GRUPO SARFATY

Sarfaty Asset Gestão de Recursos Ltda.
CNPJ 47.813.099/0001-04

RELATÓRIO DE ADERÊNCIA EM SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

Em atendimento às diretrizes da ANBIMA e à Resolução CVM nº 175/2022
Referência: Políticas Internas SFT-07 e SFT-13

Para: Área Asset / Diretoria de Compliance e Gestão
De: Departamento de Tecnologia e Segurança da Informação
Data: São Paulo, [data]
Ref.: Protocolo / Solicitação ANBIMA nº ____

1. APRESENTAÇÃO

O presente relatório tem por finalidade demonstrar a postura de segurança da informação e cibersegurança adotada pelo Grupo Sarfaty, em linha com as diretrizes autorregulatórias aplicáveis da ANBIMA, com as disposições da Resolução CVM nº 175/2022 e suas alterações, que estabelece as regras gerais sobre fundos de investimento e os requisitos de governança, bem como a Resolução CVM nº 21/2021, no que se refere aos deveres de controles internos, políticas, procedimentos e segurança cibernética aplicáveis aos gestores.

As informações aqui apresentadas são fundamentadas nas Políticas Internas SFT-07 (Política de Segurança da Informação) e SFT-13 (Política de Cibersegurança e Continuidade de Negócios), ambas vigentes.

O Grupo Sarfaty reafirma seu compromisso com a proteção dos ativos de informação, a privacidade de dados de seus clientes e parceiros, integridade e a resiliência operacional, por meio de uma estrutura de controles técnicos e de governança continuamente monitorada e aprimorada.

Este relatório deve ser interpretado como documento técnico de demonstração dos controles existentes, da governança adotada e das iniciativas de aprimoramento contínuo em segurança da informação e cibersegurança.

2. ESTRUTURA DE GOVERNANÇA EM SEGURANÇA DA INFORMAÇÃO

O Grupo Sarfaty mantém uma estrutura híbrida de gestão de segurança da informação, composta por equipe interna de Tecnologia da Informação e por empresa especializada terceirizada, responsável pela operação, monitoramento e aprimoramento dos controles de segurança. Essa estrutura garante cobertura técnica especializada em regime contínuo.

A gestão de segurança é sustentada pelas seguintes políticas formalmente aprovadas:

- **SFT-07:** Política de Segurança da Informação estabelece os princípios, diretrizes e responsabilidades para proteção dos ativos de informação do Grupo.
- **SFT-13:** Política de Cibersegurança e Continuidade de Negócios define os controles técnicos, processos de resposta a incidentes e diretrizes de continuidade operacional.

3. CONTROLES DE SEGURANÇA IMPLEMENTADOS

A seguir são descritos os controles técnicos e organizacionais atualmente implementados pelo Grupo Sarfaty, com indicação das ferramentas e soluções em operação.

3.1 Proteção de Endpoints e Detecção de Ameaças

Ferramentas: *CrowdStrike Falcon Complete (EDR) + CrowdStrike Identity*

O Grupo Sarfaty opera o CrowdStrike Falcon com o serviço gerenciado CrowdStrike Complete, provendo proteção de endpoints em tempo real por meio de tecnologia de Endpoint Detection and Response (EDR). A solução realiza monitoramento contínuo de comportamentos anômalos, detecção proativa de ameaças e resposta automatizada a incidentes em estações de trabalho, servidores e dispositivos corporativos. O módulo CrowdStrike Identity complementa a cobertura com proteção específica contra ataques baseados em credenciais e movimentação lateral.

Referência: SFT-13, seção 5.2.2 e 5.2.6 | SFT-07, seção Gestão de Incidentes e Controle contra Software Malicioso

3.2 Gestão de Identidade, Acesso e Autenticação Multifator

Ferramentas: *Active Directory (AD) + Microsoft Entra ID + Microsoft Entra Connect + Microsoft Intune + Microsoft 365 (M365)*

O gerenciamento de identidades do Grupo Sarfaty é estruturado em uma arquitetura híbrida composta pelo Active Directory (AD) corporativo, que funciona como diretório principal e fonte de verdade das contas de usuário, sincronizado em tempo real com o Microsoft Entra ID por meio do Microsoft Entra Connect. Essa integração permite que as identidades gerenciadas no AD se beneficiem das capacidades avançadas de segurança do Entra ID, incluindo políticas de acesso condicional, monitoramento de identidades e integração nativa com o ecossistema Microsoft 365. A Autenticação Multifator (MFA) está ativa para todos os usuários da organização, aplicada via Entra ID como requisito obrigatório de acesso aos ambientes corporativos e ao M365. A concessão de acessos segue o Princípio do Privilégio Mínimo e o conceito de Segregação de Funções (SoD). A gestão de dispositivos corporativos — incluindo estações de trabalho e dispositivos móveis — é realizada centralmente pelo Microsoft Intune, que assegura conformidade de configuração, aplicação de políticas de segurança e capacidade de revogação remota de acesso em caso de perda, roubo ou desligamento. A revogação de privilégios é realizada de forma imediata nos casos de desligamento ou alteração de função.

