

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

TANE CAPITAL LTDA.
CNPJ: 58.158.159/0001-19

SUMÁRIO

OBJETIVO E ABRANGÊNCIA	2
VIGÊNCIA.....	2
DIRETRIZES	2
IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS CIBERNÉTICOS	7
AÇÕES DE PROTEÇÕES E PREVENÇÃO AOS RISCOS CIBERNÉTICOS	7
MECANISMOS DE SUPERVISÃO DA SEGURANÇA CIBERNÉTICA.....	8
RESPOSTAS A INCIDENTES CIBERNÉTICOS.....	8
PROGRAMA DE TREINAMENTO	9
DISPOSIÇÕES GERAIS E ENFORCEMENT	10

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

OBJETIVO E ABRANGÊNCIA

A presente Política de Segurança da Informação e Cibernética ("Política") foi instituída pela **TANE CAPITAL LTDA.** ("Sociedade", "Gestora" ou "Tane") e tem por finalidade estabelecer diretrizes para garantir a confidencialidade, integridade e segurança das informações, bem como proteger a Sociedade contra possíveis ameaças ou ataques cibernéticos.

Esta Política se aplica aos sócios, administradores, colaboradores, funcionários, *trainees* e estagiários (em conjunto "Colaboradores", e em separado, "Colaborador") da Tane, que devem conhecer todas as disposições desta, bem como garantir o seu fiel cumprimento, zelando pela integridade, segurança e veracidade das informações, recursos e equipamentos eletrônicos a eles disponibilizados, de forma que resta estritamente vedado o compartilhamento não autorizado de qualquer informação.

Ademais, a Sociedade coletará Termo de Confidencialidade de quaisquer terceiros contratados que tiverem acesso às informações confidenciais a respeito da Sociedade, seus Colaboradores, fundos sob gestão e investidores, salvo se este compromisso já tiver sido firmado entre as partes mediante a assinatura do correspondente Contrato de Prestação de Serviços.

VIGÊNCIA

A presente Política tem vigência a partir de outubro/2026, e vigorará por prazo indeterminado.

DIRETRIZES

ADOÇÃO DE COMPORTAMENTO SEGURO E CONTROLE

A Tane disponibiliza aos seus Colaboradores recursos tecnológicos de alta performance buscando assegurar (i) o controle de acesso quanto às informações confidenciais, reservadas e privilegiadas de propriedade e/ou sob a guarda da Sociedade; (ii) a existência de testes periódicos de segurança nos sistemas da Sociedade, principalmente naqueles que possuem repositórios de informação; e (iii) a verificação diária do espaço físico da Sociedade, com o fim identificar documentos eventualmente deixados sobre as mesas, móveis ou impressoras.

Os Colaboradores devem sempre adotar práticas visando a proteção e segurança das informações da Sociedade e dos seus clientes, se mantendo sempre atualizados quanto às ameaças externas existentes, inclusive no que se refere aos vírus de computadores, *malwares* e outros meios de fraude.

A instalação de quaisquer novos *softwares* ou programas nos equipamentos eletrônicos de propriedade da Sociedade está sujeita à prévia aprovação da Área de Risco e *Compliance*. Eventuais requerimentos devem ser encaminhados ao endereço de e-mail riscos@tane.com.br sendo que o Diretor de *Compliance* deverá se manifestar quanto ao requerimento em um prazo de até 72 (setenta e duas) horas.

É estritamente vedada a utilização de informações e dados pessoais pelos Colaboradores para quaisquer fins que não sejam relativos às atividades, operações e transações da Sociedade.

A senha de acesso do Colaborador a qualquer dos sistemas utilizados pela Tane é pessoal e intransferível, de forma que é vedada a sua divulgação, compartilhamento e manutenção em local visível ou repositório não protegido.

Assuntos confidenciais relacionados às atividades da Sociedade não podem ser discutidos em ambientes públicos.

Os Colaboradores declaram-se cientes de que todos os acessos, movimentações e transações realizados nos sistemas internos da Tane são monitorados e armazenados, de forma que os registros correspondentes podem ser utilizados para detecção de fraude e, conforme necessário, servir como documento comprobatório em eventuais processos administrativos e judiciais.

ACESSO A INFORMAÇÕES

A Tane realiza o monitoramento do acesso a todos os seus espaços físicos e sistemas operacionais, de forma a garantir que apenas as pessoas devidamente autorizadas tenham acesso.

