CORRETORA DE CÂMBIO

PSC - POLÍTICA DE SEGURANÇA CIBERNÉTICA

VERSÃO: 2026

SUMÁRIO

1. OBJETIVO

Esta Política de Segurança Cibernética estabelece diretrizes, responsabilidades e controles adotados pela ARC Corretora de Câmbio, Associados Gouveia, Campedelli S.A. (ARC) para proteger seus ativos de informação, sistemas e operações contra ameaças cibernéticas, assegurando a confidencialidade, integridade e disponibilidade das informações.

A política está em conformidade com a Resolução BCB nº 85/2021, conforme alterações posteriores, incluindo a Resolução BCB nº 538/2025, sendo compatível com o porte reduzido da instituição, seu modelo de negócio e nível de complexidade operacional.

Os objetivos de segurança cibernética da instituição incluem a capacidade de prevenir, detectar e reduzir a vulnerabilidade a incidentes cibernéticos, por meio da adoção de controles técnicos, operacionais e organizacionais proporcionais ao seu porte e nível de risco.

Adicionalmente, a instituição busca responder de forma tempestiva a incidentes de segurança cibernética, minimizar seus impactos e assegurar a continuidade das operações, bem como proteger os dados de clientes e manter a conformidade regulatória junto ao Banco Central do Brasil.

2. PERFIL DA INSTITUIÇÃO, PORTE E MODELO DE NEGÓCIO

A ARC é uma instituição de pequeno porte, enquadrada no Segmento 5 (S5) do Banco Central do Brasil, com aproximadamente 12 colaboradores, especializada em:

- câmbio manual (compra e venda de moeda estrangeira em espécie);
- câmbio comercial/comex posição própria (ingresso/remessa/exportação/importação);
- intermediação em operações de câmbio (ingresso/remessa/exportação/importação).

As operações de câmbio manual são realizadas presencialmente na sede da instituição, mediante atendimento direto aos clientes. As operações de câmbio comercial/comex (posição própria e intermediação) são conduzidas por meio de contato direto com os clientes, principalmente por correio eletrônico e telefone, com posterior registro e processamento nos sistemas utilizados pela instituição e pelas instituições financeiras parceiras.

A instituição não possui correspondentes cambiais, agentes terceirizados, filiais ou postos de atendimento externos para a realização de suas operações. O atendimento aos clientes e a execução das atividades operacionais são realizados exclusivamente em sua sede, por colaboradores contratados sob o regime da Consolidação das Leis do Trabalho (CLT), sob supervisão direta da Diretoria da instituição.

A carteira de clientes das operações de câmbio comercial é composta predominantemente por clientes tradicionais e recorrentes, com relacionamento de longa data com a instituição, contribuindo para maior conhecimento do perfil dos clientes e para a estabilidade operacional dos negócios realizados.

A estrutura operacional enxuta e a atuação direta da Diretoria no acompanhamento das atividades

contribuem para o fortalecimento dos controles internos, para a adequada supervisão das operações e para a mitigação dos riscos operacionais, de conformidade e de segurança da informação.

A instituição possui baixo nível de complexidade operacional e risco tecnológico moderado, decorrente da utilização de sistemas informatizados para registro, processamento e controle das operações, bem como para a comunicação com instituições financeiras parceiras.

3. ARQUITETURA TECNOLÓGICA E AMBIENTE OPERACIONAL

A infraestrutura tecnológica da instituição é composta por:

- sistema de câmbio e base cadastral de clientes Syscâmbio (Stallos Tecnologia);
- sistema de monitoramento de operações e clientes E-Guardian (Advice Tecnologia);
- utilização do Google Workspace para correio eletrônico corporativo, armazenamento de documentos e colaboração interna;
- recursos de armazenamento e controle de documentos eletrônicos utilizados nos processos internos;
- acesso remoto controlado, quando necessário, mediante mecanismos de segurança definidos pela instituição;
- suporte técnico prestado por consultoria especializada em tecnologia da informação (Supptec Consultoria em TI).

Os acessos aos sistemas são individuais e controlados por mecanismos de autenticação, observando perfis e níveis de permissão compatíveis com as atribuições de cada colaborador.

