Política de Segurança da Informação e Segurança Cibernética

Versão:2

Av. Cesário Alvim, 2209 - Bairro Aparecida
CEP 38400-696 - Uberlândia/MG
www.tribanco.com.br

1. Segurança da Informação

1.1 Introdução

A Segurança da Informação implementa um conjunto de controles, políticas, processos, procedimentos e estruturas organizacionais para garantir a confidencialidade, integridade e disponibilidade das informações. Estes controles são estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir os objetivos declarados em atendimento ao negócio.

A área de Segurança da Informação tem como compromisso proteger e suportar a operação do Tribanco e suas Controladas com o uso responsável da informação. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

Neste sentido, a área de Segurança da Informação atua nos seguintes campos:

- Gestão de Acessos;
- Segurança de Redes, Dados e Sistemas;
- Gestão de Incidentes de Segurança;
- Conscientização, Sensibilização e Treinamento em Segurança;
- Gestão de Riscos e Vulnerabilidades;
- Projetos de Segurança;
- Segurança para Meios de Pagamentos;
- Segurança Cibernética; e
- Privacidade e Proteção de Dados Pessoais.

A Área de Segurança da Informação tem o objetivo de proteger e suportar a operação do Tribanco e suas Controladas e de fomentar o uso responsável quanto ao acesso e utilização da informação, além de:

- Dar subsídios para a organização cumprir com requisitos legais e regulatórios;
- Avaliar ameaças de segurança da informação e cibernética atuais e futuras ao negócio;
- Proteger as informações críticas;
- Orientar para o desenvolvimento de sistemas e serviços com segurança; e
- Agir de maneira profissional e ética.

1.2 Da Informação

A informação é um ativo essencial para os negócios e, por este motivo deve ser adequadamente protegida e tratada de forma ética conforme os seguintes princípios:

- **Confidencialidade:** garantir que o acesso à informação seja obtido somente por pessoas autorizadas e quando for de fato necessário;
- **Disponibilidade:** garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário; e
- **Integridade:** garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

Colaboradores, prestadores de serviços ou fornecedores possuem responsabilidade sobre as informações sob a sua custódia e devem estar cientes dos riscos que representa ao negócio, tais como, vazamento de informação e fraudes. Assim, devem se preocupar com a exposição de informações, bem como com o descarte correto de informações sensíveis.

1.3 Tratamento da Informação

Todas as informações do Tribanco e suas Controladas devem receber a segurança para proteção adequada seguindo os princípios e diretrizes estabelecidos pela área de Segurança da Informação durante todo o seu ciclo de vida, criação, manuseio, armazenamento, transporte e descarte.

Toda informação de propriedade ou em custódia do Tribanco e suas Controladas e de suas empresas controladas deverá ser classificada apropriadamente de acordo com seu grau risco, cabendo ao gestor da área notificar seus colaboradores de suas responsabilidades, de acordo com as diretrizes descritas para Classificação de Informações.

2. Diretrizes de Segurança da Informação

Toda informação corporativa deve ser utilizada apenas para a finalidade para a qual foi destinada.

Garantir a segregação de funções para os processos críticos, assim mitigando conflito de interesse, por meio da participação de mais de um colaborador ou área responsável.

Nenhum colaborador deve possuir expectativa de privacidade quando utilizando os recursos computacionais fornecidos pela empresa.

A organização possui e mantém um processo de avaliação de risco de segurança da informação, que visa estabelecer critérios para aceitação e priorização para tratamento dos riscos.

Todo o acesso será liberado e gerenciado através do uso de login corporativa único com conjunto de fatores para identificar de forma digital o usuário, o uso é pessoal e intransferível. O colaborador será caracterizado como o responsável pelas ações realizadas pela sua identidade digital.

Todo acesso estará disponível durante o período de prestação de serviços para o Tribanco e suas Controladas. Liberado na admissão e sendo bloqueado por qualquer eventualidade como desligamento, férias, licença e afastamento.

O acesso será liberado seguindo o critério de menor privilégio e a partir do mapeamento do perfil de acesso, garantindo o acesso a recursos e informações para o desempenho de suas atividades.

Na alteração de função, cargo e/ou departamento o acesso será readequado de acordo com o novo perfil, revogando todos os acessos anteriores.

Qualquer incidente de segurança deverá ser reportado para a área de Segurança da Informação, não devendo ser divulgados a terceiros ou outras partes que não estejam diretamente envolvidas com o incidente.

O Tribanco e suas Controladas disponibilizam recursos de comunicação como e-mail corporativo e sistema de mensagens instantâneas.

O Tribanco e suas Controladas fazem uso de tecnologias para defesa contra um ataque cibernético.

Quando necessário o acesso remoto será realizado somente através de meios de conexões seguras utilizando-se de técnicas criptográficas.

O Tribanco e suas Controladas assim como as empresas prestadoras de serviço que trafegam, processam e armazenam dados de cartões devem seguir requisitos do PCI-DSS em sua última versão, assim como leis e regulamentações vigentes.

