SARFATY ASSET GESTÃO DE RECURSOS LTDA

47.813.099/0001-04

POLÍTICA CIBERSEGURANÇA E PLANO DE CONTINUIDADE DE NEGÓCIOS

Março 2026

É vedada a cópia, reprodução, alteração e distribuição desse documento sem prévia e expressa autorização da Sarfaty Asset Gestão de Recursos LTDA.

1. OBJETIVO

A Política de Cibersegurança e Plano de Continuidade de Negócios das empresas do Grupo Sarfaty estabelece as diretrizes estratégicas para assegurar a proteção, integridade, disponibilidade, autenticidade, rastreabilidade, segurança e confidencialidade das informações sob sua custódia, controle, tratamento ou de sua propriedade. O objetivo central é implementar mecanismos eficazes de prevenção, detecção, monitoramento, recuperação e resposta a incidentes cibernéticos, mitigando vulnerabilidades e garantindo a resiliência operacional do Grupo.

Esta política reflete o compromisso inequívoco da alta administração com a segurança da informação e a privacidade de dados. O Grupo Sarfaty pauta suas operações na busca pela excelência e na garantia de confiança junto aos seus clientes, assegurando que o tratamento de informações sensíveis ocorra sob rígidos controles de segurança.

O Grupo Sarfaty reafirma seu compromisso com os pilares regulatórios e as melhores práticas do setor. Esta política está integralmente alinhada com as exigências legais vigentes, com destaque para:

- **Resolução CMN nº 4.893/2021 e suas alterações:** Observância aos requisitos de segurança cibernética e de contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.
- **Circular SUSEP nº 638/2021:** Cumprimento das disposições relativas à política de segurança cibernética a ser adotada pelas sociedades seguradoras, entidades abertas de previdência complementar, sociedades de capitalização e resseguradores locais.
- **Resolução CVM Nº 21/2021 e suas alterações:** observância dos deveres aplicáveis aos administradores de carteira de valores mobiliários, especialmente quanto à manutenção de controles internos adequados, políticas, procedimentos, governança, gestão de risco e monitoramento da aderência regulatória no exercício da atividade de gestão de recursos.
- **Lei nº 13.709/2018** - Lei Geral de Proteção de Dados Pessoais: observância dos princípios, bases legais, deveres de segurança, prevenção e demais obrigações aplicáveis ao tratamento de dados pessoais.
- **Resolução CVM Nº 175/2022 e suas alterações** - observância das regras aplicáveis à constituição, funcionamento, divulgação de informações e prestação de serviços para fundos de investimento.

As diretrizes aqui estabelecidas são de observância obrigatória por todas as empresas que compõem o Grupo Sarfaty, devendo ser integradas às rotinas operacionais e aos processos de gestão de risco e continuidade de negócios.

2. VIGÊNCIA

Esta política pode ser revisada anualmente ou, quando necessário, caso haja alguma mudança nas normas do Grupo Sarfaty, alteração de diretrizes de segurança da informação, objetivos de negócio ou se requerido pelo regulador local de alguma das Controladas.

3. PRINCÍPIO DE SEGURANÇA DA INFORMAÇÃO

O Grupo Sarfaty reconhece que os ativos de informação constituem os bens de maior relevância no mercado financeiro. Portanto, a gestão adequada, responsável e protegida dessas informações representa compromisso inalienável da organização. As diretrizes aqui estabelecidas fundamentam-se nos pilares da segurança da informação, visando assegurar a preservação, o uso controlado, o acesso autorizado, o compartilhamento seguro e a proteção das informações e dos dados sob sua responsabilidade.

O objetivo estratégico desta política é garantir a resiliência operacional por meio do monitoramento contínuo e do tratamento eficaz de incidentes cibernéticos, com base nos seguintes princípios fundamentais:

- **Confidencialidade:** Assegurar que o acesso à informação seja restrito exclusivamente a pessoas ou sistemas especificamente autorizados, prevenindo a exposição indevida.
- **Integridade:** Garantir que a informação seja mantida precisa e completa, protegendo-a contra modificações não autorizadas, sejam elas acidentais ou intencionais.
- **Disponibilidade:** Assegurar que a informação e os sistemas estejam prontamente acessíveis e operacionais para todos os usuários autorizados, sempre que necessário, de acordo com os níveis de serviço estabelecidos.