A instituição adota soluções tecnológicas compatíveis com seu porte, perfil operacional e volume de negócios, priorizando a continuidade das operações, a segurança das informações e a conformidade regulatória.

4. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

A presente Política de Segurança da Informação e Segurança Cibernética está fundamentada nos seguintes princípios:

- **Confidencialidade:** garantia de que as informações sejam acessadas somente por pessoas autorizadas e no exercício de suas atribuições;
- **Integridade:** preservação da exatidão, consistência e completude das informações e dos registros mantidos pela instituição;
- **Disponibilidade:** garantia de que sistemas, informações e recursos tecnológicos estejam acessíveis aos usuários autorizados sempre que necessário para a execução das atividades da instituição;

- **Rastreabilidade:** capacidade de identificar, registrar e verificar ações realizadas em sistemas, processos e informações, permitindo a adequada apuração de eventos e responsabilidades;
- **Prevenção e resposta a incidentes:** adoção de medidas destinadas à prevenção, identificação, tratamento e mitigação de incidentes que possam comprometer a segurança da informação e a continuidade das operações.

5. GESTÃO DE RISCOS E CONTROLES DE SEGURANÇA CIBERNÉTICA

A instituição adota controles de segurança da informação e segurança cibernética compatíveis com seu porte, perfil operacional e nível de exposição a riscos, visando proteger seus ativos de informação e assegurar a continuidade de suas atividades.

5.1. Controle de acesso e autenticação

O acesso aos sistemas, recursos tecnológicos, arquivos eletrônicos e informações da instituição é controlado por mecanismos de autenticação e credenciais individuais, garantindo a identificação inequívoca de cada usuário.

São adotados procedimentos e controles relacionados à autenticação, incluindo:

- utilização de identificações e senhas individuais e intransferíveis;
- adoção de critérios de complexidade e segurança para criação e manutenção de senhas;
- bloqueio automático de sessões após período de inatividade;
- utilização de mecanismos de autenticação adicional (como autenticação em múltiplos fatores), quando disponibilizados pelos sistemas utilizados;
- proibição de compartilhamento de credenciais de acesso entre usuários.

Os acessos são concedidos e revisados com base no princípio do menor privilégio, garantindo que cada usuário possua apenas as permissões necessárias para o desempenho de suas atividades.

As permissões de acesso são revisadas sempre que houver alteração de função, desligamento ou necessidade operacional identificada.

5.2. Proteção de sistemas e rede

A instituição adota medidas de proteção compatíveis com seu ambiente tecnológico e perfil operacional, visando reduzir a exposição a ameaças cibernéticas e preservar a segurança das informações.

Dentre os controles adotados, destacam-se:

- utilização de firewall para proteção da rede corporativa;

- utilização de solução de antivírus e antimalware nos equipamentos da instituição;
- aplicação de mecanismos de proteção dos serviços de correio eletrônico utilizados pela instituição;
- controle de acesso aos recursos de rede e aos ambientes tecnológicos;
- utilização de mecanismos de criptografia fornecidos por sistemas e serviços utilizados pela instituição, incluindo correio eletrônico corporativo (Google Workspace) e demais plataformas de terceiros, quando aplicável;
- proteção de dados em trânsito e, quando suportado pelos sistemas utilizados, proteção de dados armazenados por meio de mecanismos de criptografia disponibilizados pelos fornecedores;
- gestão e utilização de certificados digitais, quando aplicáveis às integrações, autenticações e comunicações seguras entre sistemas e serviços utilizados pela instituição;
- atualização periódica de sistemas operacionais, aplicativos e demais softwares utilizados nas atividades da instituição;
- monitoramento e suporte técnico realizados por prestadores especializados, quando aplicável.

A implementação e manutenção desses controles observam critérios de proporcionalidade ao porte da instituição, à complexidade de suas operações e aos riscos identificados.

5.3. Proteção de e-mails e comunicação

A instituição utiliza o Google Workspace como plataforma de correio eletrônico e colaboração, o qual dispõe de mecanismos de segurança incorporados pelo próprio provedor, incluindo recursos de proteção contra spam e tentativas de phishing, além de autenticação segura e criptografia das comunicações, conforme aplicável ao serviço.

