas devem usar modelos de documentos padronizados sempre que possível para a produção de documentos.

LXIII. A circulação de documentos e informações deve ser realizada, sempre que possível, usando tecnologias aprovadas para esse fim. Se os documentos forem enviados por e-mail, deverão ser observados os critérios de sigilo e confidencialidade.

5.4.3. Registro de documentos

LXIV. Para registrar documentos em tecnologias de gerenciamento de informações, é necessário definir os padrões de indexação exigidos para garantir a busca e a recuperação de documentos, informações e conteúdo.

LXV. Os padrões de indexação definem como a documentação é registrada nas tecnologias, de acordo com as necessidades de cada unidade/área.

LXVI. Caberá à equipe definida pelo departamento de Tecnologia da Informação definir os padrões de indexação de documentos em conjunto com os departamentos.

5.4.4. Impressão de documentos

LXVII. Um documento só deve ser impresso se exigir uma assinatura física e não for possível usar uma assinatura eletrônica ou certificação digital, ou nos casos em que o formato dificultar o acesso ou a leitura eletrônica. No entanto, é importante enfatizar que, mesmo que um documento seja impresso, ele ainda precisa de acesso restrito e todos devem trabalhar juntos para garantir que os documentos não sejam deixados "esquecidos" em dispositivos ou mesas.

LXVIII. Os documentos que não exigem legalmente um selo/assinatura devem, de preferência, ser processados eletronicamente, evitando o excesso de impressão.

LXIX. Cada colaborador é responsável pela guarda, transporte e armazenamento adequado dos documentos que imprimir, garantindo conformidade com a classificação da informação e a proteção contra acessos não autorizados.

LXX. Os arquivos enviados para impressão devem ser retirados imediatamente da bandeja da impressora, evitando esquecimento ou acesso indevido por terceiros.

5.4.5. Organização de documentos e informações

LXXI. Caberá às áreas que geram a documentação registrar e publicar os novos documentos em tecnologias de gerenciamento de informações.

LXXII. O acervo legado existente em formato digital será migrado para as tecnologias pela equipe disponibilizada pela área de Tecnologia da Informação, levando em conta as prioridades definidas pela Brazilian Nickel S/A.

LXXIII. Caberá à Área de Tecnologia da Informação disponibilizar a equipe para auxiliar as áreas da Brazilian Nickel S/A no processo de organização de documentos, sempre que necessário.

5.4.6. Armazenamento, conservação e preservação

LXXIV. Todas as informações e documentos do Grupo que sejam relevantes para as atividades da instituição, independentemente de sua classificação, devem ser armazenados nas tecnologias homologadas pela Área de Tecnologia da Informação e disponibilizadas para o gerenciamento de documentos e informações, como Microsoft SharePoint, Teams e Outlook, observando as regras de backup e retenção.

LXXV. Os documentos das unidades/áreas devem ser armazenados nas tecnologias de gestão da informação disponibilizadas pela Área de Tecnologia da Informação. A avaliação de qual das tecnologias será utilizada para armazenar os documentos será definida pela Área de Tecnologia da Informação em conjunto com as áreas geradoras da documentação no momento da análise do fluxo documental. Todos os arquivos que os funcionários precisam para desempenhar suas funções podem ser armazenados no sistema de nuvem adotado pelo Grupo, desde que estejam em conformidade com as diretrizes expressas nesta política.

LXXVI. É responsabilidade de todos os funcionários "limpar" o espaço de armazenamento do equipamento fornecido pela empresa e garantir que os arquivos que não pertencem a Brazilian Nickel S/A sejam removidos.

LXXVII. Os recursos de armazenamento da empresa devem ser usados pelos funcionários no desempenho de suas funções. Todos os arquivos digitais devem ser salvos e digitalizados usando o sistema de nuvem Sharepoint adotado pelo Grupo. O armazenamento e o gerenciamento de arquivos digitais serão automatizados utilizando as plataformas homologadas pelo TI.

LXXVIII. As informações de propriedade do Grupo armazenadas em dispositivos eletrônicos e computacionais de propriedade ou alugados pela

empresa, seus funcionários ou terceiros permanecerão como propriedade exclusiva da Brazilian Nickel S/A.

LXXIX. Caso essas informações sejam armazenadas em outros locais não previamente aprovados pela Área de Tecnologia da Informação, tais como: disco local do computador, HD externo, pen-drive, e-mail, entre outros; sua integridade e confidencialidade não serão garantidas. E em caso de extravio, o Gestor da Área é responsável por qualquer dano ou prejuízo causado ao Brazilian Nickel S/A, de acordo com a Política de Segurança da Informação da instituição. As sanções serão aplicadas de acordo com a lei e o contrato de trabalho em vigor se a causa for evidente.

LXXX. De preferência, os documentos que não são aceitos em outras mídias, como documentos técnicos de grande formato para fins de consulta e documentos históricos, devem ser armazenados em mídia física. Outros documentos, se impressos, devem ser descartados assim que forem usados.

LXXXI. Os documentos em formato físico serão armazenados na área geradora da documentação até que sejam devidamente processados pela equipe disponibilizada pela Área de Tecnologia da Informação e encaminhados para armazenamento externo, considerando o fluxo acordado entre as áreas.

LXXXII. Em caso de roubo, perda ou divulgação não autorizada de informações pertencentes ao Grupo, o funcionário que tomar conhecimento do fato deve comunicá-lo imediatamente ao seu gerente direto e ao departamento de Tecnologia da Informação;

5.4.7. Nomenclatura de documentos

LXXXIII. Os documentos eletrônicos devem ser nomeados de acordo com o Procedimento Operacional de Nomeação de Documentos específico da empresa, antes de sua inclusão nas tecnologias de gerenciamento de informações, considerando o exemplo a seguir:

20240131-BRN-Meeting Minutes-0001.doc

- Data (AAAAMMDD)
- Acrônimo da empresa
- Tipo de documento
- Assunto
- Número do documento

LXXXIV. Se a unidade/área ainda não tiver esse procedimento descrito, ele deverá ser solicitado à Área de Tecnologia da Informação. O padrão de nomeação de documentos deve ser desenvolvido, considerando a facilidade de aplicação pelos usuários.

LXXXV. Se houver necessidade de atualizar o padrão definido para nomear documentos, a área responsável pela documentação deve solicitar a revisão do procedimento à área de Tecnologia da Informação.

5.4.8. Consulta de documentos

LXXXVI. Os documentos devem ser consultados preferencialmente por meio da tecnologia de gestão da informação, considerando os níveis de acesso definidos para cada documento, de forma a minimizar o risco de consulta a versões anteriores ou obsoletas. Quando um documento não puder ser encontrado nesse ambiente, deverá ser solicitado à equipe designada pela Área de Tecnologia da Informação, que tomará as providências cabíveis.

