POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

NOVA FUTURA
INVESTIMENTOS

Tabela de controle de versões

Versão	Data	Atualização	Autor
1	27 de abril de 2021	Consolidação de Manuais	Ana Kalil
2	29 de abril de 2022	Revisão e Fechamento da Política	Ana Kalil
3			
4			
5			

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.

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 a incidentes relacionados com o ambiente cibernético.

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;
E) Normas complementares emitidas pela Anbima, B3, BSM;

1 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;

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, predominantes hoje em dia, 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: 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);

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.

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.

2 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.

3 MEDIDAS DE SEGURANÇA E PREVENÇÃO

A Nova Futura, 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, adota os seguintes procedimentos e os controles:

- ✓ **Classificação de Informação:** as informações são classificadas de acordo com a confidencialidade e o público-alvo de seu consumo. Para isso, são 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 em níveis público, interno e restrito. O ciclo de vida da informação compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.
- ✓ 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.** 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 **ambiente CPD (Centro de Processamento de Dados)** com 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.
- ✓ **Gestão de Ativos:** 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 da Nova Futura, dos clientes e do público em geral são 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.
- ✓ **Gestão de Riscos:** Os riscos são identificados por meio de um processo estabelecido para análise de ameaças, vulnerabilidades, probabilidades e impactos sobre os ativos da Nova

Futura, para que sejam recomendadas as proteções adequadas. As recomendações são discutidas nos fóruns apropriados. Produtos, processos e tecnologias têm adequada gestão dos riscos de Segurança da Informação, para redução dos riscos à níveis aceitáveis.

- ✓ **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.
- ✓ A Nova Futura, em atenção aos procedimentos e obrigações fixados pelo Banco Central do Brasil, estabeleceu **Plano de Ação contra Incidentes de Segurança**. O plano de resposta a incidentes tem como objetivo proteger a Instituição e seus clientes de ameaças à segurança e incidentes potencialmente prejudiciais à organização, tais como: (i) Usuários maliciosos ou negligentes; (ii) *Malware* (vírus de computador, *worms*, cavalos de Tróia, *spyware* e outros softwares mal-intencionados e indesejados); (iii) Engenharia social; (iv) Spam; (v) *Phishing* e *Spoofing*; (vi) Ataques *man-in-the-middle*; e(vii) Ataques de rede adicionais, incluindo hackers e outros vetores de ataque comuns;
- ✓ A Nova Futura realiza a **guarda de seus arquivos e dados** por meio de fita encaminhada mensalmente ao Access©, bem como realiza armazenamento diário incremental fornecido pela empresa Azure. Em razão de terceirizar os serviços de processamento e 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:

4 DISPOSIÇÕES FINAIS

Essa Política é uma versão resumida da Política de Segurança da Informação e Cibernética, e nela apresentamos as principais diretrizes adotadas pela Nova Futura.