Política de Segurança da Informação e Cibernética

NOVA FUTURA
INVESTIMENTOS

Versão	Data	Atualização	Autor
1.0	27 de abril de 2021	Consolidação de Manuais	Ana Kalil
2.0	29 de abril de 2022	Revisão e Fechamento da Política	Ana Kalil
2.1.	28 de abril de 2023	Revisão Periódica	Leandro Carvalho/ Ana Kalil
3.0.	30 de abril de 2025	Revisão Periódica	Leandro Carvalho/ Julia Pedroso
3.1	30 de abril de 2026	Revisão Periódica	Leandro Carvalho

Sumário

1 INTRODUÇÃO

Nas últimas duas décadas, assistimos um crescimento exponencial do acesso à internet, da rápida adoção dos recursos de tecnologia da informação e comunicação e da integração da vida ao ambiente digital.

Esses rápidos avanços resultaram no uso intenso do espaço cibernético para as mais variadas atividades. Em contrapartida, vimos novas e crescentes ameaças cibernéticas surgirem na mesma proporção e colocarem em risco a integridade das pessoas e instituições, constituindo assim um dos principais riscos não financeiros para os negócios.

Desse modo, constitui prioridade à NOVA FUTURA CORRETORA DE TÍTULOS E VALORES MOBILIÁRIOS LTDA e a NOVA FUTURA GESTÃO DE RECURSOS LTDA. (“Nova Futura”) a proteção das informações e a segurança cibernética.

2 OBJETIVO

A Política de Segurança da Informação e Cibernética (“Política”) tem por objetivo estabelecer os princípios, diretrizes e atribuições relacionadas à segurança da informação, visando assegurar a confidencialidade, a integridade e a disponibilidade das informações e sistemas de dados utilizados pela instituição, bem como proteger os dados dos clientes e do público em geral, prevenindo, detectando e reduzindo as vulnerabilidades à incidentes relacionados com o ambiente cibernético.

3 NORMAS RELACIONADAS

A presente Política está fundamentada em leis e regulamentos brasileiros e nas melhores práticas de mercado, a saber:

(a) Resolução CVM nº 35, de 26 de maio de 2021;

(b) Resolução CVM nº 21, de 25 de fevereiro de 2021;

(c) Resolução CMN nº 4.557, de 23 de fevereiro de 2017;

(d) Resolução CMN nº 4.893, de 26 de fevereiro de 2021, alterada pela Resolução CMN 5.274/2025;

(e) Normas complementares emitidas pela ANBIMA, B3, BSM;

(f) Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD); e

(g) Decreto nº 9.637, de 26 de dezembro de 2018;

(h) Resolução CD/ANPD Nº 15, de 24 de abril de 2024.

4 DEFINIÇÕES E CONCEITOS

Ativos de Informação: Os meios de armazenamento, transmissão e processamento da informação, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

Colaboradores: São os sócios, administradores, funcionários, os estagiários, jovens aprendizes, terceirizados, prestadores de serviço interno e prepostos. Dentre os prepostos se incluem os agentes autônomos de investimento (AAI).

Computação em nuvem (em inglês, *cloud computing*): É um termo coloquial para a disponibilidade sob demanda de recursos do sistema de computador, especialmente armazenamento de dados e capacidade de computação, sem o gerenciamento ativo direto do utilizador. O termo geralmente é usado para descrever centros de dados disponíveis para muitos utilizadores pela Internet. Nuvens em grande escala, geralmente têm funções distribuídas em vários locais dos servidores centrais. Se a conexão com o utilizador for relativamente próxima, pode ser designado um servidor de borda.

Criptografia: Conjunto de técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário, tornando impraticável a leitura por pessoa não autorizada.

Dado Pessoal Sensível: Dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Dado Pessoal: Informação Pessoal Identificada ou Identificável (dado pessoal e sensível) é toda e qualquer informação que separada ou em conjunto pode levar a identificação da pessoa física

ou jurídica, seja ela cliente, fornecedor ou colaborador. Exemplos são números de documentos (RG, CPF, CNPJ, Código CVM), números de contas correntes ou de negociação, endereços, e-mail, posições em custódia e outros.

