POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

POLÍTICA DA SEGURANÇA DA

INFORMAÇÃO E SEGURANÇA CIBERNÉTICA ("CYBER SECURITY")

1. Objetivo

Esta Política da Segurança da Informação e Cyber Security ("Política") tem por objetivo estabelecer os princípios, diretrizes e atribuições relacionadas à segurança da informação **ASA Sociedade de Crédito Financiamento e Investimento S.A.** ("**ASA SCFI**" ou "**Instituição**") e demais empresas do Grupo ASA (em conjunto denominadas "ASA"), com intuito de assegurar a integridade, disponibilidade e confidencialidade dos dados sua propriedade e/ou sob sua guarda e dos sistemas de de informação utilizados, 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 pelo ASA para o alcance dos objetivos de segurança da informação.

Esta Política observa a regulamentação vigente, aplicável ao ASA, em especial a Resolução CMN n° 4.893 de 26/02/2021, assim como as melhores práticas de mercado.

2. Público-alvo

Esta Política se aplica a todos os colaboradores, terceiros, auditores, parceiros, fornecedores e prestadores de serviços, que tenham acesso, direto ou indireto, às informações, sistemas, ativos ou instalações do ASA, independentemente de sua localização geográfica ou vínculo contratual, abrangendo todos os ambientes tecnológico e operacionais do ASA, inclusive, mas não se limitando a *cloud,* canais digitais, *open finance,* ambientes de integração com parceiros e operações internacionais.

3. Estratégia para a Segurança da Informação e Cyber Security

A segurança da informação e Cyber Security é considerado um valor inegociável ao ASA. Em decorrência disso, é adotada a estratégia de proteção do perímetro expandido, de forma que a informação é protegida independentemente de sua localidade, seja internamente, em uma sociedade sob controle comum, em serviço de *cloud*, em um prestador de serviço ou em uma unidade internacional. Esta proteção é adotada em todo o seu ciclo de vida, desde a coleta até o seu descarte.

4. Princípios

O processo de Programa de Segurança da Informação e Cibersegurança é pautado pelos princípios abaixo, aplicáveis igualmente nas relações com clientes e público em geral:

I. Confidencialidade: o acesso à informação deve ser obtido somente por pessoas devidamente autorizadas;

II. Integridade: deve ser garantida a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos;

III. Disponibilidade: o acesso à informação deve ser garantido às pessoas autorizadas sempre que necessário.

5. Diretrizes

As diretrizes aqui estabelecidas definem o Programa de Segurança da Informação e Cibersegurança, voltado à prevenção, detecção, mitigação e redução de vulnerabilidades, bem como à minimização dos impactos decorrentes de incidentes cibernéticos.

Os documentos de segurança da informação (política, regras e procedimentos) devem estar disponíveis em local acessível aos colaboradores e protegidos contra alterações.

A adesão à essa Política e eventuais desvios são reportados periodicamente pelo Head de Tecnologia ao Diretor responsável por esta Política e à Diretoria.

A informação deve ser utilizada de forma transparente, para as finalidades informadas ao cliente e de acordo com a legislação vigente, conforme descrito em políticas internas.

Todos os sistemas e aplicações da Instituição seguem os princípios de *security by design* e *privacy by design*, de forma a estarem sempre aderentes às melhores práticas de segurança, aderentes a política interna e à legislação vigente.

As diretrizes e eventuais exceções são complementadas em procedimentos com regras específicas que devem ser observadas.

6. Processos de Segurança da Informação

O ASA adota os seguintes processos que asseguram o tratamento e proteção adequados de informações:

6.1. Gestão de Ativos

Entende-se por ativo qualquer recurso físico, lógico, humano ou processual que possua valor para o ASA, seja considerado por este relevante para o negócio e desde que estejam relacionados à proteção da informação.

Os ativos tecnológicos, de acordo com sua criticidade, devem ser identificados, inventariados, mantidos atualizados, possuírem um proprietário, descartados de forma segura e serem protegidos contra acessos indevidos. A proteção pode ser, física (p.ex. salas com acesso controlado) e lógica (p.ex. configurações de blindagem ou *hardening*, *patch management*, autenticação, autorização e monitoramento).