Os Colaboradores deverão prezar pela segurança e confidencialidade das informações armazenadas nos equipamentos e documentos que estão sob sua posse, responsabilizando-se por eventuais vazamentos e/ou desvios de utilização.

A troca de informações entre os Colaboradores deve sempre pautar-se no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida a Área de *Compliance* deve ser acionada previamente à revelação.

O controle de acesso aos sistemas e às instalações da Sociedade deve ser documentado, formalizado e então armazenado em local seguro, sob responsabilidade do Diretor de *Compliance*. O acesso controlado às pastas e arquivos se dá mediante a outorga de senhas de acesso individuais e intransferíveis que permitem a identificação do seu usuário, afastando a

utilização das informações ali contidas por pessoas não autorizadas.

As senhas de acesso possuem prazo de validade e requisitos mínimos de segurança, devendo ser desabilitadas após um número máximo de tentativas malsucedidas de acesso, sendo esta atividade registrada pelos controles de tecnologia da informação.

Todos os computadores da Sociedade possuem duas senhas diferentes, sendo uma para desbloqueio do equipamento e outra para acesso ao sistema interno da Tane, com o fim de reduzir o risco de acessos não autorizados.

Após um tempo máximo de inatividade, os sistemas internos e dispositivos fornecidos pela Sociedade expiram, usando um protetor de tela protegido por senha que exige que a sessão somente possa ser reiniciada depois que o usuário tenha se autenticado novamente.

No caso do desligamento ou saída de algum Colaborador, o acesso aos arquivos será automaticamente bloqueado e a respectiva senha revogada. Para sistemas externos, a Sociedade deverá submeter uma solicitação de revogação de acesso imediatamente e assegurar-se de que os acessos sejam revogados.

O controle do acesso a arquivos confidenciais em meio físico é garantido através da segregação física da equipe de gestão de recursos de terceiros.

BACKUP

Todos os documentos arquivados no servidor da Sociedade são objeto de backup diário na nuvem, garantindo a segurança dos respectivos conteúdos e eventual responsabilização. O backup é armazenado da seguinte forma:

- a) **LIXEIRA SHAREPOINT MICROSOFT:** armazena até 500 (quinhentas) versões anteriores com tempo de retenção de 93 (noventa e três) dias.
- b) **BACKUP SHAREPOINT PELO IDRIVE CONECTADO DIRETAMENTE AO SHAREPOINT ONLINE:** o IDrive executa backups automatizados diariamente 3 (três) vezes, que são retidos por 30 (trinta) dias. Após esse prazo, o IDrive salva um dos 3 (três) backups diários por usuário. Após 90 (noventa) dias, o IDrive salva um backup semanal por usuário. Após 365 (trezentos e sessenta e cinco) dias, o IDrive salva um backup mensal por usuário.
- c) **E-MAIL:** está habilitado litígio de 5 (cinco) anos, preservando e-mails deletados.

Testes regulares de backup serão conduzidos para garantir a integridade e a eficácia dos procedimentos de recuperação.

Para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a equipe de Compliance deve assegurar a verificação da capacidade do potencial

prestador de serviço para o exercício da sua atividade analisando, no mínimo: (i) o acesso aos dados e às informações a serem processados ou armazenados pelo prestador de serviço; (ii) a confidencialidade, a integridade, a disponibilidade e a recuperação das informações e dados processados ou armazenados pelo prestador de serviço; (iii) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados.

Adicionalmente e caso entenda ser necessário, a Área de *Compliance* poderá solicitar o preenchimento do questionário de due diligence ANBIMA para contratação de serviço de processamento e armazenamento de dados e de computação em nuvem no país ou no exterior.

CÓPIA DE ARQUIVOS E INSTALAÇÕES

Todos os programas de computador utilizados pelos colaboradores devem ter sido previamente autorizados pelo responsável pela área de informática. Downloads de qualquer natureza podem ser realizados, desde que de forma justificada.

A cópia de arquivos e instalação de programas em computadores deverá respeitar os direitos de propriedade intelectual pertinentes, tais como licenças e patentes.

É terminantemente proibido que os colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede e circulem em ambientes externos com estes arquivos, salvo se em prol da execução e do desenvolvimento dos negócios e dos interesses da Sociedade. Nestes casos, o colaborador que estiver na posse e guarda do arquivo será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Sociedade.