Complementarmente, são adotadas práticas internas de conscientização dos colaboradores quanto ao uso seguro do e-mail corporativo, incluindo orientações para evitar a abertura de links ou anexos de origem desconhecida e para reporte imediato de mensagens suspeitas ao suporte técnico responsável.

Essas medidas visam reduzir riscos associados a fraudes eletrônicas e garantir maior segurança no uso dos canais de comunicação da instituição.

5.4. Backup e continuidade de negócios

A instituição adota práticas de backup e preservação de informações compatíveis com seu porte e ambiente tecnológico, com o objetivo de reduzir o risco de perda de dados e assegurar a continuidade das operações.

São adotadas medidas como:

- realização de backups das informações e sistemas utilizados nas atividades operacionais, conforme aplicável ao ambiente tecnológico da instituição;

- armazenamento das cópias de segurança em local logicamente segregado do ambiente principal ou em ambientes controlados por provedores de serviços;
- suporte técnico especializado responsável pelo acompanhamento e suporte às rotinas de backup e recuperação de informações.

A continuidade das operações é suportada pela utilização de sistemas redundantes fornecidos por terceiros e por procedimentos internos que visam garantir a retomada das atividades em caso de indisponibilidade de recursos tecnológicos.

5.5. Atualização e manutenção de sistemas

A instituição adota práticas de atualização e manutenção dos sistemas utilizados em suas operações, com o objetivo de manter a segurança, estabilidade e adequação tecnológica do ambiente.

Dentre essas práticas, destacam-se:

- aplicação de atualizações de segurança (patches) disponibilizadas pelos fornecedores de sistemas e softwares utilizados;
- acompanhamento e revisão periódica dos softwares instalados nos equipamentos corporativos;
- atualização dos sistemas Syscâmbio (Stallos Tecnologia) e E-Guardian (Advice Tecnologia) conforme disponibilização e orientação do fornecedor;
- adoção de validações operacionais antes e após atualizações relevantes, de forma a assegurar a continuidade adequada dos processos.

As atualizações são realizadas de forma controlada, considerando o impacto operacional e o risco associado a cada alteração.

5.6. Integração de sistemas e interfaces eletrônicas

A instituição adota controles de segurança aplicáveis às integrações entre sistemas internos e externos, incluindo aqueles utilizados na comunicação com instituições financeiras parceiras e fornecedores de tecnologia.

As integrações de sistemas, bem como eventuais ajustes ou correções manuais de dados realizados em soluções de TI, são efetuadas por meio de mecanismos controlados, observando rígidos critérios de alçada, autorização prévia, segurança de acesso e manutenção de trilhas de auditoria (logs) para a rastreabilidade total das operações modificadas.

Para assegurar a conformidade dessas integrações, a instituição prioriza a contratação de fornecedores e bancos parceiros regulados ou solidamente estabelecidos no mercado, exigindo contratualmente que suas APIs e interfaces eletrônicas possuam mecanismos nativos de autenticação segura, criptografia de dados em trânsito e registro de logs.

Localmente, a instituição limita sua atuação à configuração de travas técnicas de timeout em seus sistemas,

mitigando impactos de lentidão externa. Em caso de indisponibilidade dessas interfaces, a mesa de operações adotará canais alternativos de contingência (como portais web dos parceiros, e-mail corporativo ou ordens via mesa de voz). Interrupções nas integrações que ultrapassarem o limite de tolerância de 1 (uma) hora serão tratadas como incidentes de alto impacto e registradas na Base de Perdas Operacionais.

6. CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

As informações sob responsabilidade da instituição são classificadas de acordo com seu grau de sensibilidade e relevância para as atividades operacionais, bem como considerando o impacto potencial de sua divulgação não autorizada, alteração indevida ou indisponibilidade.

Para fins de tratamento e proteção, as informações são classificadas em:

- **públicas:** informações de divulgação geral ou disponíveis ao público;
- **internas:** informações de uso restrito aos colaboradores e prestadores de serviço no exercício de suas funções;
- **confidenciais:** informações relacionadas a clientes, operações de câmbio, transações financeiras e demais dados protegidos por sigilo regulatório e obrigações legais.

