POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. A Política de Segurança Cibernética da Sociedade visa garantir a proteção, manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, definindo as regras que representam, em nível estratégico, os princípios fundamentais incorporados para o alcance dos objetivos de segurança da informação, em especial mas não somente, conforme requisitos da regulamentação vigente, incluindo, mas não se limitando, às diretrizes da Lei Geral de Proteção de Dados.

I – Princípios da Segurança da Informação

2. Consideramos que os ativos de informação são os bens mais importantes e sensíveis do mercado financeiro, portanto, tratá-los com responsabilidade é o nosso compromisso.

3. Dessa forma, estamos fundamentados nos princípios de segurança da informação, cujos objetivos constituem a preservação da propriedade da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e compartilhamento de forma controlada, bem como o monitoramento e tratamento de forma eficiente e célere de incidentes provenientes de ataques cibernéticos:

Confidencialidade: Garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas e observem as determinações legais ou contratuais aplicáveis.
Integridade: Garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais.
Disponibilidade: Garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las

II – Informações Confidenciais

4. O acesso às informações confidenciais, incluindo dados pessoais, coletadas e armazenadas pela ACG é restrito aos profissionais autorizados ao uso direto dessas informações, e necessário à prestação de seus serviços, sendo limitado o uso para outras tarefas e vetada sua divulgação, salvo no estrito exercício das suas atividades.

5. A ACG somente poderá revelar as informações confidenciais nas seguintes hipóteses:

   (a) Sempre que estiver obrigado a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial.

Versão	Data	Motivo Alteração	Autor/Departamento	Aprovação
01	17/12/2021	Versão Inicial	Compliance	Alta Administração
02	19/12/2022	Revisão Periódica	Compliance	Alta Administração
03	31/01/2024	Revisão Periódica	Compliance	Alta Administração

(b) Aos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados pela ACG a defender seus direitos e créditos, mediante notificação prévia ao detentor das informações.
(c) Aos órgãos reguladores do mercado financeiro, quando aplicável e desde que não haja infringência de dispositivo legal.

III - Definições

6. Para devida compreensão e aplicabilidade desta Política, são consideradas as definições indicadas a seguir:

Clientes: pessoas físicas e/ou jurídicas contratantes dos serviços prestados pela ACG.
Dado(s) e/ou Informação(ões): todos os dados referentes às atividades desenvolvidas pela ACG na execução de seu objeto social, incluindo dados de Clientes, pessoais ou não.
Incidentes: qualquer ocorrência que realmente ou potencialmente comprometa a confidencialidade, integridade ou disponibilidade de um sistema de informação ou a informação que o sistema processa, armazena ou transmite ou que constitui uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitáveis. São considerados incidentes, mas não se limitando a esses: (i) acesso indevido a contas e/ou sistemas da ACG; (ii) acessos não autorizado a bases de Dados ou Informações de uso interno ou confidencial da ACG; (iii) alteração ou perda de Dados ou Informações, ou de acesso a sistemas ou ambientes lógicos, bem como da integridade destes; (iv) vulnerabilidades existentes nos sistemas, bem como situações de indisponibilidade dos sistemas e/ou das informações; (v) demais falhas de segurança que acarretem em acessos não autorizados a sistemas ou ambientes tecnológicos da ACG, por meio de técnicas, conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.
Informações confidenciais: são todas e quaisquer informações e/ou dados de natureza confidencial, incluindo, mas sem limitação, os dados pessoais e as informações, saldos e extratos dos Clientes.
Prestador de Serviço: pessoa física ou jurídica, devidamente contratada pela ACG: (i) de tecnologia; (ii) de armazenamento ou qualquer forma de tratamento de Dados e Informações; (iii) que venha a ter acesso, por conta do escopo de sua contratação, a Dados confidenciais, como classificados nesta Política.
Riscos Cibernéticos: riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, entre outros, que possam expor Dados, redes e sistemas da ACG, causando danos financeiros e/ou de reputação consideráveis, podendo, em algumas circunstâncias, prejudicar a continuidade das atividades da ACG.

Serviços Relevantes: Serviços prestados por Prestadores de Serviço à ACG cuja indisponibilidade, vulnerabilidade ou inconsistência possa prejudicar a continuidade de seus negócios: (i) afetando o atendimento ofertado ao Cliente; (ii) paralisando a operação da ACG, podendo causar perdas financeiras; (iii) impedindo o fornecimento de informações pela ACG aos entes reguladores e/ou o cumprimento de direitos e garantias dos Clientes.

