POLÍTICA DE SEGURANÇA CIBERNÉTICA - EXTERNA

CONSAD/DIRCO

SUMÁRIO

APRESENTAÇÃO

O Banpará, comprometido com a transparência, a ética e a proteção das informações de seus clientes, parceiros e colaboradores, apresenta a sua Política de Segurança Cibernética.

Em um cenário de crescente digitalização dos serviços financeiros e intensificação das ameaças cibernéticas, esta política reflete o empenho da instituição em garantir a confidencialidade, a integridade e a disponibilidade das informações, bem como em assegurar a continuidade e a confiabilidade de suas operações.

A elaboração deste documento está alinhada às diretrizes da Resolução CMN nº 4.893/2021, da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e às melhores práticas nacionais e internacionais de governança, gestão de riscos e segurança da informação.

Por meio desta política, o Banpará reafirma seu compromisso em:

I. Proteger as informações de clientes, parceiros e da própria instituição contra acessos indevidos, perdas ou uso inadequado;

II. Implementar controles e tecnologias compatíveis com seu porte e perfil de risco;

III. Promover uma cultura de segurança e conscientização digital entre todos os envolvidos;

IV. Atuar com transparência, responsabilidade e conformidade regulatória.

Esta política é parte integrante da estrutura de governança corporativa da instituição e deve servir como referência para o público em geral quanto às práticas de segurança e privacidade adotadas.

OBJETIVO

Esta Política visa informar, de forma clara e transparente, os compromissos e diretrizes do Banpará em relação à segurança da informação e à segurança cibernética, assegurando a proteção de dados, a continuidade dos serviços financeiros e a conformidade com a Resolução CMN nº 4.893/2021, a Lei Geral de Proteção de Dados (LGPD) e demais normas aplicáveis.

ABRANGÊNCIA

Esta Política de Segurança Cibernética aplica-se a todas as áreas, processos, sistemas, informações, produtos e serviços do Banpará, abrangendo:

I. Todos os colaboradores, dirigentes e estagiários da instituição, independentemente do vínculo funcional ou local de trabalho;

II. Todos os prestadores de serviços, parceiros e fornecedores que, de forma direta ou indireta, tenham acesso a informações, sistemas ou infraestrutura tecnológica da instituição;

III. Todos os clientes e usuários que utilizem os canais digitais, produtos ou serviços oferecidos pela instituição;

IV. Todos os ativos de informação, incluindo dados físicos e digitais, documentos, comunicações, sistemas, equipamentos e ambientes tecnológicos sob responsabilidade da instituição.

Esta política é aplicável em todas as unidades físicas e ambientes tecnológicos, bem como em ambientes terceirizados e serviços em nuvem contratados pela instituição, garantindo a observância dos princípios de confidencialidade, integridade e disponibilidade da informação.

DIRETRIZES

1. COMPROMISSOS COM A SEGURANÇA DA INFORMAÇÃO

O Banpará adota medidas técnicas e organizacionais para:

I. Proteger dados e informações contra acessos não autorizados, vazamentos e alterações indevidas;

II. Assegurar a continuidade dos serviços prestados aos clientes, mesmo diante de ameaças cibernéticas;

III. Gerenciar riscos tecnológicos e cibernéticos de forma proativa e proporcional à sua estrutura;

IV. Promover conscientização e orientação de segurança para colaboradores, clientes e parceiros;

V. Garantir transparência e responsabilidade no tratamento de informações e no relacionamento com o público.

2. PRINCÍPIOS DE ATUAÇÃO

Nossa política é guiada pelos seguintes princípios:

I. **Governança e alta gestão:** A segurança da informação é supervisionada pela alta administração e está integrada ao sistema de controles internos da instituição.

II. **Proporcionalidade e adequação:** Os controles são compatíveis com o porte, a complexidade e o perfil de risco da instituição.

III. **Resiliência e continuidade:** A instituição adota práticas para manter a operação diante de incidentes.

IV. **Melhoria contínua:** A política e os controles são revisados e atualizados conforme necessário.

V. **Responsabilidade compartilhada:** Clientes, colaboradores e parceiros são parte do ecossistema de segurança.

3. PROTEÇÃO AOS CLIENTES E AO PÚBLICO

O Banpará adota uma série de práticas para proteger seus clientes e parceiros:

I. Utilização de tecnologias seguras, como criptografia e autenticação multifator;

II. Monitoramento constante de ameaças, fraudes e vulnerabilidades;

III. Orientações educativas sobre boas práticas de segurança digital;

IV. Tratamento adequado dos dados pessoais, respeitando os princípios da LGPD;

V. Notificação transparente em caso de incidentes que envolvam dados sensíveis.

4. RISCOS CIBERNÉTICOS E CONTROLES TÉCNICOS

O Banpará adota uma abordagem estruturada para gestão de riscos cibernéticos, que envolve:

