Política de Segurança
Cibernética

1. Objetivo

O objetivo desta política é estabelecer as diretrizes necessárias para assegurar a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados pelo Conglomerado Prudencial, conforme estrutura societária vigente, doravante denominada SAFRA. A gestão dessa política é realizada pela empresa líder do Conglomerado Prudencial.

2. Público Alvo

As disposições desta política aplicam-se: (i) a todas as instituições pertencentes ao Conglomerado Prudencial SAFRA, bem como aos respectivos funcionários, estagiários e aprendizes, doravante denominados "colaboradores"; (ii) às entidades e aos órgãos que possuam acesso as informações do SAFRA; e (iii) aos prestadores de serviços, pessoas físicas ou jurídicas, que manuseiam dados ou informações sensíveis à condução das atividades operacionais da organização

3. Princípios de Segurança Cibernética

O processo de Segurança Cibernética do Conglomerado Prudencial, cujo objetivo é proteger as informações do negócio e clientes, é pautado pelos princípios fundamentais de:
– Confidencialidade: quando o acesso à informação deve ser disponibilizado apenas para as entidades ou pessoas devidamente autorizadas pelo proprietário ou dono da informação;
– Integridade: fato de manter a informação armazenada e trafegada com todas as suas características originais ao longo do seu ciclo de vida estabelecidas pelo proprietário ou dono da informação;
– Disponibilidade: garantir que a informação esteja disponível para uso sempre que entidades ou pessoas autorizadas necessitem;

4. Diretrizes

As diretrizes estabelecem um programa de prevenção, detecção e redução de vulnerabilidades e impactos relacionados aos incidentes cibernéticos.

4.1 Informação: Importância e Proteção

Classificação da informação e Governança
A informação é um importante ativo do SAFRA e deve ser preservada e salvaguardada, em conformidade com suas políticas, normas, procedimentos e controles, bem como, com as leis e regulamentos sobre o tema.

Proteção de Dados e Privacidade

O SAFRA tem o compromisso de promover a aderência às leis de privacidade de dados e de proteção financeira de seus clientes, sendo este compromisso transmitido aos seus colaboradores, contratados e prestadores de serviço.

4.2 Gestão de Identidades e de Acessos

A gestão e revisão das identidades e dos acessos aos recursos computacionais do SAFRA são realizados em conformidade com os requisitos descritos em Norma específica, garantindo a definição de recursos, mínimos privilégios, operações que podem ser executadas, componentes autorizados e devida rastreabilidade de acessos realizados.

4.3 Controles dos Dispositivos de Tecnologia

Os recursos de tecnologia disponibilizados pelo SAFRA para uso dos funcionários são protegidos por controles contra ataques cibernéticos, infecções e prevenção ao vazamento de dados.

4.4 Desenvolvimento de sistemas e garantia de qualidade

A avaliação dos aspectos de segurança deve ser parte integrante no desenvolvimento de sistemas relevantes. Controles de segurança devem ser estabelecidos ao longo de toda a vida útil desses sistemas para assegurar que as informações processadas estejam protegidas, de acordo com sua classificação e exposição a risco.

4.5 Segurança e monitoramento da infraestrutura, redes e sistemas

As redes e sistemas corporativos relevantes devem ser administrados, monitorados e protegidos em consonância com as exigências e requisitos de Segurança da Informação do SAFRA. Devem também ser protegidos contra acessos não autorizados por meio de tecnologias de rede devidamente atualizadas, revisadas e testadas periodicamente de forma independente.

4.6 Registro e respostas de incidentes de segurança

Os incidentes de segurança cibernética relevantes são registrados, bem como deve ser realizada a análise das suas causas e dos impactos deles decorrentes. No caso da ocorrência de incidentes relevantes, serão realizadas as avaliações de adequabilidade dos controles existentes e de necessidade de criação de novos controles e, também, a contenção dos efeitos do incidente para as atividades do SAFRA.

4.7 Continuidade do negócio e recuperação de incidentes

O planejamento de continuidade do negócio é administrado de acordo com os requisitos estabelecidos na Política de Continuidade de Negócios e do Plano de Continuidade de Negócio para Segurança Cibernética que contempla cenários de incidentes relevantes a serem considerados nos testes de continuidade de negócios.

4.8 Gestão dos Prestadores de Serviços relevantes

Devem ser estabelecidos e continuamente aprimorados os controles de segurança cibernética destinados a assegurar que as informações tratadas pelos seus fornecedores estejam devidamente protegidas.

4.9 Avaliação de riscos cibernéticos de produtos ou serviços

Os riscos de segurança cibernética devem ser avaliados e administrados de acordo com os requisitos definidos em Norma específica e nos controles de proteção. Após o registro e análise devem ser executadas as respostas proporcionais aos riscos identificados.

4.10 Backup de Dados

O SAFRA deve zelar pelo processo de salvaguarda dos dados necessários para completa recuperação dos seus sistemas relevantes, a fim de atender aos requisitos operacionais e legais, assegurar a continuidade do negócio em caso de falhas ou incidentes, além de auxiliar em sua ágil recuperação.

4.11 Conscientização de Colaboradores, clientes e fornecedores

O SAFRA mantém um plano anual de conscientização direcionado ao desenvolvimento e manutenção das habilidades dos funcionários em relação à segurança cibernética.

5. Violações de Segurança

As violações das regras definidas nesta Política poderão ensejar a aplicação de medidas disciplinares, conforme determinam as normas de conduta do Código de Ética do SAFRA.

6. Canal de Comunicação

No caso de alertas de segurança e/ou incidentes, as notificações devem ser enviadas para o canal comunicação a seguir: **csirt@safra.com.br**