DATA	Rev.	DESCRIÇÃO	Páginas e/ou parágrafo
20/03/2025	00	Primeira edição	Documento inteiro

SUMÁRIO

1. OBJETIVO E ÂMBITO DE APLICAÇÃO

Este documento estabelece as diretrizes e procedimentos para a gestão da segurança da informação e privacidade de dados pessoais da empresa Rodoanel BH S.A., assegurando a conformidade com a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), Regulamento Geral de Proteção de Dados da União Europeia (GDPR – General Data Protection Regulation), ISO/IEC 27001, ISO 27701 e demais normativos aplicáveis.

Aplica-se a todos os colaboradores da Rodoanel BH S.A., parceiros estratégicos, fornecedores, prestadores de serviço e demais partes interessadas que tenham acesso ou tratem informações relacionadas ao projeto, assegurando que a gestão da segurança da informação e privacidade de dados esteja alinhada às melhores práticas de governança, compliance e gestão de riscos.

2. DEFINIÇÕES E SIGLAS

Definição	Descrição
Partes interessadas externas ou terceiros interessados	Pessoas ou grupos envolvidos ou influenciados pelo desempenho ambiental e de saúde e segurança do trabalho da empresa Rodoanel BH S.A.

Sigla	Definição
CA	Conselho de Administração
DIR-P	Diretor Presidente
DIR	Diretor
GENG	Gestor de Engenharia
GPLA	Gestor de Planejamento
GESG	Gestor de ESG
GSUP	Gestor de Contratos e Suprimentos
GJUR	Gestor Jurídico
GCOM	Gestor de Comunicação
GPRO	Gestor de Projetos
GSSO	Gestor de Segurança e Saúde Ocupacional
GADM	Gestor de Administração e Finanças
GGEP	Gestor de Recursos Humanos
GPD	Gestor de Proteção de Dados e Tecnologia da Informação
CO	Compliance Officer

- **Dados Pessoais:** Qualquer informação relacionada a uma pessoa natural identificada ou identificável, conforme definido pela Lei Geral de Proteção de Dados (LGPD) e pelo Regulamento Geral de Proteção de Dados (GDPR).

- **Dados Sensíveis:** Dados pessoais que revelam origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, dados genéticos ou biométricos, dados de saúde ou vida sexual.
- **Segurança da Informação:** Conjunto de práticas e medidas adotadas para garantir a confidencialidade, integridade e disponibilidade das informações da organização.
- **Confidencialidade:** Princípio que assegura que as informações são acessíveis apenas por pessoas autorizadas.
- **Integridade:** Garantia de que os dados e informações não foram alterados ou corrompidos de forma não autorizada.
- **Disponibilidade:** Garantia de que as informações e sistemas estão acessíveis e utilizáveis quando necessário, conforme definido pelos requisitos da organização.
- **Violação de Dados:** Qualquer incidente que resulte na destruição, perda, alteração, divulgação não autorizada ou acesso indevido a dados pessoais ou informações sensíveis.
- **Gestor de Proteção de Dados (GPD):** Pessoa designada para supervisionar a conformidade da organização com as leis de proteção de dados e atuar como ponto de contato com autoridades reguladoras e titulares de dados.
- **Parceiro de Negócios:** Qualquer parte externa que tenha relação contratual ou comercial com a organização e que possa ter acesso a informações ou dados protegidos.
- **Terceiros:** Fornecedores, prestadores de serviços, consultores ou qualquer outra entidade que realize atividades em nome da organização e tenha acesso a dados pessoais ou informações estratégicas.
- **CO (Compliance Officer):** Responsável por supervisionar a conformidade da organização com as normas de compliance e segurança da informação, garantindo a implementação das diretrizes estabelecidas.
- **GCS (Gestor de Contratos e Suprimentos):** Área responsável pela formalização, acompanhamento e gestão dos contratos com terceiros, assegurando conformidade com os requisitos de proteção de dados.
- **SGI (Sistema de Gestão Integrado):** Estrutura organizacional voltada para a implementação e monitoramento das normas e políticas de segurança da informação e compliance.

3. LEIS E REGULAMENTOS

Esta política está em conformidade com as seguintes legislações nacionais e internacionais, além de normas relevantes para a segurança da informação e privacidade de dados:

- **Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados - LGPD):** Estabelece regras para o tratamento de dados pessoais no Brasil, garantindo direitos aos titulares e impondo obrigações às organizações.
- **Lei n.º 12.527/2011 (Lei de Acesso à Informação):** Regulamenta o direito de acesso a informações públicas e define requisitos de transparência para órgãos e entidades.
- **Código Penal Brasileiro (Art. 154-A):** Dispõe sobre crimes cibernéticos, incluindo invasão de dispositivos informáticos, interceptação de comunicações e divulgação não autorizada de dados.
- **Regulamento Geral de Proteção de Dados (GDPR – União Europeia):** Define requisitos para a proteção e privacidade de dados pessoais dentro da União Europeia e para transferências internacionais de dados.
- **ISO/IEC 27001:** Norma internacional para sistemas de gestão da segurança da informação, estabelecendo diretrizes para proteção de ativos e mitigação de riscos.
- **ISO/IEC 27701:** Extensão da ISO 27001, especificando requisitos para um sistema de gestão de privacidade de dados pessoais.
- **ISO 37301:** Norma internacional que define requisitos e diretrizes para um sistema de gestão de compliance efetivo.
- **ISO 37001:** Norma de gestão antissuborno, aplicável para a prevenção de riscos correlatos de integridade na segurança da informação.
- **Código de Ética e Conduta da empresa Rodoanel BH S.A.:** Estabelece princípios e regras para a conduta ética e a conformidade dentro da organização.
- **Procedimentos de Compliance e Gestão de Riscos:** Define controles internos para assegurar a conformidade com as diretrizes de proteção de dados e segurança da informação.
- **Procedimentos de Due Diligence e Monitoramento de Terceiros:** Determina requisitos para avaliação e monitoramento de fornecedores e parceiros que tenham acesso a informações sensíveis.

4. PRINCÍPIOS E DIRETRIZES GERAIS

4.1 Compromisso com a proteção de dados e segurança da informação

A segurança da informação e a proteção de dados são pilares fundamentais da governança da Rodoanel BH S.A., que adota uma abordagem rigorosa para assegurar a confidencialidade, integridade e disponibilidade das informações, garantindo que todos os processos e sistemas estejam alinhados aos mais elevados padrões de segurança.

Esse compromisso se reflete na implementação de um modelo de gestão estruturado, baseado em normas internacionais como a ISO/IEC 27001 (Gestão da Segurança da Informação) e a ISO/IEC 27701 (Gestão da Privacidade de Dados), além do cumprimento da Lei Geral de Proteção de Dados (LGPD) e do Regulamento Geral de Proteção de Dados da União Europeia (GDPR).

A organização prioriza a adoção de controles robustos, que previnem acessos não autorizados, vazamentos e qualquer forma de comprometimento dos ativos informacionais.

A segurança da informação não se restringe ao uso de tecnologia, mas exige disciplina organizacional e responsabilidade compartilhada. Para isso, a organização estabelece diretrizes claras para o manuseio de dados, promove capacitações contínuas e reforça mecanismos de monitoramento e auditoria.

Todos os envolvidos no projeto, incluindo colaboradores, fornecedores e parceiros estratégicos, devem aderir às políticas internas e comprometer-se com as práticas de proteção definidas.

A governança da informação também incorpora os princípios de privacy by design e security by design, assegurando que qualquer sistema, processo ou tecnologia adotado no projeto já seja concebido com mecanismos de segurança e conformidade embutidos. Dessa forma, a gestão de riscos é proativa, permitindo a antecipação de ameaças e a mitigação de vulnerabilidades antes que possam comprometer a integridade das operações.

Ao adotar uma postura preventiva e orientada pela conformidade, a Rodoanel BH S.A. fortalece a resiliência organizacional, assegurando que a proteção de dados e a segurança da informação sejam tratadas com a seriedade necessária para garantir a confiança, a continuidade das operações e o atendimento às exigências regulatórias.

4.2 Responsabilidade da alta administração na governança de segurança da informação e privacidade

A governança da segurança da informação e da privacidade de dados é uma responsabilidade direta da alta administração da Rodoanel BH S.A., que deve garantir a implementação, manutenção e aprimoramento contínuo das diretrizes estabelecidas nesta política.

