POLÍTICA DE SEGURANÇA E SIGILO DA INFORMAÇÃO

PCNA ADMINISTRAÇÃO DE RECURSOS LTDA

DEZEMBRO/2024

pncainvestimentos.com.br

Avenida das Américas, 4200, Bloco 01, Sala 305 - Centro Empresarial Barra Shopping, Barra da Tijuca, Rio de Janeiro/RJ CEP: 22640-907

1. SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação da **PNCA Administração** tem por objetivo assegurar a integridade, confidencialidade e confiabilidade de todas as informações que envolvam a atividade da empresa.

As práticas de segurança da informação adotadas pela **PNCA Administração** têm como objetivo impedir a ocorrência de: (i) transmissão não autorizada de informações confidenciais sobre clientes, colaboradores ou sobre a empresa em geral; (ii) cópia ou transmissão não autorizada de *softwares* ou dados proprietários; (iii) acesso não autorizado a arquivos, comunicações e outros dados confidenciais relacionados aos clientes, colaboradores ou à empresa em geral; (iv) tentativas de interceptação de e-mail ou mensagem instantânea; (v) quaisquer ataques cibernéticos; e (vi) liberação não autorizada de senhas e códigos de ID de usuários.

Segue, abaixo, a descrição das medidas adotadas:

- O acesso aos diversos serviços de informática, como sistemas, e-mail, rede local, entre outros, ocorre mediante autenticação do usuário através de seu nome de usuário (*login*) e senha (*password*). Tal processo visa garantir que o acesso à informação seja obtido apenas por pessoas autorizadas (garantia de confidencialidade). Cada usuário é responsável pela escolha de suas senhas pessoais.

- Os notebooks utilizados pela equipe da **PNCA Administração** foram configurados com chave de criptografia e não permitem o acesso aos dados sem a utilização da senha de criptografia. Além disso, os aparelhos "mobiles" com a configuração de acesso aos e-mails podem ser bloqueados ou mesmo "resetados" pela equipe de TI remotamente.

- Os arquivos contendo informações relacionadas à empresa e as suas atividades são armazenados em um servidor de arquivos. O acesso a estes arquivos é restrito, de acordo com a definição dos grupos de segurança definidos pelos gestores de TI.

- O sistema de correio eletrônico utilizado pela empresa, bem como os endereços atribuídos aos usuários, é exclusivamente para uso profissional e, portanto, relacionados às atividades da empresa. Por um período de pelo menos 30 dias, há a garantia de que toda e qualquer mensagem, enviada ou recebida, será armazenada com segurança, a menos que ocorra a exclusão da mensagem pelo usuário, antes desse prazo.

- Todos os equipamentos de TI (desktops, notebooks, impressoras, redes sem fio, etc) são devidamente registrados, e utilizando-se somente *softwares* licenciados e

protegidos por senhas. Apenas os gestores de TI têm permissão para configurar, manter e conceder acesso a estes ativos.

- Todos as estações de trabalho contam com solução de proteção antivírus. A proteção antivírus opera de forma centralizada e automática, independente da ação do usuário, tanto no que diz respeito às verificações programadas, como às atualizações em sua base de dados.

- Todo processo é monitorado e registrado através de rotinas periódicas executadas pela empresa mantenedora de TI da **PNCA Administração**. Os serviços estão configurados conforme as melhores práticas dos fornecedores e estão prontos para tratar as recentes ameaças de segurança.

- Os acessos externos à rede interna da **PNCA Administração** somente poderão ser feitos com a utilização de clientes VPN que estabelecem a conexão segura entre as partes. Todos os acessos são registrados.

- Os documentos físicos entregues pelos clientes são digitalizados em formato PDF e armazenados no servidor de arquivos. O acesso a estes arquivos é restrito de acordo com a definição dos grupos de segurança definidos pelos gestores de TI.

- Para garantir a manutenção dos dados, existem duas rotinas de *backup*: (i) a primeira realiza o versionamento dos arquivos de aproximadamente 30 dias nos próprios servidores, sendo executado duas vezes ao dia; (ii) a segunda rotina é feita na plataforma *Microsoft Onedrive* (nuvem) onde os *backups* são realizados diariamente e armazenados em datacenters redundantes no EUA.

- Os *backups* são realizados de segunda à sexta e armazenados por 4 semanas. Uma versão mensal com a posição da última sexta-feira de cada mês é armazenada pelos últimos 12 meses. As informações contidas no *backup* estão criptografadas por chave de 256 bits e acessíveis somente por acessos restritos por senha de segurança.

- Busca-se, com essa estratégia, manter os dados preservados e ter rápida restauração do ambiente em caso de um sinistro no escritório. As rotinas de *backup* são validadas semanalmente pelo mantenedor de TI. Testes de restauração para validação do processo de recuperação de dados são feitos mensalmente.