Os ativos do ASA, 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.

6.2. Classificação da Informação

As informações devem ser classificadas de acordo com sua confidencialidade, conforme descrito nos documentos internos. 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. De acordo com a classificação da confidencialidade devem ser estabelecidas as proteções necessárias durante todo o seu ciclo de vida.

O ciclo de vida da informação compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte Seguro.

As diretrizes para Classificação da Informação estão descritas no documento "Procedimentos de Classificação de Informação".

6.3. Gestão de Acessos

O controle de acesso físico e lógico deve garantir o princípio do menor privilégio e segregação de funções, com revisão periódica de perfis.

A identificação de qualquer colaborador e/ou prestador de serviço deve ser única, pessoal e intransferível, qualificando-o como responsável por todas e quaisquer ações realizadas.

A senha é uma informação confidencial, pessoal e intransferível, deve ser utilizada como assinatura eletrônica, sendo proibido seu compartilhamento. As diretrizes aplicáveis para senhas de usuários estão descritas no documento "Procedimentos de Senhas de Usuários".

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 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.

As diretrizes detalhadas para Gestão de Acessos estão descritos no documento "Procedimentos de Gestão de Acessos".

6.4. Gestão de Riscos

Os riscos devem ser identificados por meio de processos estabelecidos para análise de ameaças, identificação de vulnerabilidades, análise de probabilidades e impactos sobre os ativos do ASA, para que sejam recomendadas as proteções adequadas.

Cabe ao time de TI, sob supervisão do Head de TI manter o registro, a análise da causa e do impacto, bem como controle dos efeitos de incidentes relevantes para as atividades da Instituição.

Produtos, processos e tecnologias devem ter a adequada gestão dos riscos de Segurança da Informação, para redução dos riscos à níveis aceitáveis, independentemente de estarem dentro da infraestrutura do ASA, parceiros ou prestadores de serviços.

As tecnologias em uso pela instituição devem estar em versões suportadas pelos seus fabricantes e devidamente atualizadas, de acordo com os processos de gestão de *patches*. Eventuais exceções devem ser aprovadas na alçada competente ou possuir controles compensatórios.

6.5. Gestão de Riscos em Prestadores de Serviços e Parceiros

O prestador de serviço ou parceiro passará por avaliação de risco, que pode incluir a validação *in loco* dos controles de Segurança da Informação, avaliação remota das evidências ou outras avaliações, além do acompanhamento de eventuais correções e melhorias implementadas pelos prestadores de serviços e parceiros.

Os prestadores de serviços e parceiros devem informar tempestivamente os incidentes relevantes relacionados às informações do ASA, armazenadas ou processadas por eles, em cumprimento às determinações legais e regulamentares.

As diretrizes para contratação de serviços relevantes conforme definições regulamentares, estão descritas em documentos internos.

6.6. Gestão de Continuidade

Devem ser mantidos planos de continuidade e contingência documentados, testados e revisados anualmente. As diretrizes para elaboração de cenários de incidentes considerados nos testes de continuidade de negócios estão descritas no documento "Procedimentos de Continuidade de Negócios".

6.7. Tratamento de Incidentes de Segurança da Informação e *Cyber Security*

A área de *Cyber Security* monitora a segurança do ambiente tecnológico do ASA, analisando os eventos e alertas para identificar possíveis incidentes.

Os incidentes que são identificados pelos alertas são classificados com relação ao impacto, de acordo com os critérios adotados pelo ASA. Para o seu grau de relevância serão considerados aspectos como impacto ao sistema financeiro e comprometimento de dados de clientes e do público em geral.

Todos os incidentes passam por um processo de avaliação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto, classificação e demais informações necessárias.

Informações sobre incidentes que possam impactar outras instituições financeiras no Brasil, devem ser compartilhadas com as demais instituições, visando colaborar com a mitigação do risco conforme determinações legais e regulamentares.

Visando aprimorar a capacidade de resposta a incidentes, o ASA realizará anualmente testes de recuperação de desastres simulando incidentes críticos, que podem comprometer a disponibilidade e/ou a confidencialidade das informações.

