POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

CÓDIGO: **PL 08**	VERSÃO: **07**
APROVAÇÃO: **Política aprovada pela Diretoria Executiva**	DATA: **03/04/2023**
ÁREA EMISSORA: **Segurança da Informação**	

Sumário

1. OBJETIVO

A Política de Segurança da Informação e Cibersegurança tem como objetivo definir as diretrizes que norteiam a definição de procedimentos que visam proteger sistemas, infraestrutura de tecnologia, ativos de informação, bem como assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

A presente política se aplica ao Grupo Agibank, portanto sempre que citado “Agibank” leia-se todas as empresas do Grupo Agibank, quais sejam, Banco e Controladas, Coligadas e Correspondentes no país.

2. DEFINIÇÕES

Segurança da Informação: Desenvolvimento integrado das ações para a gestão inteligente de proteção orientada à recursos humanos, ativos físicos e à infraestrutura tecnológica da informação.

Cibersegurança: Conjunto de processos e tecnologias que visam proteger sistemas, ativos de informação, redes e dados de eventuais ataques cibernéticos, intrusão ilícita e vazamento de dados sigilosos.

Serviço Relevante: Para o Agibank, são considerados relevantes os serviços de fornecedores que estejam diretamente ligados a atividade principal da empresa e/ou impacte a disponibilidade de serviços aos nossos clientes ou possui faturamento anual superior a R$ 1milhão, com base no ano base anterior ou, para novos fornecedores, com essa projeção de faturamento;

Usuários: Quem irá se utilizar de informações para empreender atividades pertinentes ao negócio do Agibank. Para esta Política, consideram-se usuários os profissionais celetistas, Diretores, menores aprendizes, estagiários e terceiros que acessam qualquer tipo de informação para execução de atividades profissionais no/para o Agibank.

3. DIRETRIZES

- A informação é um ativo que possui valor estratégico e importância exponencial para o Agibank e seus negócios.
- As informações de propriedade do Agibank, dos seus clientes e parceiros de negócios são tratadas de forma ética e transparente, de acordo com as leis vigentes, regulações aplicáveis e normas internas apenas para a finalidade de negócio.
- O acesso às informações e recursos somente deve ser concedido se estiver devidamente autorizado.

- Para a concessão de acessos deve ser aplicado o conceito de privilégio mínimo, com acesso apenas aos recursos e informações imprescindíveis para a execução das atividades profissionais pertinentes ao Agibank.
- Cada usuário deve possuir uma identificação única (login de acesso), pessoal e intransferível, com garantia de rastreabilidade e não repúdio das ações executadas em recursos e informações do Agibank, de seus clientes e parceiros de negócios.

3.1 Princípios de Segurança da Informação

Confidencialidade: as informações devem ser acessadas apenas por Usuários autorizados, respeitando o conceito de mínimo acesso necessário para execução de atividades profissionais pertinentes ao Agibank;

Integridade: as informações devem estar íntegras e completas;

Disponibilidade: as informações devem estar disponíveis para os usuários autorizados sempre que necessário.

3.2 Disseminação da Cultura de Segurança

Visa o fortalecimento da cultura de Segurança da Informação através da disseminação dos princípios e diretrizes descritos na presente política, para tanto anualmente são realizados trabalhos de conscientização em segurança da informação e segurança cibernética, com diretiva educacional para um comportamento seguro dos usuários. Além disso, é realizada capacitação e avaliação periódica de todos os colaboradores via plataforma *online*.

Os colaboradores do Agibank também podem se apropriar dos conteúdos de Segurança no espaço da área, na intranet institucional, a qual é disseminada durante o processo de integração dos novos Colaboradores, além de processo de comunicação realizados pela área para todos os Colaboradores.

Para os usuários terceiros alocados diretamente no Agibank, esses também possuem acesso à Política de Segurança e devem realizar a leitura e aceite do documento, através do Portal de Gestão de Acessos (Horacius).

No que tange a prestação de informações sobre precauções na utilização de produtos e serviços financeiros a clientes e usuários, o Agibank dispõe de Cartilha Digital disponível em nosso *web site* institucional: https://www.agi.com.br/dicas-de-seguranca.

