POLÍTICA DE SEGURANÇA CIBERNÉTICA

DA

TESOURO INVESTIMENTOS LTDA.

Versão 2023.01 | **06 de Janeiro de 2023**

Em atendimento ao disposto na regulamentação em vigor, bem como em consonância com o disposto no Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, a Tesouro Investimentos Ltda. ("Tesouro Investimentos") mantém a presente Política de Segurança Cibernética, com o objetivo de definir regras, procedimentos e controles de segurança cibernética que sejam compatíveis com o seu porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas

A presente política deve ser sempre interpretada em conjunto com as demais políticas e normas internas da Tesouro Investimentos, em especial no tocante à confidencialidade, à integridade e à disponibilidade dos dados e dos sistemas de informação utilizados.

1. Avaliação de riscos

A Tesouro Investimentos estima que os principais riscos cibernéticos a serem considerados são:

- Sede Tesouro Investimentos:
  - Ausência ou instabilidade de energia elétrica na região;
  - Ausência ou instabilidade de provedor de internet na região;
  - Acesso não autorizado às instalações da Companhia;
  - Acesso não autorizado às áreas restritas da Companhia;
  - Acesso não autorizado à documentos físicos da Companhia.

- Ativos Físicos (notebook e/ou celulares):
  - Perda ou roubo de ativos tecnológicos da Companhia;
  - Acesso indevidos aos dados armazenados em ativos tecnológicos da Companhia;
  - Mal funcionamento ou mal uso de ativos tecnológicos da Companhia.

- Sistemas (todos os sistemas da Tesouro investimentos estarão hospedados em nuvem, modelos PaaS ou SaaS):
  - Operação:
    - Indisponibilidade dos serviços e sistemas contratados pela Companhia;
    - Perda de dados dos serviços e sistemas contratados pela Companhia;
    - Dados desprotegidos nos sistemas contratados pela Companhia;
  - Acesso:
    - Captura de dados entre a comunicação da Companhia e os sistemas;
    - Acesso não autorizado aos sistemas contratados pela Companhia;

        - Acesso indevido às funções e funcionalidades nos sistemas;
    - Mudança:
        - Mudança não autorizada em softwares utilizados pela companhia;
        - Mudança indevida em softwares utilizados pela companhia.

2. Ações de proteção e prevenção

As ações de proteção e prevenção adotadas pela Tesouro Investimentos são:

- Sede Tesouro Investimentos:
    - Utilização de *no-breaks* para sustentação da infraestrutura;
    - Utilização de máquinas novas com bateria capaz de sustentar horas sem carregamento;
    - Redundância de provedores de internet na sede da Companhia;
    - Porta para acesso às instalações da Companhia com chave e/ou com fechadura digital;
    - Porta e verificação biométrica para acesso às áreas restritas da Companhia;
    - Utilização de cofre para salva guarda dos documentos da Companhia.

- Ativos Físicos (notebook e/ou celulares):
    - Assinatura de termo de responsabilidade (boa utilização) por todos os colaboradores da Companhia;
    - Contrato de manutenção com os fornecedores em caso de problema com algum ativo físico;
    - Utilização de criptografia em todos os ativos físicos evitando acesso não autorizado em caso de perda ou roubo.

- Sistemas (todos os sistemas da Tesouro investimentos estarão hospedados em nuvem, modelos PaaS ou SaaS):
    - Operação:
        - Os fornecedores contratados pela Tesouro Investimento apresentam 99,9% de disponibilidade dos seus serviços através de redundância e data center tier I ou superior;
        - Os dados dos sistemas contratados pela Tesouro Investimentos estarão armazenados nas nuvens dos fornecedores, onde é garantido o backup online das informações em diferentes discos;
        - Os dados armazenados nos sistemas contratados pela Tesouro Investimento são criptografados em armazenamento.
    - Acessos:

        - A Tesouro Investimentos fará uso de serviço de VPN, visando prevenir o vazamento de dados em comunicação e salva guarda dos mesmos;
        - Os sistemas contratados pela Tesouro investimentos possuem sistema de autenticação sendo necessário o uso de usuário e senha complexos para acesso. Adicionalmente, alguns sistemas também apresentarão multifator de autenticação (MFA);
        - Os acessos aos sistemas serão segregados de acordo com a área e função de cada profissional, onde somente estes terão conhecimento das credenciais de autenticação ou perfis específicos.
    - Mudanças:
        - SaaS: Os softwares contratados no modelo SaaS seguirão o processo de desenvolvimento dos fabricantes, uma vez que são softwares de prateleira, cabendo a eles a mitigação do risco de mudança indevida.
        - PaaS: Os softwares de desenvolvimento próprio da Tesouro Investimentos estarão hospedados em nuvem, onde somente os respectivos diretores da Companhia terão acesso de modificação.
        - PaaS: Quaisquer modificações dos softwares da Tesouro Investimento serão desenvolvidas em local segregado e migrado para produção somente depois de serem testados e aprovados pelos respectivos diretores das áreas.

