Resumo da Política de Segurança da Informação

June 2019

Aprovado em [03/07/2019]
Versão [1.0]

1. Introdução

A informação é um importante ativo para a condução de negócios e sua preservação é essencial para sua existência. Independentemente da forma apresentada ou do meio pelo qual é compartilhada, a informação deve ser utilizada somente para a finalidade para a qual foi autorizada. Deste modo, toda informação de propriedade do Banco ABN AMRO S.A. ("AAB Brasil") deve ser protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.

Assim, incidentes que afetam a confidencialidade, integridade e disponibilidade do cliente ou informações bancárias podem ter impacto negativo sobre a reputação do banco e seus clientes. Isso pode resultar em substancial dano financeiro ou reputacional, como perdas financeiras diretas, diminuição nos negócios, sanções por reguladores ou reivindicações legais.

Assim, visando contemplar o art. 5° da Resolução No. 4.658, de 26 de abril de 2018 ("Resolução 4658"), divulga-se ao público o presente resumo da Política, contendo suas linhas gerais e princípios no qual o AAB Brasil baseia sua atuação.

2. Regulamentação Aplicável

A presente política de segurança da informação respeita e está em conformidade, no que se aplica, com: (i) a legislação brasileira, incluindo a lei No. 13.709, de 14 de agosto de 2018; (ii) as resoluções Conselho Monetário Nacional – CMN, normas do Banco Central do Brasil, incluindo a Resolução 4658.

3. Princípios de Segurança da Informação

3.1 A segurança da informação está focada em proteger as informações contra uma ampla gama de ameaças, a fim de garantir a continuidade do negócio e minimizar os riscos do negócio. Baseado nos conceitos definidos no ISO / IEC 27000, o AAB Brasil tem definido a segurança da informação como a "preservação da confidencialidade, integridade e disponibilidade (CIA) da informação".

3.2 A segurança da informação, de acordo com o art. 2° da Resolução 4658, visa assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados e seus ativos associados, como por exemplo, computadores e arquivos em papel, a partir de quebras acidentais ou intencionais de:

- Confidencialidade: garantir que somente usuários autorizados tenham acesso a informações e ativos associados;

- Integridade: salvaguarda da acuracidade, integridade e pontualidade das informações e processamento de informações;

- Disponibilidade: garantia de que os usuários autorizados tenham acesso quando necessário para informações e ativos associados.

3.3 Ativos de Informação

Ativos de informação incluem:

(a) Dados;

(b) Mídias de armazenamento;

(c) Aplicações;

(d) Redes de comunicação de dados; e

(e) Infra-estrutura de TI, sistemas, instalações de processamento.

O valor dos ativos de informação para o negócio leva a identificar as medidas de segurança a serem implementadas.

Os princípios de segurança da informação direcionam a gestão de riscos de segurança da informação e formam a base para as normas de segurança da informação mais específicas.

4. Papéis e responsabilidades

4.1 Responsabilidade da segurança da informação (1ª linha de defesa)

(a) As pessoas, em todos os níveis, são responsáveis pela segurança da informação.

(b) A gestão de cada linha de negócio é responsável pela implementação de normas e políticas de segurança da informação nas atividades de negócio.

(c) Os gestores devem monitorar e relatar o cumprimento das políticas de segurança de informação e normas aprovadas dentro de sua área de responsabilidade.

(d) A gestão deverá designar um responsável pela segurança da informação que irá coordenar todas as atividades de segurança da informação dentro das linhas de negócios.

(e) A gestão deve documentar como a segurança da informação é organizada dentro de suas linhas de negócios.

4.2 Supervisão da segurança da informação (2ª linha de defesa)

A coordenação e supervisão da segurança da informação no ABN AMRO Bank N.V. é de responsabilidade do CISO (Corporate Information Security Office), em estreita cooperação com os responsáveis locais e de negócio da segurança da informação.

5. Gestão de Risco de Segurança da Informação

O AAB Brasil descreve na Política um conjunto de diretrizes, controles e atividades que o AAB Brasil deve seguir para cumprimento da Política Segurança da Informação do Grupo ABN AMRO (*Group Information Security Policy*), baseados em um processo que prevê o planejamento, execução, controle e ação, buscando a melhoria contínua da gestão de segurança da informação no AAB Brasil.