THREE

SECURITIZADORA

POLÍTICA DE

SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

ATUALIZADO - ABRIL 2026

Versão 1.0 | Vigente: Abril/2026

Elaboração:	Compliance
Código:	
Aprovação:	Diretor de Compliance e PLD/FTP
Vigente Desde:	ABRIL DE 2026
Versão:	1.0
Última Versão:	Abril/2026

ÍNDICE

1. OBJETIVO

A presente Política tem como objetivo estabelecer as diretrizes e responsabilidades gerais relacionadas ao processo de gestão de informação e segurança no ambiente de tecnologia da informação da Three Companhia Securitizadora S.A. ("Three"), com vista a atender as exigências da Resolução da CVM nº 60, de 23 de dezembro de 2021, conforme atualizada pela Resolução CVM 194/2023, e demais disposições legais e infralegais aplicáveis.

As medidas de segurança da informação têm por objetivo minimizar as ameaças aos negócios da Three, buscando, principal, mas não exclusivamente, a proteção de Informações Confidenciais. As regras e procedimentos dispostos nesta Política são efetivos e consistentes e levam em consideração o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Three.

2. INTERPRETAÇÃO

Para fins de interpretação da presente Política, deverão ser consideradas as definições descritas ao final deste documento. As expressões possuirão o mesmo significado quando utilizadas no singular ou no plural.

Estão vinculados a esta Política os seguintes documentos: (i) Política de Cookies e Proteção de Dados; (ii) Política de Resposta a Incidentes de Segurança; (iii) Política de Uso do Patrimônio Tecnológico da Three; e (iv) Política de Consequências.

São consideradas Informações Confidenciais, para os fins desta Política, independentemente de estas informações estarem contidas em discos, pen-drives, fitas, e-mails, outros tipos de mídia ou em documentos físicos, qualquer informação sobre a

Three, sobre as empresas pertencentes ao seu conglomerado, seus sócios, Investidores e parceiros comerciais, incluindo:

- Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
- Informações técnicas, financeiras, estratégicas ou comerciais;
- Operações estruturadas, demais operações e seus respectivos valores, independentemente de terem sido apenas analisadas ou efetivamente realizadas;
- Estruturas, planos de ação, relação de Investidores, contrapartes comerciais, fornecedores e prestadores de serviços;
- Informações estratégicas, mercadológicas ou de qualquer natureza, obtidas junto a sócios, diretores, funcionários, trainees ou estagiários da Three;
- Informações a respeito de resultados financeiros das empresas emissoras ou adquirentes de direitos creditórios que sejam lastro para a emissão de títulos securitizados;
- Transações realizadas e que ainda não tenham sido divulgadas publicamente.

3. APLICABILIDADE

Esta Política é aplicável a todos os administradores (incluindo diretores executivos), membros do Conselho de Administração e membros dos Comitês e/ou Comissões de Assessoramento, sócios, colaboradores, estagiários, bem como a qualquer pessoa que possua cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança na Three ("Colaboradores").

Esta Política abrange todos os recursos computacionais e de informações disponíveis nos ambientes, sistemas, computadores, servidores, smartphones, tablets e redes da Three, aplicando-se a todos os Colaboradores que tiverem acesso aos equipamentos e sistemas utilizados pela Three.

4. RESPONSABILIDADE E OBRIGAÇÕES

A coordenação direta das atividades relacionadas a esta Política é responsabilidade da área de Compliance e PLD/FTP ("Diretor de Compliance e PLD/FTP"), que, em conjunto com a Área de Segurança da Informação e Tecnologia ("Área de SI"), serão responsáveis por sua revisão, realização de testes e treinamento dos Colaboradores. A Área de SI é coordenada pelo responsável de tecnologia da Three.

Serão responsabilidades da Área de Compliance e da Área de SI:

- Coordenar os esforços relacionados à proteção de dados pessoais;
- Propor e revisar documentos principais de segurança da informação, incluindo políticas de segurança, classificação, controle de acesso e metodologias de análise e tratamento de risco;
- Coordenar a análise/avaliação de riscos e propor medidas para mitigá-los;
- Preparar e realizar treinamentos e campanhas de conscientização sobre segurança da informação;
- Comunicar os benefícios da segurança da informação e propor objetivos de segurança;
- Reportar resultados de auditorias e propor melhorias de segurança;
- Definir cláusulas de segurança para acordos de terceirização;
- Coordenar a resposta a incidentes de segurança e preparar evidências para ações legais;
- Estabelecer métodos de proteção para dispositivos móveis e redes de computadores;
- Definir princípios para o desenvolvimento seguro de sistemas de informação;
- Monitorar logs de atividades de usuários para identificar comportamentos suspeitos;
- Assegurar que os recursos tecnológicos sejam utilizados de forma segura e eficiente;
- Implementar e manter sistemas de segurança, incluindo antivírus, backups e controle de acesso.