As informações classificadas como confidenciais possuem nível reforçado de proteção, com controles de acesso baseados em perfis, necessidade de conhecimento e restrição de uso às atividades operacionais da instituição.

A classificação da informação orienta a aplicação de medidas de segurança proporcionais ao seu grau de sensibilidade e relevância, incluindo controles de acesso, proteção de armazenamento e restrições de compartilhamento, com o objetivo de preservar a confidencialidade, integridade e disponibilidade das informações.

7. MONITORAMENTO E RASTREABILIDADE

A instituição mantém mecanismos de registro e rastreabilidade de atividades em seus sistemas operacionais, de acordo com as funcionalidades disponibilizadas pelos fornecedores de tecnologia utilizados.

Esses registros podem incluir, conforme aplicável:

- logs de acesso aos sistemas utilizados nas operações da instituição;
- registros de alterações em dados operacionais e cadastrais;
- histórico de autenticação de usuários;
- registros de operações realizadas no sistema Syscâmbio (Stallos Tecnologia), conforme funcionalidades disponíveis.

Os registros são utilizados para fins de monitoramento operacional, controle interno e suporte à investigação de eventuais incidentes, sendo armazenados por período compatível com as exigências regulatórias aplicáveis e com as necessidades operacionais da instituição.

8. GESTÃO DE VULNERABILIDADES E PROTEÇÃO CONTRA AMEAÇAS

A instituição adota medidas de segurança da informação e boas práticas operacionais voltadas à prevenção de ameaças cibernéticas e à redução de riscos associados ao seu ambiente tecnológico.

São consideradas ameaças relevantes, entre outras:

- malware e ransomware;
- phishing e tentativas de engenharia social;
- acessos não autorizados a sistemas e informações;
- ataques e tentativas de comprometimento de rede.

Para mitigação desses riscos, são adotadas medidas como:

- manutenção de soluções antivírus e antimalware atualizadas nos equipamentos utilizados;
- aplicação de atualizações de segurança (patches) disponibilizadas por fornecedores de sistemas e softwares;
- revisão de acessos e permissões de usuários sempre que necessário, especialmente em casos de alteração de função ou desligamento;
- acompanhamento de alertas, vulnerabilidades e informações de segurança cibernética disponibilizadas por fornecedores de tecnologia, ferramentas de proteção e sistemas utilizados pela instituição, incluindo indicadores de ameaças e tentativas de ataque;
- utilização de fontes de inteligência de ameaças cibernéticas disponibilizadas por fornecedores de tecnologia, ferramentas de proteção e sistemas utilizados pela instituição, incluindo indicadores de ameaças e tentativas de ataque;
- utilização dessas informações para adoção de medidas preventivas, atualização de controles e mitigação de riscos no ambiente operacional.

8.1. Gestão de Continuidade de Negócios e Resiliência Operacional

A instituição adota práticas voltadas à continuidade de suas operações, com o objetivo de reduzir impactos decorrentes de indisponibilidades de sistemas, falhas operacionais ou eventos de segurança da informação.

Essas práticas são compatíveis com seu porte, estrutura tecnológica e modelo operacional, incluindo, entre outras medidas:

- utilização de rotinas de backup e mecanismos de preservação de informações relacionados aos sistemas e recursos tecnológicos utilizados pela instituição;
- dependência de sistemas fornecidos por terceiros para execução de atividades operacionais essenciais, os quais possuem mecanismos próprios de disponibilidade, redundância e suporte técnico;
- existência de procedimentos operacionais internos voltados à retomada das atividades essenciais em caso de indisponibilidade de sistemas ou recursos tecnológicos;
- acionamento de suporte técnico especializado e de fornecedores de tecnologia para restabelecimento de serviços em situações de falha ou incidente;
- consideração de cenários de indisponibilidade prolongada ou descontinuidade de serviços prestados por fornecedores críticos de tecnologia, incluindo a avaliação de medidas alternativas, como substituição do prestador de serviços, adoção de soluções contingenciais ou migração para ambiente alternativo, com o objetivo de preservar a continuidade das operações essenciais.