O compromisso da liderança se traduz na definição de estratégias, alocação de recursos, supervisão da conformidade e estabelecimento de uma cultura organizacional que priorize a proteção dos ativos informacionais e o cumprimento das normativas aplicáveis.

A alta administração deve assegurar que a segurança da informação seja incorporada à governança corporativa, adotando uma abordagem estruturada para mitigar riscos e fortalecer a resiliência organizacional.

Esse compromisso exige que os princípios de proteção de dados e gestão da segurança da informação sejam considerados em todas as decisões estratégicas e operacionais, de forma a garantir que os controles de segurança sejam eficazes e adequados à complexidade do projeto.

A responsabilidade da liderança abrange:

- **Definição e aprovação das diretrizes estratégicas** para a segurança da informação e privacidade, assegurando alinhamento com as normas ISO/IEC 27001 e 27701, LGPD e GDPR.
- **Supervisão do cumprimento desta política e dos regulamentos aplicáveis**, garantindo a aderência às exigências normativas e promovendo auditorias periódicas.
- **Garantia de recursos adequados**, incluindo investimentos em tecnologia, treinamento e infraestrutura para a proteção de dados e segurança da informação.
- **Incorporação dos princípios de security by design e privacy by design**, assegurando que a proteção da informação esteja presente desde a concepção de novos processos, sistemas e serviços.
- **Monitoramento contínuo dos riscos** relacionados à segurança da informação e privacidade, promovendo revisões da matriz de riscos e assegurando que as medidas de mitigação sejam eficazes.
- **Fomento à cultura organizacional voltada à segurança da informação**, promovendo treinamentos e capacitações regulares para colaboradores, parceiros e fornecedores.
- **Resposta ágil e eficaz a incidentes de segurança e violações de dados**, garantindo que existam procedimentos definidos para mitigação de impactos e comunicação às partes interessadas e autoridades regulatórias.

4.3 Abordagem baseada em riscos: integração com a governança de segurança da informação e privacidade

A abordagem baseada em riscos (ABR) estrutura todas as decisões relativas à segurança da informação e privacidade de dados da Rodoanel BH S.A.

Esse modelo assegura que os controles implementados sejam proporcionais à criticidade dos ativos informacionais e ao impacto das ameaças identificadas, evitando tanto a subproteção quanto a aplicação de medidas desnecessárias que comprometam a eficiência operacional.

Diferente de abordagens prescritivas e estáticas, a ABR considera a dinamicidade do ambiente de ameaças e a evolução dos riscos organizacionais, assegurando que a segurança da informação não seja tratada como um conjunto fixo de barreiras, mas, sim, como um processo contínuo de avaliação e adaptação para identificação, análise, tratamento e monitoramento de riscos.

A aplicação da ABR na governança da segurança da informação e privacidade se baseia nos seguintes pilares:

- **Identificação de riscos e ameaças:** O primeiro passo consiste no mapeamento detalhado dos ativos informacionais críticos, das superfícies de ataque e das vulnerabilidades associadas. Essa análise abrange não apenas sistemas tecnológicos, mas também fluxos de informação, processos internos, fornecedores e terceiros que tenham acesso a dados sensíveis.
- **Classificação e avaliação de riscos:** Após a identificação, os riscos são analisados segundo dois eixos principais: probabilidade de ocorrência e impacto potencial. Esse impacto pode ser operacional, financeiro, reputacional ou regulatório, considerando as exigências da LGPD, do GDPR e das normas de segurança da informação aplicáveis.
- **Definição de controles proporcionais:** Com base na avaliação realizada, são implementadas medidas de mitigação adequadas à criticidade do risco. Essas medidas são estruturadas em três níveis:
    - **Prevenção:** Adoção de protocolos de controle de acesso, criptografia de dados sensíveis e segmentação de redes para restringir superfícies de ataque.
    - **Detecção:** Implementação de ferramentas de monitoramento contínuo, auditoria de logs e testes periódicos de vulnerabilidade para identificação de ameaças latentes.
    - **Resposta:** Definição de planos de resposta a incidentes, assegurando que violações ou falhas sejam rapidamente contidas e os impactos minimizados.

- **Monitoramento e reavaliação contínua:** A ABR não é um processo estático. Os riscos são monitorados e reavaliados à luz de novas ameaças emergentes, mudanças regulatórias e evolução tecnológica, garantindo que as estratégias de mitigação permaneçam eficazes e alinhadas às necessidades do projeto.

A integração da ABR à governança de segurança da informação e privacidade da Rodoanel BH S.A., assegura que todas as decisões e investimentos sejam fundamentados em critérios técnicos e análises de risco objetivas.

Esse modelo permite que a organização mantenha um equilíbrio entre proteção, conformidade regulatória e eficiência operacional, garantindo resiliência frente a ameaças e continuidade segura das operações.

4.4 Gestão de conformidade e accountability

A gestão de conformidade e accountability são princípios estruturantes na governança da segurança da informação e privacidade de dados da Rodoanel BH S.A.

Mais do que atender a exigências normativas, esses conceitos garantem que a organização possa demonstrar, de forma objetiva e rastreável, a aplicação das diretrizes de proteção de dados e segurança da informação.

A conformidade exige a implementação de um modelo sólido de governança, que assegure a aderência a regulamentos como LGPD, GDPR, ISO/IEC 27001 e ISO/IEC 27701.

No entanto, para que esse modelo seja eficaz, ele precisa ser sustentado pela accountability, que impõe à organização o dever de documentar suas práticas, atribuir responsabilidades de forma clara e garantir que as políticas estabelecidas sejam efetivamente aplicadas.

No contexto da segurança da informação e privacidade, accountability significa:

- **Comprovação da aderência às normativas aplicáveis**, não apenas por meio de políticas, mas pela execução concreta de controles de segurança e privacidade.
- **Manutenção de registros detalhados das operações de tratamento de dados pessoais e da aplicação de medidas de segurança**, assegurando rastreabilidade e transparência.
- **Definição clara de papéis e responsabilidades dentro da organização**, garantindo que cada área compreenda e execute suas atribuições na proteção da informação.

- **Supervisão contínua das práticas de segurança e privacidade**, por meio de auditorias, revisões e mecanismos formais de prestação de contas.

Para garantir a materialização desses princípios, a organização adota um modelo baseado em:

- **Políticas e normativos internos estruturados**, que estabelecem diretrizes e controles para proteção dos ativos informacionais.
- **Auditorias internas e monitoramento ativo**, permitindo a identificação e correção de desvios antes que resultem em impactos operacionais ou regulatórios.
- **Gestão de incidentes bem definida**, com protocolos de resposta que asseguram a mitigação de danos e o cumprimento de obrigações legais em caso de falha de segurança.
- **Capacitação de colaboradores e terceiros**, garantindo que a conformidade não seja apenas um requisito documental, mas um pilar da cultura organizacional.

A conformidade exige mais do que a formalização de diretrizes; ela depende de mecanismos que garantam sua aplicação consistente e verificável.

A accountability se manifesta na rastreabilidade das decisões, na solidez dos processos de auditoria e na documentação estruturada das ações implementadas, assegurando que a segurança da informação e a proteção de dados sejam geridas com transparência e precisão técnica.

5. GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

A governança da segurança da informação e da privacidade da Rodoanel BH S.A. é estruturada para garantir clareza na atribuição de responsabilidades, supervisão contínua das práticas de proteção de dados e segurança, resposta ágil a incidentes e conformidade com as normativas aplicáveis.

Esse modelo estabelece diretrizes para a atuação coordenada entre diferentes funções da organização, assegurando que as medidas de proteção sejam eficazes e alinhadas às exigências regulatórias.

5.1 Função de Compliance e Segurança da Informação

O Compliance Officer (CO) e o Gestor de Segurança da Informação e Gestão Integrada (SGI) desempenham papéis centrais na supervisão da proteção de dados e da segurança da informação.

Enquanto o CO assegura a conformidade regulatória e a governança dos processos de compliance, o SGI é responsável por implementar e gerenciar os controles técnicos e operacionais que garantem a segurança dos ativos informacionais.