4. INFORMAÇÕES CONFIDENCIAIS

O acesso a informações confidenciais, incluindo dados pessoais coletados e armazenados pelo Grupo Sarfaty, é restrito a profissionais autorizados, cuja atuação seja indispensável para a prestação dos serviços contratados. O uso dessas informações é limitado às finalidades específicas de cada função, sendo obrigatória a observância das diretrizes de Classificação da Informação definidas pelo Grupo.

O Grupo Sarfaty reafirma seu compromisso com a privacidade e a proteção de dados em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e sua Política de Privacidade de Dados vigente.

Divulgação de Informações Confidenciais

O Grupo poderá realizar o compartilhamento ou a revelação de informações confidenciais exclusivamente nas seguintes hipóteses:

- **Obrigações Legais e Regulatórias:** Sempre que exigido por dispositivo legal, ato de autoridade competente, determinação judicial ou ordens emanadas por órgãos reguladores do mercado financeiro.
- **Gestão de Crédito e Proteção:** Aos órgãos de proteção e defesa de crédito, bem como a prestadores de serviços devidamente autorizados pelo Grupo para a salvaguarda de seus direitos e interesses creditórios.
- **Interinstitucional:** A outras instituições financeiras, respeitando estritamente os parâmetros legais aplicáveis. Nesta hipótese, ao titular dos dados é assegurado o direito de, a qualquer momento, solicitar a revogação de seu consentimento, conforme os termos previstos em lei.

5. ESTRUTURA DE GERENCIAMENTO DE CIBERSEGURANÇA

O gerenciamento dos controles de segurança objetiva assegurar que os procedimentos operacionais sejam desenvolvidos, implantados e mantidos ou modificados de acordo com os objetivos estabelecidos nesta política.

5.1 GESTÃO DE ACESSOS ÀS INFORMAÇÕES

Gestão de Acessos, Infraestrutura e Conscientização

O Grupo Sarfaty adota controles rigorosos para assegurar que a proteção da informação seja mantida em todas as esferas operacionais, conforme detalhado a seguir:

- **Controle de Acessos e Privilégios:** A concessão de acessos a sistemas e informações segue o **Princípio do Privilégio Mínimo**, garantindo que cada colaborador ou prestador de serviço possua apenas as permissões estritamente necessárias para o exercício de suas funções. Todos os acessos são monitorados, submetidos a revisões periódicas e revogados tempestivamente após o encerramento do vínculo contratual.
- **Segurança Física e Ambiental:** Equipamentos e instalações que processam informações críticas ou sensíveis são mantidos em ambientes seguros. Estas áreas

contam com controles de acesso rigorosos e proteção estrutural contra ameaças físicas e riscos ambientais, visando garantir a continuidade operacional.

- **Cultura de Segurança e Treinamento:** O Grupo mantém um programa contínuo de conscientização em segurança da informação. Colaboradores e terceiros são submetidos a treinamentos periódicos para a disseminação da cultura de cibersegurança, assegurando que o fator humano seja um elemento ativo na proteção dos ativos de informação do Grupo.

5.2 PROTEÇÃO DO AMBIENTE DO GRUPO

Gestão de Infraestrutura e Resposta a Incidentes

O Grupo Sarfaty estabelece controles rigorosos e define responsabilidades claras para a gestão e operação dos recursos de processamento de informações. Esta governança visa assegurar a integridade da infraestrutura tecnológica por meio de práticas eficazes de monitoramento, tratamento e resposta a incidentes.

Tais processos são estruturados para assegurar a resiliência dos ativos, focando em:

- **Gerenciamento de Riscos e Incidentes:** Implementação de processos contínuos de detecção e resposta a anomalias, garantindo a pronta mitigação de vulnerabilidades e a redução de riscos de falhas operacionais.
- **Administração Segura de Redes:** Aplicação de protocolos de segurança avançados na gestão de redes de comunicação, assegurando que o tráfego e a transmissão de informações ocorram em ambiente protegido, estável e auditável.

5.2.1 AUTENTICAÇÃO

Políticas de Controle de Acesso e Segregação de Funções

O acesso a todos os ambientes tecnológicos e ativos de informação do Grupo Sarfaty é estritamente condicionado à autorização expressa do proprietário da informação. A concessão desses acessos é regida pelos princípios fundamentais de **Segregação de Funções (SoD - Segregation of Duties)**, **Privilégio Mínimo** e pela respectiva **Classificação da Informação**, assegurando que os colaboradores tenham acesso apenas aos recursos indispensáveis para a execução de suas responsabilidades.

