Política de Segurança Cibernética

1. Objetivo e Abrangência

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 Safra. A gestão dessa Política é realizada pela empresa líder do Conglomerado Prudencial Safra.

As diretrizes dessa Política estabelecem um programa de prevenção, detecção e redução de vulnerabilidades e impactos relacionados aos incidentes cibernéticos e em conformidade com as melhores práticas de mercado, leis e regulamentos sobre Segurança Cibernética.

Entende-se como Segurança da Informação a proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. Possui um conceito amplo de como proteger a informação, tanto em formato físico quanto digital, visando proteger as informações dos riscos que podem afetá-las. A Segurança Cibernética é a área da Segurança da informação que contempla direcionamento para proteger computadores, servidores, dispositivos móveis, sistemas eletrônicos, redes e bancos de dados.

As disposições desta política aplicam-se: (i) a todas as instituições pertencentes ao Conglomerado Prudencial Safra, bem como aos respectivos Colaboradores; (ii) às entidades e órgãos que possuam acesso as informações do Conglomerado Prudencial Safra; e (iii) aos prestadores de serviços, pessoas físicas ou jurídicas, que manuseiam dados ou informações sensíveis à condução das atividades operacionais do Safra.

2. Glossário

Ameaça: risco ou potencial perigo de um incidente, que pode resultar em dano ao Safra;

Áreas de Controles: são áreas de Auditoria, Controles Internos, Continuidade de Negócio, Jurídica, Compras, Compliance e Recursos Humanos;

Ativo: qualquer coisa que tenha valor para o Safra e precisa ser adequadamente protegido;

Backup: salvaguarda de informações, realizada por meio de reprodução e/ou espelhamento de uma base de arquivos, com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de restauração, ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada do Safra;

Colaborador(es): todos os que atuam em nome ou representação do Conglomerado Prudencial Safra, incluindo seus acionistas, sócios, administradores, conselheiros, diretores, empregados, estagiários, aprendizes e terceiros;

Conglomerado Prudencial Safra ou Safra: conjunto formado pelo Banco Safra S/A, pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil controladas pelo Banco Safra, e por outras empresas e fundos de investimentos, conforme controle realizado pela contabilidade;

CPD: Centro de Processamento de Dados, também conhecido como data center, é o local onde estão concentrados os sistemas computacionais do Safra;

Homologação: processo de avaliação e aprovação técnica de Recursos de Tecnologia da Informação e Comunicação para serem utilizados dentro do ambiente do Safra;

Incidente de Segurança cibernética: ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à política de Segurança Cibernética ou normas complementares, falha de controles ou situação previamente desconhecida, que possa ser relevante à Segurança Cibernética;

Informação: conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato;

Internet: rede mundial de computadores interconectada pelo protocolo TCP/IP cuja infraestrutura tem caráter aberto e colaborativo, acessível por meio de dispositivos com conexão e autorizações suficientes e que permite obter informação de qualquer outro dispositivo que também esteja conectado à rede, desde que configurado adequadamente;

Recursos de Tecnologia: hardware, software, serviços de conexão/comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações;

Risco: combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos; e

3. Diretrizes

3.1 Informação: Importância e Proteção

3.1.1 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. Todas as informações devem ser classificadas e regidas de acordo com os requisitos especificados na Norma de Classificação de Informação (BS-3.211.016) do Safra.

3.1.2 Proteção de Dados e Privacidade

O Safra tem o compromisso de promover a aderência às leis de privacidade e de proteção financeira de seus clientes, sendo este compromisso transmitido aos seus Colaboradores, contratados e prestadores de serviço. A proteção de dados e da privacidade das pessoas naturais devem ser

geridas em conformidade com os requisitos especificados na Política de Governança de Dados Pessoais (CS-9.284.002) e Política de Segurança da Informação (CS-9.211.005) do Safra, bem como nas leis e regulamentos que regram o tema.

3.1.3 Proteção de informações

Os recursos de tecnologia portáteis ou transportáveis que contenham informação confidencial devem possuir recursos de criptografia, de acordo com procedimentos homologados pela Área de Segurança da Informação.

As informações sensíveis deverão ser tratadas, transmitidas e armazenadas de forma segura, utilizando métodos de segurança adequados.

O uso de tecnologias de Inteligência Artificial (IA) deve ser realizado de forma ética, responsável, transparente e em conformidade com as regulamentações vigentes, sendo permitido o uso apenas de softwares previamente homologados e autorizados.

3.2 Gestão de dispositivos

3.2.1 Gestão de dispositivos e inventário de ativos

Os ativos corporativos devem ser geridos. Os em conformidade com as diretrizes estabelecidas pela área responsável.