Dado: Forma primária de informação, que não foi processada, correlacionada, integrada, avaliada, interpretada ou atribuída qualquer sentido inerente em si mesma.

Fatores de Autenticação: São métodos utilizados pelos usuários de um sistema para confirmação de sua identidade. Existem 3 tipos de fatores de autenticação: (i) algo que o usuário sabe (senhas, frases); (ii) algo que o usuário possui (token, e-mail, cartão de senhas); e (iii) algo que o usuário é (biometria digital, mapeamento da íris);

Front Running: Valer-se de informações sobre as negociações de clientes para operar antecipadamente buscando ganhos financeiros.

Informação Confidencial e/ou Privilegiada: Toda e qualquer informação que os Colaboradores obtenham por força de sua relação com a Nova Futura que não sejam públicas e que possibilitem ao Colaborador ou Pessoas Vinculadas a tomada de decisões que lhe propiciem vantagem indevida na negociação de valores mobiliários.

Insider Trading: Utilização ou revelação de Informações Confidenciais ou Privilegiadas.

Negociação: Toda e qualquer forma de operação relacionada à Valores Mobiliários, tais como, mas não se limitando a sua compra, venda, locação, manutenção em carteira ou outras formas de alienação e disposição.

Prestadores de Serviço Interno ou "PJ": São quaisquer outras pessoas físicas e jurídicas que atuem na Nova Futura, conforme indicado pelo Compliance, no momento da contratação dos serviços.

Segurança cibernética: É a capacidade de detectar; identificar, prevenir, proteger, responder e recuperar-se rapidamente de uma ameaça cibernética, com o objetivo de proteger a confidencialidade, integridade e disponibilidade dos ativos tecnológicos e informações.

Sistemas Críticos: Sistemas que tem sua função principal o suporte aos processos de negociação, custódia e liquidação ou que auxiliam estes sistemas.

5 PÚBLICO-ALVO

Estão sujeitos a esta Política todos os Colaboradores da Nova Futura e os Prestadores de Serviço que tenham acesso ao ambiente tecnológico e à rede da Sociedade.

6 DIRETRIZES

Considerando que a informação é um dos principais ativos de uma empresa, a Nova Futura define sua estratégia de segurança da Informação e cibernética, para proteger a informação a que tem acesso seus Colaboradores na execução de suas atividades, baseada na detecção, prevenção, monitoramento e resposta à incidentes, visando fortalecer a gestão do risco de segurança cibernética e a construção de um alicerce robusto para a utilização das plataformas atuais e futuras.

Dessa forma, o tratamento adequado das informações da Nova Futura e de seus clientes está fundamentado nos seguintes princípios:

(a) Confidencialidade: Garantir que o acesso à informação seja obtido somente por pessoas autorizadas;

(b) Disponibilidade: Garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário;

(c) Integridade: Garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

Conforme Resolução nº 4.557, a Nova Futura, no exercício de suas atividades observa e assegura os seguintes aspectos de segurança da informação:

(a) Integridade, segurança e disponibilidade dos dados e dos sistemas de informação utilizados;

(b) Robustez e adequação às necessidades e às mudanças do modelo de negócio, tanto em circunstâncias normais quanto em períodos de estresse; e

(c) Existência de mecanismos de proteção e segurança da informação com vistas a prevenir, detectar e reduzir a vulnerabilidade a ataques digitais.

7 DIVULGAÇÃO DA POLÍTICA

A presente política ficará disponível a todos os colaboradores da Nova Futura na rede interna e em ferramenta própria.

Os colaboradores da Nova Futura devem aderir formalmente a um termo, comprometendo-se a agir de acordo com a política de Segurança da Informação e Cibernética.