As principais responsabilidades dessas funções são:

- **CO**
  - Garantir que a organização cumpra os requisitos da LGPD, GDPR e normas ISO aplicáveis.
  - Supervisionar a implementação de políticas e procedimentos internos de proteção de dados.
  - Definir diretrizes para avaliação de terceiros e due diligence em fornecedores com acesso a dados sensíveis.
  - Gerenciar treinamentos de compliance e conscientização sobre privacidade e segurança da informação.
- **SGI**
  - Implementar controles técnicos para proteção contra acessos indevidos, vazamento de informações e ataques cibernéticos.
  - Realizar testes de segurança, auditorias e análise de vulnerabilidades.
  - Coordenar a resposta a incidentes de segurança da informação, incluindo gestão de crises e mitigação de danos.
  - Monitorar a exposição da organização a ameaças digitais e fraudes.

5.2 Estrutura de Governança

A governança da segurança da informação e da privacidade segue uma estrutura bem definida, com papéis e responsabilidades alinhados às demais diretrizes da Rodoanel BH S.A.

A liderança e a supervisão são distribuídas entre diferentes níveis organizacionais, assegurando que a gestão de riscos, conformidade e segurança seja eficaz e integrada:

- **Alta Administração:** Define as diretrizes estratégicas, subsidia ao Conselho de Administração a aprovação de políticas e aloca recursos necessários para a segurança da informação e proteção de dados.
- **CO e SGI:** Supervisionam a implementação das diretrizes e coordenam ações de compliance e segurança, assegurando conformidade com normativas externas e internas.

- **Gestores das Áreas de Negócio:** Aplicam as diretrizes de segurança e privacidade em suas operações diárias, garantindo que os processos internos sejam aderentes às políticas estabelecidas.
- **Colaboradores e Terceiros:** Devem cumprir rigorosamente os procedimentos de segurança da informação e proteção de dados, reportando qualquer não conformidade ou incidente identificado.

Essa estrutura assegura que a governança da segurança da informação seja efetiva e operacionalizável, garantindo que responsabilidades estejam bem distribuídas e que as práticas de proteção sejam sustentáveis ao longo do tempo.

5.3 Gestão de Incidentes e Resposta a Vazamentos de Dados

A capacidade de resposta a incidentes é um fator crítico na governança da segurança da informação e privacidade.

A organização adota uma abordagem estruturada para identificação, contenção, mitigação e comunicação de falhas de segurança, assegurando que qualquer incidente seja tratado com máxima eficiência e conformidade regulatória.

A gestão de incidentes segue um ciclo estruturado, baseado nas melhores práticas da ISO/IEC 27035 (Gestão de Incidentes de Segurança da Informação) e nas diretrizes de resposta a vazamentos de dados da LGPD e GDPR.

Esse ciclo inclui:

1. **Detecção e Registro:** Qualquer anomalia ou suspeita de violação de segurança deve ser identificada e formalmente registrada nos canais apropriados.
2. **Avaliação do Impacto:** O incidente é classificado com base em seu potencial de dano operacional, regulatório e reputacional.
3. **Resposta e Contenção:** São acionadas medidas para mitigar o impacto imediato do incidente e impedir sua propagação.
4. **Investigação e Identificação da Causa:** Técnicas forenses e auditorias internas são empregadas para determinar a origem da falha e estabelecer medidas corretivas.
5. **Comunicação e Notificação:** Em caso de vazamento de dados pessoais, são adotados os procedimentos de comunicação obrigatória às autoridades reguladoras e aos titulares dos dados, conforme exigido pela LGPD e GDPR.

6. **Revisão e Aprimoramento:** Após a resolução do incidente, são analisadas falhas no processo, e as lições aprendidas são aplicadas para fortalecer os controles preventivos.

Esse modelo garante que a organização não apenas reaja a incidentes, mas aprimore continuamente seus processos, reduzindo a probabilidade de novas ocorrências e assegurando conformidade com normativas de reporte obrigatório.

5.4 Auditorias e Monitoramento

O monitoramento e a auditoria são elementos essenciais da governança da segurança da informação, permitindo que a organização avalie a efetividade de seus controles, detecte vulnerabilidades e corrija falhas antes que resultem em incidentes críticos.

As auditorias são conduzidas de acordo com um cronograma formal, incluindo:

- **Auditorias internas**, realizadas pelo time de SGI para avaliar a aderência dos processos às normas e políticas internas.
- **Testes de invasão (pentests) e análises de vulnerabilidade**, conduzidos para identificar falhas exploráveis por agentes externos.
- **Monitoramento de logs e eventos de segurança**, utilizando ferramentas especializadas para análise de comportamento suspeito e anomalias.
- **Revisões independentes e auditorias externas**, assegurando conformidade com requisitos regulatórios e boas práticas internacionais.

O monitoramento é complementado por indicadores de desempenho e relatórios gerenciais, permitindo que a alta administração tenha visibilidade sobre riscos emergentes e eficácia dos controles implementados.

A governança da segurança da informação e privacidade da Rodoanel BH S.A depende de um modelo de auditoria e monitoramento que seja rígido o suficiente para garantir conformidade e adaptável o bastante para acompanhar a evolução das ameaças e das exigências regulatórias.

6. GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO

A gestão de riscos em segurança da informação da Rodoanel BH S.A. segue um modelo estruturado que permite a identificação, análise, tratamento e monitoramento das

ameaças que possam comprometer a confidencialidade, integridade e disponibilidade dos ativos informacionais.

O objetivo é garantir que os controles implementados sejam proporcionais à criticidade dos dados protegidos e à exposição a ameaças, assegurando conformidade com a LGPD, GDPR e as normas ISO aplicáveis.

A abordagem adotada está integrada à matriz de riscos do projeto, garantindo alinhamento entre segurança da informação e governança corporativa, além de permitir que riscos cibernéticos sejam tratados no mesmo nível de rigor dos riscos operacionais e estratégicos.

6.1 Identificação e Classificação de Riscos

A identificação de riscos na segurança da informação é um processo contínuo e estruturado, baseado na avaliação das vulnerabilidades, ameaças e impactos potenciais sobre os ativos informacionais da empresa.

A organização adota um modelo de varredura sistemática, que considera tanto fatores internos quanto externos, assegurando que os riscos sejam analisados com abrangência e precisão.

O processo de identificação pressupõe a análise dos seguintes elementos:

- **Ativos Informacionais:** Sistemas, bancos de dados, infraestrutura de TI, dispositivos móveis e fluxos de informação que sustentam as operações da empresa.
- **Ameaças Cibernéticas:** Ataques de malware, ransomware, phishing, engenharia social, exploração de vulnerabilidades, vazamento de dados e tentativas de intrusão.
- **Ameaças Internas:** Exposição não intencional de informações, falhas humanas, negligência na aplicação de controles e acessos indevidos.
- **Fatores Externos:** Fornecedores, prestadores de serviços e terceiros que manipulam ou armazenam dados críticos, podendo representar vetores de risco para a organização.
- **Exposição Regulatória:** Penalidades, sanções e impactos reputacionais decorrentes da não conformidade com normas como LGPD, GDPR e ISO/IEC 27001.

Após a identificação, cada risco é classificado com base em sua probabilidade e impacto, seguindo critérios estabelecidos na matriz de riscos da Rodoanel BH S.A. Essa classificação considera:

- **Gravidade do impacto:** Consequências operacionais, financeiras, regulatórias e reputacionais decorrentes da materialização do risco.
- **Probabilidade de ocorrência:** Frequência e previsibilidade do risco com base em histórico de incidentes e análise de tendências.
- **Capacidade de mitigação:** Avaliação dos controles já existentes e da necessidade de reforço ou aprimoramento.

Os riscos são categorizados em:

- **Baixo Risco:** Eventos com impacto reduzido e alta capacidade de mitigação por meio de controles já implementados.
- **Médio Risco:** Situações que exigem monitoramento ativo, podendo necessitar de reforço em controles para evitar falhas sistêmicas.
- **Alto Risco:** Ameaças críticas que podem comprometer a segurança da empresa, exigindo medidas imediatas e contínua reavaliação da eficácia dos controles.

A identificação e classificação de riscos são parte de um ciclo contínuo de monitoramento e aprimoramento da segurança da informação. A organização revisa periodicamente seus riscos e ajusta seus controles para garantir resiliência e adaptação a novas ameaças.