O Conglomerado Prudencial Safra tem o dever de estabelecer e avaliar os requisitos de Segurança Cibernética nos processos de aquisição, operação, manutenção e descarte de ativos corporativos (seja *hardware* ou *software*), de acordo com as melhores práticas do setor para garantir a disponibilidade, a integridade e a confidencialidade dos dados armazenados ou transmitidos por eles.

3.2.2 Controles dos Dispositivos de Tecnologia

Os recursos de tecnologia disponibilizados pelo Conglomerado Prudencial Safra para uso dos Colaboradores devem possuir controles contra-ataques cibernéticos, infecções e prevenção ao vazamento de dados.

Os recursos de tecnologia devem ser configurados de acordo com a última atualização de segurança (*patch*) fornecida pelo fabricante. A homologação e monitoração das atualizações é responsabilidade da área de Segurança da Informação, cabendo à área de Tecnologia da Informação a aplicação destas correções.

3.3 Controles lógicos e físicos nos dispositivos

3.3.1 Controles lógicos de servidores

O Conglomerado Prudencial Safra deve estabelecer controles para a prevenção e detecção de intrusão e armazenamento indevido em servidores relevantes, em especial:

- Configuração, incluindo os sistemas operacionais, de acordo com um Guia de Configuração de Segurança elaborado pela área de Segurança da Informação;
- Testar e implementar as atualizações de segurança (*patches*) no sistema operacional e demais sistemas instalados no servidor e assegurar que estejam aptos para atualizar, sempre que novos patches estejam disponíveis;
- Monitorar a efetividade de segurança por meio de revisões regulares das trilhas de auditoria;
- Estabelecer revisões periódicas nas configurações de segurança;
- Implementar e executar controles contra *softwares* maliciosos;
- Verificar periodicamente a inclusão de conteúdo indevido; e
- Realizar avaliações periódicas de vulnerabilidades e testes de segurança.

3.3.2 Acesso físico aos CPDs

O acesso aos CPDs deve ser restrito somente às áreas previamente autorizadas, ter o acesso controlado e monitorado, visando a proteção das informações e as instalações contra acesso físico não autorizado.

3.3.3 Controles lógicos de sistemas relevantes

Os controles na camada de sistemas relevantes de informação utilizados pelo Conglomerado Prudencial Safra devem incluir:

- Gerenciamento seguro de autenticações, autorizações e controle de sessões estabelecidas;
- Validação e manejo seguro de quaisquer entradas de dados (*inputs*);
- Desenvolvimento e manutenção do código-fonte de acordo com a Norma de Desenvolvimento Seguro (BS-3.211.022) do Conglomerado Prudencial Safra;
- Realização de testes de segurança visando a identificação de vulnerabilidades; e
- Inclusão de controles contra softwares maliciosos.

3.4 Gestão de Acessos

3.4.1 Gestão de Identidades e de Acessos

A gestão e revisão das identidades e dos acessos aos recursos computacionais do Conglomerado Prudencial Safra devem ser realizados em conformidade com os requisitos especificados na Norma de Gestão de Identidade e Acessos Lógicos aos Sistemas de Informação (BS-3.211.001), garantindo a definição de recursos, mínimos privilégios, operações que podem ser executadas e componentes autorizados.

3.5 Gestão de Vulnerabilidades

3.5.1 Gestão de configuração de segurança

A Área de Segurança da Informação deve estabelecer e monitorar as configurações básicas de segurança para os recursos de tecnologia do Conglomerado Prudencial Safra.

3.5.2 Gestão de vulnerabilidades do ambiente

A Área de Segurança da Informação deve avaliar, analisar e documentar as vulnerabilidades nos sistemas relevantes expostos para redes públicas (por exemplo, Internet) periodicamente e tomar as devidas ações, de acordo com os requisitos especificados na Norma de Gestão de Vulnerabilidades (BS-3.211.015).

3.6 Desenvolvimento Seguro

3.6.1 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 ao risco.

O desenvolvimento de sistemas relevantes deve atender aos requisitos especificados na Norma de Desenvolvimento Seguro (BS-3.211.022) do Conglomerado Prudencial Safra, além de passar por aprovação, avaliação e testes executados pela Área de Segurança da Informação.

3.6.2 Manutenção de sistemas relevantes

A manutenção dos sistemas relevantes deve garantir o cumprimento dos requisitos de Segurança Cibernética previstos nesta política. As Áreas de Desenvolvimento de Sistemas devem realizar a manutenção periódica e oportuna nos sistemas relevantes, considerando que as atualizações de segurança sejam implantadas tempestivamente.