DESCARTE DE INFORMAÇÕES

O descarte de informações confidenciais deve observar as seguintes diretrizes:

- a) o conteúdo descartado deverá ser apagado e/ou as mídias devem ser destruídas, impossibilitando a sua recuperação, de modo que a informação não fique vulnerável a acesso não autorizado;
- b) os documentos físicos que contenham informação protegida devem ser triturados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura;
- c) a eliminação ou a destruição final das mídias ou documentos, realizada por terceiros, deve ser documentada; e

- d) dispositivos de memória e dispositivos de armazenamento (por exemplo laptops, dispositivos USB, discos rígidos portáteis, tablets, smartphones) desativados pela Sociedade devem ser apagados de modo que a informação protegida que neles havia seja irrecuperável.

REDUNDÂNCIA

Além das cópias de segurança acima, outros recursos de TI são redundantes. Em caso de pane e indisponibilidade de acesso físico ao local de trabalho, a equipe poderá acessar as informações na nuvem.

SUPORTE E MONITORAMENTO

Em caso de pane da rede ou em alguma estação de trabalho, o fato deverá ser imediatamente comunicado à Área de *Compliance*, que providenciará que seja acionado o suporte externo necessário.

O sistema eletrônico utilizado pela Sociedade está sujeito à revisão e monitoramento a qualquer época sem aviso ou permissão, de forma a detectar qualquer irregularidade na transferência de informações, seja interna ou externamente.

Qualquer suspeita ou conhecimento de violação desta Política ou incidente de segurança da informação deve ser objeto de informação ao Compliance para que sejam tomadas as devidas providências com relação à apuração dos fatos, mitigação de eventuais riscos, implementação de procedimentos corretivos e responsabilização dos envolvidos.

Periodicamente e sem aviso prévio, poderão ser realizadas inspeções nos computadores para averiguação de downloads impróprios, não autorizados ou gravados em locais indevidos.

TESTES PERIÓDICOS

A Tane possui um eficiente sistema de proteção aos seus sistemas operacionais, o que inclui a instalação de programas antivírus em todos seus computadores e equipamentos. Vulnerabilidades nos computadores são frequentemente monitoradas e notificadas pelo Microsoft Defender de forma automática.

Toda a documentação arquivada no repositório eletrônico da Tane pode ser controlada remotamente, de forma que pode ser eliminada à distância, fornecendo proteção às informações confidenciais da Sociedade nas hipóteses de ataques ao sistema ou à própria sede da Sociedade.

IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS CIBERNÉTICOS

Considerando a atividade de gestão profissional de recursos de terceiros desempenhada pela Sociedade são essenciais todos os recursos tecnológicos necessários ao processo de análise, investimento e desinvestimento, tais como: (i) compra e venda de ativos para as carteiras sob gestão; e (ii) acesso aos sistemas de informação.

Diante da possibilidade de invasores utilizarem (i) *Malware*; (ii) Engenharia social; (iii) *Pharming*; (iv) *Phishing*; (v) *Vishing*; (vi) *Smishing*; (vii) Acesso pessoal; (viii) Ataques de DDoS (distributed denial of service) e *botnets*; e (ix) Invasões (*advanced persistent threats*), a Sociedade adota ações de prevenção e proteção, nos termos do Capítulo seguinte.

AÇÕES DE PROTEÇÕES E PREVENÇÃO AOS RISCOS CIBERNÉTICOS

Os planos de ação e prevenção descritos neste Capítulo têm por objetivo mitigar e minimizar a possibilidade de ocorrência de um ataque cibernético, na tentativa de evitar que os riscos identificados se concretizem.

Neste sentido, a Sociedade ratifica a adoção de controles de acesso físico e lógico implementados em linha com a Política de Segurança da Informação adotada. Tais controles visam a identificação, autenticação e autorização de acesso pelos usuários a sistemas ou ativos da Sociedade, evitando o acesso por terceiros não autorizados.

Isto posto, todos os Colaboradores devem observar de forma estrita as rotinas relacionadas à definição de senhas de acesso aos sistemas e rede.

Os eventos de login e alteração de senhas são rastreáveis e auditáveis, sendo qualquer inconsistência ou inadequação com relação aos acessos recomendados pelo Diretor de Compliance reportada imediatamente. Especial atenção deverá ser envidada aos casos de desligamento ou gozo de férias de Colaboradores.

São adotadas as seguintes medidas preventivas para cada risco identificado:

Risco Interno	Ação de Proteção/Prevenção
Indisponibilidade dos arquivos	Redundância para assegurar a disponibilidade dos sistemas.
Perda de arquivos de usuários	Lixeira da Nuvem, 500 versões por 93 dias
Possibilitar acessos indevidos às aplicações restritas da empresa	Senhas cadastradas com alto nível de criticidade e segurança; Trilha de auditoria habilitada; Bloqueio de tela; Autenticação multifator.