6.2 Controles Preventivos e Detecção

A segurança da informação da Rodoanel BH S.A. exige a implementação de controles preventivos eficazes, que garantam a proteção de documentos técnicos, contratos, dados estratégicos e informações sensíveis de fornecedores e parceiros. Como se trata de um ambiente de engenharia e infraestrutura, os riscos estão mais associados ao acesso não autorizado a informações críticas, vazamentos de dados e falhas na governança documental, em vez de ameaças cibernéticas avançadas.

Os controles preventivos adotados incluem:

- **Gestão de Acessos a Documentos e Dados Sensíveis**: Implementação de perfis de acesso restrito, garantindo que apenas pessoas autorizadas possam manipular documentos estratégicos, contratos e informações financeiras do projeto. Essa medida reduz riscos associados a vazamentos de dados e uso indevido de informações sigilosas.
- **Proteção da Informação em Mídias Físicas e Digitais:** Como o ambiente de obras envolve o manuseio frequente de projetos técnicos, plantas, relatórios de fiscalização e outros documentos críticos, são adotados protocolos de armazenamento seguro, controle de cópias físicas e uso de marcas d'água em arquivos digitais confidenciais para rastrear a origem de informações sensíveis.
- **Segurança na Troca de Informações com Fornecedores e Órgãos Reguladores:** A comunicação de dados contratuais, orçamentários e operacionais entre as partes envolvidas no projeto segue protocolos de transparência e confidencialidade, reduzindo riscos de compartilhamento indevido de informações estratégicas.
- **Política de Uso de Dispositivos e Armazenamento Removível:** Para evitar o extravio ou a cópia indevida de informações, há regras claras sobre o uso de dispositivos USB, armazenamento em nuvem e transferência de arquivos para dispositivos pessoais, garantindo que a integridade dos dados do projeto seja preservada.
- **Gestão de Acessos Físicos aos Locais Sensíveis:** Como a fase de execução da obra envolverá instalações críticas, há um controle rigoroso de entrada e circulação em áreas restritas, evitando acessos indevidos que possam comprometer a segurança da informação e a integridade do projeto.

Além dos controles preventivos, a organização adota mecanismos de detecção que permitem identificar falhas de segurança, acessos não autorizados e eventuais tentativas de vazamento de informações:

- **Registro e Monitoramento de Acessos:** Todos os acessos a sistemas internos e arquivos digitais críticos são registrados, permitindo a auditoria de ações realizadas por colaboradores e terceiros.
- **Monitoramento de Conformidade Contratual e Regulamentar:** Há um acompanhamento contínuo do cumprimento das normas de segurança da informação e privacidade de dados, garantindo que fornecedores e parceiros respeitem as diretrizes estabelecidas.

- **Auditorias de Segurança Documental:** Avaliam o correto armazenamento e compartilhamento de informações, identificando possíveis fragilidades na proteção de dados sensíveis.

A Rodoanel BH S.A. opera com sistemas digitalizados e lida com dados estratégicos e documentos técnicos que exigem proteção adequada.

Nesse sentido, os controles preventivos e mecanismos de detecção adotados devem salvaguardar essas informações, minimizando riscos operacionais e regulatórios, além de assegurar conformidade com exigências contratuais e normativas aplicáveis.

6.3 Plano de Resposta a Incidentes

A resposta a incidentes na segurança da informação e privacidade de dados da Rodoanel BH S.A. segue um conjunto estruturado de diretrizes para garantir a detecção, contenção, remediação e comunicação de falhas de segurança, minimizando impactos operacionais, contratuais e regulatórios.

Esse plano estabelece um fluxo padronizado de tratamento de incidentes, assegurando que as informações críticas da empresa permaneçam protegidas e que qualquer irregularidade seja tratada de forma célere e eficaz.

O processo de resposta a incidentes segue as seguintes etapas:

1. **Identificação e Registro do Incidente**
   - Todos os eventos suspeitos devem ser identificados e registrados formalmente, incluindo vazamento de documentos técnicos, acessos indevidos, extravio de informações sigilosas ou falhas em processos de segurança.
   - O registro do incidente deve conter data e hora do ocorrido, descrição detalhada do evento, possíveis impactos e ações imediatas adotadas.
2. **Classificação do Incidente**
   - Cada ocorrência deve ser classificada com base na gravidade e no impacto, permitindo priorizar a resposta e alocar os recursos necessários.
   - A classificação segue os seguintes critérios:
     - **Crítico:** Eventos com potencial de comprometer dados estratégicos, exigindo ação imediata e notificação à alta administração.

- **Alto:** Incidentes com impacto significativo, mas controlável com medidas corretivas rápidas.
- **Médio:** Ocorrências que não representam ameaça imediata, mas requerem ajustes para evitar reincidência.
- **Baixo:** Eventos menores que podem ser corrigidos com ações simples, sem impacto relevante.

3. **Ação de Contenção e Mitigação**
   - Medidas emergenciais devem ser adotadas para impedir a propagação do problema e mitigar impactos.
   - Ações podem incluir revogação de acessos indevidos, restrição temporária a documentos críticos, isolamento de informações comprometidas e reforço nos controles internos.
4. **Investigação e Identificação da Causa Raiz**
   - A equipe responsável deve conduzir uma análise detalhada para identificar a origem da falha e os fatores que contribuíram para sua ocorrência.
   - Se necessário, auditorias internas e entrevistas com os envolvidos serão realizadas para determinar a extensão do incidente.
5. **Comunicação e Notificação**
   - Se houver exposição de dados sigilosos, documentos técnicos estratégicos ou informações protegidas, será avaliada a necessidade de reporte formal às partes afetadas e, se aplicável, às autoridades competentes.
   - Nos casos em que a LGPD ou o GDPR exijam notificação, a comunicação será feita conforme os requisitos regulatórios.
6. **Correção e Aprimoramento dos Controles**
   - Com base na investigação, serão implementadas medidas corretivas e preventivas para evitar reincidência do incidente.
   - Podem ser aplicadas revisões de processos, reforço nos controles de acesso e atualização de diretrizes internas.
7. **Revisão e Melhoria**
   - Todos os incidentes serão revisados para identificação de padrões de risco e fragilidades estruturais.
   - A equipe de governança conduzirá simulações e treinamentos para aprimorar a resposta a incidentes futuros.

A aplicação dessas diretrizes tem o condão de tratar de forma rápida, eficaz e alinhada às melhores práticas internacionais, garantindo a proteção da Rodoanel BH S.A. contra riscos operacionais e regulatórios.

6.4 Acompanhamento de Medidas Corretivas e Melhorias

A gestão da segurança da informação e privacidade de dados da Rodoanel BH S.A. exige um processo estruturado de supervisão e aperfeiçoamento, garantindo que vulnerabilidades sejam corrigidas de forma eficaz e que os controles existentes sejam ajustados para acompanhar mudanças no ambiente regulatório e operacional.

Esse acompanhamento é essencial para evitar recorrências de falhas e para assegurar que as medidas adotadas tenham impacto mensurável na redução de riscos.

Sempre que uma não conformidade ou fragilidade nos controles for identificada, a organização formaliza um plano de ação, que deve contemplar:

- **Descrição do problema identificado**, detalhando a falha e seus potenciais impactos.
- **Medidas corretivas a serem implementadas**, especificando prazos e responsáveis.
- **Critérios de validação**, assegurando que a solução adotada seja testada e devidamente incorporada aos processos.

Além da correção de falhas pontuais, a revisão das práticas de segurança é essencial para garantir que os controles permaneçam eficazes frente à evolução dos riscos. Para isso, a Rodoanel BH S.A. realiza:

- **Avaliações regulares dos processos de segurança e privacidade**, verificando a aderência às diretrizes e a necessidade de ajustes.
- **Monitoramento de ameaças emergentes**, permitindo que novas vulnerabilidades sejam identificadas e mitigadas antes que resultem em incidentes.
- **Engajamento de stakeholders internos e externos**, reforçando a cultura de conformidade e prevenindo falhas decorrentes de comportamento humano ou processos obsoletos.

A efetividade das medidas corretivas e dos aprimoramentos implementados é avaliada com base em indicadores de desempenho, permitindo que eventuais ajustes sejam feitos conforme necessário.

