POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Arbor Gestão de Recursos Ltda.

2026

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

1. APRESENTAÇÃO

A Política de Segurança da Informação e Cibernética da Arbor Gestão de Recursos Ltda. ("Arbor" ou "Arbor Capital") aplica-se a todos os sócios, Colaboradores, prestadores de serviços, sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Arbor ou que acesse informações a ela pertencentes. Todo e qualquer usuário de computadorizados ou digitais da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

2. OBJETIVOS

A Política de Segurança da Informação da Arbor Capital visa proteger as informações de sua propriedade e/ou sob sua guarda, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Arbor, que não necessitem ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais relacionadas à empresa.

Qualquer informação sobre a Arbor, ou de qualquer natureza relativa às atividades da empresa e a seus sócios, colaboradores e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Riscos e Compliance.

3. SEGURANÇA DE INFORMAÇÕES

As medidas de segurança da informação utilizadas pela Arbor têm por finalidade minimizar as ameaças ao patrimônio, à imagem e aos negócios da empresa.

Este documento foi elaborado pela Arbor Gestão de Recursos LTDA., não podendo ser copiado, reproduzido ou distribuído sem a prévia autorização da gestora de recursos.

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis da Arbor Capital e circulem em ambientes externos à empresa, sem prévia autorização do Diretor de Riscos e Compliance. Isso porque tais arquivos contêm informações que são consideradas informações confidenciais e/ou sensíveis. Cabe ressaltar que, em relação a informações de caráter sensível ou confidencial da empresa ou de clientes, estas serão armazenados em diretórios de rede com acesso restrito da Arbor.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Arbor. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação, sendo recomendável o seu descarte total.

Adicionalmente, os Colaboradores devem se abster de utilizar pen-drives, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Arbor.

É proibida a conexão de equipamentos na rede da Arbor que não estejam previamente autorizados.

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. Será obrigatória a alteração de senha de acesso aos equipamentos (login de usuário) ao menos a cada três meses, utilizando modelo de definição de senha de difícil identificação por parte de potenciais invasores externos.

O acesso a sites e blogs, bem como o envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo também é terminantemente proibido, como também o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da Arbor.

Não é permitida a instalação de nenhum software ilegal ou que possuam direitos autorais protegidos, ou mesmo legal, sem prévia autorização do Diretor de Riscos e Compliance.

Este documento foi elaborado pela Arbor Gestão de Recursos LTDA., não podendo ser copiado, reproduzido ou distribuído sem a prévia autorização da gestora de recursos.

Todo conteúdo que está na rede pode ser acessado pelos sócios ou pelo Diretor de Riscos e Compliance caso haja necessidade, inclusive e-mails. Arquivos pessoais salvos em cada computador poderão ser acessados, caso seja necessário. A confidencialidade dessas informações deve ser respeitada, e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais, ou em atendimento a determinações judiciais ou administrativas.

Por fim, convém ressaltar que a Arbor Capital conta com sistemas e ferramentas contratados para arquivamento (rede), firewall, antivírus, backup e prevenção de invasão.

4. SERVIÇOS DE REDE

As redes de serviços são segmentadas para garantir a segurança e desempenho entre elas. Está implantado um sistema de prevenção de invasão na rede e nos equipamentos para garantir a segurança da informação e disponibilidade de serviços.

5. ARMAZENAMENTO DE DADOS

O armazenamento de dados (backup) é realizado diariamente na nuvem.

6. INSTALAÇÕES FÍSICAS TECNOLÓGICAS

Para garantir o ambiente em alta disponibilidade, a Arbor Capital adota o uso de laptops ao invés de desktops. Esses equipamentos garantem tanto a mobilidade quanto tornam redundante o uso de nobreaks.

7. TREINAMENTO DE SEGURANÇA DAS INFORMAÇÕES

A Arbor Capital entende como essencial que o seu treinamento anual, supervisionado pelo Diretor de Riscos e Compliance, abranja todos os preceitos contidos na presente política, de modo que seus Colaboradores estejam sempre cientes e consonantes os procedimentos de segregação e segurança das informações.

Este documento foi elaborado pela Arbor Gestão de Recursos LTDA., não podendo ser copiado, reproduzido ou distribuído sem a prévia autorização da gestora de recursos.

8. TESTES DE SEGURANÇA DAS INFORMAÇÕES

A Arbor Capital, em razão de circunstâncias que demandem tal providência, realizará testes dos seus sistemas de segurança de informações, bem como de todos os preceitos contidos na presente política, incluindo, mas não se limitando apenas aos procedimentos de descarte de informações pelos Colaboradores, individualização dos usuários, dentre outros.

Os resultados desses testes, bem como os procedimentos para saneamento de eventuais problemas, serão registrados na Ata da seguinte reunião do Comitê de Compliance da Arbor.

Estes testes serão realizados por empresa de suporte de TI terceirizada, e buscará cobrir os seguintes pontos:

- Identificação e avaliação de potenciais riscos cibernéticos, envolvendo ativos de hardware e software, além de processos que necessitem de proteção. Importante estimar impactos financeiros, operacionais e reputacionais em caso de evento;
- Estabelecimento de medidas de prevenção e mitigação de riscos identificados na atividade de identificação de riscos, de forma buscar evitar eventuais ataques cibernéticos aos dados e equipamentos da empresa;
- Detecção de possíveis anomalias e/ou fragilidades no ambiente tecnológico, incluindo acessos não permitidos, usuários não cadastrados, e dispositivos não autorizados;
- Criação de um plano de resposta e recuperação de incidentes, que contenha comunicação interna e externa, se necessário. Tal plano será elaborado em conjunto entre as áreas internas de Riscos e Compliance, e da empresa de TI terceirizada, e terá testes anuais para validar sua eficiência. O plano identificará papéis e responsabilidades, com previsão de acionamento de colaboradores e contatos externos;
- Manter tal programa de segurança cibernética atualizado, identificando novos e potenciais riscos, ativos e processos.

As documentações relacionadas aos planos definidos e testes realizados, assim como os resultados auferidos e ações corretivas e mitigadoras, deverão ser mantidas em diretório interno da área de Riscos e Compliance.

Os temas relacionados à segurança da informação e cibernética serão tratados no Comitê Semestral de Riscos e Compliance, de forma ordinária, ou mesmo em reunião específica, em casos de eventos extraordinários, para que sejam tomadas de forma tempestiva medidas de recuperação, limitação de danos, e resposta relevante.

Este documento foi elaborado pela Arbor Gestão de Recursos LTDA., não podendo ser copiado, reproduzido ou distribuído sem a prévia autorização da gestora de recursos.

9. VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

Este documento foi elaborado pela Arbor Gestão de Recursos LTDA., não podendo ser copiado, reproduzido ou distribuído sem a prévia autorização da gestora de recursos.