Os testes de continuidade de negócios são baseados em cenários definidos a partir dos principais riscos operacionais e cibernéticos identificados pela instituição, considerando a criticidade dos processos e a dependência de sistemas e fornecedores essenciais.

Os cenários podem incluir, entre outros, indisponibilidade de sistemas críticos, falhas de comunicação eletrônica, interrupção de serviços de fornecedores relevantes e incidentes de segurança cibernética capazes de afetar a continuidade das operações.

A continuidade das operações é sustentada pela combinação de controles internos e do suporte fornecido pelos sistemas e prestadores de serviço utilizados pela instituição, visando minimizar impactos operacionais e assegurar a retomada das atividades em tempo razoável.

9. TREINAMENTO E CONSCIENTIZAÇÃO

A instituição adota práticas de orientação aos colaboradores quanto à segurança da informação e à prevenção de riscos cibernéticos, de forma compatível com seu porte e estrutura operacional.

As orientações abrangem, entre outros temas:

- identificação de e-mails fraudulentos e tentativas de phishing;
- boas práticas relacionadas ao uso de senhas e credenciais de acesso;
- cuidados no uso da internet e dos recursos tecnológicos da instituição;
- proteção de informações confidenciais e sigilosas;
- procedimentos para reporte de incidentes ou comportamentos suspeitos.

A instituição promove a disseminação contínua da cultura de segurança cibernética por meio de orientações periódicas e reforço das boas práticas de segurança da informação no ambiente operacional.

Essas ações são incorporadas à rotina de trabalho, visando aumentar a conscientização dos colaboradores sobre riscos cibernéticos e estimular comportamentos seguros no uso dos recursos tecnológicos.

A disseminação da cultura de segurança envolve todos os níveis da instituição, incluindo colaboradores e Diretoria, contribuindo para a proteção dos ativos de informação e a prevenção de incidentes de segurança.

10. USO DE RECURSOS TECNOLÓGICOS

O uso de internet, correio eletrônico e sistemas corporativos disponibilizados pela instituição deve estar prioritariamente relacionado às atividades profissionais desempenhadas pelos colaboradores.

É vedado:

- a instalação ou utilização de softwares não autorizados nos equipamentos corporativos;
- o compartilhamento de credenciais de acesso a sistemas, redes ou aplicações;
- a utilização dos recursos tecnológicos da instituição para fins ilícitos, indevidos ou incompatíveis com as atividades da empresa.

Os recursos tecnológicos disponibilizados pela instituição devem ser utilizados de forma responsável, preservando a segurança das informações, a integridade dos sistemas e a continuidade das operações.

11. CONTROLE DE ACESSO FÍSICO

O acesso às instalações da instituição é controlado por medidas de segurança física compatíveis com seu porte e estrutura operacional, com o objetivo de proteger pessoas, informações e ativos da organização.

Essas medidas incluem, entre outras:

- controle de entrada de visitantes, com registro e acompanhamento quando necessário;
- acompanhamento de terceiros durante sua permanência nas dependências da instituição;
- restrição de acesso a áreas internas de uso operacional, limitadas a colaboradores autorizados;
- adoção de práticas de controle de acesso físico às áreas onde são mantidos equipamentos e recursos tecnológicos utilizados na operação.

O controle de acesso físico visa reduzir riscos de acesso não autorizado e preservar a integridade do ambiente operacional da instituição.

12. GESTÃO DE INCIDENTES DE SEGURANÇA

A instituição considera como incidentes de segurança da informação e segurança cibernética eventos que possam comprometer a confidencialidade, integridade ou disponibilidade de sistemas, dados ou operações,

incluindo, entre outros:

- indisponibilidade de sistemas ou recursos tecnológicos;
- tentativas ou ocorrências de ataques cibernéticos;
- suspeita de acesso indevido ou não autorizado a informações;
- falhas em sistemas, equipamentos ou infraestrutura tecnológica;
- suspeita de fraude envolvendo informações ou transações.

A identificação de incidentes ocorre por meio da observação operacional, alertas de sistemas utilizados e comunicação de colaboradores, fornecedores ou parceiros tecnológicos.