Obrigações dos Colaboradores

Todos os Colaboradores comprometem-se a:

- Não transmitir dados ou informações da Three para terceiros não autorizados, seja de maneira verbal, escrita, impressa ou digital;

- Utilizar somente softwares originais e devidamente licenciados, bem como dispositivos previamente autorizados pela Three;

- Não usar dados ou informações da Three para fins pessoais ou diversos daqueles necessários ao desempenho da função contratada;

- Zelar pela segurança de seu login e senha (ID) de acesso individual, ficando proibido usar como próprio o ID de terceiro ou ceder o seu a outrem;

- Zelar por todo dado e informação armazenada na rede corporativa contra alteração, destruição, transmissão, divulgação, cópia e acessos não autorizados;

- Guardar sigilo das informações confidenciais, mantendo-as em caráter restrito;

- Respeitar a propriedade intelectual da Three e/ou de terceiros;

- Zelar pelos equipamentos que utiliza, não sendo permitida remoção, desconexão de partes ou qualquer alteração nas características físicas ou técnicas;

- Utilizar computadores, sistemas de telefonia, redes e outros serviços de informática apenas e exclusivamente para fins profissionais;

- Não executar programas que tenham como finalidade a decodificação de senhas, a monitoração da rede, a leitura de dados de terceiros ou a propagação de vírus;

- Informar prontamente ao superior imediato sobre a ocorrência ou suspeita de quaisquer falhas, incidentes de segurança ou condutas inadequadas e/ou ilícitas.

5. IDENTIFICAÇÃO DE RISCOS (RISK ASSESSMENT)

No âmbito de suas atividades, a Three identificou os seguintes principais riscos internos e externos:

- **Dados e Informações:** as Informações Confidenciais, incluindo informações a respeito de Investidores, parceiros comerciais, Colaboradores e da própria Three;

- **Sistemas:** informações sobre os sistemas utilizados pela Three e as tecnologias desenvolvidas internamente e por terceiros;

- **Processos e Controles:** processos e controles internos que sejam parte da rotina das áreas de negócio da Three;

- **Contingência e Continuidade dos Negócios:** a eficácia dos planos de contingência e de continuidade de negócios da Three.

Principais ameaças cibernéticas identificadas:

- **Malware:** softwares desenvolvidos para corromper computadores e redes (Vírus, Cavalo de Troia, Spyware, Ransomware);

- **Engenharia social:** métodos de manipulação para obter informações confidenciais (Pharming, Phishing, Vishing, Smishing e Acesso Pessoal);

- **Ataques de DDoS (distributed denial of services) e botnets:** ataques visando negar ou atrasar o acesso aos serviços ou sistemas;

- **Invasões (advanced persistent threats):** ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas.

6. AÇÕES DE PREVENÇÃO E PROTEÇÃO

Regra Geral de Conduta

A Three realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam envolvidos no projeto que demanda o seu conhecimento e análise. É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados

na rede da Three sem autorização.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham informações confidenciais deverão ser triturados e descartados imediatamente após seu uso.

Acesso Escalonado do Sistema

A Three mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de login e senha são utilizadas para autenticar as pessoas autorizadas. Os colaboradores deverão ter seus perfis de acesso limitados de acordo com as necessidades exigidas pela sua função.

Senha e Login

A senha e o login para acesso aos dados são pessoais e intransferíveis, não devendo ser divulgados para quaisquer terceiros. As senhas deverão ser trocadas conforme aviso fornecido pelo responsável pela área de informática. Por segurança, as senhas devem seguir os seguintes requisitos:

- Expiração de senha a cada 90 (noventa) dias;
- Senhas fortes com no mínimo 09 caracteres, contendo: números, letras (maiúsculas e minúsculas) e caracteres especiais, não podendo repetir as 03 últimas senhas utilizadas;
- Uso da autenticação multifator para logar na conta de domínio da Three.

Instalação de Software

Os computadores serão configurados exclusivamente com softwares licenciados e necessários para a execução das atividades da Three. É considerada falta grave instalar no computador qualquer software sem autorização e/ou as devidas licenças corporativas.

Uso de Equipamentos e Sistemas

A utilização dos ativos e sistemas da Three, incluindo computadores, internet, e-mail e demais aparelhos, destina-se prioritariamente a fins profissionais. É terminantemente proibido ao Colaborador:

- Enviar mensagens de correio eletrônico cujo conteúdo seja confidencial a terceiros não autorizados;
- Divulgar informações não autorizadas, como fotos, imagens de tela, dados de sistemas, documentos sem autorização expressa e formal da Three;
- Divulgar material protegido por propriedade intelectual sem a permissão da Three ou do detentor dos direitos;
- Enviar e-mails não solicitados (SPAM);
- Falsificar qualquer informação da mensagem original que está sendo enviada;
- Abrir ou executar arquivos anexados enviados por remetentes desconhecidos ou suspeitos com extensões .bat, .exe, .src, .lnk, .com e .dmg;
- Utilizar o e-mail profissional para fins e/ou assuntos pessoais.