5.4.9. Descarte de documentos

LXXXVII. Os documentos devem ser descartados de acordo com as normas e procedimentos internos da Brazilian Nickel S/A. Todas as informações que não forem mais necessárias devem ser descartadas de forma segura, considerando os períodos de armazenamento definidos no QUADRO DE GESTÃO DA INFORMAÇÃO para cada uma das áreas/programas do Grupo. Os prazos de validade dos documentos devem ser considerados em conformidade com a legislação de proteção de dados e demais normas vigentes.

LXXXVIII. Os documentos somente poderão ser descartados após aprovação do gestor de cada unidade/área responsável pela documentação, em conjunto com a Área Jurídica e a Diretoria do Brazilian Nickel S/A.

5.4.10. E-mail

LXXXIX. Todo e-mail que contenha qualquer informação oficial, tais como: comunicações entre a Brazilian Nickel S/A e partes interessadas; notificações, demandas ou esclarecimentos a órgãos reguladores, agências, prefeituras, governos, entre outros, contratos com fornecedores e parceiros, entre outros, deve ser armazenado nas tecnologias disponibilizadas pela empresa.

XC. Qualquer documento que seja anexado a um e-mail, seja ele enviado ou recebido, e que seja um registro ou evidência dos processos da Brazilian Nickel S/A, deve ser incluído nas tecnologias de gerenciamento de informações. Para gestão dos anexos, os Usuários

deverão utilizar a plataforma homologada pelo TI.

XCI. É responsabilidade do gerente de cada unidade/área garantir que todos os registros formais recebidos por e-mail sejam armazenados de acordo com os padrões estabelecidos pela Política de Segurança e Governança de Dados.

XCII. O e-mail corporativo é um patrimônio da empresa e tem a finalidade única e exclusiva de realizar atividades profissionais de interesse da Brazilian Nickel S/A.

XCIII. A empresa poderá utilizar medidas de segurança para proteger a rede e garantir a integridade dos dados e programas, podendo assim inspecionar qualquer arquivo armazenado na rede, bem como monitorar o uso interno das informações, navegações e envio/recebimento de e-mails, visando assegurar o cumprimento desta Política.

XCIV. Os funcionários devem ter cuidado ao abrir anexos e links de e-mail recebidos de remetentes desconhecidos, que podem conter malware. Em caso de dúvida, sempre entre em contato com a TI para obter orientação.

XCV. Exemplos de atividades inaceitáveis relacionadas ao uso de e-mail e comunicação:

a) Enviar mensagens usando contas de e-mail pertencentes à empresa sem declarar claramente que "comentários, mensagens e/ou opiniões não representam necessariamente a opinião da empresa e/ou são endossados pela empresa";

b) Envio de e-mails não relacionados ao trabalho para destinatários internos ou externos;

c) Envio de mensagens de e-mail não solicitadas, incluindo o envio de "lixo eletrônico" ou outro material publicitário a indivíduos que não o solicitaram, especificamente spam de e-mail;

d) Fazer uso não autorizado ou falsificar informações de cabeçalho de e-mail;

e) Solicitação de e-mail para qualquer outro endereço de e-mail, exceto o da conta do autor da postagem, com a intenção de assediar ou coletar informações;

f) Criar ou encaminhar esquemas de "correntes" ou "pirâmides" de qualquer tipo;

g) Fornecimento de informações ou listas de funcionários da empresa a terceiros;

h) Fornecer a terceiros os dados pessoais de funcionários, clientes, fornecedores e parceiros comerciais;

i) Compartilhar usuários e senhas, bem como o uso de e-mails de departamento por usuários que não são autorizados;

j) Acessar os e-mails de outros usuários da Brazilian Nickel S/A;

k) Reproduzir e/ou encaminhar conteúdo com ameaças eletrônicas, tais como: vírus, spam e outros malwares;

l) Acessar arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que apresente riscos à segurança dos Ativos da Informação da Brazilian Nickel S/A;

m) Enviar mensagens que busquem monitorar secretamente, assediar ou ameaçar outros Usuários, bem como burlar o
n) sistema de segurança, interromper determinado serviço, sistema, servidor ou rede de computadores por meio de método ilícito ou não autorizado.

5.5. Segurança e informações proprietárias

XCVI. As senhas em nível de sistema e de usuário devem estar em conformidade com a política de senhas estabelecida. É proibido fornecer acesso a outro indivíduo, seja deliberadamente ou por falha nos procedimentos projetados para proteger o acesso não autorizado.

XCVII. É proibido utilizar qualquer informação da empresa para fins pessoais, educacionais ou particulares, bem como é proibido utilizar/registrar dados pessoais ou de outras pessoas que não sejam relevantes para a Brazilian Nickel S/A em suas respectivas máquinas. Excepcionalmente, o uso de tais informações para fins exclusivamente acadêmicos ou educacionais poderá ser realizado, desde que previamente autorizado pela diretoria da área e o time Jurídico, e que não haja risco à confidencialidade, segurança da informação ou ao segredo comercial da Companhia. Nesse caso, conforme aplicável, deverá ser realizada a anonimização ou agregação das informações, de modo a impedir a identificação de titulares de dados pessoais.

XCVIII. Cada funcionário deve garantir, por meios legais ou técnicos, que as informações proprietárias sejam protegidas de acordo com os padrões de proteção de dados adotados pela empresa.

5.6. Ações de contingência

XCIX. Todos os documentos e informações críticos para a operação da Brazilian Nickel S/A ou cruciais para o bom andamento de seus processos devem ser preservados. Todas as medidas de contingência para a preservação dos registros vitais da Brazilian Nickel S/A serão executadas de acordo com a presente política.

5.7. Utilização da internet

C. O uso da internet na Brazilian Nickel S/A deve se dar exclusivamente para atender fins legítimos e relacionados à execução de funções laborais.

CI. As solicitações de downloads deverão ser feitas diretamente ao suporte, e estarão sujeitas à avaliação da equipe de TI.