A avaliação da relevância dos incidentes é realizada com base em critérios de impacto operacional, criticidade dos sistemas afetados, potencial ou efetivo comprometimento de informações e extensão dos efeitos sobre as atividades da instituição.

Os incidentes são classificados de acordo com sua severidade e relevância, considerando, entre outros parâmetros, a indisponibilidade de sistemas essenciais, o comprometimento de dados de clientes ou operações e a possibilidade de impacto na continuidade das atividades da instituição.

Essa classificação orienta a priorização do tratamento, o escalonamento interno e, quando aplicável, a comunicação aos órgãos reguladores e demais partes interessadas.

A instituição poderá estabelecer níveis de serviço (SLA) internos para tratamento e resolução de incidentes de segurança da informação, considerando sua classificação, criticidade e impacto operacional. A priorização do atendimento observará a severidade do incidente e seu potencial impacto sobre a continuidade das operações, sistemas críticos e dados de clientes.

A instituição adota iniciativas de compartilhamento de informações relacionadas a incidentes de segurança da informação considerados relevantes, envolvendo a Diretoria, áreas internas e fornecedores de tecnologia, conforme necessário para apoiar a contenção, mitigação e recuperação dos eventos.

Esse compartilhamento também tem por objetivo contribuir para o aprimoramento contínuo dos controles internos e para a prevenção de novos incidentes.

12.1. Tratamento de incidentes

Ao identificar ou suspeitar de um incidente de segurança da informação, os colaboradores devem comunicar imediatamente o suporte técnico ou responsável designado.

O tratamento dos incidentes segue fluxo estruturado, contemplando o registro formal do evento, a análise de sua causa raiz e de seu impacto potencial ou efetivo, bem como a adoção de medidas de contenção, mitigação e controle de seus efeitos sobre os sistemas, operações e informações da instituição.

O processo de tratamento inclui, quando aplicável:

1. comunicação do evento ao suporte técnico ou prestador de serviço responsável;
2. avaliação inicial do incidente quanto ao seu impacto e criticidade;
3. análise técnica das causas do incidente;
4. adoção de medidas de contenção e mitigação, quando tecnicamente viável;
5. comunicação à Diretoria da instituição, conforme a relevância do incidente;
6. recuperação das operações afetadas, incluindo a utilização de cópias de segurança e procedimentos de restabelecimento disponibilizados pelos sistemas e fornecedores.

Os incidentes são registrados e documentados com o objetivo de apoiar a melhoria contínua dos controles internos, bem como prevenir a recorrência de eventos semelhantes.

Após a resolução de incidentes relevantes, a instituição poderá realizar análise pós-incidente, incluindo a identificação da causa raiz, avaliação da efetividade das medidas adotadas e registro de lições aprendidas, com o objetivo de aprimorar continuamente os controles internos e reduzir a recorrência de eventos similares.

A instituição poderá realizar testes periódicos dos procedimentos de resposta a incidentes de segurança da informação, com base em cenários definidos internamente, visando validar a efetividade das ações de contenção, mitigação e recuperação.

Os resultados desses testes poderão subsidiar a revisão dos procedimentos de tratamento de incidentes e o aprimoramento contínuo dos controles de segurança.

12.1.1. Declaração de Crise Operacional

A instituição poderá declarar situação de crise operacional quando um incidente de segurança da informação ou segurança cibernética apresentar potencial ou efetivo impacto relevante sobre a continuidade das operações, a disponibilidade de sistemas críticos, a integridade ou confidencialidade de informações sensíveis, o cumprimento de obrigações regulatórias ou a prestação de serviços aos clientes.

Poderão caracterizar situação de crise operacional, entre outros:

- indisponibilidade prolongada de sistemas ou recursos tecnológicos essenciais às operações da instituição;
- comprometimento, perda, alteração indevida ou vazamento de informações de clientes, operações ou dados confidenciais;
- ocorrência de ataque cibernético com impacto relevante sobre os processos operacionais da instituição;
- indisponibilidade ou falha de fornecedor crítico de tecnologia que comprometa a continuidade das atividades;
- eventos que possam gerar impactos financeiros, regulatórios ou reputacionais significativos;

- necessidade de acionamento de procedimentos extraordinários de contingência para manutenção ou retomada das operações.