3. Descrição dos mecanismos de supervisão

Para fins da supervisão dos riscos acima mencionados, a Tesouro Investimentos desempenha as seguintes atividades:

- Sede da Tesouro Investimentos:
    - Anualmente, os *no-breaks* são revisados, visando avaliar o correto funcionamento;
    - Anualmente, os sistemas de acesso às instalações físicas da Tesouro Investimentos são revisados, visando avaliar o correto funcionamento;
    - Anualmente, o cofre contendo as informações físicas da Tesouro Investimentos é revisado, visando garantir a estrutura do mesmo e salva guarda dos documentos que estão armazenados dentro dele.

- Ativos Físicos (notebook e/ou celulares):
    - Anualmente, os notebooks e/ou celulares passarão por inspeção, visando avaliar: bateria, criptográfica, softwares instalados e configurações aplicadas.

- Anualmente, os termos de responsabilidade serão atualizados com os respectivos usuários.

- Sistemas (todos os sistemas da Tesouro investimentos estarão hospedados em nuvem, modelos PaaS ou SaaS):
  - Operação:
    - Anualmente, os fornecedores da Tesouro Investimentos serão revisados, visando garantir que: 1. Os dados estão sendo devidamente criptografados na fonte; 2. Os backups estão sendo realizados adequadamente; 3. A disponibilidade dos serviços tem sido entregue de acordo com os contratos estabelecidos.
  - Acesso:
    - Anualmente, os acessos de todos os sistemas da Tesouro Investimentos serão revisados, levando em consideração: 1. Profissional x Função x Acesso (Segregação de Funções); 2. Uso de VPN; 3. Alteração de Senha (mínimo anual e utilização de padrão complexo); 4. Sempre que possível, MFA habilitado para acesso.
  - Mudança:
    - SaaS: Anualmente, a Tesouro Investimentos solicitará aos fornecedores evidências dos processos internos de governança, visando obter o conforto que as mudanças são realizadas seguindo controles estabelecidos e não impactando o software contratado.
    - PaaS: A cada nova mudança, a Tesouro Investimentos fará: 1. Especificação da mudança; 2. Teste do novo pacote desenvolvido antes de ser aplicado em produção; 3. Aprovação do novo pacote a ser aplicado em produção.

4. Plano de resposta a incidentes

- Sede da Tesouro Investimentos:
  - Ausência de energia: acionar o provedor de energia da região (CEMIG) e registrar chamado para normalização da situação. Adicionalmente, em casos em que o *no-break* não for suficiente, os profissionais da Tesouro Investimento deverão seguir para suas residências e trabalhar em regime *home office* até a normalização da situação. Por fim, um e-mail com a descrição do problema e possivelmente telas, deverá ser enviado para: backoffice@tesouroinvestimentos.com;
  - Ausência de internet: em caso de ambos os provedores de internet estarem indisponíveis na região, o profissional deverá contatar os Diretores da

Tesouro Investimento, bem como acionar os provedores e registrar chamado para normalização da situação. Adicionalmente, os profissionais da Tesouro Investimento deverão seguir para suas residências e trabalhar em regime *home office* até a normalização da situação. Por fim, um e-mail com a descrição do problema e possivelmente telas, deverá ser enviado para: backoffice@tesouroinvestimentos.com;

- Ausência de acesso às dependências físicas: em caso de haver alguma restrição para acesso físico às instalações da Tesouro Investimentos, o profissional deverá acionar os Diretores da Companhia e deverão seguir para suas residências e trabalhar em regime *home office* até a normalização da situação. Por fim, um e-mail com a descrição do problema e possivelmente telas, deverá ser enviado para: backoffice@tesouroinvestimentos.com.

- Ativos Físicos (notebook e/ou celulares):
  - Em caso de perda ou roubo de algum ativo físico, o profissional deverá registrar um boletim de ocorrência junto às autoridades locais, bem como comunicar os Diretores da Tesouro Investimentos. Adicionalmente, uma cópia do boletim de ocorrência deverá ser enviada para a seguinte caixa: backoffice@tesouroinvestimentos.com.;
  - Em caso de mal funcionamento de algum ativo físico, o profissional deverá contatar os Diretores da Tesouro Investimentos, para registro de chamado de suporte junto ao fabricante. Adicionalmente, um e-mail com a descrição do problema e possivelmente telas, deverá ser enviado para: backoffice@tesouroinvestimentos.com.

- Acesso:
  - Em caso de vazamento ou indisponibilidade de acesso de algum sistema da Tesouro Investimento, o profissional deverá contatar imediatamente os Diretores da Companhia, bem como enviar um e-mail para backoffice@tesouroinvestimentos.com e risco.compliance@tesouroinvestimentos.com.

5. Indicação de responsável por questões de segurança cibernética

A Área de Risco e *Compliance* é a responsável por questões de segurança cibernética, sendo que conta com a assistência de profissionais de tecnologia da informação terceirizados para a avaliação de riscos e eventuais remediações, nos termos desta política.

6. Revisão da política de segurança cibernética

É feita uma revisão, no mínimo, anual desta política, ou em menor periodicidade quando houver alteração na regulação referente a segurança cibernética, de modo a manter sempre atualizadas as suas disposições.

* * *