POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br

1. Introdução

Esta política estabelece diretrizes para a proteção dos ativos de informação da ONIX, garantindo a conformidade com a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, e com as melhores práticas de segurança da informação. Baseia-se também na norma ABNT NBR ISO/IEC 27002:2013. A política se aplica a todas as áreas da instituição, visando proteger dados pessoais e informações sensíveis contra acessos não autorizados, alterações ou destruição.

2. Objetivos

- Estabelecer padrões de comportamento claros para colaboradores, clientes e parceiros, visando a proteção das informações e dados pessoais em todas as interações com a ONIX.
- Garantir a integridade, confidencialidade e disponibilidade das informações, prevenindo acessos não autorizados, alterações, vazamentos ou destruição de dados sensíveis.
- Implementar controles, processos e medidas de segurança para assegurar a conformidade com a Lei Geral de Proteção de Dados (LGPD), respeitando os direitos dos titulares de dados e promovendo a transparência nas operações.

3. Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço, parceiros e qualquer outro indivíduo ou entidade que tenha acesso aos ativos de informação da ONIX, abrangendo dados em qualquer formato (digital, físico, verbal etc.).

A ONIX se reserva o direito de monitorar, registrar e auditar o uso de seus sistemas e recursos, em conformidade com a legislação brasileira, garantindo a segurança e a conformidade com as normas estabelecidas. Todos os c**olaboradores devem manter-se atualizados sobre normas e procedimentos e treinamentos relacionados à segurança da informação e proteção de dados.**

4. Princípios da LGPD

- **Finalidade:** Os dados pessoais devem ser processados exclusivamente para finalidades legítimas, específicas e informadas ao titular no momento da coleta, garantindo que o tratamento tenha um propósito claro e transparente.
- **Adequação:** O tratamento dos dados deve ser compatível com as finalidades informadas ao titular, sendo utilizado de maneira adequada e proporcional às necessidades do processamento.
- **Necessidade:** O tratamento de dados pessoais deve ser restrito ao mínimo necessário para atingir as finalidades informadas, evitando o uso excessivo ou irrelevante de informações.
- **Transparência:** A ONIX se compromete a fornecer informações claras, precisas e acessíveis sobre como os dados são coletados, tratados e compartilhados, permitindo que os titulares compreendam integralmente o uso de suas informações.
- **Segurança:** A empresa adota medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, vazamentos, alterações ou qualquer forma de uso indevido, garantindo a integridade e confidencialidade dos dados.
- **Prevenção:** A ONIX implementa práticas preventivas para minimizar riscos e danos aos titulares de dados, utilizando políticas de segurança, treinamentos e auditorias regulares.

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br

- **Não Discriminação:** O tratamento de dados pessoais não será utilizado para fins discriminatórios, ilícitos ou abusivos, respeitando sempre os direitos e a dignidade dos titulares.

5. Responsabilidades

- **Colaboradores:** Devem cumprir as diretrizes e normas estabelecidas pela política de segurança da informação e proteção de dados, sendo responsáveis por qualquer dano ou violação resultante do não cumprimento dessas orientações. Também devem participar de treinamentos e manter-se atualizados sobre as práticas de segurança.
- **Gestores:** São responsáveis por promover uma cultura de segurança da informação e proteção de dados dentro de suas equipes, assegurando que as diretrizes da política sejam seguidas. Devem exigir a assinatura de termos de compromisso de segurança, acompanhar a implementação de medidas de segurança e garantir que suas equipes cumpram as normas estabelecidas.
- **TI:** Deve testar, implementar e manter controles de segurança adequados, monitorar constantemente os sistemas de informação e garantir a proteção dos ativos de dados pessoais e sensíveis. A equipe de TI também deve realizar auditorias regulares para identificar possíveis falhas e atuar de maneira proativa na resolução de vulnerabilidades (possíveis riscos no processo).

6. Direitos dos Titulares de Dados

- **Acesso:** Garantir que os titulares possam acessar seus dados pessoais de forma clara e fácil, permitindo que consultem quais informações estão sendo tratadas pela ONIX.
- **Correção:** Oferecer aos titulares a possibilidade de corrigir dados pessoais incorretos, desatualizados ou incompletos, conforme necessário.
- **Exclusão:** Permitir que os titulares solicitem a exclusão de seus dados pessoais quando estes não forem mais necessários para as finalidades para as quais foram coletados, ou quando houver fundamento legal para a exclusão.
- **Restrição de Tratamento:** Garantir que os titulares possam restringir o tratamento de seus dados pessoais em situações específicas, como quando os dados forem contestados ou quando o tratamento for considerado ilegal.
- **Informação sobre Incidentes de Segurança:** Comprometer-se a informar os titulares sobre qualquer incidente de segurança que possa comprometer seus dados pessoais, em conformidade com as exigências da LGPD, e tomar as medidas necessárias para mitigar os danos.
- **Tempo de armazenamento dos dados do titular:** Os dados pessoais dos titulares serão mantidos pela empresa pelo período de 5 (cinco) anos, contados a partir da última interação ou da data de coleta dos dados, salvo se houver outro prazo estabelecido por obrigações legais ou contratuais.