I. Identificação e avaliação de riscos associados à tecnologia e à informação;

II. Implantação de controles preventivos, detectivos e corretivos;

III. Monitoramento contínuo do ambiente tecnológico;

IV. Condução de testes e simulações de segurança, sempre que necessário.

5. SERVIÇOS EM NUVEM E TERCEIRIZAÇÕES

Na contratação de serviços de computação em nuvem ou provedores terceirizados o Banpará:

I. Avalia previamente os riscos de segurança e privacidade;

II. Exige cláusulas contratuais que garantam a confidencialidade, integridade e disponibilidade das informações;

III. Monitora a conformidade dos prestadores com os requisitos regulatórios.

6. TRATAMENTO DE INCIDENTES DE SEGURANÇA

O Banpará mantém um processo estruturado para o tratamento de incidentes de segurança, garantindo:

I. Resposta rápida e eficaz a eventos que possam comprometer dados ou operações;

II. Comunicação aos clientes e autoridades competentes, sempre que necessário;

III. Registro, análise e melhoria contínua dos processos de segurança;

IV. Apoio ao cliente em situações de fraudes ou ataques cibernéticos.

7. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

O Banpará trata os dados pessoais com responsabilidade, respeitando a LGPD (Lei nº 13.709/2018), com base nos seguintes princípios:

I. Finalidade, necessidade e transparência no uso das informações;

II. Consentimento e direitos dos titulares respeitados em todos os processos;

III. Implementação de medidas de segurança adequadas ao tipo de dado tratado.

PAPÉIS E RESPONSABILIDADES

1. INSTITUIÇÃO

I. O Banpará possui uma estrutura de governança voltada à segurança da informação e à segurança cibernética, com papéis e responsabilidades claramente definidos em todos os níveis da organização.

II. A política é aprovada e supervisionada pela alta administração, assegurando que a segurança da informação esteja integrada à estratégia corporativa e ao sistema de controles internos.

III. A instituição mantém profissionais e comitês especializados responsáveis por coordenar ações de prevenção, monitoramento e resposta a incidentes, bem como por promover a conscientização e o uso seguro das informações.

IV. Todos os colaboradores, parceiros e prestadores de serviços têm o dever de cumprir esta política e atuar de forma ética e responsável na proteção das informações e dos sistemas sob sua responsabilidade.

2. CLIENTES E USUÁRIOS DOS SERVIÇOS

I. Adotar boas práticas de segurança digital, como atualização de senhas, uso de canais oficiais e não compartilhamento de dados sigilosos;

II. Comunicar prontamente a instituição em caso de suspeita de fraude, vazamento ou uso indevido de informações;

III. Respeitar os termos de uso e confidencialidade definidos pela instituição em seus canais digitais.

ÁREA GESTORA

Caberá ao Núcleo de Segurança da Informação e Proteção de Dados Pessoais atuar como gestor na criação/alteração das diretrizes a serem aplicadas neste documento.

ÁREA DE APROVAÇÃO

Esta política é revisada sempre que necessário, pela Diretoria de Tecnologia, especialmente em decorrência de mudanças nos riscos, em atualizações legais ou em alterações na estrutura tecnológica da instituição. A nova versão será publicada em nossos canais oficiais.

GLOSSÁRIO

ATAQUE CIBERNÉTICO: Ação maliciosa com o objetivo de comprometer sistemas, roubar dados, interromper serviços ou obter vantagens indevidas por meio de recursos tecnológicos.

CONFIDENCIALIDADE: Princípio da segurança da informação que garante que apenas pessoas autorizadas possam acessar determinadas informações.

CRIPTOGRAFIA: Técnica utilizada para proteger informações, transformando-as em códigos que só podem ser lidos por quem possui a chave de acesso.

DADOS PESSOAIS: Informações que identificam ou podem identificar uma pessoa física, como nome, CPF, endereço, e-mail ou dados bancários.

DISPONIBILIDADE: Princípio que assegura que as informações e sistemas estejam acessíveis e operacionais sempre que necessário.

GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO: Estrutura que define responsabilidades, processos e controles voltados para garantir a proteção das informações e o cumprimento das normas legais.

INTEGRIDADE: Princípio que assegura que as informações sejam exatas, completas e não alteradas de forma indevida.

LGPD (LEI GERAL DE PROTEÇÃO DE DADOS): Lei nº 13.709/2018, que estabelece regras para o tratamento de dados pessoais, garantindo direitos aos titulares e deveres às organizações.

RISCO CIBERNÉTICO: Probabilidade de ocorrência de um evento que possa causar impacto negativo à instituição em decorrência de falhas ou ataques relacionados à tecnologia e informação.

SEGURANÇA CIBERNÉTICA: Conjunto de práticas, processos e tecnologias voltados à proteção de sistemas, redes e dados contra ataques e acessos indevidos.

SERVIÇOS EM NUVEM: Infraestrutura ou software hospedado remotamente (geralmente na internet) e utilizado pela instituição para armazenamento, processamento ou execução de aplicações.

VULNERABILIDADE: Fragilidade ou falha que pode ser explorada por um atacante para comprometer a segurança de sistemas ou informações.

REFERÊNCIA

Banco Central - Resolução CMN nº 4.893/2021.