POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. OBJETIVO

A presente **Política de Segurança Cibernética** ("**Política**") visa estabelecer os princípios, diretrizes e responsabilidades sobre os aspectos relacionados à segurança cibernética, na intenção de garantir a proteção das informações que são de propriedade do "**Conglomerado Prudencial**" composto pela Administradora de Consórcio Nacional Gazin LTDA ("**Consórcio Nacional Gazin**") e pela GazinCred S.A. Sociedade de Crédito, Financiamento e Investimento ("**GazinBank**") - Líder do Conglomerado Prudencial, buscando preservar a sua integridade, disponibilidade e confidencialidade.

2. PÚBLICO-ALVO

Esta Política tem como público-alvo todos os diretores, colaboradores, parceiros, prestadores de serviços ou terceiro que tenham ou venham a ter acesso às informações controladas pelo **Conglomerado Prudencial**.

3. REGULAMENTAÇÕES E NORMAS APLICÁVEIS

- Lei n.º 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Resolução n.º 4.893/2021 do Banco Central do Brasil (Bacen);
- Regulamentações e normas internas do **Conglomerado Prudencial** que estão relacionadas à segurança da informação, inclusive a Política de Segurança da Informação do Grupo Gazin.

4. CONCEITOS E CLASSIFICAÇÕES

Para garantir a segurança dos ativos do Conglomerado Prudencial, esta Política está pautada nos pilares da Confidencialidade, Integridade e Disponibilidade, que podem ser assim definidos:

- **Confidencialidade:** garantia que as informações sejam acessíveis exclusivamente para pessoas autorizadas;
- **Integridade:** garantia de que as informações sejam mantidas de forma íntegra, sem a ocorrência de modificações sem autorização;
- **Disponibilidade:** garantia que as informações estejam disponíveis às pessoas autorizadas.

As informações e dados sob controle do **Conglomerado Prudencial,** serão classificados da seguinte maneira:

- **Público:** informação sem restrição, passível de consulta e divulgação externa. Geralmente possuem caráter informativo e são direcionados ao público externo em geral;

- **Confidencial:** informação que se destina ao uso específico por um usuário ou grupo de usuários, a sua divulgação pode afetar os negócios do **Conglomerado Prudencial**;

- **Interno:** informação que é destinada ao uso interno do **Conglomerado Prudencial**, disponível aos usuários, não sendo desejável o seu conhecimento ao público externo.

5. RESPONSABILIDADES

5.1 DIRETORIA

- Aprovar e supervisionar o desenvolvimento, a implementação e o desempenho da estrutura de gerenciamento de segurança cibernética, incluindo as diretrizes constantes na presente Política.

- Prover os recursos necessários para gestão e implementação da segurança da informação;

- Assegurar a aderência às políticas de segurança cibernética e da informação;

- Comprometimento com a melhoria contínua dos procedimentos relacionados à segurança cibernética.

5.2 TECNOLOGIA DA INFORMAÇÃO

- Implementar e gerenciar as medidas de segurança cibernética e da informação, sendo responsável por monitorar e responder às ameaças cibernéticas;

- Realizar testes de melhoria contínua que avaliem a eficácia das diretrizes adotadas, levando-se em conta: o tempo de solução, os mecanismos, procedimentos e controles utilizados e o conhecimento dos envolvidos no plano;

- Realizar relatório contendo o escopo e os resultados dos testes realizados e as mudanças necessárias deverá ser criado e entregue à Alta Administração;

- Desenvolver e atualizar, sempre que necessário, melhorias no tratamento de segurança cibernética e da informação;

- Ser proativo na identificação de eventuais violações de segurança cibernética, promovendo ações de prevenção de incidentes, vulnerabilidade e demais ameaças nos ambientes físicos e digitais do **Conglomerado Prudencial**;

- Conscientizar os colaboradores sobre as diretrizes da segurança da informação e cibernética.

5.3 ÁREA DE CONTROLES INTERNOS E COMPLIANCE

- Garantir que os regulamentos e políticas internas de conformidade e retenção de documentos sejam cumpridos.

5.4 AUDITORIA INTERNA

- Reportar-se diretamente ao Diretor Presidente a fim de garantir isenção e autonomia no exercício de suas atividades nas demais diretorias do **Conglomerado Prudencial**;
- Estar atualizada e ser constantemente treinada para exercer suas atividades com eficácia;
- Supervisionar os processos de segurança cibernética e da informação.

5.5 COLABORADORES

- Cumprir as políticas e procedimentos de segurança cibernética e da informação;
- Utilizar de modo consciente e seguro os sistemas do **Conglomerado Prudencial**;
- Reportar para a área de Tecnologia da Informação sobre eventuais incidentes de segurança cibernética e da informação que venham tomar conhecimento, o mais rápido possível.

6. ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA

A estrutura de gerenciamento de segurança inclui três componentes importantes:

6.1 Gestão de Acesso

As informações e dados serão monitorados, controlados e restringidos aos usuários que efetivamente necessitam ter o acesso, ao término da relação contratual o colaborador ou prestador de serviço não terão mais acessos, a fim de garantir a privacidade e integridade das informações.