7. Uso de Correio Eletrônico

- O e-mail corporativo deve ser utilizado exclusivamente para fins relacionados às atividades profissionais da ONIX, garantindo a comunicação eficaz e segura no ambiente de trabalho.
- É estritamente proibido o envio de mensagens não autorizadas, como e-mails pessoais ou promocionais, bem como a falsificação de informações, incluindo o uso indevido de identidades ou dados.
- Os colaboradores não devem divulgar dados confidenciais ou sensíveis sem a devida autorização, respeitando as políticas de segurança e as normas de proteção de dados da empresa.

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br

- Mensagens de e-mail devem ser cuidadosamente redigidas, evitando o envio de conteúdo que possa ser mal interpretado ou causar danos à imagem da ONIX.

8. Uso da Internet

- A ONIX monitora o uso da internet nos dispositivos corporativos para garantir a integridade e a segurança dos dados, além de assegurar o cumprimento das políticas internas de segurança e proteção de informações.
- Os colaboradores devem utilizar a internet de maneira responsável, evitando sites e serviços que possam colocar em risco a segurança dos sistemas da ONIX, como downloads não verificados ou o acesso a sites de terceiros com alto risco de malware.

9. Identificação e Senhas

- Dispositivos de identificação e senhas são pessoais, intransferíveis e de responsabilidade exclusiva do colaborador. O compartilhamento ou uso indevido de credenciais constitui violação das políticas da ONIX e pode ser considerado crime, de acordo com a legislação vigente.
- As senhas devem ser criadas de forma segura, utilizando combinações complexas que incluam letras, números e caracteres especiais, evitando o uso de informações pessoais óbvias (como datas de nascimento ou nomes de familiares).
- É proibido o armazenamento de senhas em locais acessíveis ou de fácil visualização, como anotações físicas ou arquivos não protegidos.
- Sempre que possível, devem ser utilizadas ferramentas de autenticação multifatorial (MFA) para aumentar a segurança no acesso a sistemas críticos.

10. Dispositivos Móveis

- Dispositivos móveis fornecidos pela ONIX devem ser usados exclusivamente para fins relacionados às atividades profissionais e de acordo com as diretrizes de segurança estabelecidas pela empresa.
- É **proibido** realizar alterações não autorizadas nos sistemas operacionais dos dispositivos móveis, que possam comprometer a segurança ou integridade dos dispositivos e dados corporativos.

11. Backup

Backups são realizados diariamente e armazenados de forma segura. Incluem arquivos de sistema e servidores virtualizados.

- **Backups** são realizados de forma regular, com **frequência diária**, e armazenados em locais seguros e protegidos contra acessos não autorizados, garantindo a integridade e disponibilidade dos dados em caso de incidentes.
- O processo de backup inclui **arquivos de sistema**, **servidores virtualizados** e **dados críticos** essenciais para o funcionamento da ONIX.
- Os backups devem ser verificados periodicamente para garantir que os dados possam ser restaurados de maneira eficiente e sem perdas, caso necessário.
- A equipe de TI deve manter um **plano de recuperação de desastres** atualizado, para garantir a continuidade dos negócios em caso de falha nos sistemas.
- **Armazenamento seguro**: Os backups devem ser criptografados e armazenados de forma redundante, garantindo a segurança tanto em mídias físicas quanto em ambientes de nuvem.

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br

12. Gestão de Riscos

A ONIX está ciente dos potenciais riscos que podem comprometer a segurança da informação e a proteção de dados pessoais. A seguir, estão listados alguns dos principais riscos e as ações necessárias para mitigá-los:

Acesso não autorizado a dados sensíveis

- **Ação Necessária**: Implementar controles de acesso rigorosos, como autenticação multifatorial (MFA) e revisão periódica dos privilégios de acesso. Garantir que os colaboradores e prestadores de serviços só tenham acesso aos dados necessários para suas funções.

Vazamento de dados devido a dispositivos móveis não seguros

- **Ação Necessária**: Aplicar políticas de segurança rigorosas para o uso de dispositivos móveis, incluindo a utilização de senhas fortes, criptografia de dados e soluções de gerenciamento de dispositivos móveis (MDM). Em caso de perda ou roubo, realizar a remoção remota de dados sensíveis.

Uso inadequado de e-mails e Internet

- **Ação Necessária**: Estabelecer políticas claras de uso de e-mail corporativo e internet, com foco na prevenção de acessos a sites maliciosos, compartilhamento de informações confidenciais e uso de recursos corporativos para fins pessoais. Implementar filtros de conteúdo e monitoramento de tráfego.

Violação das normas de proteção de dados pessoais (LGPD)

- **Ação Necessária:** Garantir a conformidade contínua com a LGPD por meio de auditorias regulares, treinamentos sobre direitos dos titulares e monitoramento do tratamento de dados pessoais. Estabelecer um processo claro para a gestão de incidentes e vazamentos de dados.

13. Considerações Finais

A segurança da informação e a proteção de dados pessoais são pilares essenciais da cultura organizacional da ONIX. A empresa compromete-se a tratar essas questões com a mesma seriedade e ética que dedica a todas as suas atividades.

Todos os colaboradores, prestadores de serviço e parceiros devem entender que a proteção dos dados não é apenas uma obrigação legal, mas também uma responsabilidade compartilhada que reflete nosso compromisso com a confiança dos nossos clientes e com a integridade dos nossos processos.

A ONIX continuará a atualizar e aprimorar suas práticas de segurança, buscando sempre as melhores soluções para mitigar riscos e garantir a conformidade com as leis e regulamentos aplicáveis.

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br