A avaliação para declaração de crise operacional será realizada pela Diretoria ou pelo Diretor Estatutário responsável pela Política de Segurança Cibernética, considerando a criticidade, abrangência, duração e os impactos potenciais ou efetivos do incidente.

A declaração da crise operacional, as decisões adotadas, as medidas de contenção, mitigação e recuperação implementadas e o encerramento da situação de crise deverão ser formalmente registrados e documentados pela instituição.

12.2. Comunicação ao Banco Central

A instituição avalia a necessidade de comunicação de incidentes de segurança da informação ao Banco Central do Brasil, observando a regulamentação aplicável e os critérios de relevância estabelecidos pelos normativos vigentes.

Quando aplicável, podem ser considerados incidentes relevantes, entre outros:

- interrupção relevante de serviços ou sistemas essenciais;
- suspeita ou ocorrência de acesso indevido a informações de clientes ou operações;
- eventos que possam gerar impacto operacional significativo para a instituição.

A comunicação, quando necessária, contempla a descrição do evento, sua abrangência e as medidas adotadas para contenção, mitigação e recuperação.

13. GESTÃO DE TERCEIROS

Os fornecedores de tecnologia e serviços de suporte utilizados pela instituição, incluindo, entre outros, Stallos Tecnologia, Advice Tecnologia e Supptec Consultoria em TI, desempenham atividades essenciais ao funcionamento dos sistemas e operações da instituição.

A relação com esses terceiros é baseada em instrumentos contratuais e requisitos de segurança compatíveis com as atividades desempenhadas, incluindo diretrizes mínimas de segurança da informação e segurança cibernética aplicáveis aos serviços prestados.

Essas diretrizes incluem, entre outras:

- obrigação de confidencialidade quanto às informações acessadas em razão dos serviços prestados; acesso restrito às informações e sistemas estritamente necessários à execução das atividades contratadas;
- adoção de boas práticas de segurança da informação compatíveis com a natureza dos serviços prestados;

- implementação de medidas voltadas à prevenção, identificação e mitigação de riscos de segurança cibernética;
- realização de atividades de suporte técnico somente quando autorizadas ou formalmente solicitadas pela instituição.

A instituição busca assegurar que o acesso de terceiros aos seus ambientes tecnológicos ocorra de forma controlada, limitada e alinhada às necessidades operacionais, com foco na proteção da confidencialidade, integridade e disponibilidade das informações.

13.1. Obrigação de Comunicação de Incidentes por Terceiros

Os fornecedores de serviços de tecnologia e demais terceiros que tenham acesso a sistemas, dados ou infraestrutura da instituição devem comunicar à ARC Corretora de Câmbio, de forma tempestiva, qualquer suspeita ou ocorrência de incidente de segurança cibernética que possa impactar, direta ou indiretamente, os ativos, sistemas ou informações da instituição.

Essa comunicação deve ocorrer em prazo compatível com a criticidade do evento, de modo a permitir a adoção de medidas de contenção, mitigação e resposta pela instituição, em alinhamento com seus procedimentos internos de gestão de incidentes.

Incidentes identificados em ambientes sob responsabilidade de terceiros são considerados relevantes para a operação da instituição e tratados com prioridade compatível com seu potencial impacto.

14. GOVERNANÇA E RESPONSABILIDADES

14.1. Responsabilidades das Áreas e dos Colaboradores

A segurança da informação e a segurança cibernética constituem responsabilidade compartilhada por todos os colaboradores, administradores e prestadores de serviços da instituição, observadas as atribuições de cada função.

Compete à Diretoria: assegurar a disponibilização de recursos compatíveis com o porte, a complexidade operacional e o perfil de risco da instituição, bem como supervisionar a implementação das diretrizes estabelecidas nesta política.

Compete ao Diretor Estatutário responsável pela Política de Segurança Cibernética: acompanhar a efetividade dos controles adotados, supervisionar a gestão dos riscos cibernéticos, monitorar a implementação desta política e reportar assuntos relevantes à Diretoria da instituição.