IV - Abrangência

7. Esta Política abrange todas as ferramentas, aplicações, processos e monitoramento de segurança da informação e segurança cibernética no ambiente da ACG, independente da sua localização física.

V – Atribuições e Responsabilidades

8. A Alta Administração (composta pelo Diretor Presidente e as duas Diretoras Vice Presidentes) é a responsável por aprovar a presente Política de Segurança Cibernética, bem como assegurar os recursos adequados para melhoria contínua dos procedimentos relacionados a ela.

9. Área de Tecnologia da Informação é responsável por:

(a) Realizar a gestão de incidentes de segurança da informação na ACG;
(b) Verificar a conformidade desta Política em conjunto com a área de Compliance;
(c) Implantar controles de segurança da informação de acordo com as melhores práticas de Segurança Cibernética;
(d) Desenvolver e atualizar, sempre que necessário, as diretrizes gerais para a gestão de riscos de segurança da informação e Segurança Cibernética;
(e) Elaborar diretrizes para coleta e preservação de evidências de incidentes de segurança da informação;
(f) Elaborar diretrizes para comunicação sobre incidentes de segurança da informação.
(g) Elaborar/aprovar procedimentos técnicos de tratamento de incidentes de segurança da informação, com apoio das demais áreas;
(h) Implementar melhorias no tratamento de incidentes de segurança da informação;
(i) Proteger os dados, o valor e a reputação da ACG;
(j) Identificar com eficiência violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos objetivando a mitigação dos riscos cibernéticos, dentre outros;
(k) Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;

(l) Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;
(m) Conscientizar, educar e treinar os Colaboradores nas suas atividades diárias com foco na Segurança Cibernética;
(n) Estabelecer e melhorar continuamente um processo de gestão de riscos de Segurança Cibernética.

Gestor de Segurança da Informação

10. Atuar como proprietário do Processo de Gestão de Tratamento e Resposta a Incidentes de Segurança da Informação.

Colaboradores

(a) Conhecer e cumprir as diretrizes estabelecidas nesta Política;
(b) Reportar qualquer incidente de Segurança da Informação, mesmo que suposto, o mais rapidamente possível, para seu superior hierárquico ou para o Gestor de Segurança da Informação.

VII – Objetivo e Diretrizes

11. Os incidentes de segurança da informação podem ser notificados por qualquer usuário da ACG ou identificados pela área de Tecnologia da Informação "TI".

12. Esta Política estabelece os seguintes objetivos:

(a) Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;
(b) Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade;
(c) Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pela ACG.;
(d) Garantir que os sistemas e as informações sob responsabilidade da ACG estejam adequadamente protegidos;
(e) Garantir a continuidade do processamento das informações críticas de negócios;
(f) Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo.

13. A ACG deve:

(a) Descrever os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de

segurança cibernética, abrangendo a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações;

(b) Efetuar o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição, os quais devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros;

(c) Estabelecer as diretrizes para a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da ACG;

(d) Descrever os mecanismos para disseminação da cultura de segurança cibernética na ACG, incluindo a implementação de programas de capacitação e de avaliação periódica de pessoal.;

(e) Organizar treinamento para seus Colaboradores sobre o tema de segurança cibernética visando minimizar o risco de qualquer incidente de segurança;

(f) Prestar informações a seus Clientes e mantê-los atualizados sobre precauções na utilização de produtos e serviços oferecidos pela ACG, inclusive mediante treinamento in loco para grandes Clientes e com as informações disponíveis aos usuários finais no regulamento de uso do produto.

VIII - Proteção do Ambiente

14. Devem ser constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração segura de redes de comunicações, incluindo a gestão de serviços contratados de processamento e armazenamento de dados e informações em nuvem.

15. Os equipamentos e instalações de processamento de informação críticas ou sensíveis devem ser mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

16. Os requisitos de segurança de sistemas de informação devem ser identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim

possam ser protegidos visando a manutenção de sua confidencialidade, integridade e disponibilidade.

17. Os Colaboradores e terceiros da ACG devem ser treinados periodicamente sobre os conceitos de Segurança da Informação, através de um programa de conscientização.