Esse monitoramento possibilita a identificação de pontos de melhoria, assegurando que a governança da segurança da informação e privacidade da Rodoanel BH S.A. evolua de maneira consistente e alinhada às exigências operacionais e regulatórias.

7. PROTEÇÃO DE DADOS PESSOAIS

A proteção de dados pessoais da Rodoanel BH S.A. segue um modelo escalonado, adequado às diferentes fases do projeto. A abordagem considera os requisitos regulatórios aplicáveis (LGPD e GDPR), a criticidade das informações tratadas em cada etapa e os controles necessários para mitigar riscos relacionados ao uso, armazenamento e compartilhamento de dados pessoais.

7.1 Tratamento de Dados e Escalonamento da Proteção

O tratamento de dados pessoais acompanha a evolução , exigindo diferentes níveis de controle e governança ao longo das fases de mobilização, execução e operação. O escalonamento da proteção garante que as medidas adotadas sejam proporcionais ao volume de dados tratados e ao risco associado a cada etapa, evitando exposição desnecessária e assegurando conformidade regulatória desde o início das atividades.

Mobilização e Planejamento

Na fase inicial, o tratamento de dados está concentrado em cadastros de colaboradores, fornecedores e parceiros comerciais, além da estruturação de contratos e obrigações regulatórias.

Constituem as principais diretrizes para esta etapa:

- **Coleta mínima de dados pessoais**, restringindo-se àqueles estritamente necessários para os processos administrativos e regulatórios.
- **Definição de bases legais para o tratamento**, assegurando que cada operação esteja fundamentada em um critério legítimo conforme a LGPD e o GDPR.
- **Criação de protocolos de governança documental**, garantindo que informações sensíveis sejam armazenadas de forma segura e acessadas apenas por pessoas autorizadas.

Execução da Obra

Durante a execução do projeto, o volume de dados tratados se expande, abrangendo informações sobre a força de trabalho, controle de acesso a áreas restritas, registros operacionais e comunicação com órgãos reguladores.

A proteção de dados nessa fase requer controles adicionais, tais como:

- **Monitoramento da conformidade de fornecedores e terceiros**, assegurando que todas as partes envolvidas cumpram as diretrizes de proteção de dados.
- **Regras específicas para compartilhamento de informações**, prevenindo o uso indevido ou o vazamento de dados estratégicos.
- **Criação de mecanismos de anonimização ou pseudonimização**, reduzindo a exposição de dados pessoais em relatórios operacionais e sistemas de monitoramento.

Operação e Manutenção

Na fase final, o foco da proteção de dados está na **gestão do histórico do projeto, no arquivamento seguro das informações e na definição de políticas de retenção e descarte**, devendo ser observadas as seguintes diretrizes:

- **Implementação de prazos de retenção claros**, assegurando que dados sejam armazenados apenas pelo tempo necessário e eliminados de forma segura ao término do período definido.
- **Monitoramento da governança de dados**, garantindo que os controles implementados permaneçam eficazes durante toda a vida útil do projeto.
- **Auditorias** para avaliar riscos remanescentes e evitar armazenamento desnecessário de informações pessoais.

A aplicação dessa abordagem escalonada viabiliza que a proteção de dados pessoais no da Rodoanel BH S.A. seja progressiva e adaptável, de modo que os controles acompanhem a evolução das operações e que a conformidade regulatória seja mantida em todas as fases.

7.2 Bases Legais para o Tratamento

O tratamento de dados pessoais da Rodoanel BH S.A. está fundamentado nos princípios e exigências da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) e do Regulamento Geral de Proteção de Dados da União Europeia (GDPR).

Dessa forma, todas as operações envolvendo informações pessoais são realizadas com respaldo jurídico adequado e em conformidade com as diretrizes de privacidade e segurança.

A definição da base legal apropriada para cada tratamento é essencial para assegurar a legitimidade das operações e a proteção dos direitos dos titulares dos dados. Conforme previsto na LGPD (Art. 7º) e no GDPR (Art. 6º), o tratamento de dados pessoais deve estar vinculado a pelo menos uma das hipóteses legais previstas na legislação aplicável.

Bases Legais Aplicáveis às Diferentes Fases do Projeto

Como o projeto possui diferentes fases operacionais, as bases legais utilizadas para o tratamento de dados pessoais variam conforme a necessidade e o tipo de informação envolvida.

Mobilização e Planejamento

Na fase inicial do projeto, o tratamento de dados pessoais está principalmente vinculado a processos administrativos, contratuais e regulatórios.

As principais bases legais utilizadas são:

- **Execução de contrato ou procedimentos preliminares relacionados a contrato (LGPD, Art. 7º, V / GDPR, Art. 6º, b)** – Aplicável à coleta de dados de fornecedores, prestadores de serviço e colaboradores envolvidos na estruturação do projeto.

- **Cumprimento de obrigação legal ou regulatória (LGPD, Art. 7º, II / GDPR, Art. 6º, c)** – Fundamenta o tratamento de informações pessoais exigidas por órgãos reguladores e fiscais, como cadastros obrigatórios e controle trabalhista.

Execução da Obra

Durante a fase de execução, há um aumento no volume e na diversidade dos dados pessoais tratados, incluindo informações de colaboradores, terceiros e prestadores de serviço que atuam diretamente nas operações do projeto.

Nessa fase, as bases legais predominantes são:

- **Legítimo interesse (LGPD, Art. 7º, IX / GDPR, Art. 6º, f)** – Aplicável a processos internos de segurança, como controle de acesso a áreas restritas e monitoramento para prevenção de riscos operacionais.
- **Proteção da vida ou da incolumidade física do titular ou de terceiro (LGPD, Art. 7º, VII / GDPR, Art. 6º, d)** – Justifica o tratamento de informações para garantir a segurança dos trabalhadores no canteiro de obras, incluindo registros de emergência e comunicação de incidentes.

Operação e Manutenção

Na fase de operação e manutenção do empreendimento, o foco passa a ser a preservação do histórico do projeto, a retenção de documentos essenciais e o descarte seguro de informações desnecessárias.

As bases legais aplicáveis são:

- **Cumprimento de obrigação legal ou regulatória (LGPD, Art. 7º, II / GDPR, Art. 6º, c)** – Fundamenta o armazenamento de registros exigidos por leis fiscais, ambientais e trabalhistas.
- **Execução de contrato (LGPD, Art. 7º, V / GDPR, Art. 6º, b)** – Justifica a retenção de dados de fornecedores e parceiros contratados durante a operação do empreendimento.

Além disso, o tratamento de dados sensíveis, como informações médicas de trabalhadores, segue regras mais restritivas, sendo permitido apenas em hipóteses específicas previstas na LGPD (Art. 11) e no GDPR (Art. 9), como cumprimento de obrigações legais trabalhistas e garantia da segurança do ambiente de trabalho.

A definição das bases legais da Rodoanel BH S.A. orienta o tratamento de dados pessoais dentro dos requisitos regulatórios, reduzindo riscos jurídicos e promovendo transparência na gestão das informações ao longo de todas as suas fases.

7.3 Direitos dos Titulares de Dados e Canais de Atendimento

A Rodoanel BH S.A. adota diretrizes para garantir que os direitos dos titulares de dados sejam respeitados em todas as operações que envolvam o tratamento de informações pessoais.

Em conformidade com a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados (GDPR), os titulares têm o direito de acessar, corrigir, restringir, excluir e, quando aplicável, portar seus dados pessoais.

Direitos dos Titulares de Dados

Os titulares de dados podem exercer os seguintes direitos, conforme previsto na LGPD (Art. 18) e no GDPR (Arts. 12 a 22):

- **Confirmação da existência de tratamento:** Solicitar informações sobre a existência ou não de tratamento de seus dados pessoais.
- **Acesso aos dados:** Obter uma cópia das informações pessoais mantidas pela organização.
- **Correção de dados incompletos, inexatos ou desatualizados:** Requerer a retificação de informações incorretas ou desatualizadas.
- **Anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos:** Solicitar que dados sejam tratados de forma anônima, bloqueados ou excluídos, quando não houver justificativa legal para seu armazenamento.
- **Portabilidade dos dados:** Quando aplicável, requerer a transferência de seus dados para outra organização, em formato estruturado e interoperável.
- **Eliminação dos dados tratados com base no consentimento:** Nos casos em que o tratamento tenha ocorrido com base no consentimento, solicitar a exclusão dos dados.
- **Informação sobre o compartilhamento de dados:** Perguntar com quais terceiros seus dados foram compartilhados.
- **Revogação do consentimento:** Caso o tratamento tenha sido baseado no consentimento, o titular pode revogá-lo a qualquer momento, sem impacto sobre tratamentos anteriores realizados sob essa base legal.