CII. Exemplos de atividades inaceitáveis em geral:

a) Jogar ou participar de jogos digitais on-line ou off-line;

b) Jogar ou participar de jogos de azar digitais on-line;

c) Acessar material ofensivo, ilegal, pornográfico ou inadequado;

d) Conduzir negócios pessoais usando os recursos da empresa;

e) Transmitir qualquer conteúdo que seja ofensivo ou fraudulento;

f) Acesso a informações que o funcionário não está autorizado a acessar ou que não precisa para realizar seu trabalho;

g) Acessar ou compartilhar software ou material pirateado;

h) Tentativa de interromper ou hackear outros sistemas (interna ou externamente) ou de produzir resultados maliciosos,
i) como danificar sistemas, roubar e remover dados e implantar vírus;

j) Vender ou fornecer a terceiros os dados pessoais de funcionários, clientes, fornecedores e parceiros comerciais;

k) Tentativa de burlar os controles de internet, usando software, plug-in ou outros métodos, bem como de utilizar programas para download/upload de arquivos suspeitos;

l) Utilizar a internet para acessar salas de bate-papo, redes sociais, download/envio de filmes e músicas, spam e outros tipos de acessos que não dizem respeito ao trabalho do dia a dia.

5.8. Uso da rede corporativa

CIII. Todos os dispositivos móveis e de computação que se conectam à rede interna devem estar em conformidade com os padrões de segurança da informação implementados pela empresa.

5.9. Uso de mídias removíveis

CIV. Mídias removíveis são dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Blu-Ray, Disquete, Pen Drive, cartão de memória, HDs portáteis, telefones celulares, entre outros.

CV. Para minimizar os riscos de incidentes de segurança envolvendo informações mantidas pela empresa e reduzir o risco de proliferação de malwares na rede de computadores, é vedada a execução de mídia removível sem o consentimento da equipe de TI.

CVI. Mesmo em equipamentos liberados, o tráfego de dados entre as unidades USB e os computadores deverá ser monitorado por meio de relatórios providos pelo sistema de gerenciamento, auditorias internas e externas, quando aplicável, e validações feitas pela equipe de TI.

5.10. Mesa e Tela Limpa

CVII. Todas as informações utilizadas em meio físico devem ser mantidas com controle de acesso e somente permanecer nas estações de trabalho durante o desenvolvimento da atividade.

CVIII. Após o término do expediente ou ao se ausentar da mesa de trabalho, as informações devem ser armazenadas em local seguro.

CIX. É proibido deixar documentos sobre a mesa, nas bandejas de impressão ou em qualquer local desprotegido.

CX. No descarte de documentos, estes não devem ser reciclados; devem ser picotados, preferencialmente em picotadeiras.

CXI. É proibido utilizar rascunhos que contenham dados pessoais ou informações sigilosas.

CXII. As estações de trabalho e os notebooks devem estar configurados com bloqueio automático de tela, garantindo a proteção das informações quando o usuário se afastar.

CXIII. Caso o notebook ou desktop não possua configuração de bloqueio de tela, o setor de TI deve ser acionado.

5.11. Uso e aquisição de software, sistema, aplicação e licenciamento

CXIV. Softwares, sistema, aplicações e licenciamento de direito de uso, somente poderão ser contratados após homologado, validado e aprovados pela equipe de TI, divulgadas por meio do formulário de análise e homologação de softwares, disponibilizados no Portal de Serviços de TI, na Intranet da Brazilian Nickel S/A.

CXV. Antes de serem utilizadas no ambiente da Brazilian Nickel S/A, todos os softwares, sistemas, aplicações e licenças de uso, devem passar por processo de homologação pela área de Tecnologia da Informação. O procedimento inclui:

a) **Solicitação formal:** o Usuário ou área interessada deverá encaminhar pedido de avaliação à área de Tecnologia da Informação, descrevendo finalidade, escopo de uso e tipos de dados envolvidos, por meio do Formulário de Análise e Homologação de Softwares, disponível no Portal de Serviços de TI, na Intranet da Brazilian Nickel S/A.

b) **Análise técnica e de segurança:** verificação dos requisitos de proteção de dados, uso de tecnologias de autenticação (MFA, SSO, por exemplo), tecnologias de integração (APIs por exemplo), mecanismos de segurança, localização dos servidores, controles de acesso e de versão, riscos de incidentes e backups.

c) **Avaliação jurídica e de conformidade:** revisão dos termos de uso, licenças, cláusulas de propriedade intelectual, bases legais aplicáveis e aderência às políticas internas e à legislação vigente (incluindo proteção de dados, com apoio do Encarregado de Proteção de Dados ou figura equivalente, conforme exigido ou designado nas Leis de Proteção de Dados Aplicáveis ao país) e Avaliação de Impacto sobre a Proteção de Dados (DPIA/PIA) se aplicável.

d) **Classificação de riscos e definição de restrições:** identificação do nível de risco da solução e definição das condições ou limites para seu uso pela Equipe de Tecnologia da Informação.

e) **Aprovação formal:** somente após a validação técnica, jurídica e de conformidade a ferramenta será considerada homologada, devendo ser incluída na lista de soluções autorizadas divulgadas pela Brazilian Nickel S/A.

f) **Registro e monitoramento:** ferramentas aprovadas devem ser registradas e sujeitas a revisões periódicas, a fim de verificar continuidade da conformidade, segurança e adequação ao uso corporativo.

5.12. Uso de inteligência artificial

CXVI. Para uso de IA com dados internos, a Brazilian Nickel S/A priorizará soluções em plataformas seguras, controladas e com contratos que garantam que os dados da Companhia não serão utilizados para treinar o modelo de IA do fornecedor. Portanto, somente poderão ser utilizadas as plataformas previamente aprovadas pela equipe de TI, divulgadas por meio do formulário de análise e homologação de softwares, disponibilizados na Intranet (**Corporate Financial Portal**) da Brazilian Nickel S/A.

CXVII. A implementação e o uso de sistemas de IA deverão ocorrer em conformidade com a Leis sobre Inteligência Artificial Aplicáveis sobre o tema, regulamentos e orientações de autoridades competentes vigentes em cada jurisdição em que a Brazilian Nickel S/A opera.

CXVIII. A IA pode operar como ferramenta assistiva ou tomar decisões com diferentes níveis de autonomia, e o seu uso deve sempre respeitar os princípios de ética, segurança, legalidade, privacidade e finalidade legítima.