Por fim, a Política de Segurança da Informação e Cibersegurança é divulgada para todos os colaboradores, através dos processos de comunicação interna e fica disponível para consulta na intranet institucional.

3.3 Estratégia de Segurança da Informação e Cibersegurança

A estratégia de Segurança da Informação do Agibank é baseada em arquitetura com os seguintes domínios: Gestão de Segurança da Informação, Gestão de Identidades e Acessos, Segurança Ofensiva, Segurança Defensiva e Gestão de Continuidade de Negócios.

3.3.1 Gestão de Segurança da Informação

Prevê as melhores práticas para governança de Segurança no que diz respeito à políticas, processos, regulações, auditorias e demais controles.

Gestão de Ativos de Informação: Os ativos de informação devem ser identificados, inventariados e protegidos de acessos indevidos. Devem possuir documentação e rotinas de manutenção atualizados.

3.3.2 Gestão de Identidades e Acessos

As concessões, revogações, transferências e revisões de acesso devem respeitar os fluxos de aprovação e execução determinados pela Instituição, bem como se utilizar das ferramentas oficiais disponibilizadas para estes processos. Todos os acessos devem ser rastreáveis, possibilitando auditoria e responsabilidade individual de um usuário.

3.3.3 Segurança Ofensiva

Entende-se por Segurança Ofensiva a forma de detectar vulnerabilidades e se precaver de ataques cibernéticos de forma proativa, por meio da aplicação de técnicas e ferramentas.

Gestão de Vulnerabilidades:

Os riscos de Segurança da Informação são identificados e acompanhados através de um processo de análise de vulnerabilidades, quantificando e qualificando as ameaças e seus respectivos impactos sobre os ativos de informação, para associação dos níveis de proteção adequados. Os testes e varreduras são realizados semestralmente.

Princípios do plano de Gestão de Vulnerabilidades:

- Inventariar os ativos de tecnologia da informação;
- Verificar e avaliar as vulnerabilidades nos Ativos de TI;
- Avaliar o Risco Potencial;
- Definir a Remediação;
- Verificar Efetividade da Remediação;
- Validar a solução final ou acompanhar o seu plano de ação.

As vulnerabilidades identificadas pelo processo executado no SOC (Centro de Operações de Segurança), bem como demais testes executados pela área de segurança da informação ou parceiros, são regidos pelo "*Plano de Gestão de Vulnerabilidades"*.

Desenvolvimento Seguro de Aplicações e Sistemas:

Os procedimentos para desenvolvimento de aplicações e sistemas devem seguir as boas práticas de mercado para a disciplina e estar aderentes aos normativos de segurança da informação do Agibank.

Demandas e Projetos:

As demandas e projetos de negócio, serviços de retaguarda ou tecnologia devem estar em conformidade com as diretrizes, processos e arquitetura corporativa de segurança da informação. As demandas e projetos devem ser submetidos aos checklists de Segurança da Informação aplicados pela área de Governança de TI, garantindo a sua aderência às melhores práticas e normativos de segurança.

3.3.4 Segurança Defensiva

Entende-se como Segurança Defensiva a estratégia de defesa, que possui o objetivo de prevenção, identificação e resposta de possíveis incidentes de Segurança.

Os controles de Segurança adotados referente a criptografia, rastreabilidade de operações transacionais, segmentação de redes e manutenção de cópias de segurança são detalhados em Normativos.

Gestão de Incidentes de Segurança da Informação:

O objetivo da gestão de incidentes de segurança da informação é documentar as ações necessárias para resposta quando da ocorrência de incidentes ou em momentos de crise, para tanto foi elaborado o "*Plano de Gestão de Incidentes de Segurança da Informação*", no qual define os procedimentos para prevenção e respostas a incidentes e os parâmetros para classificação da criticidade dos incidentes, sendo que os incidentes classificados como relevantes serão objeto de registro por meio do relatório anual e de reporte tempestivo ao Banco Central do Brasil.

Adicionalmente, são disponibilizados canais de comunicação para que qualquer usuário possa reportar incidentes de Segurança da Informação de forma a possibilitar a análise e tratamento adequado do incidente. O reporte pode ser realizado através dos seguintes e-mails: seguranca.informacao@agi.com.br ou incidente.seguranca@agi.com.br.