Canais de Atendimento

Para garantir o exercício desses direitos, a Rodoanel BH S.A. disponibiliza canais específicos para o atendimento de solicitações relacionadas à privacidade e proteção de dados.

O contato pode ser feito por meio de:

- **E-mail**, destinado a esclarecimentos sobre o tratamento de dados e envio de solicitações formais.
- **Contato telefônico**, para suporte e orientações sobre os direitos previstos na legislação.

Todos os pedidos recebidos serão analisados e respondidos nos prazos estabelecidos pelas normativas aplicáveis.

Conforme o Art. 19 da LGPD, a organização tem o prazo máximo de 15 dias para fornecer uma resposta ao titular de dados. No caso do GDPR (Art. 12, §3º), o prazo é de até um mês, podendo ser estendido por mais dois meses em situações complexas, desde que o titular seja devidamente informado sobre a necessidade da prorrogação.

As solicitações devem ser registradas nos sistemas internos da Rodoanel BH S.A. , com indicação do tipo de pedido, data de recebimento, medidas adotadas e prazo de resposta, assegurando rastreabilidade e conformidade com os requisitos regulatórios. Nos casos em que houver necessidade de validação da identidade do titular, o requerente será informado sobre os documentos ou procedimentos adicionais necessários para dar seguimento à solicitação.

7.4 Retenção, Armazenamento e Descarte Seguro

A retenção, o armazenamento e o descarte de dados pessoais na Rodoanel BH S.A. seguem critérios rigorosos para garantir conformidade regulatória, segurança da informação e mitigação de riscos associados ao uso prolongado ou inadequado de informações sensíveis.

Esses processos estão alinhados à Lei Geral de Proteção de Dados (LGPD, Art. 15), ao Regulamento Geral de Proteção de Dados (GDPR, Art. 5, I, e) e às melhores práticas estabelecidas na ISO/IEC 27001, garantindo que os dados sejam mantidos apenas pelo período necessário e eliminados de forma segura quando atingirem o fim de seu ciclo de vida.

Retenção de Dados

A retenção de dados pessoais é definida com base na finalidade do tratamento, na obrigação legal ou regulatória aplicável e na necessidade operacional da empresa. O armazenamento excessivo ou injustificado de informações pessoais é expressamente vedado.

Os prazos de retenção seguem três categorias principais:

- **Dados administrativos e contratuais:** Informações relacionadas a fornecedores, parceiros e prestadores de serviço são mantidas pelo prazo necessário para cumprimento contratual e obrigações legais, incluindo auditorias e prestações de contas.
- **Dados de trabalhadores e terceiros:** Registros vinculados à força de trabalho do projeto seguem as determinações da legislação trabalhista e previdenciária, sendo preservados pelo período exigido por lei.
- **Dados de acesso e monitoramento:** Informações obtidas por meio de controles de segurança, como registros de entrada em áreas restritas, são armazenadas pelo período estritamente necessário para a finalidade definida, respeitando os limites legais e de proporcionalidade.

Nos casos em que a retenção se baseia em obrigações legais específicas, os prazos aplicáveis são:

- 5 anos para documentos fiscais e contábeis, conforme Código Tributário Nacional (CTN, Art. 173, I).
- 20 anos para registros previdenciários, conforme Lei nº 8.212/1991.
- 10 anos para documentos relacionados a obrigações cíveis e comerciais, conforme Código Civil Brasileiro (Art. 205).
- Até 2 anos após o encerramento da relação contratual para documentos trabalhistas não sujeitos à retenção obrigatória de longo prazo, considerando o prazo prescricional para ações trabalhistas individuais, conforme CLT (Art. 11).
- Demais prazos definidos por contratos firmados com fornecedores, prestadores de serviços e órgãos reguladores.

Findo o período de retenção, os dados devem ser eliminados, salvo se houver justificativa expressa para manutenção, como interesse legítimo documentado ou exigência regulatória excepcional.

Armazenamento de Dados

Os dados pessoais são armazenados de forma segura, garantindo proteção contra acesso não autorizado, perda, alteração indevida e vazamentos.

O armazenamento pode ocorrer em formatos físicos ou digitais, com aplicação de controles adequados a cada meio:

- **Documentos físicos:** Mantidos em locais de acesso restrito, com controle de entrada e saída, evitando extravios ou manipulação indevida.
- **Arquivos digitais:** Armazenados em repositórios com controle de acesso baseado em perfil de usuário, criptografia de informações sensíveis e mecanismos de rastreabilidade para monitoramento de atividades.
- **Backup e recuperação de dados:** Procedimentos estruturados garantem que informações essenciais possam ser restauradas em caso de falha, respeitando os princípios de segurança e disponibilidade.

O acesso a dados armazenados é controlado por um modelo de permissões baseado em necessidade operacional, assegurando que apenas usuários autorizados possam consultá-los.

Qualquer compartilhamento ou transferência de informações segue protocolos formais de governança, garantindo transparência e conformidade com as exigências legais.

Descarte Seguro de Dados

O descarte de dados pessoais deve ocorrer de maneira definitiva e irreversível, garantindo que as informações não possam ser recuperadas ou reutilizadas.

Os métodos de eliminação variam conforme o suporte utilizado:

- **Documentos físicos:** Devem ser fragmentados ou triturados antes do descarte, impedindo a reconstituição de informações sensíveis.
- **Registros digitais:** Devem ser eliminados por meio de sobrescrita segura ou remoção definitiva dos bancos de dados, com registro formal do procedimento realizado.

- **Dados armazenados em backup:** Devem ser excluídos ao final do período de retenção correspondente, evitando a persistência de informações sem necessidade operacional.

O descarte de qualquer dado deve ser documentado por meio de registros formais que indiquem a data da eliminação, o tipo de informação descartada e o método utilizado, garantindo rastreabilidade e controle sobre a efetiva aplicação das regras de retenção. Esse acompanhamento possibilita a verificação do cumprimento dos prazos estabelecidos, prevenindo tanto a eliminação prematura de informações necessárias quanto a retenção indevida de dados sem justificativa legal ou operacional.

Além da documentação do descarte, a eficácia dos procedimentos de eliminação deve ser avaliada periodicamente, assegurando que os métodos empregados sejam compatíveis com a sensibilidade das informações envolvidas e que a organização mantenha um controle rigoroso sobre a destinação final dos dados.

8. REGRAS PARA FORNECEDORES, PARCEIROS E TERCEIROS

A Rodoanel BH S.A. estabelece diretrizes rigorosas para a seleção, contratação e monitoramento de fornecedores, parceiros e terceiros, assegurando conformidade com as normas de segurança da informação e proteção de dados.

Essas regras estão alinhadas ao Procedimento de Avaliação e Monitoramento de Terceiros da empresa, garantindo que os riscos associados ao relacionamento com terceiros sejam devidamente identificados, mitigados e monitorados ao longo da execução do projeto.

8.1 Due Diligence de Terceiros e Segurança da Informação

Antes da formalização de qualquer contrato, os terceiros devem passar por um processo de due diligence, conduzido em conjunto pelo Compliance Officer (CO) e pelo Gestor de Suprimentos e Contratos (GCP).

Esse processo avalia a conformidade legal, reputacional e operacional do terceiro, incluindo aspectos relacionados à segurança da informação.

A due diligence segue as seguintes diretrizes:

- **Avaliação inicial**: Antes da contratação, deve ser realizada uma análise detalhada do terceiro, considerando regularidade fiscal e trabalhista, participação em litígios, histórico reputacional e conformidade com exigências ambientais e regulatórias.
- **Classificação de risco**: Com base nos achados da due diligence, os terceiros são classificados em baixo, médio ou alto risco, conforme seu histórico de conformidade e eventuais alertas identificados.
- **Monitoramento contínuo**: Fornecedores classificados como médio ou alto risco estão sujeitos a avaliações periódicas, auditorias e monitoramento de sua conformidade ao longo do contrato.

