A Gerencianet, atenta ao quesito do Art. 5º da Circular 3.909/18 do Banco Central do Brasil (BACEN), divulga ao público um resumo contendo as linhas gerais de sua Política de Segurança Cibernética e da Informação.

1. INTRODUÇÃO

A Circular 3.909/18 do BACEN dispõe sobre a política de segurança cibernética e os requisitos para os serviços de processamento e armazenamento de dados e de computação em nuvem contratados por instituições de pagamento.

Tal Circular exige que as instituições de pagamento implementem e mantenham política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

2. OBJETIVO

Estabelecer princípios e diretrizes de segurança cibernética e da informação para proteção e disciplina do uso dos ativos de informação da Gerencianet ou sob sua custódia, com observância dos princípios da confidencialidade, integridade e disponibilidade.

3. ABRANGÊNCIA

Destina-se a todos os colaboradores da Gerencianet e às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações. Além disso, abrange também o público em geral, como clientes da plataforma Gerencianet e quaisquer interessados.

4. DEFINIÇÕES

Segurança da Informação: visa a preservar as propriedades de confidencialidade, integridade, disponibilidade, não se limitando a sistemas computacionais, informações eletrônicas e/ou sistemas de armazenamento.

5. GERENCIANDO A SEGURANÇA DA INFORMAÇÃO

O objetivo da Segurança Cibernética e da Informação da Gerencianet é garantir a gestão sistemática e efetiva dos aspectos relacionados à segurança da informação e cibernética, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos a instituição.

A informação é um ativo que deve ser protegido e cuidado por meio de regras e procedimentos das políticas de segurança, do mesmo modo que protegemos nossos recursos financeiros e patrimoniais.

5.1. Objetivos da Segurança da Informação

A segurança da informação tem como objetivo a preservação de três princípios básicos pelos quais se norteiam a implementação desta prática:

1. *Confidencialidade:* garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso. Caso a informação seja acessada por uma pessoa não autorizada, intencionalmente ou não, ocorre a quebra da confidencialidade.

2. *Integridade:* garantia da exatidão e completeza da informação e dos métodos de processamento. Garantir a integridade é permitir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e permaneça consistente. Quando a informação é alterada, falsificada ou furtada, ocorre a quebra da integridade.

3. *Disponibilidade:* garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. Quando a informação está indisponível para o acesso, ou seja, quando os servidores estão inoperantes, por exemplo, ocorre quebra de disponibilidade.

5.2. Objetivos da Segurança Cibernética

A segurança cibernética envolve os processos empregados para salvaguardar e proteger os ativos utilizados para transportar informações de uma organização contra roubo ou ataque. O gerenciamento de identidades, o gerenciamento de riscos e de incidentes formam a base das estratégias de segurança cibernética da instituição.

Além dos objetivos da segurança cibernética estarem alinhados com a prevenção de ataques contra as infraestruturas críticas, redução das vulnerabilidades e minimizar os danos e o tempo de recuperação pós-ataques, busca-se proteger os pilares confidencialidade, integridade e disponibilidade dos ativos tecnológicos e de informações.

6. PRINCÍPIOS DA SEGURANÇA NA GERENCIANET

- A instituição segue diretrizes para a classificação, manuseio e rotulagem da informação, podendo ser:
    - Pública
    - Uso Interno
    - Confidencial

- Elaborar, implantar e seguir políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação da Gerencianet sejam atingidos através da adoção de controles contra ameaças provenientes de fontes internas e externas;

- Manter a capacidade de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, utilizando-se de registros de rastreabilidade de informações da Instituição e de seus clientes;

- Proteger as informações contra acessos e modificações indevidas, destruição ou divulgação não autorizada;
- Proteger ativos tecnológicos e estabelecer procedimentos de monitoramento das redes da Instituição e dos dispositivos dos colaboradores com vistas a prevenir, detectar e reduzir a vulnerabilidade a ataques digitais;
- Aplicação de práticas de desenvolvimento seguro de softwares, incorporando lições aprendidas em projetos, treinamentos, busca da redução do custo de manutenção ao antecipar bugs e vulnerabilidades, identificar e mitigar o risco de segurança em novos projetos e tecnologias empregadas nas atividades da instituição;
- Tratar integralmente incidentes de segurança cibernética e da informação, garantindo que sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicado às autoridades apropriadas;
- Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;
- Adoção do princípio da "mesa limpa e tela limpa" voltado aos colaboradores, estagiários e prestadores de serviço para que não deixem informações à vista e as descartem adequadamente sempre que necessário;
- Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como colaboradores, estagiários, fornecedores, prestadores de serviço e, onde pertinente, clientes;
- Garantir a educação e conscientização sobre as práticas adotadas pela Gerencianet quanto a segurança da informação para colaboradores, estagiários, fornecedores, prestadores de serviço e, onde pertinente, clientes;
- Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais.

7. REVISÃO E ATUALIZAÇÃO

Esta política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência, conforme entendimento da Gestão da Gerencianet.

8. CONSIDERAÇÕES FINAIS

Outras políticas, normas, procedimentos ou termos, bem como outros complementares que detalhem ou evidenciem esta matéria, serão mantidas à disposição dos colaboradores, reguladores e auditorias.