8 GOVERNANÇA

Os papéis e responsabilidades atribuídos aos integrantes de cada órgão estão detalhados a seguir:

8.1 Área de Segurança da Informação (Tecnologia):

- É o responsável primário sobre a manutenção da segurança da informação e cibernética buscando aprimorar a qualidade e efetividade de seus processos.
- Certificar-se do atendimento de todas as normas relativas à segurança da informação definidas pelo BACEN, CVM, ANBIMA e BSM;
- Estabelecer, implementar, operar, monitorar e garantir a melhoria contínua do sistema de segurança de informações;
- Definir as políticas e padrões mínimos de segurança da informação para a avaliação de terceiros contratados;
- Manter atualizada a lista de aplicativos e os respectivos responsáveis (Donos do Sistema) e garantir que os acessos sejam revisados periodicamente;
- Manter atualizado o Plano de Continuidade de Negócios e a área e garantir que sejam realizados testes periódicos;
- Realizar testes periódicos de intrusão à rede da Nova Futura e acessos indevidos através da internet;
- Certificar-se que as estações de trabalho estejam protegidas por antivírus, bloqueadas para dispositivos removíveis e alterações em sua configuração;

- Manter atualizado o Plano de Gerenciamento de Resposta a Incidentes e garantir que os incidentes sejam adequadamente analisados e que as melhorias necessárias sejam implementadas;
- Assegurar que os terceiros contratados para processamento ou armazenamento estejam de acordo com as normas definidas pelo Banco Central;
- Estabelecer a governança para Gerenciamento de Mudanças nos sistemas internos e os procedimentos de desenvolvimento seguro de sistemas;
- Estabelecer procedimentos para a manutenção e recuperação dos registros internos (*Backup*);
- Assegurar que existam sistemas adequados para gravação telefônica, inclusive em filiais e AAIs e que os arquivos sejam mantidos no prazo estabelecido pela BSM;
- Estabelecer e disseminar uma cultura de segurança da informação;
- Propor o investimento para a segurança da informação; e
- Revisar periodicamente a presente política.

8.2 Compliance e Controles Internos:

- Disseminar novas normas sobre segurança da informação e cibernética e monitorar a sua implementação pela área responsável;
- Monitorar o permanente atendimento às normas de segurança da informação definidas pelo BACEN, CVM, ANBIMA e BSM;
- Avaliar, em conjunto com a tecnologia, os planos de ação para correção de incidentes;
- Monitorar a correta classificação dos documentos de acordo com esta Política e apurar indícios de vazamento de informações;
- Promover treinamentos sobre o tema de Segurança de Informação e Cibernética (segurança cibernética, pishing);
- Alertar as autoridades sobre incidentes de segurança da informação com potencial de vazamento dos dados;

- Estabelecer normas para a proteção dos dados pessoais na forma da Lei Geral de Proteção de Dados;
- Manter atualizada a Árvore de Contatos para acionamento da contingência;
- Disseminar a cultura de segurança da informação na instituição; e
- Esclarecer dúvidas sobre o assunto.

8.3 Áreas de negócio e suporte:

- Proteger todas as informações a que tiver acesso;
- Proceder a classificação da informação de acordo com as diretrizes desta Política;
- Consultar o *Compliance* ou a área de segurança da informação sobre a possibilidade do compartilhamento informações que não sejam públicas.

8.4 Diretoria Colegiada:

- Aprovar a estratégia, objetivo e orçamento relacionados aos processos de segurança da informação;
- Contribuir na disseminação da cultura de segurança da informação;
- Deliberar sobre as sanções e penalidades.

9 PROCEDIMENTOS E CONTROLES

Para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética e assegurar que as informações tratadas estejam adequadamente protegidas, a Nova Futura adota os seguintes procedimentos e os controles:

9.1 Segurança da Informação

(a) <u>Classificação da Informação</u>

As informações são classificadas de acordo com a confidencialidade e o público-alvo de seu consumo. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações. As informações são classificadas quanto a sua confidencialidade nos seguintes níveis:

(i) **Pública**: é pública toda informação que consta na parte aberta do site da Nova Futura, políticas e manuais, documentos societários registrados externamente e demais documentos conforme indicados em seu rodapé com os dizeres: Informação Pública

(ii) **Interna**: toda a informação da qual não conste classificação de confidencialidade deve ser considerada Informação Interna, em especial relatórios relacionados às rotinas da Nova Futura. Os documentos internos só podem ser compartilhados com o público externo com a autorização do compliance ou da diretoria.