O processo de controle de acesso aos sistemas deve ser formalizado e observar os seguintes requisitos obrigatórios:

- **Identificação Individualizada e Rastreabilidade:** A utilização de credenciais de acesso deve ser estritamente individual e intransferível. Todos os acessos são

submetidos a monitoramento contínuo e estão sujeitos a bloqueios ou restrições, executados por meio de mecanismos automatizados e manuais.

- **Gestão de Ciclo de Vida do Acesso:** É obrigatória a revogação imediata de privilégios de acesso para colaboradores afastados, desligados ou que tenham sofrido alteração de função (movimentação interna), eliminando acessos residuais que não condizem com a nova realidade operacional.
- **Revisão Periódica:** As permissões concedidas devem ser objeto de revisões sistemáticas e periódicas, garantindo que a concessão de acessos permaneça alinhada com as necessidades atuais de negócio e os níveis de segurança estabelecidos.

5.2.2 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O Grupo Sarfaty mantém uma estratégia de **Defesa em Profundidade**, utilizando controles técnicos automatizados para a detecção proativa de ameaças e comportamentos anômalos no ambiente tecnológico. A identificação de possíveis incidentes é realizada por meio de uma camada de monitoramento que inclui:

- **Controles de Segurança de Perímetro e Endpoint:** Implementação de ferramentas de filtragem de conteúdo, sistemas de proteção contra códigos maliciosos (*Endpoint Detection and Response* - EDR), soluções de Antivírus de última geração e filtros AntiSpam avançados.
- **Detecção de Comportamentos Anômalos:** Utilização de ferramentas capazes de identificar desvios nos padrões de uso da infraestrutura, permitindo a pronta identificação de ameaças sofisticadas.
- **Fluxo de Resposta:** Todo incidente detectado, independentemente de sua severidade, deve ser submetido ao **Processo de Resposta a Incidentes** do Grupo, assegurando que o tratamento ocorra de forma padronizada, documentada e eficiente, visando a contenção, erradicação e recuperação dos serviços afetados.

5.2.3 PREVENÇÃO A VAZAMENTO DE INFORMAÇÕES

O Grupo Sarfaty implementa controles rigorosos de Prevenção contra Perda de Dados (DLP - Data Loss Prevention), visando assegurar a integridade e a confidencialidade dos ativos de informação. Esta estratégia tem como objetivo mitigar riscos de exfiltração, roubo, uso indevido ou vazamento não autorizado de dados confidenciais através da rede e de outros canais de comunicação.

O sistema de DLP opera de forma contínua, utilizando as seguintes capacidades:

- **Identificação e Classificação:** Monitoramento em tempo real para identificar dados classificados como confidenciais ou sensíveis dentro do tráfego de rede e endpoints.
- **Controle de Exfiltração:** Bloqueio automático de tentativas de transferência não autorizada de informações para destinos externos ou dispositivos não permitidos.
- **Mitigação de Riscos:** Aplicação de políticas que impedem o compartilhamento inadequado de dados por usuários não autorizados, garantindo que apenas processos e pessoas devidamente validadas possam interagir com informações críticas.

5.2.4 TESTES DE INTRUSÃO

Com o objetivo de validar a eficácia dos controles de segurança implementados e identificar vulnerabilidades antes que sejam exploradas, o Grupo Sarfaty estabelece a realização obrigatória de **Testes de Intrusão (Pentests)**. Estes exercícios de simulação de ataque devem ser executados, no mínimo, em periodicidade anual, abrangendo os seguintes escopos:

- **Pentest de Infraestrutura (Rede):** Avaliação técnica dos dispositivos, serviços e protocolos que compõem a arquitetura de rede do Grupo, visando identificar vulnerabilidades em servidores, firewalls e elementos de conectividade.
- **Pentest de Aplicação:** Inspeção detalhada das aplicações e sistemas de negócio, focada na detecção de falhas de lógica, injeções de código, quebras de autenticação e outros riscos específicos ao ciclo de vida de desenvolvimento de software (SDLC).
- **Abrangência:** Os testes devem considerar tanto o perímetro **externo** (exposição pública) quanto o ambiente **interno** (movimentação lateral dentro da rede corporativa), garantindo uma visão holística da postura de segurança.