18. Os acessos às informações devem ser controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente com a aprovação do gestor do responsável e o da informação, e cancelados tempestivamente ao término do contrato de trabalho do Colaborador ou do prestador de serviço.

19. Os acessos aos sistemas da ACG são realizados através de login e senha, sendo que as senhas são criptografadas, de modo que apenas o portador da senha pode utilizá-la. Os acessos podem ser rastreados.

20. A ACG possui procedimentos efetivos para a aderência às regras previstas na regulamentação em vigor e realiza seu armazenamento de dados e computação em nuvem.

21. É utilizado controle para prevenção de perda de dados, o qual é responsável por garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados ou vazados na web por usuários não autorizados.

22. Periodicamente devem ser realizadas varreduras das redes internas e externas e as vulnerabilidades encontradas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

23. Trilhas de auditoria automatizadas devem ser implantadas para todos os componentes de sistema para reconstruir os principais eventos, tais como, autenticação de usuário, acesso a informação e ações executadas pelo usuário.

24. O backup é realizado periodicamente em relação a todas as informações relevantes, de forma a evitar ou, pelo menos, minimizar a perda de dados em razão de qualquer incidente de segurança.

25. Todos os Prestadores de Serviços devem declarar: (i) o conhecimento e o cumprimento desta política, inclusive em relação a proteção das Informações Confidenciais a que tiver acesso; (ii) que cumprem com as normas legais que regulamentam a propriedade intelectual e a proteção de dados e a normas vigentes relacionadas à segurança cibernética e afins do Banco Central do Brasil; (iii) que os dados obtidos em razão da prestação de serviços para a ACG, bem como os sistemas da Sociedade somente serão utilizados para cumprir a finalidade do objeto do

contrato; e (iv) que se compromete a informar imediatamente caso tome conhecimento de descumprimento da presente política.

IX – Contratação de Prestadores de Serviços

26. A contratação de Prestadores de Serviços para a execução de serviços relevantes de processamento de dados e de computação em nuvem, deve ser aprovada pela Alta Administração.

27. Previamente à contratação de qualquer Prestador de Serviço, este deverá ser aprovado pela área de compliance no processo de *"due diligence"* previsto nas políticas internas da ACG, bem como pelo diretor de tecnologia da informação em relação à capacidade técnica da execução dos referidos serviços.

28. Sempre que os serviços a serem contratados envolverem serviços relevantes de processamento de dados e de computação em nuvem, que no entendimento da ACG sejam relevantes para seus negócios e consequentemente classificados como de alto risco, deve ser verificada a capacidade do potencial Prestador de Serviço, a fim de assegurar: (i) o cumprimento da legislação e da regulamentação em vigor; (ii) o acesso da Sociedade 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 para a prestação do serviço a ser contratado; (v) o acesso da ACG 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 usuários finais da Sociedade por meio de controles físicos ou lógicos; e (viii) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da Sociedade.

29. No caso da contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem serem prestados no exterior, deve ser observada a regulamentação do Banco Central do Brasil em vigor sobre o assunto.

X – Continuidade de Negócios

30. O processo de gestão de continuidade de negócios relativo a segurança da informação, deve ser implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, mapeamento de

processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados de nuvem e os testes previstos para os cenários de ataques cibernéticos.

XI – Incidentes e Plano de Ação e de resposta a incidentes

31. Todos os Incidentes devem ser reportados para o Gestor de Segurança da Informação, que munido das informações necessárias deverá elaborar o Plano de Ação e de Resposta a Incidentes, que tem como objetivos:

a) Identificar e reportar os Incidentes;
b) Registrar os eventos que acarretaram problemas de segurança/continuidade;
c) Direcionar medidas paliativas para solucionar os problemas causados pelos Incidentes, bem como soluções para minimizar o risco de Incidentes semelhantes.

32. Sempre que é identificado um Incidente na ACG que envolva a prestação dos serviços ofertados pela Sociedade relacionados a cartão de crédito e boleto, a Sociedade imediatamente comunica a ocorrência e as informações até então obtidas a todos os participantes do mercado envolvidos diretamente na operação, por exemplo, o adquirente, a processadora e a bandeira.

33. Caberá a Alta Administração aprovar o Plano de Ação e de Resposta a Incidentes e definir a prioridade e urgência relacionada a cada Incidente.