O processo de due diligence inclui a exigência de documentação comprobatória, como certidões negativas, relatórios financeiros e registros de conformidade regulatória, garantindo que o terceiro cumpra os padrões exigidos pelo projeto.

8.2 Cláusulas Contratuais de Proteção de Dados

Todos os contratos firmados com terceiros devem conter cláusulas específicas de proteção de dados pessoais e segurança da informação, assegurando que os parceiros comerciais cumpram os requisitos da LGPD e do GDPR.

Essas cláusulas devem prever:

- **Obrigação de confidencialidade**, proibindo o compartilhamento ou uso indevido de informações recebidas no âmbito do contrato.
- **Definição clara das responsabilidades do terceiro quanto ao tratamento de dados pessoais**, incluindo os limites para coleta, armazenamento e eliminação das informações.
- **Direito de auditoria**, permitindo que a Rodoanel BH S.A. verifique o cumprimento das obrigações contratuais relacionadas à proteção de dados.
- **Requisitos para reporte de incidentes**, obrigando o terceiro a notificar imediatamente qualquer violação de segurança que envolva informações do projeto.

Além disso, fornecedores que tenham acesso direto a dados pessoais ou sistemas da organização devem assinar um Termo de Responsabilidade, reforçando o compromisso com as diretrizes estabelecidas desta Política.

8.3 Requisitos de Segurança e Confidencialidade nos Contratos

A segurança da informação e a proteção da confidencialidade devem ser garantidas em todas as fases da relação com terceiros.

Para isso, os contratos devem conter regras específicas para mitigação de riscos, incluindo:

- **Segregação de funções**, evitando que um único fornecedor tenha acesso irrestrito a informações estratégicas da empresa.
- **Restrições ao armazenamento e transferência de dados**, impedindo a cópia não autorizada ou o uso de informações fora do ambiente controlado pela empresa.
- **Exigência de medidas técnicas de segurança**, como criptografia, controle de acessos e logs de atividades, quando aplicável.
- **Previsão de sanções e rescisão contratual**, em caso de descumprimento das obrigações de segurança e confidencialidade.

O Compliance Officer (CO) e o Gestor de Suprimentos e Contratos (GCP) são responsáveis por monitorar a implementação das cláusulas contratuais, garantindo que terceiros classificados como médio ou alto risco sejam submetidos a auditorias regulares e que os controles de segurança sejam efetivamente aplicados.

O Gestor pelo Tratamento de Dados Pessoais (GPO), por sua vez, exerce uma função de supervisão independente, verificando se as obrigações contratuais relacionadas à proteção de dados estão adequadas à LGPD e GDPR e avaliando a conformidade dos fornecedores no que se refere ao tratamento de informações pessoais.

O GPO não executa a due diligence diretamente, mas acompanha sua aplicação em relação a riscos de privacidade e pode intervir para exigir ajustes contratuais, recomendar medidas adicionais de mitigação ou alertar a alta administração sobre falhas nos controles de terceiros que possam comprometer a segurança e a conformidade regulatória.

9. CONTROLES TÉCNICOS E ADMINISTRATIVOS

No Projeto Rodoanel BH, os controles técnicos e administrativos são voltados à garantia da segurança física e documental de informações sensíveis, como documentos técnicos, contratos e dados de fornecedores.

Esses controles têm como objetivo proteger informações críticas contra acessos não autorizados, vazamentos e falhas na governança documental, respeitando as exigências regulatórias de segurança e privacidade.

9.1 Controle de Acessos e Identificação

O controle de acessos na Rodoanel BH S.A. é essencial para garantir que apenas pessoas autorizadas possam acessar informações críticas, como documentos técnicos, contratos e dados financeiros. O princípio do menor privilégio é adotado, assegurando que cada colaborador ou parceiro tenha acesso apenas às informações necessárias para suas funções.

Em termos de controle físico, a entrada e circulação em áreas sensíveis, como salas de documentos e arquivos, é controlada por procedimentos administrativos, com registro das pessoas autorizadas a acessar essas áreas. O uso de armários e arquivos fechados garante a proteção de documentos e a segurança das informações, com acesso restrito a documentos críticos, de acordo com as responsabilidades e funções de cada pessoa envolvida no projeto.

9.2 Criptografia e Proteção de Informações Sensíveis

A proteção de documentos digitais sensíveis é importante e, portanto, executada.

Para contratos, relatórios financeiros, projetos e documentos técnicos, são aplicados protocolos de segurança, como marcas d'água em arquivos digitais para rastrear sua origem, e restrição de edição e cópia para documentos eletrônicos.

Além disso, documentos críticos em formato físico são armazenados de maneira segura em arquivos fechados, com acesso restrito a funcionários e parceiros específicos, e documentos sigilosos são arquivados de acordo com políticas de segurança documental para impedir acessos indevidos.

9.3 Gestão de Vulnerabilidades e Testes de Segurança

A gestão de vulnerabilidades no contexto da Rodoanel BH S.A. não se limita a sistemas digitais, mas também envolve a avaliação da segurança física e a proteção de documentos físicos e dados sensíveis. Isso inclui inspeções nos processos de armazenamento, manuseio e compartilhamento de documentos críticos, para identificar possíveis falhas ou riscos de segurança, como acessos não autorizados ou extravio de informações confidenciais.

Testes de segurança não digitais, como a auditoria de controle de acesso físico e a avaliação dos protocolos de manuseio de documentos, são realizados. Esses testes

garantem que as medidas preventivas sejam eficazes e que qualquer vulnerabilidade seja corrigida de forma rápida, minimizando riscos operacionais e protegendo a integridade dos dados.

9.4 Backup e Recuperação de Dados

No contexto da Rodoanel BH S.A., o backup e a recuperação de dados referem-se não apenas a sistemas digitais, mas também à preservação de documentos físicos críticos.

Para documentos eletrônicos sensíveis, como contratos e relatórios financeiros, é garantido o backup em locais seguros, com controle de versões e armazéns protegidos.

Além disso, cópias digitais de documentos essenciais são armazenadas de forma segura, com restrições de acesso e criptografia, se necessário.

No caso de documentos físicos, é realizado um controle rigoroso de cópias, onde as cópias originais e de backup são armazenadas separadamente, protegendo as informações contra danos, perda ou deterioração.

Quando necessário, a recuperação de dados e documentos ocorre de forma ágil, com processos definidos para garantir que, em caso de extravio ou falha, a integridade e disponibilidade dos dados essenciais sejam restabelecidas rapidamente, de acordo com as prioridades do projeto.

10. TREINAMENTO, CONSCIENTIZAÇÃO E COMUNICAÇÃO

Na Rodoanel BH S.A., a conscientização e capacitação sobre segurança da informação e privacidade de dados são essenciais para garantir que todos os envolvidos compreendam suas responsabilidades e os riscos associados ao manuseio de informações sensíveis.

A formação e engajamento de colaboradores, fornecedores e parceiros são fundamentais para fortalecer a cultura de segurança e garantir a proteção dos dados em todas as fases do projeto.

Treinamento periódico sobre segurança e privacidade

Todos os colaboradores e parceiros são submetidos a treinamentos sobre segurança da informação, proteção de dados pessoais e boas práticas no manuseio de documentos e informações sensíveis.

Esses treinamentos abrangem tópicos como segurança física, controle de acesso, proteção contra vazamento de dados e conformidade regulatória (LGPD, GDPR), garantindo que todos compreendam a importância da proteção de dados e a necessidade de seguir as normas estabelecidas.

O objetivo é reduzir riscos de falhas de segurança causadas por desinformação ou falta de conscientização.

Divulgação da política e boas práticas

A Política de Segurança da Informação e Privacidade de Dados é amplamente divulgada para todos os colaboradores, fornecedores e parceiros da Rodoanel BH S.A., assegurando que todos compreendam seus direitos e responsabilidades no tratamento de dados.

Essa divulgação é feita por meio de canais internos, como e-mails corporativos, murais informativos e reuniões de alinhamento, garantindo que a política seja acessível e entendida por todos.

Além disso, boas práticas de segurança e procedimentos para proteger documentos e dados pessoais são compartilhados regularmente para reforçar a necessidade de adesão contínua à política.