(iii) **Restrita**: devem ser consideradas como restritas, as informações relacionadas a clientes, saldos, relatórios de auditoria, requisições de autorreguladores, algumas políticas e manuais, senhas de acesso, entre outras informações. A informação restrita deve ser de domínio individual (senhas de acesso) ou ter seu domínio determinado no próprio documento. As informações relacionadas a clientes são restritas ao seu assessor, ao *backoffice* correspondente e aos diretores. A informação restrita não contida nas categorias nas acima descritas devem conter em seu rodapé: Informação Restrita

O ciclo de vida da informação compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte. Em geral as informações devem ser mantidas por pelo menos 5 anos, arquivadas e descartadas de forma segura. Informações internas e restritas deverão ser picotadas ou rasgadas antes do descarte.

(b) Guarda de documentos

A Nova Futura possui política de guarda de documentos que prevê a manutenção de todos os registros internos e de operações por no mínimo 5 (cinco) anos. Alguns documentos tais como extratos e posições de clientes podem ter prazos maiores conforme as normas em vigor.

(c) Gestão de Acessos

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos corporativos da Nova Futura. Os acessos devem ser rastreáveis, a fim de permitir a identificação individual do colaborador ou prestador de serviço que tenha acessado ou alterado as informações, permitindo sua responsabilização.

A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários devem ter acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades e devidamente autorizados.

A segregação de funções deve permear todos os processos críticos, evitando que um único responsável possa executar e controlar o processo durante todo seu ciclo de vida.

A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas. A senha é uma informação confidencial, pessoal e intransferível, deve ser utilizada como assinatura eletrônica, sendo proibido seu compartilhamento.

As rotinas de segurança garantem que as informações sejam continuamente protegidas na sua integridade, disponibilidade e confidencialidade, garantindo que cada Colaborador tenha acesso apenas as informações necessárias para a execução de suas atividades.

O setor de tecnologia da informação (TI) responde pela gestão dos meios de armazenamento e processamento de dados e pela concessão de acessos.

O processo de concessão de acessos tem início na inclusão do colaborador na Planilha de Controle de Colaboradores e com o encaminhamento pelo colaborador do formulário de solicitação de acesso ou através de e-mail ou canal próprio da empresa. A área de Segurança da Informação que confronta os acessos solicitados com a Matriz de Segregação de Funções. Caso não sejam identificados conflitos, os acessos são automaticamente concedidos. Caso contrário, os acessos são negados e o colaborador é informado por e-mail, pela área de TI. A Diretoria e o Compliance são copiados no processo de concessão de acessos, para que possam opinar caso necessário.

A revisão periódica dos acessos ocorrerá, no mínimo, a cada seis meses, de forma a impedir a acumulação de privilégios ou “privilege creep”.

A empresa adota o princípio do menor privilégio, assegurando que cada usuário possua somente os acessos indispensáveis para desempenhar suas funções. Todos os acessos – inclusive contas genéricas, serviços e integrações – devem ser formalizados e associados a um responsável identificado.

O acesso remoto e/ou privilegiado exigirá autenticação multifator (MFA) e será concedido somente mediante aprovação da diretoria.

A Nova Futura mantém a Matriz de Segregação de Funções com o intuito de identificar e evitar conflitos de interesse ocasionados por acessos conflitantes.

A Matriz define os perfis de acesso específicos por área, com a identificação de sistemas e privilégios, situações de exceção devem ser aprovadas formalmente pela Diretoria.

Anualmente, a área de Segurança da Informação encaminha lista de acesso dos colaboradores para os gestores e donos de sistema, para certificação. Eventuais situações de conflito, encaminha para nova aprovação pela Diretoria.

Proteção de Senhas e Segredos

Todos os dados sensíveis (senhas, tokens, chaves de acesso e certificados) são armazenados em diretórios com acesso restrito, acessíveis apenas a administradores de TI devidamente autorizados.