Os resultados provenientes dessas avaliações devem ser formalmente reportados à gestão de segurança e à alta administração, acompanhados de um Plano de Ação para a correção (remediação) das vulnerabilidades identificadas, respeitando os prazos de criticidade estabelecidos.

5.2.5 VARREDURA DE VULNERABILIDADES

Para assegurar a resiliência dos ativos tecnológicos, o Grupo Sarfaty estabelece a execução sistemática de varreduras de segurança em seus ambientes de rede. O

objetivo é a identificação proativa de vulnerabilidades antes que sejam exploradas por ameaças cibernéticas.

A gestão do processo de vulnerabilidades seguirá as seguintes diretrizes:

- **Periodicidade das Varreduras:** As varreduras de redes internas e externas devem ser realizadas em cronogramas definidos, garantindo uma cobertura contínua dos ativos críticos.
- **Análise e Classificação de Criticidade:** Todas as vulnerabilidades identificadas devem ser catalogadas e classificadas de acordo com seu impacto potencial e probabilidade de exploração (ex: utilizando métricas como CVSS – *Common Vulnerability Scoring System*).
- **Plano de Remediação:** A priorização do tratamento deve obedecer ao nível de criticidade apurado, com prazos estabelecidos para a aplicação de correções (patches) ou medidas compensatórias.

5.2.6 CONTROLE CONTRA SOFTWARE MALICIOSO

Proteção de Ativos e Segurança de Endpoints

Para assegurar a integridade do ambiente tecnológico, todos os ativos — incluindo, mas não se limitando a estações de trabalho, servidores e dispositivos móveis — que estejam conectados à rede corporativa ou que acessem ativos de informação do Grupo Sarfaty, devem estar protegidos.

Esta proteção é regida pelas seguintes diretrizes:

- **Padronização de Soluções:** É obrigatória a instalação e manutenção de soluções de proteção (*Anti-malware/EDR*) homologadas e determinadas pela área de Segurança da Informação.
- **Compatibilidade e Cobertura:** A aplicação da solução de segurança é mandatória para todo ativo compatível. Casos de incompatibilidade técnica devem ser submetidos à avaliação da área de Segurança da Informação para a definição de controles compensatórios.
- **Manutenção Contínua:** É de responsabilidade da gestão de TI garantir que os agentes de proteção estejam ativos, atualizados (versões e assinaturas) e devidamente configurados conforme as políticas de segurança vigentes.

5.2.7 CRIPTOGRAFIA

Criptografia e Proteção de Dados Sensíveis

Toda e qualquer solução de criptografia adotada no ambiente tecnológico do Grupo Sarfaty deve ser submetida à aprovação da área de Segurança da Informação, devendo observar estritamente as diretrizes internas de governança e os padrões técnicos exigidos pelos órgãos reguladores competentes.

O uso de criptografia deve ser aplicado conforme os seguintes critérios:

- **Padrões de Algoritmos:** A escolha de algoritmos deve basear-se em padrões reconhecidos internacionalmente e pela regulamentação setorial, garantindo a robustez contra tentativas de quebra ou acesso indevido.
- **Gestão de Chaves:** O ciclo de vida das chaves criptográficas (geração, armazenamento, distribuição, renovação e destruição) deve ser formalizado e monitorado, assegurando que o acesso às chaves seja restrito apenas a sistemas ou pessoas autorizadas.
- **Proteção em Repouso e em Trânsito:** A criptografia deve ser aplicada tanto para dados em repouso (*at-rest*), garantindo a proteção de bancos de dados e dispositivos de armazenamento, quanto para dados em trânsito (*in-transit*), utilizando protocolos seguros para toda a comunicação de rede.

5.2.8 RASTREABILIDADE

Para assegurar a rastreabilidade integral das atividades dentro do ambiente tecnológico do Grupo Sarfaty, a implantação de trilhas de auditoria automatizadas é mandatória em todos os componentes de sistemas e infraestrutura.