Sensibilização sobre phishing, engenharia social e outras ameaças

A sensibilização contínua sobre ameaças como phishing, engenharia social e outras tentativas de manipulação é um componente chave do programa de segurança.

Em um ambiente de engenharia e infraestrutura, onde a interação com fornecedores, parceiros e prestadores de serviços é frequente, o risco de ataques cibernéticos e tentativas de fraude aumenta consideravelmente.

Portanto, os treinamentos incluem simulações e alertas sobre como reconhecer e se proteger contra essas ameaças, reforçando a importância da vigilância e da prudência no trato de dados e informações sensíveis.

11. AUDITORIA, MONITORAMENTO E MELHORIA CONTÍNUA

A auditoria, o monitoramento e a melhoria da política de segurança da informação e proteção de dados são essenciais para garantir que as práticas e controles adotados na Rodoanel BH S.A. permaneçam eficazes e alinhados às exigências regulatórias e boas práticas do mercado.

A organização adota uma abordagem sistemática para avaliar e melhorar continuamente os processos de governança da informação, assegurando a conformidade e a proteção contínua dos dados ao longo de todas as fases do projeto.

11.1 Auditorias periódicas da política

As auditorias periódicas têm como objetivo avaliar a eficácia da implementação da política de segurança da informação e proteção de dados, identificando possíveis áreas de melhoria ou ajustes necessários nos controles e processos adotados. Essas auditorias são conduzidas por equipes internas de compliance ou por auditores externos especializados, e envolvem a verificação do cumprimento das diretrizes estabelecidas, o monitoramento da efetividade dos controles de segurança e a identificação de riscos emergentes.

As auditorias podem cobrir tanto aspectos técnicos, como a segurança de sistemas e redes, quanto aspectos operacionais, como a gestão de documentos físicos e controle de acesso.

Os resultados das auditorias são analisados pela alta administração, que toma as medidas corretivas necessárias, ajustando controles e processos para melhorar a proteção de dados e a governança da segurança da informação.

11.2 Indicadores de desempenho e eficácia

Para garantir que a política de segurança da informação e a proteção de dados pessoais sejam efetivas e sustentáveis, são estabelecidos indicadores de desempenho que medem a eficácia dos controles implementados, incluindo, mas não se limitando a:

- Número de incidentes de segurança identificados e resolvidos.
- Taxa de conformidade com os processos de controle de acesso e proteção de dados.
- Tempo de resposta a incidentes e falhas de segurança.
- Avaliação de eficácia nos treinamentos e programas de conscientização.

Esses indicadores são monitorados e reportados regularmente à alta administração, garantindo que a organização tenha uma visão clara sobre o desempenho da política e a necessidade de ajustes contínuos.

A análise desses dados fornece insights valiosos para ajustar as medidas de segurança e adaptar a política às novas exigências e riscos identificados.

11.3 Processo de revisão e atualização da política

A revisão e atualização periódica da política de segurança da informação e proteção de dados garantem que as diretrizes estejam sempre alinhadas com as mudanças regulatórias, tecnológicas e operacionais. Essa atualização considera a evolução do ambiente regulatório (incluindo mudanças nas leis de privacidade como a LGPD e o GDPR), as novas ameaças cibernéticas e as lições aprendidas de incidentes anteriores.

O processo de revisão envolve a avaliação contínua dos controles de segurança implementados, garantindo que permaneçam eficazes no mitigar riscos emergentes.

Quando necessário, a política é ajustada para reforçar medidas preventivas, adaptar estratégias de mitigação de riscos e assegurar que novos requisitos legais sejam atendidos.

A alta administração é responsável por revisar a política e subsidiar a aprovação perante o Conselho de Administração da Companhia, assegurando que os ajustes necessários sejam implementados de maneira eficaz e que a política se mantenha atualizada e relevante para as operações da empresa.

12. DISPOSIÇÕES FINAIS

12.1 Entrada em vigor e aplicabilidade

Esta política entra em vigor a partir de sua aprovação pelo Conselho de Administração Rodoanel BH S.A., sendo aplicável a todos os colaboradores, fornecedores, prestadores de serviço e terceiros envolvidos no tratamento de dados ou no manejo de informações confidenciais.

Sua aplicabilidade abrange todas as fases do projeto, desde a mobilização até a operação, e se estende a todas as partes envolvidas, incluindo terceiros que manipulem dados sensíveis ou tenham acesso a documentos estratégicos.

Todos os novos contratos, acordos ou modificações contratuais com fornecedores e parceiros devem refletir a aderência a esta política, garantindo que a segurança da informação e a proteção de dados sejam priorizadas em toda a cadeia de operações do projeto.

12.2 Consequências para o descumprimento da política

O não cumprimento de qualquer diretriz estabelecida nesta política resultará em sanções proporcionais à natureza e gravidade da infração, que podem incluir medidas disciplinares internas, sanções contratuais e penalidades legais e regulatórias.

A organização adota um processo claro de responsabilização, assegurando que as violações sejam tratadas de forma justa, proporcional e consistente. As consequências incluem:

Medidas Disciplinares Internas

- **Advertência formal**: Serão aplicadas advertências formais quando o descumprimento for considerado leve ou não intencional. Este tipo de sanção tem como objetivo a correção do comportamento sem prejudicar a relação contratual ou funcional.
- **Suspensão**: Em casos de infrações mais graves ou recorrentes, será aplicada a suspensão das funções ou responsabilidades do colaborador ou parceiro, acompanhada de uma análise do impacto operacional e da necessidade de reforço nas medidas corretivas.
- **Rescisão contratual**: Para infrações graves que comprometam a segurança da informação ou violem os princípios de proteção de dados, será adotada a rescisão contratual. A rescisão será formalizada de acordo com as cláusulas estabelecidas no contrato, incluindo o pagamento de penalidades previstas.

Sanções Contratuais

- **Multas contratuais**: Para fornecedores e prestadores de serviço, o descumprimento das obrigações de segurança e privacidade resultará na aplicação de multas, conforme as cláusulas contratuais. O valor das multas será determinado com base na gravidade da infração e nos danos operacionais ou financeiros causados.
- **Suspensão ou término do contrato**: Em casos de violação de segurança grave ou de recorrência de infrações, a SPE Rodoanel BH pode suspender imediatamente o contrato ou rescindir a relação comercial, conforme cláusulas respectivas.

Consequências Legais e Regulatórias

O descumprimento das obrigações de segurança da informação e proteção de dados na Rodoanel BH S.A. pode resultar em sanções legais e regulatórias para a organização, além de penalidades específicas para os colaboradores diretamente responsáveis pelas falhas que causarem tais infrações:

- **Responsabilidade individual por danos**: Se um colaborador ou terceiro for responsável pela violação de dados ou informações sensíveis, ele poderá ser responsabilizado legalmente por danos materiais ou morais causados aos titulares dos dados ou a terceiros prejudicados. A organização também poderá ser envolvida em ações judiciais, dependendo do impacto da violação.
- **Sanções administrativas e contratuais**: A Rodoanel BH S.A. poderá ser sujeita a multas ou sanções impostas por órgãos reguladores, como a ANPD, em decorrência do não cumprimento das normas de segurança e privacidade de dados. Colaboradores diretamente envolvidos nas falhas poderão ser sujeitos a sanções internas, incluindo advertências, suspensão ou rescisão contratual, conforme a gravidade do descumprimento.
- **Impacto nas operações e no cronograma**: Violações graves podem levar a restrições operacionais, como intervenções por órgãos reguladores, que podem afetar o cronograma e a execução das atividades do projeto. Colaboradores ou parceiros responsáveis por essas falhas podem ser removidos de funções específicas ou sofrer consequências legais, dependendo da gravidade da infração.

Responsabilidade Proativa

A Rodoanel BH S.A. se compromete a agir rapidamente para corrigir qualquer falha de segurança ou não conformidade, implementando ações corretivas e monitorando continuamente o cumprimento das obrigações de segurança e privacidade. Isso visa minimizar riscos legais e proteger a integridade do projeto.

Esta Política foi aprovada pelo Conselho de Administração da Concessionária Rodoanel BH, e deve ser revisada, sempre que identificadas mudanças relevantes nos processos.