As senhas e demais segredos são mantidos em arquivos cifrados, protegidos por uma chave e uma senha mestra; a chave de descriptografia é armazenada separadamente e é protegida por senha, conforme orientações da NIST de manter a chave secreta separada dos dados cifrados.

O arquivo cifrado e suas chaves de acesso não são versionados ou compartilhados em repositórios de código ou e-mails. O acesso e a leitura desses arquivos só podem ocorrer mediante autenticação de múltiplos fatores (quando aplicável) e dentro da infraestrutura local segura.

Periodicamente (no mínimo a cada seis meses), a área de TI realiza a revisão e rotação das senhas mestres e das chaves de acesso, removendo usuários que não necessitam mais de acesso.

(d) Rotinas de Segurança da Informação:

Estações de trabalho: *Softwares* de prevenção contra vírus estão instalados nos servidores locais e nas estações de trabalho, sempre atualizados conforme última versão disponível. As estações de trabalho utilizadas pelos colaboradores dispõem de ferramentas que protegem o equipamento e a rede de dados, impossibilitando, que os usuários extraiam informação através de mídias removíveis ou instalem programas não autorizados pela área de Tecnologia da Informação.

Servidores: Os servidores com acesso à internet e e-mail dispõem de *firewalls* e ferramentas de segurança de rede com proteções contra tentativas de acessos não autorizados.

Os controles de cyber segurança são constantemente verificados e passiveis de evolução de acordo com o gestor de tecnologia. Os incidentes de segurança são classificados como:

(i) Críticos;

(ii) De sustentabilidade;

(iii) Estruturante.

Os planos de ação são endereçados de acordo com tais critérios.

Os *softwares* referentes aos processos de negócios e de controle dispõem de trilhas de auditoria para assegurar o rastreamento de eventos. Diariamente, são realizadas copias de segurança, uma das copias é enviada para local externo às instalações da Sociedade.

Alguns sistemas dispõem de armazenamento em nuvem, como é o caso do sistema de administração de carteiras. A área de TI segue todas as normas de validação de provedores de nuvem, conforme as resoluções do Banco Central e melhores práticas.

A área de tecnologia mantém no ambiente do CPD sensores de temperatura e umidade relativa do ar, monitorando as condições do ambiente por meio de alertas aos responsáveis. O acesso da área do servidor é restrito aos responsáveis pela sua manutenção.

(e) <u>Gestão de Ativos</u>

Entende-se por ativo, tudo aquilo que a instituição considerar como relevante para o negócio, desde ativos tecnológicos (ex. *software* e *hardware*) como não tecnológicos (ex. pessoas, processos e dependências físicas) desde que estejam relacionados à proteção da informação.

Os ativos, de acordo com sua criticidade, devem ser identificados, inventariados, mantidos atualizados, possuírem um proprietário e serem protegidos contra acessos indevidos.

A proteção pode ser, física (ex. salas com acesso controlado) e lógica (ex. configurações de blindagem ou *hardening, patch management,* autenticação e autorização).

Os ativos da Nova Futura, dos clientes e do público em geral devem ser tratados de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, promovendo o uso adequado e prevenindo exposição indevida das informações.

(f) <u>Gestão de Riscos</u>

Para que sejam recomendadas as proteções adequadas, os riscos devem ser identificados por meio de um processo estabelecido para análise de ameaças, vulnerabilidades, probabilidades e impactos sobre os ativos da Nova Futura. As recomendações são discutidas nos fóruns apropriados. Produtos, processos e tecnologias devem ter a adequada gestão dos riscos de Segurança da Informação, para redução dos riscos à níveis aceitáveis.

As tecnologias em uso pela instituição devem estar em versões suportadas pelos seus fabricantes e devidamente atualizadas. Eventuais exceções devem ser aprovadas pela Diretoria ou possuir controles compensatórios.

A Nova Futura possui **processo contínuo de identificação e correção de vulnerabilidades**, incluindo varreduras automatizadas trimestrais ou semestrais e **testes de intrusão (pentest) anuais**.

