POLÍTICA DE SEGURANÇA CIBERNÉTICA

Em atendimento à Resolução nº 4658 de 26 de abril de 2018, apresentamos a seguir os principais pontos de nossa Política de Segurança Cibernética.

- A Diretoria do Banco Tricury aprovou a Política e está comprometida com a melhoria contínua dos procedimentos relacionados com a Segurança Cibernética.
- O Banco Tricury designou Diretor Responsável pela Política e pela execução do plano de ação e de resposta a incidentes relevantes
- O Banco Tricury conduz e documenta, no mínimo anualmente, testes de continuidade de negócios em Back Up site próprio localizado no centro de São Paulo e no site contingencial específico de SPB em empresa contratada. O cenário avaliado nos testes é de total impossibilidade de utilização dos equipamentos e sistemas no endereço da matriz do Banco Tricury.
- Nossa Política prevê estrita observação dos direitos de autor dos softwares utilizados nos seus computadores. Para garantia da uniformidade dos sistemas utilizados, os computadores disponibilizados não possuem qualquer mecanismo que possibilite a transferência de programas ilícitos, tais como leitores de CD, pen drives ou outros e a área de TI estabelece travas lógicas nos equipamentos para garantir a integridade dos dados e sistemas.
- Todos os computadores disponibilizados são acionados através do uso de login e senha pessoais permitindo, dessa forma, a rastreabilidade de sua utilização.
- O Banco adquiriu de empresa especializada, firewall para prevenção e detecção de intrusão e gerenciamento de segurança que passa periodicamente por atualizações, e análise de eficiência.
- A Política prevê princípios de uso aceitável de e-mail corporativo e de consultas a web sites. A instituição possui ferramentas para bloqueio de acesso a sites considerados potencialmente perigosos para a integridade dos dados e sistemas.
- O Banco adquiriu sistema antivírus que é atualizado automaticamente e acompanhado da própria área de TI em todos os computadores utilizados pelos colaboradores.
- A Política prevê plano de ação de resposta à incidentes relevantes com registro da ocorrência, protocolos de encaminhamento imediato à áreas pré-definidas, planejamento de ação corretiva e, finalmente, apreciação pelo Comitê de Riscos Operacionais com registro em ata específica. Para efeito de classificação de relevância, todos os dados da instituição são considerados

confidenciais e os incidentes sempre serão considerados no mais alto grau de severidade e relevância.

- Anualmente a Área de TI elabora relatório para apreciação da Diretoria, contendo os incidentes registrados e os resultados dos testes de continuidade conduzidos.
- A revisão completa da Política acontece anualmente e envolve a área de TI, o Diretor Responsável e a Diretoria do Banco.
- A versão completa e atualizada da Política de Segurança Cibernética encontra-se disponibilizada a todos os colaboradores em nossa rede e atalho para os manuais nas respectivas “áreas de tralho” dos computadores e em versão impressa em nosso Manual de Procedimentos e Controles Internos.

BANCO TRICURY S/A
Diretoria
Março de 2019