- O departamento de Tecnologia é responsável por realizar, periodicamente, testes de segurança e procedimentos para detectar falhas e vulnerabilidades nos sistemas da **PNCA Administração**.

- Todos os colaboradores da **PNCA Administração** têm ciência do dever de reportar imediatamente qualquer indício de falha, invasão ou comportamento suspeito dos sistemas.

- E ainda, todos os colaboradores da **PNCA Administração** que tratam de assuntos confidenciais, assinam termo de confidencialidade e passam por treinamentos periódicos. Além disso, a **PNCA Administração** disponibiliza uma cartilha de segurança da informação e boas práticas para usuários.

- Em caso de vazamento de dados ou de qualquer informação relevante para o funcionamento da **PNCA Administração**, serão tomadas as medidas necessárias para evitar qualquer dano aos sócios, colaboradores, clientes e parceiros de negócios da **PNCA Administração.**

2. SIGILO DAS INFORMAÇÕES

A confidencialidade consiste em princípio fundamental da **PNCA Administração**, e deve ser aplicada pelos colaboradores com relação a todas as informações relativas da empresa, seus clientes, prestadores de serviços e fornecedores.

Em especial, são consideradas confidenciais as informações obtidas de clientes (dados pessoais, posições, movimentações, etc.) e também as informações relacionadas às operações dos fundos ou administrados (posições, risco, decisões de investimento, informações materiais não públicas, etc.).

Algumas informações poderão se tornar públicas, exclusivamente para os fins de divulgação e marketing relativos aos prestadores de serviços e fornecedores, desde que não haja nenhum conflito com suas atividades e sejam, pelo mesmo, expressamente autorizados.

O colaborador da **PNCA Administração** deve tratar as atividades e os planos internos como confidenciais, a serem divulgados somente dentro da estrutura interna da empresa, restringindo-se a base de necessidade de seu conhecimento. Cada colaborador é responsável pelo cuidado e guarda das informações sob os seus cuidados.

Medidas de segurança devem ser adotadas, tais como:

(i) não compartilhamento de senhas pessoais de acesso;
(ii) bloqueio dos recursos eletrônicos quando se ausentarem das mesas de trabalho;
(iii) não utilização da área de trabalho do computador para arquivo de documentos, devendo todos os documentos ficarem armazenados no servidor;

(iv) descarte seguro e controlado de documentos físicos ou cópias de documentos, não devendo ser armazenados nas mesas ou gavetas originais ou cópias de documentos dos clientes; e
(v) quando necessário, o arquivamento de documentos em meio físico deverá ser feito em local adequado.

Nenhum colaborador está autorizado a fazer declarações ou conceder entrevistas em nome da **PNCA Administração**.

Qualquer veiculação de informações através da mídia deverá ser aprovada pelo Comitê Executivo, que poderá contratar assessoria de imprensa, conforme definido no plano de comunicação.

Toda informação financeira da **PNCA Administração** ou de Fundos de Investimentos sob sua administração/gestão deverá ser tratada como confidencial, exceto quando tenham sido divulgados por meios de relatórios públicos, jornais ou outros meios de comunicação.

A confidencialidade de quaisquer informações, que não pertençam ao domínio público, deve ser protegida mesmo após o colaborador deixar a instituição.

São informações que não dizem respeito ao domínio público: operações, informações sobre planos de negócios, informações confidenciais sobre funcionários, clientes, distribuidores, prestadores de serviços e fornecedores.

É dever da **PNCA Administração**: (i) garantir a segurança e confidencialidade das informações pessoais não públicas; (ii) proteger a segurança de tais informações contra qualquer ameaça ou perigo antecipados; (iii) proteger tais informações contra o acesso ou uso não autorizado; e (iv) garantir a correta eliminação dos dados quando necessário.

Todos os colaboradores da **PNCA Administração** devem manter e preservar a confidencialidade das informações pessoais não públicas confiadas à **PNCA Administração** e é de absoluta importância que os titulares de dados pessoais saibam que as informações que eles fornecem serão tratadas com integridade e discrição.

Informações confidenciais fornecidas, verbalmente ou por meio de documentos, por Cliente que posteriormente decide não iniciar negócios com a **PNCA Administração** também estão sujeitas a essas políticas e procedimentos e devem ser preservadas com o mesmo cuidado dispensado aos demais Clientes.

3. CONSIDERAÇÕES FINAIS

Todas as dúvidas sobre as diretrizes desta Política podem ser esclarecidas com a área

de Compliance.

4. CONTROLE DE VERSÕES

- **Versão**
  Data: 12/12/2024

pncainvestimentos.com.br

Avenida das Américas, 4200, Bloco 01, Sala 305 - Centro Empresarial Barra Shopping, Barra da Tijuca, Rio de Janeiro/RJ CEP: 22640-907