CXIX. Antes de serem utilizadas no ambiente da Brazilian Nickel S/A, todas as ferramentas de Inteligência Artificial devem passar por processo de homologação pela área de Tecnologia da Informação, disponibilizados na Intranet (**Corporate Financial Portal**). O procedimento inclui:

a) **Solicitação formal:** o Usuário ou área interessada deverá encaminhar pedido de avaliação da ferramenta à área de Tecnologia da Informação, descrevendo finalidade, escopo de uso e tipos de dados envolvidos, por meio do Formulário de Análise e Homologação de Softwares, disponível no Portal de Serviços de TI, na Intranet da Brazilian Nickel S/A.

b) **Análise técnica e de segurança:** verificação dos requisitos de proteção de dados, com apoio do Encarregado de Proteção de Dados ou figura equivalente, conforme designado nas Leis de Proteção de Dados Aplicáveis ao país, se necessário, mecanismos de segurança, localização dos servidores, controles de acesso e riscos de incidentes.

c) **Avaliação jurídica e de conformidade:** revisão dos termos de uso, licenças, cláusulas de propriedade intelectual, bases legais aplicáveis e aderência às políticas internas e à legislação vigente (incluindo proteção de dados, com apoio do Encarregado de Proteção de Dados ou figura equivalente, conforme exigido ou designado nas Leis de Proteção de Dados Aplicáveis ao país).

d) **Classificação de riscos e definição de restrições:** identificação do nível de risco da ferramenta, com avaliação dos possíveis impactos adversos associados, e definição das condições ou limites para seu uso pela Equipe de Tecnologia da Informação, em conformidade com as Leis de Inteligência Artificial Aplicáveis.

e) **Aprovação formal:** somente após a validação técnica, jurídica e de conformidade a ferramenta será considerada homologada, devendo ser incluída na lista de soluções autorizadas divulgadas pela Brazilian Nickel S/A. A decisão adotada pela Equipe de Tecnologia da Informação deverá ser formalmente documentada.

f) **Registro e monitoramento:** ferramentas aprovadas devem ser registradas e sujeitas a revisões periódicas, a fim de verificar continuidade da conformidade, segurança e adequação ao uso corporativo.

CXX. Para avaliação do risco previsto, devem ser considerados os seguintes fatores:

Nível de Risco	Descrição	Exemplos	Implicações para a Brazilian Nickel S/A
Risco Inaceitável	Sistemas que causam danos ou violam direitos fundamentais	Sistemas de manipulação subliminar, sistemas de pontuação social obrigatória.	Uso ou contratação proibido.
Risco Elevado	IA que impacta diretamente direitos fundamentais, segurança, saúde, emprego, ou processos jurídicos.	Sistemas de recrutamento automático, reconhecimento facial em segurança, IA em saúde crítica, avaliação de crédito.	Exige avaliação rigorosa, transparência, mitigação de riscos e auditoria.
Risco Limitado	IA com impacto moderado, mas sem risco direto a direitos críticos.	Chatbots, assistentes virtuais, recomendadores de conteúdo, filtros de spam.	Exige transparência, com divulgação clara ao usuário, monitoramento de uso e proteção básica.
Risco Mínimo ou Nulo	IA que não apresenta impacto significativo na segurança ou direitos.	Ferramentas internas, sistemas de automação simples.	Pode ser usado livremente, sem exigências regulatórias específicas.

CXXI. Para sistemas de Inteligência Artificial classificados como de Risco Elevado (conforme Item CXIV) e que se enquadrem nas categorias de alto risco do Regulamento de Inteligência Artificial da União Europeia (EU AI Act), a Companhia observará requisitos adicionais, incluindo, mas não se limitando a:

a) **Sistema de Gestão da Qualidade**: Implementação e manutenção de um sistema de gestão da qualidade, garantindo a conformidade ao longo de todo o ciclo de vida do sistema de IA.

b) **Avaliação de Conformidade**: Realização de avaliação de conformidade antes da colocação no mercado ou entrada em serviço, demonstrando a aderência aos requisitos do EU AI Act.

c) **Documentação Técnica e Manutenção de Registros**: Elaboração e manutenção de documentação técnica e de registos (logs) gerados durante a operação do sistema de IA, a fim de garantir a rastreabilidade.

d) **Supervisão Humana**: Implementação de medidas para garantir a supervisão humana significativa, permitindo que

indivíduos monitorem, avaliem e intervenham nas operações do sistema de IA, conforme apropriado.

e) **Cibersegurança**: Adoção de medidas técnicas e organizacionais para assegurar que os sistemas de IA de alto risco sejam precisos e seguros, visando minimizar erros e vulnerabilidades.

f) **Transparência e Fornecimento de Informações**: Fornecimento de informações claras, completas e compreensíveis aos usuários sobre as capacidades, limitações e o propósito dos sistemas de IA, conforme os requisitos de transparência do EU AI Act.

CXXII. A Companhia monitorará a evolução legislativa e as orientações das autoridades competentes sobre o EU AI Act, para garantir a contínua adequação de suas políticas e práticas.

CXXIII. Antes de utilizar ferramentas de IA, os Usuários deverão analisar os benefícios e os riscos associados a cada uso. Dentre os riscos, destacam-se:

a) **Alucinações, discriminação e vieses na IA Generativa:** modelos de IA podem gerar informações incorretas, imprecisas ou enviesadas, inclusive gerando tratamento desigual ou discriminatório a indivíduos ou grupos, bem como impactando a qualidade das decisões e criando riscos reputacionais ou operacionais.

b) **Direito autoral e propriedade intelectual:** conteúdos gerados ou utilizados pela IA podem violar direitos de terceiros, especialmente quando baseados em materiais protegidos ou quando não houver clareza sobre titularidade e permissões de uso.

c) **Incidente de segurança envolvendo dados pessoais e corporativos:** o uso inadequado da IA pode resultar em exposição indevida, vazamento ou tratamento irregular de informações sensíveis, violando normas internas e legislações de proteção de dados. IAs generativa públicas (ex.: chatbots, geradores de código, ferramentas de resumo) podem submeter as informações inseridas ao treinamento contínuo desses modelos, transformando dados confidenciais da Companhia em parte do conhecimento público da ferramenta, o que é estritamente proibido sem autorização e garantia de não utilização dos dados para treinamento, conforme estabelecido no item CX. O uso dessas ferramentas deve considerar a base legal para o tratamento e os mecanismos de transferência internacional de dados, quando aplicáveis..

d) **Informações desatualizadas ou imprecisas:** modelos podem utilizar bases não atualizadas, levando a conclusões incorretas para o contexto corporativo.

e) **Falta de rastreabilidade e transparência:** algumas ferramentas não permitem compreender integralmente como as respostas são geradas, dificultando a auditoria, a verificação de fontes e a responsabilização.

f) **Dependência excessiva da tecnologia:** a confiança desmedida na IA pode reduzir a supervisão humana, comprometer a qualidade de análises e levar a decisões automatizadas inadequadas.

