INTESA SANPAOLO BRASIL SA

RESUMO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

EM ATENDIMENTO A RES.4.658/18

EMITIDO POR: DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO

DATA DA EMISSÃO: ABRIL DE 2021

Introdução

Os sistemas de informação do Intesa Sanpaolo Brasil S.A. – Banco Múltiplo ("ISPBR") armazenam informações financeiras, contratuais e de negócios, além de informações sensíveis relacionadas a clientes e colaboradores. Estas informações representam um ativo estratégico para o ISPBR e estão expostas a riscos cibernéticos relacionados à segurança da informação inerente aos métodos e mecanismos de tratamento e utilização destes dados para a prestação dos serviços. Desta forma, estes ativos devem ser protegidos para assegurar a sua integridade, disponibilidade e confidencialidade.

A Política de Segurança da Informação do ISPBR estabelece as diretrizes para implantação de processos e controles relacionados à segurança da informação, de forma a assegurar o gerenciamento dos riscos associados ao tema de forma efetiva. Tais diretrizes devem ser adotadas pelos colaboradores e parceiros de negócios do ISPBR no exercício de suas atividades, em cumprimento a Resolução CMN nº 4.658, publicada pelo Banco Central do Brasil em 26 de Abril de 2018.

1. Principais objetivos da Segurança da Informação

- Garantir a integridade, disponibilidade e confidencialidade das informações gerenciada, processada e armazenada pelos sistemas de informação do ISPBR;
- Estabelecer controles de acesso, criptografia, monitoramento e proteção dos recursos e sistemas de forma a preservar a sua confidencialidade e integridade;
- Capacitar o ISPBR de mecanismos que permitam a avaliação dos riscos de segurança da informação de maneira rápida e efetiva, permitindo a recuperação segura em caso de incidentes, com a consequente normalização dos serviços;
- Detectar e responder de maneira efetiva a eventos de segurança da informação visando a eliminação ou redução dos fatores de risco a um nível aceitável;
- Identificar e avaliar os riscos internos e externos relacionados à segurança da informação que possam representar ameaças diretas ou indiretas aos sistemas de informação do ISPBR;

2. Controles e recursos utilizados pela Segurança da Informação

O ISPBR se utiliza de diversos controles e mecanismos que visam garantir o nível de segurança da informação adequado, de acordo com as orientações de sua Casa Matriz e dos órgãos reguladores. As funções destes controles técnicos variam entre bloqueios de acessos indesejados, sites maliciosos ou de conteúdo impróprio, análises de vulnerabilidade do ambiente tecnológico, garantia de replicação e backups dos dados, entre outros.

Esses controles visam manter os pilares da segurança da informação no que diz respeito a privacidade, continuidade e disponibilidade, reduzindo vulnerabilidades da instituição a incidentes. As áreas técnicas, assim como os funcionários e prestadores de serviços devem zelar para que estes controles estejam sempre presentes e que sejam respeitados e seguidos corretamente.

O ISPBR trabalha continuamente na evolução dos seus controles e políticas, assim como na identificação de novas necessidades, que poderão exigir novas implementações ou modificações nos controles existentes.

Dentre os controles e recursos podemos citar:

- **Controles de firewall, detecção de intrusos e detecção de tentativas de invasão**

  Visam bloquear ataques e tentativas de invasão ao ambiente de processamento de dados
- **Cofre de senhas**

  Visa manter o controle das atividades administrativas executadas no ambiente de processamento de dados do ISPBR.
- **Controle de acesso**

  Visam limitar acessos aos sistemas de operação, documentos internos e ferramentas de comunicação como e-mail ou comunicadores.
- **Bloqueio de mídias removíveis**

  Visa restringir o acesso às mídias removíveis como CDs, DVDs, Pendrive e similares reduzindo o risco de contaminação do ambiente por estes vetores.
- **Antimalware**

  Visa a proteção contra programas maliciosos em todo o ambiente de processamento de dados do ISPBR
- **Controle de cópias de segurança (Backups) e replicação de dados**

  Cópias de segurança dos dados e sistemas do ISPBR são executadas regularmente de forma segura, visando garantir a sua recuperação em caso de necessidade, buscando assegurar a continuidade de negócios. Além disso existe um processo de replicação de dados entre os ambientes de TI para a recuperação mais rápida de arquivos de uso diário
- **Inteligência Cibernética**

  O ISPBR se utiliza de inteligência sobre ameaças de fontes internas e externas, (incluindo fontes públicas, agências governamentais locais e do exterior, organizações privadas, mídias sociais, deep web, e outras fontes) para se prevenir contra as intenções, ferramentas e técnicas que possam representar ameaça ao ambiente de processamento de dados do ISPBR.
- **Planos de Recuperação:**

  Visam garantir que o ISPBR esteja pronto para se recuperar caso ocorra um dano que não permita a utilização de seus sistemas e recursos de processamento de dados.

Todos estes recursos e mecanismos são testados e avaliados periodicamente quanto à sua efetividade e rapidez na resposta de forma a identificar os riscos e melhorar o nível de proteção ao ambiente de processamento de dados do ISPBR.

3. Papéis e Responsabilidades

O gerenciamento e controle da segurança da informação é realizado através de controles, funções e responsabilidades definidas para assegurar a devida segregação das atividades e controles, em atendimento a Res. 4.557/17.

4. Gestão da Segurança da Informação

A gestão do risco de Segurança da Informação está associada à gestão integrada dos riscos, e é exercida pelo Oficial de Segurança da Informação, que reporta à Direção Executiva do ISPBR. O Oficial de Segurança da Informação é responsável pela segurança física e lógica da instituição, tanto para aspectos técnicos quanto de negócio. Sua função é proteger pessoas, ativos, infraestrutura e tecnologias.
Dentre suas tarefas, podemos destacar a criação e manutenção do programa de segurança da informação, que inclui definição de políticas e procedimentos, implementação de plano de comunicação para alertas sobre incidentes de segurança da informação, plano de resposta a incidentes, atualização ou implementação de tecnologias para segurança dos ativos físicos e lógicos.

5. Revisão e atualização das diretrizes

A Política de Segurança da Informação do ISPBR é revisada no mínimo, anualmente, a fim de assegurar a adesão às normas legais, regulamentares, estatutárias e demais instruções relevantes de forma efetiva, para o correto desempenho das atividades.