

OSTRYA INVESTIMENTOS LTDA

CNPJ: 56.992.790/0001-93

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Novo Hamburgo, 25 de agosto de 2024

1. OBJETIVO

1.1. Esta política tem como objetivo proteger as informações confidenciais, sensíveis e estratégicas da Ostrya Investimentos LTDA ("Ostrya"), assegurando a integridade, confidencialidade e disponibilidade dos dados, em conformidade com a legislação aplicável, incluindo a Lei Geral de Proteção de Dados (LGPD), e os princípios éticos da empresa.

2. ABRANGÊNCIA

2.1. Esta política aplica-se a todos os sócios, diretores, administradores, colaboradores, prestadores de serviços, consultores e qualquer outro profissional contratado pela Ostrya ("Colaboradores"). Todos os colaboradores são responsáveis por garantir a segurança da informação desde o início de seu vínculo com a empresa até o término.

3. PRINCÍPIOS E DIRETRIZES

3.1. Confidencialidade

3.1.1. Todas as informações confidenciais e sensíveis da Ostrya devem ser protegidas contra acesso não autorizado. Somente os responsáveis designados terão acesso a essas informações.

3.1.2. O acesso a informações críticas será limitado a colaboradores que necessitem delas para o desempenho de suas funções específicas.

3.2. Integridade

3.2.1. Assegurar que as informações armazenadas sejam precisas e estejam protegidas contra alterações não autorizadas. Qualquer modificação deve ser autorizada e documentada.

3.3. Disponibilidade

3.3.1. Garantir que as informações armazenadas em nuvem estejam disponíveis para os responsáveis autorizados sempre que necessário, assegurando a continuidade das operações da empresa.

3.4. Conformidade

3.4.1. Todos os colaboradores devem assegurar que suas atividades relacionadas à segurança da informação estejam em conformidade com a LGPD, regulamentos da CVM, Banco Central, e outras normativas aplicáveis.

3.4.2. Em caso de conflito entre as normas internas e as exigências legais, a regra mais rigorosa deve ser seguida.

4. CONTROLES E MEDIDAS DE SEGURANÇA

4.1. A Ostrya deve implementar controles rigorosos de acesso para garantir que somente os responsáveis autorizados possam acessar as informações armazenadas.

4.2. As informações armazenadas devem ser criptografadas tanto em trânsito quanto em repouso, garantindo a proteção contra acessos não autorizados e vazamentos de dados.

4.3. A Ostrya deve utilizar soluções de segurança robustas, como firewalls e sistemas de detecção e prevenção de intrusões, para proteger as informações contra ataques cibernéticos.

4.4. A Ostrya deve realizar monitoramento contínuo do acesso e uso das informações armazenadas, identificando e respondendo rapidamente a quaisquer atividades suspeitas.

4.5. A Ostrya deve realizar auditorias regulares para garantir que as políticas de acesso e segurança estejam sendo rigorosamente seguidas.

4.6. A Ostrya deve realizar backups regulares das informações armazenadas, garantindo que os dados possam ser recuperados rapidamente em caso de falha ou incidente de segurança.

4.7. Os backups devem ser armazenados em locais seguros e separados para minimizar o risco de perda de dados.

5. TREINAMENTO E CONSCIENTIZAÇÃO

5.1. Os colaboradores devem ser treinados para identificar e responder a potenciais ameaças à segurança da informação, incluindo práticas de segurança em nuvem.

6. RESPOSTA A INCIDENTES

6.1. Qualquer incidente de segurança relacionado ao armazenamento em nuvem, como vazamento de dados ou acesso não autorizado, deve ser imediatamente reportado à Diretoria de Compliance.

6.2. A Ostrya seguirá um plano de resposta a incidentes, que inclui a contenção, erradicação, recuperação e análise do incidente.

6.3. Em caso de violação de dados pessoais armazenados em nuvem, a Ostrya deverá notificar as autoridades e os agentes financeiros envolvidos dentro dos prazos estipulados pela legislação aplicável.

7. AUDITORIA E MONITORAMENTO

7.1. A Diretoria de Compliance realizará monitoramento permanente para verificar a conformidade com esta política e identificar áreas de melhoria relacionadas à segurança da informação em nuvem.

7.2. Qualquer não conformidade identificada durante o monitoramento deve ser corrigida imediatamente.

8. REVISÃO E ATUALIZAÇÃO

8.1. Esta política será revisada periodicamente para assegurar que continue em conformidade com as melhores práticas, mudanças na tecnologia e as leis aplicáveis.

8.2. Qualquer alteração nesta política será comunicada a todos os colaboradores, que deverão aderir imediatamente às novas disposições.

9. DISPOSIÇÕES GERAIS

9.1. Todos os colaboradores devem manter a confidencialidade das informações internas e estratégicas da Ostrya. Qualquer compartilhamento de informações deve seguir as diretrizes estabelecidas por esta política e pelas políticas internas da empresa.

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Eu, **[Nome]**, portador do documento de identidade nº **[Número do RG]** e do CPF nº **[Número do CPF]**, residente e domiciliado em **[Endereço]**, declaro ter lido e compreendido a Política de Segurança da Informação da Ostrya Investimentos LTDA, em sua versão datada de **[Data]**.

Comprometo-me a cumprir integralmente as diretrizes e obrigações estabelecidas na referida Política, bem como a observar as vedações e demais disposições nela previstas. Estou ciente de que o descumprimento das normas poderá resultar em consequências disciplinares, incluindo medidas legais, conforme a gravidade da infração.

Assumo a responsabilidade de atuar de acordo com os princípios éticos e padrões de segurança da informação definidos pela Ostrya Investimentos LTDA, buscando sempre a conformidade com as leis, regulamentos e melhores práticas de mercado.

Este termo de adesão é parte integrante do meu vínculo com a Ostrya Investimentos LTDA, aplicando-se a todos os sócios, diretores, administradores, colaboradores, prestadores de serviços, consultores e qualquer outro profissional contratado pela empresa. Reconheço que a assinatura deste documento é condição indispensável para o exercício de minhas atividades na Ostrya Investimentos LTDA.

Novo Hamburgo, 25 de agosto de 2024

OSTRYA INVESTIMENTOS LTDA