As vulnerabilidades identificadas deverão ser classificadas por criticidade e tratadas em prazos compatíveis com o risco. A gestão de patches de aplicações (GMUD) será registrada, com evidências de aplicação e verificação de eficácia.

Os prestadores de serviços contratados devem ser classificados considerando alguns critérios, conforme descrito no Manual de Seleção e Monitoramento de Prestadores de Serviço. Os Prestadores de serviço que tenham acesso a rede da Nova Futura ou acesso a informações internas ou restritas devem ter seu risco avaliado pela área de Segurança da Informação.

A rede está segmentada em ambientes de desenvolvimento, homologação e produção, com regras de firewall revisadas trimestralmente e documentadas.

Utilizar IPS/IDS, WebProxy e antivírus de forma coordenada, com atualização e verificação regular das regras e assinaturas.

9.2 Propriedade Intelectual

A propriedade intelectual é a proteção que recai sobre bens imateriais, tais como: marcas, sinais distintivos, slogans publicitários, nomes de domínio, nomes empresariais, indicações geográficas, desenhos industriais, patentes de invenção e de modelo de utilidade, obras intelectuais (tais como obras literárias, artísticas e científicas, base de dados, fotografias, desenhos, ilustrações, projetos de arquitetura, obras musicais, obras audiovisuais, textos e etc.), programas de computador e segredos empresariais (inclusive segredos de indústria e comércio).

Pertencem exclusivamente à Nova Futura e não devem ser utilizados para fins particulares, nem repassado a terceiros sem autorização prévia e expressa, todas e quaisquer invenções, criações, obras e aperfeiçoamentos, informações e conteúdos que tenham sido obtidos, inferidos ou desenvolvidos ou venham a ser criados ou realizados pelos seus colaboradores e prestadores de serviços, utilizando recursos da Nova Futura, durante todo o prazo de vigência do contrato de prestação de serviços, contrato de trabalho ou contrato de estágio do colaborador.

É dever de todos os colaboradores zelar pela proteção da propriedade intelectual da Nova Futura.

9.3 Disseminação da cultura de segurança cibernética

A Nova Futura, periodicamente, disponibiliza aos seus colaboradores programas de capacitação e de avaliação periódica de pessoal, com o intuito de disseminar a cultura de segurança cibernética e da informação.

Da mesma forma, mantém em seus canais de comunicação destinados a clientes e usuários informações sobre precauções na utilização de produtos e serviços financeiros em ambiente digital.

10 PLANO DE AÇÃO E DE RESPOSTA A INCUDNETES

A Nova Futura, em atenção aos procedimentos e obrigações fixados pelo Banco Central do Brasil, estabeleceu Plano de Ação contra Incidentes de Segurança, que elencam sete (7) categorias principais da Gestão de Incidentes de Segurança e plano de resposta incluem o seguinte:

(1) Preparação;

(2) Identificação/Detecção;

(3) Contenção/Erradicação;

(4) Análise/Recuperação;

(5) Comunicação;

(6) Atividades Pós-Incidentes;

(7) Conscientização.

O plano de resposta a incidentes tem como objetivo proteger a Instituição das seguintes ameaças à segurança e incidentes potencialmente prejudiciais à organização, tais como:

- Usuários maliciosos ou negligentes;
- *Malware* (vírus de computador, *worms*, cavalos de Tróia, *spyware* e outros softwares mal-intencionados e indesejados);
- Engenharia social;
- Spam;
- *Phishing* e *Spoofing*;
- Negativa de serviço;
- Negativa de serviço distribuída;
- Ataques *man-in-the-middle;*
- Ataques de rede adicionais, incluindo hackers e outros vetores de ataque comuns;
- Condições físicas e ambientais que resultam em ameaças aos recursos de sistema da Empresa.

A Nova Futura constituiu Comitê de Gestão de Crises a Incidentes cujo objetivo é fornecer monitoramento ativo de segurança, além de análise e resposta a incidentes. A equipe foi estabelecida para tomar medidas proativas de proteção do ambiente da empresa e para desenvolver e publicar procedimentos de resposta e disseminar documentação e recomendações de melhores práticas para os colaboradores.