Não é permitido aos colaboradores o ingresso na rede corporativa através de dispositivos pessoais.

O uso de ambiente em nuvem deve possuir garantias a segurança da informação em todo processo de transferência, armazenamento e processamento de dados garantindo a disponibilidade, confidencialidade e integridade das informações, assim como legislações e regulamentações vigentes no Brasil.

Ambiente em nuvem deverá prover características equiparáveis de segurança da estrutura física. Todo dado armazenado em nuvem deverá ser criptografado quando em descanso e em transferência.

2.1 Processos de Segurança da Informação

- Gestão de Ativos de Informação: garantir que os ativos associados ao armazenamento e trafego de informações deverão ser identificados, classificados quanto a sua criticidade para a organização, inventariados, protegidos e ter uma documentação e planos de manutenção estruturados, mantidos e atualizados.
- Classificação da Informação: toda informação deve ser classificada em conforme o seu valor, requisitos legais, sensibilidade e criticidade. De acordo com os seguintes rótulos: Confidencial, Interna e Pública. Deve ser considerada a necessidade do negócio e o impacto no caso de utilização indevida da informação.
- Gestão de acessos: o processo de concessão, revisão e revogação de acessos deve ser documentado e analisado criticamente, baseado nas premissas de segurança da informação e de negócio, em observância aos requisitos de menor privilégio e de segregação de função, onde um colaborador não deverá exercer mais de uma função no processo de aprovação.
- Segurança Cibernética: a área de Segurança da Informação por meio da estratégia de segurança cibernética deverá executar ações de monitoramento ativo para prever e antecipar possíveis estratégias e ou métodos de ataque, para combater as ameaças em ambientes corporativos.
- Ambiente em nuvem: a área de Segurança da Informação aplica as diretrizes de controles de segurança para os ambientes em nuvem em observância as legislações, órgãos regulatórios como BACEN.
- Gestão de Riscos e vulnerabilidades de segurança: a área de Segurança da Informação atuará na gestão dos riscos e vulnerabilidades de segurança através do monitoramento contínuo e proativo, apoiando a área de tecnologia nas correções necessárias.
- Gestão de Incidentes de Segurança da Informação: o processo de gerenciamento de incidentes de Segurança da Informação determina que todo incidente deve ser registrado e reportado a área de Segurança da Informação.
- A área de Segurança da Informação será responsável pela notificação à área de Risco Operacional, quando identificado a necessidade de ação imediata destas áreas e reporte do incidente aos órgãos externos.
- Conscientização, sensibilização e Treinamento em Segurança: a área de Segurança da Informação promove o treinamento, educação e conscientização dos princípios de segurança da informação e cibernético através de atualizações de políticas, documentações e treinamentos relevantes.
- Governança de Segurança da Informação: a área de Segurança da Informação realiza a gestão e a governança alinhados aos objetivos estratégicos do Tribanco

e suas Controladas, para agregar valor e garantir que os riscos estão adequadamente endereçados e tratados.

Os projetos das áreas de negócio e tecnologia da informação devem estar alinhados às diretrizes de segurança da informação, em observância aos princípios básicos de confidencialidade, integridade e disponibilidade das informações.

- Segurança Física do Ambiente: a área de segurança da informação tem como premissa estabelecer os controles e regras de acesso de acordo com a criticidade e importância das informações residentes nos dispositivos físicos no local.
- Segurança no Desenvolvimento de Sistemas: o processo de desenvolvimento de sistemas deve garantir a aderência da Política de Segurança da Informação e Cibernética, mitigação de ameaças e vulnerabilidades críticas, reduzindo incidentes e consequentemente a exploração das vulnerabilidades em aplicações de negócio.

2.2 Propriedade Intelectual

A propriedade intelectual é um conceito que visa abranger bens materiais e imateriais como marcas, nomes de domínio, nomes empresariais, obras intelectuais, como por exemplo, base de dados, fotografias, desenhos, ilustrações, texto, de uso exclusivo do Banco.

Quaisquer ativos de propriedade intelectual do Tribanco e suas Controladas, não devem ser utilizadas para fins particulares ou repassadas, ainda que tenham sido obtidas, desenvolvidas ou inferidas pelo próprio colaborador em suas atividades de trabalho.

3. Declaração de Responsabilidade

Todos os colaboradores contratados devem aderir formalmente a Política de Segurança da Informação e Cibernética, comprometendo-se a agir de acordo com as diretrizes descritas na mesma.

4. Violações da Política

Qualquer violação à Política de Segurança da Informação e Cibernética poderá implicar em penalidades administrativas e penalidades legais, não obstante, podendo implicar em sanções cíveis e criminais.

5. Risco Operacional

A área de Segurança da Informação é responsável pela Política de Segurança da Informação e Cibernética. A política também é revisada e supervisionada pela Diretoria de Riscos, discutida em comitês específicos e aprovada pelo Conselho de Administração.