CXXIV. Durante o uso de ferramentas da IA, os seguintes princípios devem ser observados pelos Usuários:

a) **Legalidade e conformidade:** a utilização de ferramentas de IA deve sempre observar a legislação vigente, incluindo normas de proteção de dados, direitos autorais, propriedade intelectual e demais regulamentos aplicáveis.

b) **Transparência:** os Usuários devem indicar quando um conteúdo foi gerado com apoio de IA, sempre que relevante, e assegurar clareza sobre limitações, fontes e premissas utilizadas.

c) **Supervisão humana:** a IA deve atuar como ferramenta de apoio, não substituindo o julgamento humano. Usuários permanecem responsáveis pelas decisões tomadas com base nos resultados fornecidos pela tecnologia.

d) **Segurança e Privacidade:** é proibido inserir dados pessoais ou corporativos sensíveis em ferramentas não homologadas. O uso da IA deve preservar a confidencialidade, integridade e disponibilidade das informações.

e) **Qualidade e Acurácia:** os conteúdos gerados devem ser verificados, validados e ajustados pelo Usuário, considerando possíveis erros, vieses ou imprecisões inerentes aos modelos de IA.

f) **Proporcionalidade**: a IA deve ser utilizada somente quando necessária, adequada ao propósito pretendido e alinhada aos interesses legítimos da organização.

g) **Minimização**: devem ser utilizados apenas os dados estritamente necessários para a finalidade do

processamento, preferencialmente anonimizados ou pseudonimizados.

CXXV. Todo conteúdo gerado por IA com base em dados ou instruções da Companhia pertence à Companhia. É responsabilidade do colaborador assegurar que o output da IA não viole direitos autorais de terceiros, especialmente se for para uso externo ou comercial. Quando um resultado de IA for usado externamente, a Companhia deve considerar a necessidade de atribuição adequada e transparente (ex.: "este documento foi gerado com o auxílio de IA").

CXXVI. É estritamente proibido:

a) inserir, copiar ou enviar dado classificado como Confidencial, Segredo Comercial, Estratégico ou Pessoal de Clientes/Colaboradores em plataformas públicas de Inteligência Artificial (ChatGPT, Copilot, Gemini, Claud, Bard, DeepSeek, etc.) sem autorização formal;

b) uso geral de IA não licenciadas ou aprovadas pela Companhia, bem como contornar mecanismos de segurança, políticas de privacidade, restrições de uso ou limitações definidas no processo de homologação;

c) empregar IA para fins ilícitos, antiéticos ou contrários às políticas internas, incluindo fraude, manipulação, discriminação ou violação de direitos de terceiros;

d) utilizar conteúdos gerados por IA como se fossem resultados verificados, sem revisão humana adequada;

e) atribuir decisões automatizadas à IA sem supervisão, especialmente em situações que possam impactar pessoas, clientes, parceiros ou processos críticos;

f) Utilizar IA para criar conteúdos enganosos, como deepfakes, informações falsas ou comunicações que possam induzir terceiros ao erro.

5.13. Backup

CXXVII. Todos os procedimentos relativos ao Backup e à recuperação de dados armazenados nos servidores da BRN devem observar as disposições desta Política.

CXXVIII. Os procedimentos de Backup devem ser atualizados sempre que ocorrer:

a) Novas aplicações desenvolvidas;

b) Novos locais de armazenamento de dados ou arquivos;

c) Novas instalações de banco de dados;

d) Novos aplicativos instalados;

e) Outras informações que exijam proteção por meio de Backup.

CXXIX. As cópias de segurança devem contemplar arquivos, sistemas digitais, máquinas virtuais e bancos de dados armazenados ou hospedados nos data centers da BRN.

CXXX. Para dispositivos móveis, o colaborador deve utilizar os softwares homologados pela BRN para realização de Backup.

CXXXI. Recomenda-se que os colaboradores mantenham seus arquivos em nuvem, evitando salvá-los no diretório local ou área de trabalho dos dispositivos móveis.

CXXXII. As cópias de segurança devem ser testadas regularmente para garantir sua usabilidade em caso de recuperação.

CXXXIII. O procedimento deverá definir requisitos técnicos e operacionais adequados para geração, restauração e testes de validação dos Backups.

CXXXIV. As ferramentas de Backup devem ser mantidas e atualizadas conforme recomendações do fornecedor e com licenças válidas, alinhadas ao contrato firmado para essa finalidade.

5.14. Propriedade Intelectual

CXXXV. É dever de todos os Usuários exercer suas funções de forma ética, comprometida com a integridade e confidencialidade necessárias aos temas tratados na Brazilian Nickel S/A, bem como proteger os ativos de propriedade intelectual da organização, incluindo marcas, códigos-fonte, modelos, métodos, documentos, pesquisas, know-how e demais informações estratégicas.

CXXXVI. É proibido utilizar, reproduzir, adaptar ou distribuir materiais protegidos por direitos autorais, patentes, segredos comerciais ou licenças sem a devida autorização formal ou sem observar as condições previstas pelos titulares dos direitos.

CXXXVII. Todo conteúdo, documentação, software, análise, relatório ou solução desenvolvida no exercício das atividades profissionais, utilizando recursos corporativos ou informações da empresa, é considerado propriedade intelectual da organização, salvo disposição contratual em contrário.

CXXXVIII. A instalação ou uso de softwares, bibliotecas, serviços em nuvem ou ferramentas de terceiros deve ocorrer exclusivamente mediante licenças válidas e conformidade com os termos contratuais aplicáveis, sendo proibida qualquer forma de uso indevido ou não licenciado.

CXXXIX. Os Usuários devem sempre atuar em defesa dos interesses da BRN e manter sigilo sobre negócios, operações, dados pessoais e demais informações confidenciais.

CXL. É proibida a utilização, divulgação, fotografia, digitalização e/ou gravação de informações de propriedade da BRN para benefício próprio ou de terceiros, mesmo após o término da relação com a BRN.

CXLI. É proibida a produção de cópias ou Backups, por qualquer meio, de documentos e informações fornecidos aos Usuários ou que tenham chegado ao seu conhecimento em razão da relação com a BRN, independentemente da classificação da informação.

CXLII. É proibido utilizar os Sistemas da BRN para carregar, reproduzir ou distribuir músicas, vídeos, dados ou outros conteúdos não licenciados pela BRN.

CXLIII. Todos os documentos e informações constantes dos sistemas e da rede da BRN são confidenciais e não podem ser divulgados a terceiros nem utilizados para qualquer finalidade diversa da determinada pela BRN, inclusive após o fim da relação com a organização.

Ao encerrar a relação com a SCMP, o Usuário deve devolver todos os Ativos de Informação ou comprovar que destruiu, de forma segura e mediante autorização, as informações a que teve acesso.

5.15. Gestão de Riscos e Incidentes

CXLIV. Riscos e Incidentes envolvendo temas de segurança da informação devem ser permanentemente monitorados, conforme Política de Gestão de Incidentes e as melhores normas técnicas disponíveis no mercado. Todos os incidentes envolvendo Ativos da Informação devem servir de base para a implementação de novas metodologias e/ou controles.