Referência: SFT-13, seção 5.2.1 | SFT-07, seção Autenticação e Gestão de Acesso

3.3 Segurança de E-mail e Proteção contra Phishing

Ferramentas: *Check Point Harmony Email & Collaboration*

A proteção do ambiente de e-mail corporativo é provida pela solução Harmony (Check Point), que opera com filtros avançados de antispam, antiphishing e bloqueio de anexos e links maliciosos. A solução protege o ambiente Microsoft 365 contra ameaças de engenharia social, spoofing e disseminação de malware por e-mail, alinhando-se às diretrizes de prevenção de fraudes estabelecidas nas políticas internas.

Referência: SFT-13, seção 6.2.1 e 6.2.2 | SFT-07, seção Prevenção contra Phishing e Gestão de SPAM

3.4 Segurança de Rede e Controle de Perímetro

Ferramentas: *Fortinet FortiGate (Firewall + Web Filter + WAF + VPN SSL/IPSec)*

O perímetro de rede corporativa é protegido por firewall Fortinet FortiGate, com políticas de segurança ativas, filtragem de conteúdo web (Web Filter) e Web Application Firewall (WAF) para proteção das aplicações expostas. O acesso remoto é provido exclusivamente via VPN SSL corporativa, com IPSec em processo de implantação para reforço adicional. Conexões diretas via RDP ou SSH sem túnel seguro são expressamente proibidas pelas políticas internas. Toda criação, alteração ou exclusão de regras de firewall passa por processo formal de requisição, análise de risco e aprovação pela área de Segurança da Informação.

Referência: SFT-13, seção 5.2.9 e 5.2.10 | SFT-07, seção Desenvolvimento Seguro

3.5 Computação em Nuvem, Armazenamento de Dados e Gestão de Credenciais

Ferramentas: *Amazon Web Services (AWS) + Microsoft Azure Key Vault + Azure DevOps Boards + Microsoft 365 (M365)*

Os serviços de processamento e armazenamento de dados do Grupo Sarfaty são suportados pela Amazon Web Services (AWS) e pelo Microsoft 365 (M365), contratados em observância estrita à Resolução CMN nº 4.893/2021 e sua alteração 5.274/2025, que regula a terceirização de serviços de tecnologia por instituições do mercado financeiro. O Microsoft Azure é utilizado de forma específica e restrita para dois propósitos: (i) Azure Key Vault, que funciona como cofre centralizado e seguro para armazenamento de credenciais de APIs e senhas de contas de serviço, com controle de acesso granular e auditoria de uso; e (ii) Azure DevOps Boards, utilizado como ferramenta de governança e rastreabilidade das demandas, mudanças e projetos da área de Tecnologia. O Grupo não possui infraestrutura de máquinas virtuais, instâncias ou aplicações hospedadas no Azure. A contratação de todos os provedores contempla avaliação de suas práticas de segurança, resiliência e conformidade regulatória (due diligence), com responsabilidades formalmente estabelecidas em contrato e garantia de acesso às informações para fins de auditoria e fiscalização.

Referência: SFT-13, seção 5.4 | CMN 4.893/2021 e suas alterações.

3.6 Cópias de Segurança (Backup)

Ferramentas: *AWS (armazenamento gerenciado em nuvem)*

O Grupo Sarfaty mantém rotina estruturada de cópias de segurança, executadas em ciclos periódicos e armazenadas no ambiente de nuvem AWS, garantindo proteção off-site e alta disponibilidade. O processo contempla validação periódica da integridade dos dados armazenados para assegurar a recuperabilidade das informações. Os backups são mantidos em ambientes seguros, com controle de acesso restrito.

