POLÍTICA
DE SEGURANÇA CIBERNÉTICA

DEZEMBRO - 2020

Índice

1.Objetivo

A Política de Segurança Cibernética desta Instituição tem como objetivo definir e garantir a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda, assim como o tratamento dos riscos e ameaças relacionadas ao ambiente cibernético com base na Resolução Nº 4.4658 de 26 de abril de 2018 do Banco Central do Brasil e demais normas e disposições aplicáveis.

2. Responsabilidades

O cumprimento da Política de Segurança Cibernética desta Instituição é de responsabilidade de todos os colaboradores e prestadores de serviços, com a abrangência sobre as atividades que envolvam dados e informações no ambiente cibernético.

A alta Administração desta instituição, compromete-se com a melhoria contínua dos procedimentos e controles relacionados nesta Política, assim como com a atualização no mínimo, anualmente.

Quaisquer indícios de incidentes ou irregularidades citadas nesta Política, devem ser comunicadas imediatamente para o departamento de Governança, Risco e Compliance

3. Definições e Conceitos

Segurança da Informação: Concentrar os esforços contínuos à proteção dos ativos de informação. Tem como objetivos a confidencialidade, integridade e disponibilidade.

Confidencialidade: Garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

Integridade: Garantir que as informações sejam mantidas integras, sem modificações indevidas – acidentais ou propositais;

Disponibilidades: Garantir que as informações estejam disponíveis às pessoas autorizadas a tratá-las;

Segurança cibernética: Capacidade de identificar, prevenir, proteger, detectar, responder e recuperar rapidamente de uma ameaça no espaço cibernético;

Espaço cibernético: Relacionado a internet, os sistemas de informação, os dispositivos móveis e as tecnologias digitais que dão suporte ao negócio, a infraestrutura e os serviços;

Ataque cibernético: São situações nas quais hackers maliciosos tentam danificar, destruir ou violar uma rede ou sistema, por meio de diferentes técnicas.

4. Procedimentos e Controles de Segurança Cibernética

Para rastrear as informações na busca de garantir a segurança e reduzir a vulnerabilidade da instituição a incidentes, serão adotado os procedimentos e controles a seguir:

4.1 Autenticação e Controle de acesso

O acesso as informações e aos ambientes tecnológicos da Instituição devem ser permitidos apenas às pessoas autorizadas pelo proprietário da informação.

O controle de acesso aos sistemas deve ser formalizado e feito através de credencial individual, monitorada, revisada e passíveis de bloqueios e restrições.

4.2 Criptografia

Toda solução de criptografia utilizada deve seguir as regras de segurança da informação e padrões de segurança dos órgãos reguladores.

4.3 Proteção contra softwares maliciosos

Todos os ativos que estejam conectados à rede corporativa ou faça uso de informação da Instituição, sempre que compatível, devem ser protegidos com uma solução de endpoint.

4.4 Gestão e detecção de vulnerabilidades

As varreduras das redes internas e externas devem ser executadas periodicamente. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

4.5 Testes de Invasão

Teste de invasão das redes internas e externas devem ser realizados no mínimo anualmente.

4.6 Respostas a incidentes de segurança cibernética

O plano de respostas a incidentes considera o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para a atividades da instituição.

Para definir o grau de relevância são considerados aspectos como comprometimento de dados de clientes e impacto ao sistema financeiro.

A área de risco elaborará um relatório anual contendo os incidentes ocorridos no período, as ações realizadas, respostas aos incidentes e resultados de testes de continuidade, com data base 31 de dezembro. Este relatório deve ser apresentado a alta gestão.

4.7 Rastreabilidade

Deve acontecer a gravação de logs ou trilhas de auditória para todos os componentes de sistema de forma a permitir identificar quem fez o acesso, quando o acesso foi feito, o que foi acessado e como foi acessado.

As informações dos registros (logs) ou trilhas de auditoria devem ser protegidas contra modificações e acessos não autorizados.

4.8 Prevenção a vazamento de Informações

Utilização de controle para garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados ou vazados na web por usuários não autorizados.

4.9 Segmentação da rede de computadores

Computadores conectados à rede corporativa não devem ser acessíveis diretamente pela internet.

A criação, alteração e exclusão de regras dos firewalls e ativos de rede só podem ser realizadas mediante análise a aprovação da Área de Governança de TI.

4.10 Cópias de segurança dos dados e das informações

O processo de execução de backups é realizado, periodicamente, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

5. Processamento, armazenamento de dados e computação em nuvem

Esta instituição tem critérios definidos, aderentes a Resolução 4.658/2018, para contratação de serviços relevantes de processamento e armazenamento de dados e incluem a identificação e segregação de dados dos clientes, além de garantia de confidencialidade, integridade, disponibilidade e recuperação de dados e informações processadas ou armazenadas.

6. Continuidade dos negócios

O processo de continuidade de negócios é implementado com intuito de reduzir os impactos e perdas de ativos da informação após incidente crítico a um nível aceitável, por meio do mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados na nuvem e os testes previstos para os cenários de ataque cibernético.

7. Recomendações de segurança aos clientes e usuários

O cliente e os usuários são responsáveis pelos atos executados com seu identificador de login, que é único para o acesso à informação e aos recursos de tecnologia.

É recomendado:

- Manter a confidencialidade, memorizar e não registrar senha em lugar algum;
- Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
- Impedir o uso do seu equipamento por outras pessoas, enquanto estiver conectado com sua identificação;
- Bloquear sempre o equipamento ao se ausentar

8. Disseminação da cultura de segurança cibernética

Esta instituição promove a disseminação dos princípios e diretrizes de segurança cibernética através de programas de conscientização e treinamentos específicos, visando o fortalecimento da cultura interna de gestão de segurança da informação.

9. Compartilhamento de Informações

Os incidentes classificados com relevância alta/crítica deverão ser reportados aos órgãos reguladores competentes e aptos a receber a informação no momento de sua detecção.

Adicionalmente, a equipe responsável pelo gerenciamento de incidentes deverá buscar ferramentas seguras e de ampla utilização pelo mercado para compartilhar com outras instituições os incidentes relevantes com o objetivo de impedir que o ato malicioso se espalhe.

10. Divulgação

Esta política de segurança deverá ser compartilhada com todos os funcionários da Instituição e publicada nos canais de comunicação acessíveis aos clientes.