6.2 Proteção do Ambiente Físico

Inclui medidas de segurança para os equipamentos, hardwares e demais instalações físicas contra acesso não autorizado ou danos físicos, que devem ser mantidos em ambientes seguros com níveis e controles de acessos adequados.

6.3 Proteção do Ambiental Virtual

Envolve a proteção contra ameaças cibernéticas, como vírus, malware e ataques de rede. Inclui soluções de segurança de rede, software antivírus e firewall, bem como o **Conglomerado Prudencial** adota controles e responsabilidades para garantir a segurança de seu ambiente virtual, aplicando um gerenciamento efetivo dos acessos aos dados e à informação.

Estes componentes trabalham juntos para garantir a segurança e a privacidade das informações do **Conglomerado Prudencial** e proteger contra ameaças internas e externas.

7. DIRETRIZES GERAIS PARA O TRATAMENTO DE INCIDENTES DE SEGURANÇA CIBERNÉTICA

O **Conglomerado Prudencial** busca de forma responsável e consciente evidenciar os cuidados para recuperação de eventuais ativos que possam estar envolvidos em eventos que venham abalar os pilares de segurança da informação.

Nesse sentido, o **Conglomerado Prudencial** elaborou o Plano de Respostas de Incidentes, que elenca as principais diretrizes e responsabilidades para o tratamento de incidentes de segurança da informação, podendo ser acessada por todos os diretores, colaboradores e prestadores de serviços que possuem qualquer relação com o **Conglomerado Prudencial**.

8. PROCEDIMENTOS E CONTROLES DE SEGURANÇA CIBERNÉTICA

Na intenção de adotar medidas administrativas e técnicas para mitigação de riscos, o **Conglomerado Prudencial** adotará os seguintes procedimentos e controles de segurança cibernética:

- Autenticação de dois fatores e controle criptográfico;
- Proteção contra softwares maliciosos;
- Controle de Acesso;
- Gestão de vulnerabilidade;
- Controle de mídia móvel;
- Testes de invasão;

- Segurança de aplicações;
- Segmentação da rede de computadores.

9. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

O processo de gestão de continuidade de negócios relativo à segurança cibernética, deverá estabelecer, documentar e implementar procedimentos para minimizar os impactos e recuperar os ativos de informação afetado em eventuais incidentes de segurança, bem como preservar a reputação e imagem do **Conglomerado Prudencial** diante de uma crise.

O modelo a ser adotado para a gestão de continuidade de negócio será baseado na Norma ISO 27001:2013 e as demais normas elencadas no Plano de Continuidade de Negócio do **Conglomerado Prudencial**.

10. CONTRATAÇÃO DE PRESTADORES DE SERVIÇOS

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem devem ser comunicadas ao Banco Central do Brasil, informando a denominação da empresa e os serviços contratados, bem como a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, conforme resolução 4.893/2021 do Bacen.

Nesse contexto, o **Conglomerado Prudencial** adotará critérios para a contratação de prestadores de serviços e parceiro para o processamento e armazenamento de dados e de computação em nuvem, avaliando a capacidade do potencial prestador de serviço de assegurar:

- O cumprimento da legislação e da regulamentação em vigor;
- O acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
- A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
- A sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;
- O acesso do **Conglomerado Prudencial** 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;

- O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos; e
- A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

11. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Todos os procedimentos realizados de acordo com esta Política devem observar as legislações relacionadas à proteção de dados aplicáveis, em especial a Lei Geral de Proteção de Dados (Lei n. 13.709/208), e às políticas internas do **Conglomerado Prudencial**.

12. ELABORAÇÃO DE RELATÓRIO ANUAL

A elaboração do relatório sobre a implementação dos planos de ações e de respostas a incidentes da segurança cibernética deverá ser realizada anualmente, utilizando como data base o dia 31 de dezembro de cada ano e submetido à análise da Alta Administração até 31 de março do ano subsequente. O relatório anual deverá conter:

- Descrição resumida dos resultados obtidos na implementação dos procedimentos relacionados à segurança cibernética;
- Os procedimentos a serem utilizados e a efetividade na prevenção e na resposta a eventuais incidentes;
- Os incidentes relevantes ocorridos no período;
- Os resultados dos testes de continuidade de negócios.

13. CONSIDERAÇÕES FINAIS

O **Conglomerado Prudencial** visa pela disseminação da cultura da privacidade, proteção e segurança da informação e cibernética entre seus colaboradores, prestadores de serviços ou terceiro que tenham ou venham a ter qualquer relação com o **Conglomerado Prudencial**. Dessa forma, o **Conglomerado Prudencial** implementará os seguintes procedimentos:

Divulgação pública – interna e externa – da presente Política em versão resumida;

- Implementação de programas de capacitação e avaliação periódica de pessoal;

- Conscientização de usuários e clientes sobre os cuidados para utilização de produtos financeiros;

- Comprometimento da Alta Administração com a melhoria contínua dos procedimentos previstos nesta Política.

14. VIGÊNCIA

Esta Política entra em vigor na data de sua publicação e será revisada no mínimo anualmente, ou quando necessário, caso haja alguma mudança das normas e políticas do **Conglomerado Prudencial** ou se requerido por autoridade competente.