O sistema de auditoria deve ser capaz de registrar, armazenar e permitir a reconstrução dos seguintes eventos:

- **Gestão de Identidade e Acesso:** Registro detalhado de todas as tentativas de autenticação, distinguindo êxitos de falhas, com o objetivo de identificar potenciais tentativas de acesso não autorizado ou ataques de força bruta.
- **Monitoramento de Acesso à Informação:** Rastreamento de consultas e visualizações realizadas sobre ativos de informação, garantindo a visibilidade de quem acessou, quando e quais dados foram consultados.
- **Rastreabilidade de Ações de Sistema:** Registro completo das operações executadas pelos usuários, incluindo, mas não se limitando à criação, modificação, exclusão de objetos do sistema, alterações em configurações críticas e comandos administrativos.

A integridade e a guarda desses registros devem seguir políticas de retenção definidas, garantindo que as trilhas permaneçam disponíveis para auditorias internas,

externas e demandas regulatórias, de forma protegida contra alterações não autorizadas.

5.2.9 SEGMENTAÇÃO DE REDE

5.2.10 DESENVOLVIMENTO SEGURO

A segurança da infraestrutura de rede e dos processos de desenvolvimento deve seguir protocolos estritos de isolamento e governança de mudanças, conforme as diretrizes abaixo:

- **Isolamento de Rede:** Computadores conectados à rede corporativa devem estar protegidos por mecanismos de defesa de perímetro, sendo vedada a exposição direta de *endpoints* à internet.
- **Restrição de Acesso Remoto:** É estritamente proibida a conexão direta de redes de terceiros aos servidores do Grupo utilizando protocolos de controle remoto (ex: RDP, SSH direto). O acesso remoto para fins de manutenção deve ocorrer exclusivamente por meio de túneis seguros, VPNs com autenticação multifator ou soluções de *Jump Server* homologadas pela Segurança da Informação.
- **Governança de Alterações em Ativos de Rede:** Qualquer solicitação para criação, alteração ou exclusão de regras de firewall e demais ativos de rede deve ser formalmente submetida à área de Segurança da Informação. O processo deve seguir o fluxo de:
    1. **Requisição:** Submissão do pedido detalhando o propósito e a criticidade da regra.
    2. **Análise de Risco:** Avaliação técnica pela Segurança da Informação quanto aos impactos à segurança e conformidade.
    3. **Execução:** Após aprovação formal, o pedido é encaminhado à equipe de TI para implementação, com a devida evidência de mudança (log).

5.2.11 COPIAS DE SEGURANÇA (BACKUP)

Gestão de Backups e Continuidade de Negócios

O Grupo Sarfaty adota uma estratégia estruturada de backup para assegurar a resiliência operacional e garantir que, na eventualidade de incidentes, o impacto sobre a disponibilidade e integridade das informações seja mitigado.

O processo de backup é regido pelas seguintes diretrizes:

- **Periodicidade e Abrangência:** Os backups são executados em ciclos periódicos definidos com base na criticidade de cada ativo de informação, garantindo que os RPOs (*Recovery Point Objectives*) e RTOs (*Recovery Time Objectives*) estejam alinhados às necessidades do negócio.
- **Integridade e Recuperabilidade:** O processo de backup inclui a validação periódica da integridade dos dados armazenados, assegurando que as informações possam ser restauradas de forma íntegra, confiável e tempestiva quando necessário.
- **Segurança no Armazenamento:** As cópias de segurança são mantidas em ambientes seguros, protegidas contra acessos não autorizados e, quando aplicável, armazenadas fora da sede principal (*off-site*) para assegurar a recuperação frente a desastres físicos.

5.3 CONTINUIDADE DOS NEGÓCIOS

O Grupo Sarfaty entende a continuidade de negócios como uma disciplina estratégica essencial para a preservação de valor e a resiliência operacional. O objetivo central deste processo é garantir que, diante de incidentes críticos ou desastres, os impactos sejam mitigados a níveis aceitáveis, assegurando a retomada das operações essenciais dentro dos prazos críticos estabelecidos.