3.7 Monitoração e Segurança

3.7.1 Monitoramento e inspeção

A Área de Segurança da Informação pode monitorar ou inspecionar os recursos de tecnologia que estiverem em suas dependências ou de fornecedores que interajam com os ambientes lógicos do Safra sempre que considerar necessário, atendendo aos princípios da proporcionalidade, razoabilidade e privacidade de seus proprietários ou portadores.

3.7.2 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.

Trilhas de auditoria devem fornecer dados suficientes para, no mínimo, estabelecer dados sobre o evento, como: (i) o tipo de evento; (ii) quando o evento ocorreu (ou seja, a data e a hora); (iii) local em que ocorreu o evento; (iv) a origem do evento; e (v) o resultado do evento.

3.8 Resposta a incidentes

3.8.1 Registro e respostas de incidentes de segurança

Os incidentes de Segurança Cibernética relevantes devem ser registrados, bem como deve ser realizada a análise das suas causas e dos impactos deles decorrentes. Quando ocorrerem incidentes relevantes, devem ser 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.

A resposta a um incidente deve ser administrada em conformidade com os requisitos especificados na regulamentação vigente e na Norma de Resposta a Incidentes de Segurança da Informação (BS-3.211.028) que estabelece ainda os critérios e parâmetros adotados na avaliação da relevância de um incidente.

A área de Segurança da Informação deve acompanhar e avaliar as iniciativas criadas que visam o compartilhamento de informações sobre os incidentes relevantes com as demais instituições financeiras.

Caso a área de Segurança da Informação identifique ocorrência de violação de dados pessoais em um incidente de Segurança Cibernética, deve-se seguir o processo descrito na NPI– 10414 - Classificação e comunicação de violações de dados pessoais.

3.9 Continuidade de Negócios

3.9.1 Continuidade do negócio e recuperação de incidentes de Segurança Cibernética

O planejamento de continuidade do negócio deve ser administrado de acordo com os requisitos estabelecidos na Política de Continuidade de Negócios (CS-9.002.001) 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.

3.9.2 Salvaguarda / Backup

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.

A execução e gestão dos procedimentos de salvaguarda devem ser realizadas conforme os requisitos especificados pelo Safra.

3.10 Risco de contratação e gestão de fornecedores

3.10.1 Avaliação de riscos cibernéticos de produtos ou serviços

A Área de Segurança da Informação deve apoiar nas reuniões com a área de Arquitetura de TI nas recomendações de controles e proteções de Segurança Cibernética no desenvolvimento de novos produtos ou serviços do Safra, bem como na avaliação de riscos, buscando identificar ameaças e impactos sobre os ativos de informação.

Os riscos devem ser avaliados e administrados de acordo com os requisitos especificados na Norma de Gestão de Riscos de Segurança da Informação (BS-3.211.024) do Safra e nos controles de proteção. Após o registro e análise devem ser executadas as respostas proporcionais aos riscos identificados.

3.10.2 Aquisição de sistemas e serviços relevantes

Para sistemas relevantes adquiridos, sob qualquer modalidade, denominados "*softwares* de terceiros", o Gestor do Contrato deve estabelecer, em conjunto com a Área de Segurança da Informação, os devidos requisitos de segurança a serem aplicados.

No licenciamento de soluções de armazenamento, processamento de dados ou serviços em nuvem, devem ser adotados os procedimentos de segurança indicados pelo fornecedor e validados pela Área de Segurança da Informação, de forma a garantir os níveis adequados de segurança nas soluções adotadas pelo Safra, conforme diretrizes contidas na Norma de Utilização de Serviços em Nuvem (BS-3.211.023).

A Área de Segurança da Informação deve apoiar nas reuniões com a área de Arquitetura de TI nas recomendações de controles e proteções de Segurança Cibernética na aquisição de novos sistemas e serviços relevantes, bem como na avaliação de riscos, buscando identificar ameaças e impactos sobre os ativos de informação.

3.10.3 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. Os requisitos de controle devem incluir, no mínimo:

- Avaliações de Risco de Segurança Cibernética dos fornecedores com acesso às informações sensíveis ou protegidas por regulação específica;
- Requisitos mínimos baseados em risco relativos à encriptação de dados, controles de acesso, classificação de dados, bem como planos de recuperação de desastre e continuidade do negócio;
- Avaliar a adequabilidade das práticas de Segurança Cibernética de prestadores de serviços;
- Avaliações periódicas de acordo com o risco que representam e na manutenção das suas práticas de Segurança Cibernética;
- Diretrizes ou requisitos contratuais estabelecendo práticas mínimas de Segurança Cibernética, ou declarações e garantias relativas à segurança da informação, conforme aplicável:
    - Controles de acesso, incluindo autenticação de múltiplos fatores;
    - Requisitos de encriptação e proteção de dados;
    - Reporte imediato de eventos de Segurança Cibernética que envolva dados de propriedade ou sob responsabilidade do Safra; e

- Adequabilidade de seus procedimentos as diretrizes desta política.

