POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

BANCO ALFA

Março/2018

ÍNDICE

1. OBJETIVO

Definir as diretrizes que nortearão a elaboração das normas e padrões que tratam da proteção das informações detidas pelas empresas do Conglomerado Alfa, abrangendo sua geração, utilização, armazenamento, distribuição, confidencialidade, disponibilidade e integridade, independentemente do meio em que elas estejam contidas.

2. RESPONSABILIDADES

É de responsabilidade do Comitê Diretivo de Segurança e Contingência garantir a atualização e publicação da Política de Segurança da Informação no portal corporativo.

Todos os colaboradores são responsáveis por manter a segurança das informações sob sua responsabilidade, posse ou guarda, assim como garantir o cumprimento desta Política, das Normas Corporativas de Segurança da Informação e dos Manuais de Instrução do Conglomerado Alfa publicados no portal corporativo.

3. DIRETRIZES

A. Tratamento da Informação

A informação sob custódia das empresas do Conglomerado, mesmo que pertencente a clientes ou fornecedores, deve ser protegida contra o acesso de pessoas não autorizadas.

A geração, utilização, armazenamento, manutenção, distribuição e destruição da informação devem ser feitas de acordo com as necessidades das empresas. Estes processos devem estar devidamente documentados e serem passíveis de monitoração e auditoria.

Devem ser usados somente recursos autorizados para garantir o compartilhamento seguro da informação, quando for necessário, além da identificação das pessoas que possuem acesso a informações confidenciais.

A informação deve ser armazenada, pelo tempo determinado pelas empresas ou legislação vigente, o que for maior, protegida por backups e recuperável quando necessário. O local de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos de pessoas não autorizadas.

B. Acesso à Informação

As redes externas de comunicação (Internet, redes privadas, etc.) devem ser controladas através de Servidores de Firewalls, Servidores de Acesso à Internet, Servidores de AntiSpam, ferramentas de Antivírus e políticas de sistemas operacionais que garantam

que somente os recursos necessários estejam disponíveis para o trabalho, sem riscos para o ambiente operacional.

Devem ser realizados testes nos sistemas e dispositivos de rede e de segurança que visem identificar vulnerabilidades conhecidas, sendo que para os sistemas e dispositivos expostos à internet estes testes devem ser diários.

A remessa de dados das empresas do Conglomerado Alfa, seja para atender requisitos de negócios, seja para viabilizar a resolução de problemas encontrados, deve ser avaliada em função dos riscos, bem como devem ser adotados procedimentos que garantam o controle e a integridade dos dados e a legitimidade do receptor das informações. O que for acordado deve ser formalizado e aprovado pelos gestores responsáveis pela informação.

C. Sistemas Aplicativos

Sistemas aplicativos desenvolvidos dentro das empresas do Conglomerado Alfa devem ser documentados e controlados quanto às alterações ou correções feitas, com trilhas do que foi feito e guarda segura da biblioteca de fontes. Toda informação necessária para eventual reconstrução dos aplicativos deve constar de sua documentação.

Sistemas aplicativos desenvolvidos fora das empresas do Conglomerado Alfa, de propriedade de terceiros (com licença de uso para o Conglomerado), devem ter a biblioteca de fontes e de recursos adicionais (bibliotecas adquiridas, componentes, etc.) sob custódia de uma entidade idônea, de comum acordo entre o Conglomerado e a empresa fornecedora do *software*. Tais fontes devem sempre ser atualizadas e verificadas quanto a sua validade e sincronização com a versão em uso no ambiente de produção.

O mau uso dos sistemas, feito de forma acidental ou deliberada, deve ser combatido pela segregação das funções de administração do sistema das funções de execução de certas atividades, ou entre áreas de responsabilidade. Tal segregação de funções visa criar controles para evitar fraudes ou conluios no desempenho de atividades críticas do sistema. Quando for impraticável implantar a segregação, outros controles como monitoramento das atividades, trilhas de auditoria e acompanhamento gerencial devem ser considerados.

As senhas para acesso aos aplicativos devem ser complexas e possuir quantidade de caracteres suficientes para que dificulte a quebra das mesmas.

Para minimizar o risco de falhas nos sistemas, deve-se fazer planejamento e preparações prévias para garantir a disponibilidade e capacidade adequada dos recursos. Para novos

sistemas os requisitos operacionais devem ser documentados e testados antes da sua aceitação e uso. Para sistemas já em uso devem ser feitas projeções da demanda de recursos e da carga da máquina futura a fim de reduzir o risco de indisponibilidade por sobrecarga (*Capacity Planning*).