Diretrizes de Continuidade e Recuperação

O planejamento de continuidade é sustentado pelos seguintes pilares:

- **Mapeamento e Análise de Impacto (BIA):** O Grupo realiza continuamente o mapeamento dos processos críticos e a Análise de Impacto nos Negócios (*Business Impact Analysis*), identificando quais ativos de informação e sistemas são vitais para a operação.
- **Ciclo de Recuperação de Desastres (DRP):** São realizados testes periódicos de recuperação de desastres para validar a eficácia dos procedimentos de restauração, incluindo cenários específicos de ataques cibernéticos (como ataques de *ransomware*).
- **Continuidade em Nuvem:** Os serviços contratados em nuvem estão integralmente cobertos pelo plano de continuidade, observando as responsabilidades compartilhadas entre o Grupo e o provedor de serviços, garantindo a disponibilidade e a integridade dos dados em cenários de indisponibilidade regional ou de serviço.
- **Segurança no Desenvolvimento (DevSecOps):** A segurança cibernética é integrada ao ciclo de vida de desenvolvimento de sistemas (*Secure SDLC*),

garantindo que as premissas de proteção sejam nativas à arquitetura das soluções tecnológicas.

5.4 PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

Em estrita observância à Resolução CMN nº 4.893/2021, CVM nº 21/2021, CVM nº 175/2022 e suas alterações, ao Código Anbima, Lei nº 13.709/2018 e à Circular SUSEP nº 638/2021, o Grupo Sarfaty estabelece procedimentos de governança robustos para a contratação e gestão de serviços de processamento, armazenamento de dados e computação em nuvem.

O Grupo assegura a aderência integral às normas vigentes por meio de:

- **Due Diligence de Terceiros:** Avaliação criteriosa dos provedores de serviços, garantindo que suas práticas de segurança, resiliência e proteção de dados sejam compatíveis com os requisitos regulatórios e com as políticas internas do Grupo.
- **Governança de Contratos:** Monitoramento contínuo das obrigações contratuais, assegurando que o provimento de serviços em nuvem contemple os controles de segurança necessários, a segregação de responsabilidades e a garantia de acesso às informações para auditorias e fiscalizações.
- **Gestão de Riscos Operacionais:** Implementação de controles específicos para mitigar riscos associados à terceirização de tecnologia, assegurando que a qualidade, a segurança e a disponibilidade dos serviços sejam mantidas em conformidade com as normas legais, regulatórias, autorregulatórias e políticas internas aplicáveis.

6. PRINCIPAIS RECOMENDAÇÕES DE SEGURANÇA AOS CLIENTES E USUÁRIOS

6.1 AUTENTICAÇÃO E SENHA

A segurança do ambiente tecnológico do Grupo Sarfaty é uma responsabilidade compartilhada. Todo colaborador ou prestador de serviço é integralmente responsável pelos atos executados por meio de seu identificador (login) e senha, que são pessoais, intransferíveis e únicos.

Para garantir a integridade da autenticação e a proteção aos recursos de tecnologia, são estabelecidas as seguintes diretrizes de uso obrigatório:

- **Gestão de Credenciais:** O usuário deve assegurar a confidencialidade de sua senha, evitando o registro ou anotação em qualquer meio físico ou digital. Senhas devem ser complexas, compostas por caracteres variados e de difícil dedução.
- **Autenticação Segura:** É mandatória a utilização de **Autenticação Multifator (MFA)** sempre que disponibilizada pelo sistema, garantindo uma camada adicional de segurança além da senha.
- **Integridade da Sessão:** É proibido compartilhar equipamentos logados com terceiros. O usuário deve realizar o bloqueio da estação de trabalho sempre que se ausentar, prevenindo acessos não autorizados.
- **Resposta a Incidentes de Acesso:** Em caso de suspeita de comprometimento da credencial, o usuário deve proceder com a alteração imediata da senha e reportar o incidente à área de Segurança da Informação.

6.2 ENGENHARIA SOCIAL

Segurança de Endpoints e Prevenção à Engenharia Social

A proteção do ambiente tecnológico é uma responsabilidade compartilhada. Para assegurar que o acesso aos serviços do Grupo Sarfaty ocorra de forma segura, todos os usuários devem observar as diretrizes de higiene digital e prevenção contra ameaças:

- **Proteção e Atualização de Ativos:** É obrigatória a manutenção de soluções de proteção (*antivírus* e *anti-malware*) devidamente instaladas, ativas e atualizadas em todos os dispositivos utilizados para acessar os serviços do Grupo. Adicionalmente, o sistema operacional e os softwares instalados devem estar na versão mais recente, com todos os pacotes de correção de segurança (*patches*) aplicados.
- **Prevenção contra Engenharia Social:** O Grupo adota uma postura de vigilância ativa contra tentativas de engenharia social — técnica na qual agentes maliciosos utilizam a manipulação psicológica, a exploração da confiança ou a indução ao erro para obter informações confidenciais ou viabilizar acessos não autorizados.
- **Diretrizes de Segurança:**
  - **Desconfiança Crítica:** Jamais compartilhe credenciais, senhas ou informações sigilosas via e-mail, telefone ou mensagens, mesmo que a solicitação pareça legítima ou urgente.
  - **Verificação de Identidade:** Sempre verifique a legitimidade de qualquer comunicação que solicite ações críticas ou acesso a dados sensíveis, utilizando os canais oficiais de comunicação do Grupo.