Compete ao Administrador de Redes e aos prestadores de serviços de tecnologia da informação: manter os controles técnicos de segurança, apoiar a prevenção e o tratamento de incidentes, contribuir para a continuidade operacional dos sistemas utilizados pela instituição e prestar suporte às atividades relacionadas à segurança cibernética.

Compete às áreas comercial e operacional: observar os procedimentos internos de segurança da informação durante a execução de suas atividades, proteger as informações sob sua responsabilidade, zelar pela adequada utilização dos sistemas corporativos e comunicar tempestivamente qualquer evento ou situação que possa representar risco aos sistemas, dados ou operações da instituição.

Compete a todos os colaboradores: cumprir as diretrizes desta política, utilizar adequadamente os recursos tecnológicos disponibilizados pela instituição, preservar a confidencialidade das informações e colaborar para a proteção dos ativos de informação da instituição.

Compete à Auditoria Interna: atuar como terceira linha de defesa, realizar avaliações independentes e periódicas sobre a adequação e a efetividade dos controles internos, incluindo aqueles relacionados à segurança da informação e segurança cibernética, verificando a aderência às políticas internas, aos procedimentos operacionais e aos normativos regulatórios aplicáveis.

A atuação da Auditoria Interna é independente das áreas operacionais e de tecnologia, contribuindo para o aprimoramento contínuo do ambiente de controles da instituição.

Os fornecedores de tecnologia que possuam acesso a sistemas, informações ou recursos tecnológicos da instituição devem observar os requisitos de segurança aplicáveis às atividades contratadas, manter a confidencialidade das informações acessadas e cooperar com a instituição na prevenção, identificação e tratamento de incidentes de segurança cibernética.

14.2. Responsabilidade pela Política

A responsabilidade pela implementação, manutenção e atualização desta Política de Segurança Cibernética é da Diretoria da instituição, com apoio das áreas internas envolvidas e dos fornecedores de serviços tecnológicos contratados.

O Diretor Estatutário responsável pela Política de Segurança Cibernética, devidamente registrado no UNICAD do Banco Central do Brasil, responde pela governança, supervisão e acompanhamento da efetividade das diretrizes, controles e procedimentos previstos nesta política.

A execução e o suporte às rotinas operacionais relacionadas à segurança cibernética são realizados pelo Administrador de Redes, com apoio dos prestadores de serviços de tecnologia da informação contratados, incluindo suporte técnico especializado.

A aprovação desta política é de responsabilidade da Diretoria da instituição.

14.3. Linhas de Defesa e Resiliência Operacional

A instituição adota o modelo de Três Linhas de Defesa como referência para a gestão de riscos, controles internos, segurança cibernética e resiliência operacional.

A primeira linha de defesa é composta pelas áreas operacionais e comerciais, responsáveis pela execução das atividades, observância dos procedimentos internos e aplicação dos controles estabelecidos.

A segunda linha de defesa é composta pela Diretoria e pelo Diretor Estatutário responsável pela Política de Segurança Cibernética, responsáveis pela supervisão dos riscos, monitoramento da efetividade dos controles e acompanhamento da conformidade regulatória.

A terceira linha de defesa é exercida pela Auditoria Interna, responsável por avaliações independentes da adequação e efetividade dos controles internos, da gestão de riscos e dos processos relacionados à segurança da informação e à resiliência operacional.

15. REVISÃO E APROVAÇÃO DA POLÍTICA

Esta política será revisada no mínimo anualmente, ou sempre que houver alterações regulatórias relevantes, mudanças significativas na estrutura organizacional, nos processos ou na infraestrutura tecnológica da instituição.

O documento **“PSC” - Política de Segurança Cibernética”** encontra-se formalmente aprovado pela Diretoria da instituição, com registro em ata de reunião, e é de cumprimento obrigatório por todos os colaboradores e prestadores de serviços que tenham acesso a sistemas, informações ou recursos tecnológicos da instituição.

Esta política entra em vigor na data de sua aprovação e permanecerá válida até sua substituição por versão posterior devidamente aprovada pela Diretoria.