CXLV. Na Companhia, a fim de mitigar riscos de segurança da informação, realizamos o uso de antivírus em todas as máquinas, bem como implementamos firewall.

CXLVI. Os Usuários também são parte importante da gestão de riscos de segurança da informação. Quando ocorrer de algum colaborador perceber algo estranho acontecendo com seu computador, isto pode ser um sinal de invasão de hacker, nestes casos avisar o setor de TI o quanto antes para evitar que o potencial ataque cibernético tenha êxito. Além disso, atente-se às condutas vedadas:

a) Instalar softwares que não foram devidamente acompanhados ou autorizados pelo setor de TI;

b) Desativar e/ou atrasar a atualização do programa antivírus instalado nos equipamentos, devendo o Usuário efetuar checagens regulares com o antivírus tanto da informação baixada via Internet como a contida em qualquer tipo de backup;

c) Realizar manutenção de computadores sem o acompanhamento do TI;

d) Alterar configurações dos computadores sem a prévia autorização e o devido acompanhamento do TI.

CXLVII. Caso seja necessário realizar qualquer tipo de manutenção em seu computador, entre em contato com a equipe de TI por meio do e-mail **suporte.ti@brnickel.com** e ou **itsupport@brnickel.com**, conforme aplicável.

5.16. Dispositivos e critérios técnicos

CXLVIII. Todos os dispositivos **(desktops, laptops e móveis)** devem seguir os padrões técnicos homologados pela TI, com requisitos mínimos de desempenho e segurança.

5.16.1. Diretrizes gerais para desktops e laptops:

CXLIX. Somente equipamentos com TPM 2.0, compatibilidade com Windows 11 Pro/Enterprise, memória mínima de 16 GB (32 GB avançado), SSD mínimo de 512 GB NVMe, CPU i7/i9 ou Ryzen Pro e antivírus corporativo ativo serão aceitos.

a) Somente poderão ser utilizadas GPUs dedicadas da Nvidia.

b) Não são permitidas configurações de canal único.

c) Quando aplicável, todo o hardware sem fio deverá ser de fabricação Intel.

d) Todo equipamento de telas deverá possuir resolução mínima de 1920 x 1080, proporção de 16:9, alta definição total.

e) Todas as telas sensíveis ao toque poderão incluir a caneta Dell Premium Active Pen (PN579X) como opcional.

f) Todos os laptops deverão possuir câmera infravermelha certificada pelo Windows Hello for Business.

CL. Os seguintes modelos de hardware da Dell são estritamente proibidos para uso no Brazilian Nickel S/A:

- Dell Inspiron.
- Dell G-Series.
- Dell Alienware.

CLI. Os seguintes modelos de hardware Android são estritamente proibidos para uso na Brazilian Nickel S/A:

- Huawei ®
- Positivo ®

CLII. Somente Monitores 27” / 32” 4K, docks Thunderbolt 4, headsets certificados Teams são permitidos.

CLIII. Dispositivos pessoais utilizados em home office devem estar sob gerenciamento MDM (Mobile Device Manager) / Intune.

CLIV. As especificações estabelecidas neste regulamento são especificações mínimas requeridas. As especificações não impedem a escolha ou aquisição de máquinas com uma especificação mais alta (por exemplo, memória, armazenamento etc.), caso a disciplina assim o exija, com base em uma justificativa técnica e/ou comercial no momento da aquisição.

CLV. A Brazilian Nickel S/A exige que o fabricante de equipamento original (OEM) seja de nível 1 e seja aprovado pelo setor de Tecnologia da Informação.

CLVI. O fabricante OEM deverá fornecer todo o hardware. Isso não apenas garante a continuidade países, mas também um fluxo constante de hardware consistente com suporte associado disponível em todas as áreas em que o Grupo opera. Esse padrão poderá ser usado para determinar a aquisição de desktops, laptops e dispositivos complementares no ambiente de tecnologia operacional (OT).

CLVII. Atualmente, são contratados fornecedores globais aprovados como o fabricante de equipamento original (OEM) de nível 1:

- Dell para monitores, desktop e laptop;
- Lenovo para laptops.

CLVIII. Atualmente, os fornecedores não são contratados, mas permitidos:

- Apple para hardware complementar.
- Microsoft para hardware alternativo de laptop;

CLIX. O hardware que está disponível para uso mediante motivação e aprovação da gerência de linha, mas não é imposto como obrigatório ou substituto de um desktop/laptop. Os desktops/laptops continuarão sendo o dispositivo principal para todos os funcionários.

CLX. Todas as novas séries Dell Precision virão de fábrica com uma GPU.

5.16.2. Critérios de Configuração de Equipamentos por Perfil de Cargo:

CLXI. Definir critérios técnicos mínimos e recomendações de configuração para aquisição, substituição e manutenção de desktops/laptops corporativos, conforme o perfil de uso e nível de responsabilidade dos colaboradores, garantindo desempenho, segurança e padronização tecnológica.

5.16.3. Marcas Padronizadas

CLXII. Equipamentos devem ser, preferencialmente, de marcas que ofereçam suporte corporativo, garantia on-site e compatibilidade com as políticas de segurança e MDM da Companhia: Dell (Linha Latitude, Precision, XPS), Lenovo (linha X1, X9), Microsoft (Linha Surface Pro, Surface Laptop) e Apple (Linha MacBook Air ou MacBook Pro, conforme necessidade).

5.16.4. Configuração Mínima Base (Todos os Perfis)

Item	Especificação Mínima
Processador (CPU)	Intel Core i5 (12ª geração ou superior) **ou** AMD Ryzen 7 equivalente
Memória RAM	16 GB DDR4 ou DDR5
Armazenamento	SSD NVMe 512 GB
Tela	14" Full HD (mínimo) – antirreflexo
Conectividade	Wi-Fi 6 ou superior, Bluetooth 5.x
Portas	USB-A, USB-C, HDMI
Sistema Operacional	Windows 11 Pro
Segurança	TPM 2.0, BitLocker, suporte MDM Intune