- **Notificação Imediata:** Caso identifique qualquer tentativa de manipulação, solicitação suspeita ou suspeita de golpe, reporte o ocorrido imediatamente à área de Segurança da Informação.

6.2.1 PHISHING

Prevenção contra Phishing e Fraudes Cibernéticas

O *Phishing* é uma técnica de engenharia social amplamente utilizada por cibercriminosos para a obtenção ilícita de informações sensíveis — como credenciais de acesso, dados bancários, números de documentos (CPF/CNPJ) e informações de cartões de crédito — mediante o envio de comunicações fraudulentas, frequentemente por e-mail, mensagens instantâneas ou redes sociais.

O Grupo Sarfaty considera o *Phishing* uma ameaça crítica à integridade de seus dados e orienta todos os seus colaboradores e terceiros sobre as táticas comuns utilizadas por fraudadores:

- **Apelos Psicológicos e Gatilhos Mentais:** As mensagens frequentemente utilizam estratégias de persuasão para atrair a atenção do usuário, como a promessa de vantagens financeiras indevidas, curiosidade sobre assuntos sensacionais, ou falsos apelos de caridade.
- **Falsificação de Identidade (Spoofing):** Os criminosos simulam a comunicação oficial de instituições de confiança, como bancos, órgãos governamentais e grandes empresas de e-commerce, utilizando logotipos, tom de voz e endereços de remetente falsificados para conferir legitimidade à fraude.
- **Coleta de Dados e Instalação de *Malware*:** O objetivo final dessas comunicações é induzir o usuário a:
  - Preencher formulários fraudulentos que capturam dados pessoais e financeiros em tempo real.
  - Realizar o download e a execução de arquivos ou *softwares* maliciosos, projetados para monitorar atividades, capturar teclas digitadas (*keyloggers*) ou roubar informações sigilosas instaladas no dispositivo.

6.2.2 SPAM

Gestão de Conteúdo Indesejado (Spam)

O *Spam* é caracterizado pelo envio massivo de comunicações eletrônicas não solicitadas, cuja finalidade primária é a publicidade invasiva. Entretanto, o Grupo Sarfaty reconhece o *Spam* não apenas como uma inconveniência, mas como um vetor crítico de ameaças cibernéticas.

A organização adota controles para a mitigação dos riscos associados a essas comunicações, considerando que o *Spam* é frequentemente utilizado como porta de entrada para:

- **Disseminação de Códigos Maliciosos:** Utilização de mensagens massivas para a propagação de *malware*, *ransomware* e outros artefatos que comprometem a integridade dos sistemas.
- **Veiculação de Golpes e Fraudes:** Disseminação de esquemas fraudulentos, *scams* e ofertas de venda ilegal de produtos ou serviços, visando induzir o usuário ao erro.
- **Comprometimento de Disponibilidade:** O volume excessivo de mensagens indesejadas pode sobrecarregar infraestruturas de comunicação, impactando a produtividade e a disponibilidade dos serviços de e-mail corporativo.

Diretrizes de Segurança: O Grupo implementa filtros de proteção avançados para a identificação e bloqueio de *Spam*. Aos usuários, é estritamente proibido interagir com remetentes desconhecidos ou clicar em links contidos em e-mails que apresentem características de *Spam*, sendo obrigatório o encaminhamento destes itens à equipe de Segurança da Informação ou a utilização da ferramenta de denúncia interna disponível.

6.2.3 FALSO CONTATO TELEFÔNICO

O Grupo Sarfaty reconhece que os ativos de informação são constantemente alvos de tentativas de obtenção ilícita. Entende-se por "fraude" qualquer técnica utilizada por agentes maliciosos com o objetivo de capturar dados sensíveis — incluindo, mas não se limitando a: dados de identificação pessoal, credenciais de acesso, senhas, códigos de autenticação (tokens), números de cartões e identificadores únicos de hardware (como o IMEI de dispositivos móveis).