Referência: SFT-13, seção 5.2.11 | SFT-07, seção Cópias de Segurança

3.7 Rastreabilidade e Trilhas de Auditoria

Ferramentas: *CrowdStrike Falcon + Microsoft Entra ID + FortiGate + AWS CloudTrail + Azure Key Vault (audit log)*

O ambiente tecnológico do Grupo Sarfaty conta com trilhas de auditoria automatizadas em seus principais componentes de infraestrutura, registrando eventos de autenticação (êxitos e falhas), operações administrativas, alterações de configurações e acesso a recursos de rede. Os logs gerados pelo CrowdStrike, Entra ID, FortiGate e pelos provedores de nuvem permitem a rastreabilidade das ações executadas no ambiente, em suporte a auditorias internas, externas e demandas regulatórias.

Referência: SFT-13, seção 5.2.8 | SFT-07, seção Rastreabilidade

4. CONTROLES EM PROCESSO DE IMPLANTAÇÃO OU APRIMORAMENTO

O Grupo Sarfaty reconhece que a maturidade em segurança da informação é um processo contínuo. Os itens abaixo encontram-se em fase de implantação ou aprimoramento formal, com iniciativas em andamento:

- **Testes de Intrusão (Pentest):** A realização de testes de intrusão anuais, cobrindo infraestrutura e aplicações (perímetro externo e ambiente interno), está prevista nas políticas internas e em processo de contratação junto a empresa especializada.
- **Continuidade de Negócios (BIA/DRP):** O Grupo Sarfaty reconhece a necessidade de formalização do BIA e do DRP e tem como iniciativa prioritária sua estruturação, incluindo a definição de RTO e RPO por sistema crítico e a realização de testes periódicos de recuperação.
- **Revisão Periódica de Acessos:** O Active Directory corporativo possui política de renovação de acessos configurada em ciclo semestral (180 dias). A estruturação do processo formal de revisão de acessos via recurso nativo de Access Reviews do Microsoft Entra ID está em andamento, com avaliação de adequação da periodicidade ao padrão recomendado pelos principais frameworks de segurança (ISO 27001, NIST 800-53).
- **Criptografia em Repouso:** Levantamento em andamento para confirmação e padronização da criptografia at-rest nos bancos de dados hospedados na AWS.
- **Prevenção contra Vazamento de Dados (DLP):** Avaliação em curso para implementação de solução de Data Loss Prevention (DLP), visando monitoramento e bloqueio automático de exfiltração de dados confidenciais.

5. CONFORMIDADE REGULATÓRIA

A estrutura de segurança do Grupo Sarfaty está fundamentada nos seguintes normativos e melhores práticas:

- **Resolução CMN nº 4.893/2021 e suas alterações:** Requisitos de segurança cibernética e governança de contratação de serviços em nuvem — observada integralmente nas políticas SFT-07 e SFT-13.
- **Resolução CVM nº 175/2022 e suas alterações:** Regras gerais de fundos de investimento, incluindo requisitos de controles internos, segurança da informação e gestão de riscos operacionais.
- **Resolução CVM nº 21/2021**: Regras que dispõe sobre a administração profissional de carteiras de valores mobiliários, manutenção de controles internos, gestão de riscos e conformidade aplicáveis à atividade de gestão de recursos.
- **Circular SUSEP nº 638/2021:** Disposições de segurança cibernética para o setor de seguros e previdência — considerada no escopo das políticas do Grupo.
- **LGPD — Lei nº 13.709/2018:** O tratamento de dados pessoais de clientes, colaboradores e parceiros observa os princípios da Lei Geral de Proteção de Dados, com controles de acesso e confidencialidade formalmente estabelecidos.
- **ISO 27001 / NIST 800-53:** As práticas de controle de acesso, gestão de incidentes, criptografia e continuidade são orientadas pelos principais frameworks internacionais de segurança da informação.

6. DECLARAÇÃO

O Grupo Sarfaty declara que as informações constantes neste relatório são verdadeiras e refletem o estado atual dos controles de segurança da informação implementados em sua infraestrutura tecnológica, em conformidade com as políticas internas vigentes e com os normativos regulatórios aplicáveis.

A organização reafirma seu compromisso com a melhoria contínua de sua postura de segurança cibernética, com a proteção dos ativos de informação de seus clientes e com a plena transparência perante os órgãos reguladores e entidades autorreguladoras do mercado financeiro.

[Responsável pela área de TI / Segurança da Informação]
Departamento de Tecnologia e Segurança da Informação
Grupo Sarfaty

[Responsável pela Diretoria de Compliance, Risco e PLD/FTP]
Diretoria de Compliance, Risco e PLD/FTP
Grupo Sarfaty

Grupo Sarfaty - Av. Angélica, 2.330, 15º andar, São Paulo, SP - Documento de uso interno e regulatório