A fim de se antecipar às novas ameaças, o ASA mantém processos de inteligência sobre ameaças virtuais, além de participar ativamente de fóruns de cibersegurança da indústria e do governo, no Brasil e no exterior, para o fortalecimento das defesas.

Todo colaborador deve ser proativo e diligente na identificação, comunicação para a área de Segurança da Informação e na mitigação dos riscos relacionados à segurança da informação.

6.8. Conscientização em Segurança da Informação e *Cyber Security*

O ASA promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação para fortalecer a cultura de Segurança da Informação, fazendo parte do Programa de Treinamentos, conforme descrito em documento interno.

Periodicamente, são disponibilizadas campanhas de conscientização ou treinamentos que podem ser presenciais ou on-line, relacionados a confidencialidade, integridade e disponibilidade da informação. Estas campanhas são veiculadas através de e-mails, website da instituição, portal corporativo, e-learning e em mídias ou redes sociais aos colaboradores e clientes.

6.9. Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com os princípios e diretrizes de segurança da informação.

6.10. Segurança Física do Ambiente

O processo de Segurança Física estabelece controles relacionados à concessão de acesso físico aos ambientes, de acordo com a criticidade das informações tratadas nestes ambientes, conforme descrito nos documentos internos.

6.11. Uso de Ativos de TI

Ativos tecnológicos e informacionais são de propriedade do ASA e devem ser utilizados exclusivamente para fins corporativos.

6.12. Criptografia

A aplicação de controles criptográficos deve seguir diretrizes de criptografia simétrica, assimétrica e hash, conforme Política interna.

6.13. Programa de *Cyber Security*

O Programa de *Cyber Security* do ASA é norteado pelos seguintes princípios:

- Regulamentações vigentes;
- Melhores práticas;
- Cenários mundiais;
- Análises de risco da própria instituição.

Conforme sua criticidade, as ações do programa dividem-se em:

- **Críticas:** Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;
- **Sustentação:** Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da instituição e permitindo que ações de longo prazo/estruturantes possam ser realizadas;
- **Estruturantes:** Iniciativas de médio/longo prazo que tratam a causa raiz dos riscos e que preparam o ASA para o futuro.

6.14. Proteção de perímetro.

Para mitigação do risco de vazamento de informações utilizamos ferramentas preventivas instaladas em dispositivos móveis, estações de trabalho e servidores, no serviço de correio eletrônico, no serviço de navegação WEB, no serviço de impressão, além do uso de criptografia para dados em repouso e em transporte.

6.15. Proteção interna

Para proteção da infraestrutura do ASA contra-ataques internos, utilizamos ferramenta de antimalware homologada contra ameaças cibernéticas. O antimalware é responsável pela detecção, proteção e mitigação dessas ameaças.

7. Declaração de anuência

No momento da admissão, os colaboradores do ASA aderem formalmente as Políticas do ASA, comprometendo-se a agir de acordo com os normativos internos da Instituição, incluindo, mas não se limitando, a Política de Segurança da Informação. As atualizações da Política de Segurança de Informação são divulgadas para os colaboradores no website do ASA.

8. Sigilo e Confidencialidade:

Tanto o contrato de trabalho firmado entre o ASA e seus colaboradores, quanto os contratos contratos firmados com o ASA com fornecedores, parceiros e terceiros, devem contemplar cláusula de confidencialidade que assegure o dever de sigilo e confidencialidade das

informações as quais as partes tenham acesso em decorrência do relacionamento com o ASA, além daobrigatoriedade de seguir as regulamentações vigentes, referentes ao tema de segurança da informação.

9. Papéis e Responsabilidades

São os papéis e responsabilidades:

Diretoria:

- Aprovar, em última instância, esta Política de Segurança da Informação;
- Garantir a disponibilização de recursos humanos, tecnológicos e financeiros adequados para a implementação e manutenção dos controles de segurança da informação.
- Patrocinar e apoiar a cultura organizacional de segurança, garantindo o comprometimento das lideranças e áreas de negócio.
- Acompanhar periodicamente os indicadores estratégicos de risco cibernético e de conformidade, assegurando o atendimento às normas internas e regulatórias.
- Acompanhar planos de ação e melhorias contínuas, com base em resultados de auditorias, avaliações de riscos e incidentes relevantes.