A organização mantém vigilância e controles contra as táticas mais comuns de obtenção de dados:

- **Manipulação Psicológica:** Uso de técnicas de persuasão para induzir o usuário a revelar voluntariamente informações confidenciais ou a realizar ações que comprometam a segurança de seus dispositivos.
- **Coleta de Identificadores Técnicos:** Tentativas de capturar metadados do dispositivo, como o IMEI, para fins de clonagem de identidade, interceptação de comunicações ou realização de transações em nome do usuário legítimo.
- **Exploração de Vulnerabilidades de Autenticação:** Tentativas de obter tokens de autenticação ou códigos de uso único, essenciais para transpor camadas de segurança (como o MFA).

Postura Defensiva do Grupo:

O Grupo Sarfaty enfatiza que **jamais solicita senhas, tokens de autenticação ou códigos de identificação de dispositivos (IMEI)** por meio de e-mail, telefone, SMS ou redes sociais. Qualquer solicitação dessa natureza deve ser considerada uma tentativa de fraude e comunicada imediatamente à área de Segurança da Informação.

7. COMUNICAÇÃO

O Grupo Sarfaty adota uma política de **tolerância zero** para o descumprimento das diretrizes estabelecidas neste documento. A adesão a esta Política de Cibersegurança e Continuidade de Negócios é obrigatória para todos os colaboradores, prestadores de serviço e parceiros de negócio.

Investigação e Consequências

Qualquer indício de irregularidade, desvio de conduta, falha técnica ou tentativa de violação destas diretrizes será submetido a uma investigação interna rigorosa. A comprovação de descumprimento poderá resultar em medidas disciplinares, conforme o Código de Ética e a legislação vigente, sem prejuízo de eventuais ações nas esferas cível e criminal.

Canal de Comunicação e Reporte

É dever de todos os integrantes do Grupo Sarfaty zelar pela segurança dos nossos ativos de informação. Qualquer incidente, suspeita de fraude ou irregularidade observada deve ser comunicada **imediatamente** através dos nossos canais oficiais de atendimento.

O Grupo assegura o tratamento confidencial de todas as comunicações recebidas, garantindo a proteção contra qualquer forma de retaliação aos colaboradores que reportarem, de boa-fé, suspeitas de irregularidades, desvio de conduta ou violações às diretrizes desta Política.

8. DEFINIÇÕES

Para fins desta política, entende-se por "Informação Confidencial" toda e qualquer informação, dado, documento, registro ou conteúdo, escrito, verbal, eletrônico ou de qualquer outro modo apresentado, tangível ou intangível, patenteada ou não, que seja de propriedade do Grupo Sarfaty ou que esteja sob sua responsabilidade, posse, controle, tratamento ou utilização. Este conceito compreende, mas não se limita a, informações de natureza técnica, operacional, comercial, financeira e jurídica.

Abrangência do Escopo

O escopo da confidencialidade inclui, especificamente:

- **Propriedade Intelectual e *Know-How*:** Invenções, fórmulas, processos, métodos de contabilidade, códigos-fonte, diagramas, modelos, projetos, especificações e experiências acumuladas.
- **Dados de Negócios e Estratégia:** Planos de negócios (*business plans*), orçamentos, estruturas de preços, estratégias comerciais, planos de expansão, marketing e vendas.
- **Informações de Terceiros e Stakeholders:** Dados de clientes, parceiros, fornecedores e colaboradores.
- **Suportes de Armazenamento:** Todas as formas de registro, incluindo discos, fitas, meios digitais e documentação física.

9. Vigência e Atualização

9.1 A presente política será revisada anualmente e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo em decorrência de: (i) mudanças regulatórias e eventuais deficiências encontradas; e (ii) testes de aderência/eficácia das métricas e procedimentos aqui previstos.

9.2 Essa política revoga todas as versões anteriores e passa a vigorar a partir da data de sua aprovação pelo Comitê de Riscos e de Compliance.

9.3 Controle de Versão:

Data	Versão	Responsável
20/01/26	1.0	Diretoria de Gestão e Diretoria de Compliance, Risco e PLD/FTP.