A área de Segurança da Informação elabora relatório anual sobre a implementação do plano de ação e de resposta a incidentes, conforme estabelecido no artigo 8º da Resolução CMN nº 4.893/21. O relatório deve ser submetido ao comitê de risco e apresentado ao comitê executivo até 31 de março do ano seguinte ao da data base.

11 CONTRATAÇÃO DE SERVIÇOS DE PROCEDIMENTO E ARMAZENAMENTOS DE DADOS E DE COMPUTAÇÃO EM NEVEM

A Nova Futura realiza a guarda de seus arquivos e dados por meio de fita encaminhada mensalmente para fora da organização e mantida por uma empresa especializada em guarda de

ativos, bem como realiza armazenamento diário incremental fornecido em ambiente de cloud protegido por criptografia, login e senha da própria organização. Em razão de terceirizar os serviços de processamento, armazenamento de dados e de computação em nuvem, a Nova Futura adota os seguintes procedimentos visando a segurança e aderência de suas políticas, estratégias e estruturas de gerenciamento de risco:

- Adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas;

- Verificação da capacidade do potencial prestador de serviço de assegurar (i) o cumprimento da legislação e da regulamentação em vigor; (ii) o acesso da nova futura aos dados e às informações a serem processados ou armazenados pelo prestador de serviço; (iii) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço; (iv) a sua aderência a certificações exigidas pela nova futura para a prestação do serviço a ser contratado;(v) o acesso da nova futura aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados; (vi) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados; (vii) a identificação e a segregação dos dados dos clientes da nova futura por meio de controles físicos ou lógicos; e (viii) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da nova futura;

- Quanto à execução de aplicativos por meio da internet, verificação da adoção de controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo, pelo prestador de serviços;

- A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, bem como todas as alterações contratuais, devem ser comunicadas ao Banco Central do Brasil, até dez dias após a contratação dos serviços e deve conter as informações exigidas no artigo 15º da Resolução CMN nº 4.893/21;

- Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem observam todas as disposições exigidas no artigo 17º da Resolução CMN nº 4.893/21.

Antes de contratar provedores de nuvem ou serviços terceirizados, a empresa realizará **due diligence de segurança**, exigindo evidências de compliance com padrões (ISO 27001, SOC 2 etc.), revisando cláusulas de confidencialidade. Os prestadores serão monitorados e avaliados periodicamente quanto à conformidade.

12 SANÇÕES

Quaisquer descumprimentos ou suspeitas de descumprimentos às regras estipuladas na Política deverão ser encaminhados para a análise da área de Compliance e estarão sujeitas nas penalidades previstas no Código de Ética, sem prejuízo de ações legais cabíveis.

13 DISPOSIÇÕES FINAIS

A presente Política deverá ser revisada e atualizada pela área de Segurança da Informação, Compliance e Controles Internos e submetida à aprovação da Diretoria, anualmente.

Sem prejuízo do dever de sigilo e da livre concorrência, a Nova Futura desenvolverá iniciativas para o compartilhamento de informações sobre os incidentes relevantes. Nesse sentido, abrangendo as informações sobre incidentes relevantes recebidas de empresas prestadoras de serviços a terceiros. Essas informações estão disponíveis ao Banco Central do Brasil.

A Nova Futura manterá à disposição do Banco Central do Brasil: (i) a política de segurança cibernética; (ii) o documento relativo ao plano de ação e de resposta a incidentes; (iii) o relatório anual; (iv) a documentação sobre os procedimentos prévios à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem; (iv) os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem; (v) os dados, registros e informações relativos aos mecanismos de acompanhamento e de controle da implementação e da efetividade da política de segurança cibernética; (vi) a documentação com os critérios que configurem uma situação de crise; e (vii) as iniciativas para compartilhamento de informações sobre os incidentes relevantes; pelo prazo de **cinco anos**.

O prazo, quanto ao “item iv” será contado a partir da extinção do contrato, bem como quanto ao item (v) a partir da implementação dos citados mecanismos.