Relatório Anual:

Anualmente, será elaborado relatório sobre a implementação do Plano de Gestão de Incidentes de Segurança da Informação abordando os seguintes aspectos:

- A efetividade da implementação das ações para adequar a estrutura organizacional e operacional do Agibank aos princípios e às diretrizes da presente política;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
- Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

Os relatórios estarão à disposição do Banco Central do Brasil pelo prazo de cinco anos, podendo ele fazer uso das informações a qualquer momento.

Compartilhamento de Informações sobre os Incidentes Relevantes:

O Agibank compromete-se com o compartilhamento de informações sobre incidentes relevantes com as demais instituições do Mercado financeiro como forma de contribuir com o mapeamento de vulnerabilidades e ameaças envolvendo a segurança cibernética, bem como desenvolver mecanismos para sua mitigação.

3.3.5 Gestão de Continuidade de Negócios

Visa garantir que existam planos de continuidade de negócios e recuperação de desastres que contemplem alocação de profissionais, os principais processos e ativos de tecnologia e negócio do Agibank.

Os cenários de incidentes considerados nos testes de continuidade de negócios, bem como as diretrizes sobre esse tema estão descritas na Política “PL38 - Gestão de Continuidade do Negócio”.

3.4 Classificação da Informação

As informações do Agibank devem ser classificadas em níveis, de acordo com a sua criticidade. Devem ser consideradas as necessidades de negócio e de compartilhamento ou restrição de acesso, com análise de impactos em relação ao uso indevido das informações. A classificação das informações deve respeitar o ciclo de vida da informação

desde a sua geração até o descarte. Os níveis de classificação são: Confidencial, Interna e Pública.

3.5 Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem

A contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem é realizada através de processos que contemplam:

- A adoção de práticas de governança proporcionais a relevância do serviço a ser contratado;
- A avaliação da capacidade do fornecedor em assegurar o cumprimento da legislação vigente, o acesso da instituição aos dados e informações a serem processados ou armazenados pelo prestador de serviço, a confidencialidade, a integridade a disponibilidade e a recuperação dos dados e das informações processadas ou armazenadas pelo prestador de serviço;
- Identificar o local de armazenamento de dados e suas especificidades para aderência regulatória;
- Controles de acesso voltados a proteção de dados;
- Os critérios de decisão quanto terceirização de serviços relevantes.

Todos os contratos com empresas que armazenam dados em nuvem contemplam cláusulas que asseguram o armazenamento e processamento seguro, seu local exato de armazenamento, bem como a disponibilização dos dados para o Agibank quando da necessidade de auditoria pelo Banco Central.

Sempre que houver novas contratações ou alterações contratuais de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, estes serão comunicados ao Banco Central com até 10 dias após a contratação ou alteração dos serviços conforme procedimentos estabelecidos no Comunicado BCB 32.694 de 22 de outubro de 2018.

Para os serviços contratados no exterior, deve-se observar a existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados.
No caso de inexistência de convênio, a instituição deve solicitar autorização do Banco Central do Brasil para a contratação ou alteração do serviço, no prazo mínimo de sessenta dias antes da contratação ou alteração.

3.6 Direito de Propriedade

Qualquer informação ou produto resultante do trabalho dos Usuários, no escopo de suas atividades contratadas, é de propriedade do Agibank. Ao término do contrato de trabalho, os Usuários devem manter as informações privadas e produtos gerados, salvo por cláusula contratual prevista, sob posse do Agibank.

3.7 Termo de Responsabilidade

É exigido um termo de responsabilidade e ciência em que os Colaboradores e Fornecedores se comprometem a agir de acordo com os padrões de confidencialidade e disponibilidade dos dados do Agibank. Este termo é assinado no ato da contratação.