5.16.5. Critérios por Perfil de Cargo

Cargo / Perfil	Tipo de Equipamento	Configuração Recomendada*	Observações
Grupo 01 (Jovem Aprendiz, Auxiliares e Assistente)	Desktop/Notebook corporativo intermediário	CPU i5 | Ryzen 7 | 16 GB RAM |SSD 512 GB	Equipamento padrão para tarefas administrativas e operacionais.
Grupo 02 (Analistas e Técnicos)	Notebook corporativo intermediário	CPU i7 | Ryzen 7 Pro / 16/32 GB RAM / SSD 512 GB	Equipamento padrão para tarefas administrativas e operacionais.
Grupo 03 Especialista	Notebook de alto desempenho	CPU i7 / Ryzen 7 Pro / 32/64 GB RAM / SSD 1 TB	Indicado para atividades técnicas intensivas (Dados, BI, Dev., Engenharia).
Grupo 04 Supervisor	Notebook corporativo premium	CPU i7 / Ryzen 7 Pro / 16 GB RAM / SSD 512 GB	Desempenho equilibrado e boa portabilidade.
Grupo 05 Coordenador	Notebook premium ultrafino	CPU i7 / Ryzen 7 Pro / 16 GB RAM / SSD 512 GB	Preferência por modelos leves e com bateria de longa duração.
Grupo 06 Gerente	Notebook executivo	CPU i7 / Ryzen 7 Pro / 32 GB RAM / SSD 1 TB	Priorizar performance e conectividade. Possível opção Surface
Grupo 07 Gerente Geral / Diretor	Ultrabook executivo	CPU i7 / Ryzen 9 Pro / 32 GB RAM / SSD 1 TB	Equipamento premium, desempenho e design corporativo.
Grupo 08 C-Levels (CEO, CFO, COO, CPO, etc.)	Ultrabook executivo	CPU i7 / Ryzen 9 Pro / 32 GB RAM / SSD 1 TB ou superior	Equipamento de maior confiabilidade, performance e estética.

***As demandas que requeiram a utilização de placa gráfica dedicada deverão ser submetidas à avaliação prévia da área de Tecnologia da Informação, sendo analisadas caso a caso, com base em critérios técnicos, operacionais e de custo. A disponibilização deste recurso estará condicionada à aprovação formal da TI, após a validação da real necessidade para o desempenho das atividades do usuário.**

5.16.6. Ciclo de Renovação e Gestão

Tipo de Equipamento	Ciclo de Renovação	Observações
Desktops	5 anos	Troca antecipada em caso de obsolescência ou falha crítica.
Notebooks corporativos	4 anos	Troca antecipada em caso de obsolescência ou falha crítica.
Ultrabooks executivos / premium	3 anos	Sujeito a atualização conforme evolução tecnológica.
Dispositivos móveis	3 anos	Reavaliação de capacidade técnica a cada ciclo.
Equipamentos de alta performance (dados, engenharia, TI)	3 anos	Reavaliação de capacidade técnica a cada ciclo.

CLXIII. No caso de alteração de cargo, o equipamento poderá ser substituído, de acordo com o novo grupo no qual o usuário fará parte e em conformidade com os critérios previstos no item 5.17.5.

5.16.7. Especificações mínimas definidas para os dispositivos complementares móveis de Hardware.

CLXIV. Para aumentar a produtividade do usuário final permitindo o trabalho em trânsito é recomendado a utilização de dispositivos complementares móveis como tablets e smartphones.

CLXV. Todos os dispositivos complementares estão sujeitos ao gerenciamento de dispositivos móveis. Por isso, os equipamentos móveis deverão ser avaliados e aprovados pelo setor de Tecnologia da Informação e Facilities.

CLXVI. Os dispositivos complementares são opcionais e dependem da motivação do cargo e função do colaborador.

CLXVII. Os dispositivos complementares não substituem desktop's ou laptop's e não são obrigatórios. Não obstante os dispositivos complementares também não determinam necessariamente os dispositivos robustos usados na operação.

CLXVIII. A tabela abaixo traz ESPECIFICAÇÕES MÍNIMAS DEFINIDAS PARA OS DISPOSITIVOS COMPLEMENTARES MÓVEIS DE HARDWARE. Essas definições tem como objetivo proteger o ambiente de máquinas que não atendam aos requisitos de execução de softwares da Brazilian Nickel S/A. Tal especificação indica os requisitos mínimos para um novo dispositivo móvel complementar no ambiente de produção.

Perfil	Dispositivo	Capacidade	Tamanho da tela
Light	Apple iPad Air 5th geração	256 GB / 8 GB*/256 GB	10.9" / 10.0"
Padrão	Apple iPad Pro 11" 5th geração	256 GB / 8 GB*/256 GB	11.0"
Avançado	Apple iPad Pro 12.9" 5th geração	256 GB / 8 GB*/256 GB	12.9" / 12.4"

CLXIX. Tanto o hardware do Apple iPad quanto o do Surface Pro, vêm em duas configurações:

- Wi-Fi;
- Wi-Fi + celular;

CLXX. Nos modelos somente com Wi-Fi, os usuários podem conectar o tablet a seus telefones celulares para obter conectividade com a Internet.

CLXXI. Todos os dispositivos APPLE deverão ser adquiridos com um Apple Pencil (2ª geração);

CLXXII. Todos os dispositivos MICROSOFT deverão ser adquiridos com um Surface Pro Pen;

CLXXIII. Todos os dispositivos ANDROID, mesmo que a fabricante SAMSUMG seja a preferida pelos usuários, deverão seguir o requisito mínimo de ser produzido por um fabricante OEM nível 1. O dispositivo ainda deverá ser capaz de executar a Google Play Store.

CLXXIV. Dispositivos produzidos pelos fabricantes HUAWEI e POSITIVO são estritamente proibidos mesmo que atendam as demais diretrizes estabelecidas neste regulamento;

CLXXV. As especificações estabelecidas neste regulamento para dispositivos complementares são especificações mínimas requeridas. As especificações não impedem a escolha ou aquisição de máquinas com uma especificação mais alta, caso a disciplina assim o exija, com base em uma justificativa técnica e/ou comercial no momento da aquisição.

5.16.8. Diretrizes para a Escolha Desktops, Laptops e Periféricos

CLXXVI. A tabela abaixo apresenta dispositivos, opcionais e acessórios, recomendados pelo setor de Tecnologia da Informação. A tabela apresenta tais dispositivos conforme o fabricante OEM de nível 1:

Fabricante OEM de Nível 1	Dispositivo	Modelo	Especificações
DELL	DockStation (Ver item XXXIII)	Dell WD19DCS	Base dupla USB-C
DELL	Monitores	Dell P2422H	Resolução de 1080p (1920x1080)
DELL	Monitores	Dell P2723QE	Resolução 2160p/4K (3840x2160)
MICROSOFT	Tablet	Microsoft Surface Dock 2	-
MICROSOFT	Caneta para Tablet	Surface Slim Pen 2	-
MICROSOFT	Teclado para Tablet	Teclado para Surface Pro	-
APPLE	Caneta inteligente	Apple Pencil	2ª geração
APPLE	Teclado	Apple Magic Keyboard ®	-
APPLE	Teclado	Teclado inteligente Apple Folio®	-

CLXXVII. Para DOCKSTATION do fabricante DELL deverá ser observado que as estações de acoplamento USB e USB Tipo C são compatíveis com DisplayPort sobre USB e Thunderbolt 3. Isso permite que os computadores sejam acoplados a teclados, mouses, telas e outras funções externas. Todo computador com o hardware necessário funciona com uma estação de acoplamento USB ou USB Tipo C. Há requisitos para que as estações de acoplamento sejam compatíveis ou recomendadas para uso com computadores específicos.