Controle de Acesso Físico

O acesso de pessoas estranhas à Three a áreas restritas somente é permitido com a autorização expressa de Colaboradores autorizados pelo Diretor de Compliance e/ou pelo responsável de tecnologia. A Three monitora a utilização de computadores, internet, e-mail e demais aparelhos.

Firewall, Software, Varreduras e Backup

A Three utiliza hardware de firewall projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. São conduzidas varreduras periódicas para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede. O processo de execução de Backup é realizado diariamente de forma a evitar ou minimizar a perda de dados.

Uso de Antivírus

Todas as estações de trabalho devem conter um antivírus instalado, atualizado e operando automaticamente. Nenhum equipamento deve ser conectado na rede sem o antivírus padrão. O Colaborador não está autorizado, em hipótese alguma, a desabilitar ou interromper o antivírus.

Uso da Internet e Mídias Sociais

O uso da Internet deve se limitar a pesquisas e necessidades específicas do trabalho. É proibido:

- Acessar sites suspeitos, não confiáveis, com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados;
- Divulgar e compartilhar dados ou informações da Three em listas de discussão, sites ou comunidades de relacionamento;
- Copiar ou distribuir quaisquer materiais que violem direitos de propriedade intelectual de terceiros;
- Usar ferramentas de torrent e de troca de informação e conteúdo online em redes P2P (Peer-to-peer);
- Acessar sites de redes sociais nos computadores corporativos, exceto pelas áreas que possuam autorização.

7. MONITORAMENTO E TESTES

O Diretor de Compliance e PLD/FTP, com o auxílio da Área de SI, adota as seguintes medidas para monitorar determinados usos de dados e sistemas, em base no mínimo anual:

- Monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, webmails, bem como os e-mails enviados e recebidos;
- Verificação, por amostragem, das informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso.

8. PLANO DE IDENTIFICAÇÃO DE RESPOSTAS

Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, comprometimento da rede ou dos dispositivos da Three, ou ainda no caso de vazamento de Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Compliance e PLD/FTP prontamente.

Procedimentos de Resposta

O Diretor de Compliance e PLD/FTP responderá a qualquer informação de suspeita de acordo com os critérios:

- Avaliação do tipo de incidente ocorrido (infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;
- Identificação de quais sistemas devem ser desconectados ou desabilitados;
- Determinação dos papéis e responsabilidades do pessoal apropriado;
- Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços prejudicados;
- Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas;
- Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente.

9. PROPRIEDADE INTELECTUAL

Todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto à Three, tais como minutas de contrato, memorandos, apresentações, e-mails, planilhas, fórmulas, planos de ação, bem como modelos de avaliação e análise, em qualquer formato, são e permanecerão sendo propriedade exclusiva da Three.

O Colaborador compromete-se a não utilizar tais documentos para quaisquer fins que não o desempenho de suas atividades na Three, devendo todos os documentos permanecer em poder e sob a custódia da Three. É vedado ao Colaborador

apropriar-se de quaisquer desses documentos e arquivos após seu desligamento da Three, salvo se autorizado expressamente.

10. VIOLAÇÃO E PENALIDADES

O descumprimento desta Política implica em falta grave e será passível de responsabilização, conforme Política de Consequências. O colaborador que violar esta Política poderá ser notificado e a ocorrência da transgressão será prontamente comunicada ao seu gestor imediato, sem prejuízo do dever de comunicação ao Diretor de Compliance e PLD/FTP.

11. TREINAMENTOS

O Diretor de Compliance e PLD/FTP, com o auxílio da Área de SI, organizará treinamento anual dos Colaboradores com relação às regras e procedimentos acima, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de compliance descrito no Manual de Compliance e Controles Internos da Three.

12. REVISÃO DA POLÍTICA

O Diretor de Compliance e PLD/FTP realizará a revisão desta Política a cada 24 (vinte e quatro) meses, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliar os riscos residuais.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da Three e acontecimentos regulatórios relevantes.

13. CONSIDERAÇÕES GERAIS

Esta Política entra em vigor imediatamente na data de sua aprovação pelo Comitê de Compliance e PLD/FTP e por ele poderá ser modificada a qualquer momento. Em caso de conflito entre esta Política e o Código de Ética e Conduta, este último prevalecerá.

A Three pode analisar e revisar periodicamente as práticas, as políticas e os procedimentos de proteção de dados, inclusive esta Política. Se forem feitas quaisquer alterações significativas, a Three tomará as medidas razoáveis para informar todos os colaboradores e demais pessoas afetadas.

14. HISTÓRICO DAS ATUALIZAÇÕES

Data	Versão	Responsável
Abril/2026	v.01	Diretor de Compliance e PLD/FTP

JANICE ELIAS DE MORAES ORLANDO:21417289830

Assinado de forma digital por JANICE ELIAS DE MORAES ORLANDO:21417289830
Dados: 2026.04.23 12:01:50 -03'00'