4. PAPÉIS E RESPONSABILIDADES

Conselho de Administração

- Aprovar a presente política, bem como o plano de ação e de resposta a incidentes;
- Aprovar o relatório anual sobre a implementação do plano de ação e de resposta a incidentes.

a) Diretor responsável por Segurança da Informação e Cibersegurança

- Promover elevados padrões de segurança de forma a garantir a melhoria contínua dos procedimentos relacionados à segurança da informação e cibersegurança;
- Zelar pelo cumprimento das diretrizes contidas na Política de Segurança da Informação e Cibersegurança em todos os níveis de todas as instituições que compõem o Agibank.

b) Área de Segurança da Informação

- Conduzir os esforços estratégicos para cumprimento dos objetivos desta Política;
- Estabelecer mecanismos de proteção e Segurança da Informação com vistas a prevenir, detectar e reduzir a vulnerabilidade a ataques digitais;
- Definir os procedimentos necessários para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem de forma a garantir a aderência da presente Política, bem como da regulamentação aplicável;
- Registrar os incidentes relevantes e controlar seus efeitos na Instituição;
- Garantir que usuários desligados ou com contrato encerrado não tenham acesso aos ativos de informação, utilizando-se dos procedimentos adequados de desligamento/encerramento contratuais vigentes.
- Revisar, com periodicidade mínima anual, a Política de Segurança da Informação e Cibersegurança, bem como o plano de ação e de resposta a incidentes;

- Gerar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, e quando necessário, compartilhar com as estruturas organizacionais internas e órgãos reguladores.

c) Governança de TI

- Acompanhar e executar os procedimentos de contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem conforme definição da área de Segurança Informação.
- Aplicar os *checklists* de segurança da informação para as demandas de projeto garantindo a aderência as diretrizes de segurança.

d) Gestão de Riscos

- Definir os critérios de decisão quanto à terceirização de serviços, considerando a regulamentação vigente no que tange o processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior.
- Monitorar os indicadores de risco estabelecidos por fornecedor.

e) Usuários

- Responder pela utilização inadequada dos direitos de acesso concedidos, inclusive de outros Usuários que estão sob sua gestão e/ou responsabilidade;
- Zelar pela segurança de suas credenciais (login de acesso e senha) corporativas, departamental ou de rede.

f) Gestores de Ativos de Informação

Gestor do ativo de informação é o Usuário com responsabilidade direta sobre determinado ativo na Organização. Salvo exceções, os gestores das áreas são os gestores do ativo de informação sob responsabilidade da sua área de atuação, e devem:

- Cumprir e transmitir as suas equipes as disposições estabelecidas pela Política e Normas de Segurança da Informação a fim de que tenha ampla divulgação no ambiente de trabalho;
- Garantir que as inconformidades ocorridas em suas áreas sejam identificadas e reportadas, e que sejam adotadas as medidas corretivas apropriadas conforme controles de segurança da informação;
- Realizar os procedimentos adequados para desligamento e encerramentos contratuais vigentes;
- Proteger os ativos de sua área (físico e lógico), de acordo com os critérios de classificação das informações definidos pela Instituição;

- Aplicar sanções àqueles que deliberadamente violarem as determinações desta Política, suas Normas e Instruções, mediante orientação da área de Segurança da Informação.

5. BASE REGULATÓRIA / LEGISLAÇÃO APLICÁVEL

- Resolução CMN n° 4.893 de 26 de fevereiro de 2021;
- Resolução CMN nº 4.557 de 23 de fevereiro de 2017;
- Comunicado BCB nº 31.999 de 10 de maio de 2018;
- Comunicado BCB nº 32.694 de 22 de outubro de 2018;
- Lei nº 13.709, de 14 de agosto de 2018.

6. REGULAMENTAÇÃO INTERNA RELACIONADA

- Código de Ética e Conduta do Agi
- PL 38 – Gestão de Continuidade do Negócio
- NP 08.001 – Comunicação Eletrônica e Acesso à Internet
- NP 08.002 – Controle de Acesso e Autenticação
- NP 08.004 – Norma de uso de Recursos de TI
- NP 08.006 – Classificação da Informação
- NP 08.007 – Acesso Office365
- NP 44.006 – Terceirização de Serviços

7. DISPOSIÇÕES FINAIS

O Agibank se reserva o direito de monitorar, inspecionar ou auditar o acesso e o uso de aplicativos e informações de sua propriedade ou sob sua guarda com ou sem o consentimento, presença ou conhecimento dos Usuários, mas respeitando aspectos legais.

Nenhum software utilizado pelo Agibank para controle e proteção de suas informações pode ser alterado ou desabilitado pelos Usuários.

Esta Política será revisada com a periodicidade mínima anual ou sempre que houver alteração no processo e/ou regulatória.