CLXXVIII. As especificações para desktops e laptops consideram um usuário ou perfil de usuário. Os perfis de uso são criados com base em como os usuários normalmente usam uma máquina. O uso típico pode ser classificado nas três categorias a seguir:

a) **Perfil Básico:** Trabalhador de uma única tarefa;

b) **Perfil Médio:** Trabalhador multitarefa;

c) **Perfil Avançado:** Trabalhador de tarefas críticas.

CLXXIX. Com base na categoria do trabalhador, as especificações e as classes de CPU (laptops OptiPlex, OptiPlex Workstation, Latitude e Precision) foram projetadas para atender aos critérios dessas categorias. A especificação nessas categorias foi escolhida de modo que houvesse o mínimo de sobreposição, sempre que possível, e um nível aceitável de sobreposição era inevitável para permitir a variedade de modelos selecionados com base no perfil do usuário.

CLXXX. Os trabalhadores de tarefa única podem não implicar em um trabalhador de tarefa de baixo nível. Algumas tarefas individuais são críticas para os negócios, e isso precisa ser tratado de forma adequada, aumentando a especificação, por exemplo, de Ultra-Baixo ou Baixo para Padrão.

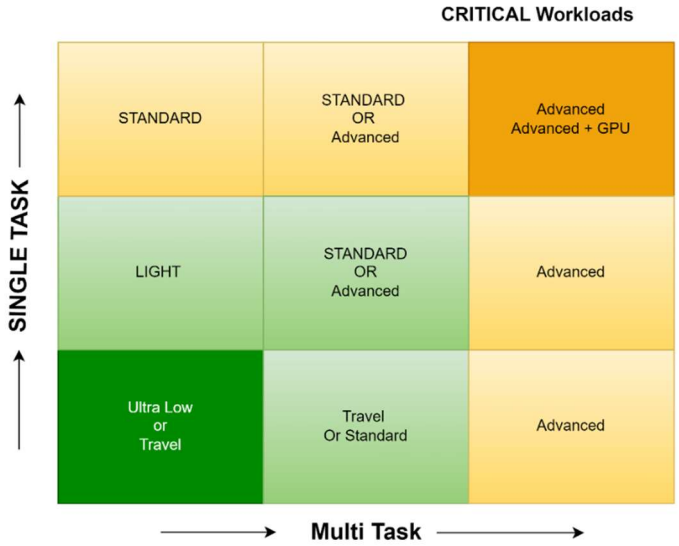

Figura 1 - Escolha de desktop/laptop

5.16.9. Diretrizes para a Escolha de um Dispositivos Móveis

CLXXXI. As especificações dos dispositivos complementares foram consideradas com base em um usuário ou perfil de usuário. Os perfis de uso são criados com base em como os usuários normalmente combinam um dispositivo complementar em sua vida profissional diária. O uso típico pode ser classificado nas três categorias a seguir:

a) Promoção da mobilidade

b) Promoção da produtividade

c) Altamente móvel e produtivo

CLXXXII. Com base na categoria da tarefa, usar um laptop com um dispositivo complementar seria a melhor experiência. A produtividade sempre favorecerá o hardware de laptop ou desktop de última geração, pois acreditamos que o desempenho, e não a conveniência, melhora a produtividade; no entanto, a combinação de produtividade e mobilidade com um dispositivo complementar pode aprimorar a experiência das pessoas que se deslocam dentro e fora do escritório. A mobilidade não determina necessariamente a viagem.

CLXXXIII. A especificação nessas categorias foi escolhida de modo que houvesse uma sobreposição mínima sempre que possível e um nível aceitável de sobreposição fosse inevitável para permitir a variedade de configurações selecionadas com base no perfil do usuário.

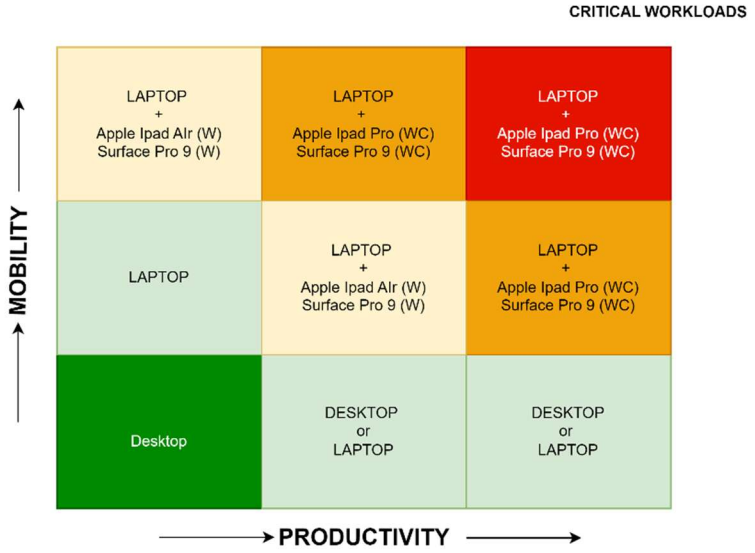

Figura 2 - Escolha do dispositivo complementar

WC: Wi-Fi + celular

W: Somente Wi-Fi (conectado ao celular quando necessário)

5.16.10. Ciclo de Vida do Hardware

CLXXXIV. Os modelos de hardware existentes devem ser eliminados gradualmente de acordo com o padrão de ciclo de vida do hardware.

CLXXXV. Diretrizes para substituição e descarte de hardwares em geral deverão seguir procedimento específico elaborado para esse objetivo. Diante da necessidade de substituição ou descarte o usuário final deverá observar essas diretrizes e realizar o procedimento específico sob orientação direta do setor de Tecnologia da Informação.

5.16.11. Sustentabilidade e Descarte

CLXXXVI. Equipamentos substituídos devem seguir política de logística reversa certificada (ESG).

CLXXXVII. Possibilidade de doação corporativa ou recompra mediante avaliação técnica e de acordo com as políticas internas da Brazilian Nickel S/A.

6. CONTROLE DE REVISÃO

Revisão	Data	Motivo da revisão
Rev. 01	31/03/2026	- Edição inicial;

7. COLABORADORES

Nome	Área
Eduardo Almeida	Tecnologia da Informação

****