Head de TI

- Planejar, garantir a implementação e manter a Gestão de Segurança da Informação em conformidade com as nomas aplicáveis ao ASA, em especial, da Resolução CMN 4.893/2021.
- Realizar avaliações periódicas de risco, propondo controles, políticas e normas complementares necessárias à proteção dos ativos informacionais.
- Elaborar planos de ação e melhorias contínuas, com base em resultados de auditorias, avaliações de riscos e incidentes relevantes;
- Reportar periodicamente à Alta Administração o desempenho, a eficácia dos controles e os riscos de segurança identificados.
- Garantir a realização testes de continuidad de negócios;

Equipe de Segurança Informação:

- Desempenhar suas atividades em conformidade com a presente política bem como os manuais e procedimentos internos aprovados pelo Head de TI;
- Conduzir monitoramento contínuo de eventos e incidentes de segurança, garantindo resposta rápida e comunicação adequada às partes interessadas.

- Desenvolver e promover programas de capacitação e conscientização voltados à segurança da informação e cibersegurança.

- Apoiar as áreas de negócio e tecnologia no desenho seguro de soluções e produtos digitais, incluindo cloud, open finance, canais e core bancário.

- Revisar as práticas e controles de segurança da informação, assegurando aderência às políticas, normas e legislação vigente.

Área de Recursos Humanos

- Assegurar que as práticas de gestão de pessoas, desde o processo seletivo até o

desligamento, estejam alinhadas às diretrizes de segurança da.

- Garantir que todos os colaboradores e terceiros assinem Termos de Confidencialidade e Uso Responsável de Ativos.

- Integrar conteúdos de segurança e ética digital nos programas de integração, reciclagem e desenvolvimento profissional.

Compliance

- Avaliar a aderência regulatória da Política;.

Auditoria Interna

- Fornecer aos órgãos de governança e à Alta Administração avaliações abrangentes, independentes e objetivas relativas aos riscos de PLD.FTPda Instituição.

- Revisar de modo sistemático a eficácia dos processos, contribuindo para o seu aprimoramento.

Colaboradores, Terceiros e Parceiros

- Cumprir integralmente esta Política e as normas derivadas do Programa de Segurança da Informação do ASA.

- Proteger os ativos e informações sob sua responsabilidade, independentemente das medidas tecnológicas aplicadas.

- Reportar imediatamente incidentes, suspeitas de vazamentos ou violações aos canais oficiais de segurança.

- Manter o sigilo e a confidencialidade das informações acessadas, durante e após o vínculo contratual.

- Adotar conduta ética e responsável no uso de dados, sistemas, dispositivos e redes

corporativas.

10. Sanções Disciplinares

As violações a esta política estão sujeitas às sanções disciplinares previstas em normas internas das empresas do ASA e na legislação vigente onde as empresas estiverem localizadas.

11. Reporte e Canais de Contato

O ASA mantém canais formais e seguros para o reporte de incidentes, não conformidades, fraudes, vulnerabilidades e violações de segurança ou privacidade, assegurando a confidencialidade das informações e a proteção do denunciante.

Em caso de identificação de qualquer evento que possa representar risco à segurança das informações, sistemas, clientes ou colaboradores, o registro deve ser realizado de forma imediata por meio de um dos canais abaixo:

E-mail institucional de Segurança da Informação: seguranca.informacao@asa.com.br

12. Revisão da Política

Esta Política entra em vigor na data de publicação e permanecerá válida por prazo indeterminado, devendo ser revisada pelo Head de TI, no mínimo, anualmente ou sempre que houver necessidade.

13. Aprovação da Política

Esta Política deve ser aprovada em primeira instância pelo Head de TI e pelo Head de Compliance e, em última instância, pela Diretoria do ASA.

14. Documentos Relacionados

Esta Política Corporativa de Segurança da Informação é complementada por procedimentos internos específicos de Segurança da Informação, em conformidade com as normas e regulamentações vigentes e aprovados pelo Head de TI.

São Paulo, 11 de março de 2026.