Risco Externo	Ação de Proteção/Prevenção
Tentativa de invasão à rede interna	A empresa utiliza o XDR como solução de segurança para monitorar continuamente seus ativos digitais, detectar atividades suspeitas e prevenir ataques cibernéticos. A ferramenta emprega recursos avançados de detecção e resposta a incidentes, contribuindo para a proteção dos dados e da infraestrutura tecnológica da organização. Política de geolocalização ativada, permitindo acesso apenas do Brasil.

Todos os novos equipamentos e sistemas instalados na Sociedade devem contar com as configurações de proteção acima descritas, sendo realizado teste em ambientes de homologação e de prova antes do início da sua utilização.

Todos os programas de computador utilizados pelos Colaboradores devem ter sido previamente autorizados pelo responsável pela área de informática, sendo vedadas aplicações não autorizadas por meio de controles de execução de processos. Downloads de qualquer natureza podem ser realizados, desde que de forma justificada.

MECANISMOS DE SUPERVISÃO DA SEGURANÇA CIBERNÉTICA

São realizados os seguintes testes de verificação para fins de identificação de anomalias, detecção de ameaças, acessos, componentes ou dispositivos não autorizados.

São mantidos inventários atualizados de *hardware* e *softwares* utilizados pela Sociedade.

Sempre que houver alteração relevante na estrutura tecnológica da Sociedade serão realizadas análises de vulnerabilidade.

RESPOSTAS A INCIDENTES CIBERNÉTICOS

A Sociedade adota os seguintes planos de ação de resposta a incidentes em função das ameaças identificadas:

Ameaça Interna	Severidade (Classificação)	Plano de Ação
Perda de arquivo na rede ou arquivo corrompido.	Alto	Restauração de arquivo no backup.
Falha no backup	Alto	Tratativa da falha e novo agendamento de backup.

Compartilhamento de senhas.	Alto	Treinamento sobre as práticas de segurança.
-----------------------------	------	---

Ameaça Externa	Severidade (Classificação)	Plano de Ação
Tentativa de invasão	Alto	Acionar o time de Segurança da Informação para análise de logs do firewall e mitigação da tentativa de invasão.
<i>Phishing</i>	Alto	Varredura do antivírus; Troca de senha; Verificação da máquina do usuário e Análise da integridade do Sistema Operacional da máquina do usuário.
Colaboradores desligados ainda com seus usuários ativos na empresa	Alto	Revisão dos acessos dos usuários e manter o log ativo.

Compete à Equipe de Compliance a comunicação da contingência aos demais Colaboradores da Sociedade, orientando-os sobre a postura e providências cabíveis, de acordo com a natureza e severidade da contingência, em observância do Plano de Continuidade de Negócios.

Cabe à Equipe de Compliance desenvolver relatórios acerca dos danos ocorridos, percentual das atividades afetadas, impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente. Tais relatórios deverão ser submetidos à Diretoria da Sociedade que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

Após o retorno à normalidade, na tentativa de evitar incidentes da mesma qualidade, a Sociedade estudará procedimentos preventivos a serem implementados e incluídos neste plano de continuidade de negócios.

PROGRAMA DE TREINAMENTO

A Sociedade conta com um programa de treinamento dos Colaboradores que tenham acesso a

informações confidenciais, na forma descrita em seu Manual de Compliance. Nos treinamentos promovidos serão repassados os cuidados com segurança cibernética, em linha com a presente Política.

DISPOSIÇÕES GERAIS E ENFORCEMENT

A cada 2 (dois) anos, ou em prazo inferior, se necessário, deverão ser revistos os termos e condições desta Política pelo Diretor de *Compliance* e de Prevenção à Lavagem de Dinheiro da Tane.

Todos os Colaboradores deverão receber uma cópia atualizada desta Política quando de seu ingresso na Sociedade, além de receber treinamento por parte do Diretor de *Compliance* e de Prevenção à Lavagem de Dinheiro, que deverá se manter à disposição do Colaborador para sanar eventuais dúvidas.

A Sociedade informará os Colaboradores quanto a qualquer alteração e/ou atualização realizada na presente Política.

A título de enforcement, vale notar que a não observância dos dispositivos da presente Política resultará em advertência, suspensão, demissão ou exclusão por justa causa, conforme a gravidade e a reincidência na violação, sem prejuízo das penalidades civis e criminais.