- Diretrizes e requisitos contratuais para substituição de prestadores de serviços relevantes de processamento de dados e de computação em nuvem para o caso de interrupção dos serviços prestados com vistas ao reestabelecimento da operação normal do Safra; e

- Quando a contratação pretendida envolver dados classificados como dados pessoais pela legislação em vigor, a Área de Privacidade de Dados deve avaliar o nível de maturidade do Programa de Privacidade do prestador de serviço e, quando pertinente, fazer recomendações que devem ser implementadas antes da contratação.

3.11 Conscientização de Colaboradores, clientes e fornecedores

3.11.1 Capacitação e conscientização

O Safra deve manter um plano anual de conscientização direcionado ao desenvolvimento e manutenção das habilidades dos Colaboradores em relação à Segurança Cibernética.

Deverão ser aplicadas avaliações periódicas para medição da aderência e cumprimento desta política e demais normas de Segurança Cibernética junto aos seus Colaboradores e orientar seus clientes na utilização de seus produtos e serviços, sobre determinadas precauções relacionadas ao ambiente cibernético.

As diretrizes gerais de Segurança Cibernética deverão ser alvo de divulgação junto a clientes e usuários do Safra. Adicionalmente, deverá ser dada ampla divulgação do conteúdo desta política a Colaboradores e prestadores de serviço, além de disponibilizados os dados de contato para consultas sobre eventuais dúvidas.

4. Responsabilidades

Conselho de Administração

- Aprovar o Plano de Ação e de Resposta a Incidentes;

- Tomar conhecimento do relatório anual sobre a implementação do plano de ação e de resposta a incidentes; e

- Assegurar o comprometimento do Safra com a melhoria contínua dos procedimentos relacionados à Segurança Cibernética.

Comitê de Gestão de Riscos Operacionais, Cibernéticos e Prevenção ao Crime Financeiro – CGROC

- Apoiar o Diretor de Segurança Cibernética na análise e deliberação de assuntos relacionados à Segurança Cibernética.

Diretor de Segurança Cibernética

- Gerenciar as atividades necessárias ao cumprimento das disposições desta política;
- Aprovar e empreender ações, em conjunto com a Diretoria Executiva, que promovam a melhoria contínua da Segurança Cibernética no Safra;
- Analisar e deliberar ações sobre os relatórios que tratam da implementação do Plano de Ação e de Resposta a Incidentes de Segurança Cibernética;
- Submeter relatório anual sobre a implementação do Plano de Ação e de Resposta a Incidentes, ao Comitê Superior de Riscos e ao Conselho de Administração; e
- Estabelecer a estrutura organizacional e os recursos humanos e tecnológicos para garantir o adequado funcionamento da Área de Segurança da Informação.

Área de Segurança da Informação

Implementar e fazer cumprir as disposições desta política e, em conjunto com as áreas de Arquitetura de TI, Infraestrutura de TI, Desenvolvimento de Sistemas, Tecnologia da Informação, Auditoria Interna, Controles Internos, Continuidade de Negócio, Jurídico, Compras, *Compliance* e Recursos Humanos:

- Prover a manutenção de normas e procedimentos relacionados à Segurança Cibernética;
- Avaliar riscos e recomendar investimentos e ações de controle e proteção de dados, assegurando a disponibilidade, a integridade e a confidencialidade das informações;
- Participar dos processos de qualificação e contratação de serviços de armazenamento, processamento de dados e computação em nuvem;
- Assegurar que o desenvolvimento de sistemas e a aquisição de recursos de tecnologia estejam de acordo com requisitos de Segurança Cibernética;
- Definir e implantar os controles para proteção dos dispositivos de tecnologia contra-ataques cibernéticos, infecções e prevenção a vazamento de dados;
- Identificar e gerenciar o ciclo de vida das vulnerabilidades de Segurança Cibernética;
- Gerenciar plano de tratamento e resposta a incidentes de Segurança Cibernética, reportando os que são relevantes;

- Apoiar a área de Continuidade de Negócios na definição de requisitos do plano de continuidade para Segurança Cibernética, quanto à avaliação de relevância dos incidentes, fluxo de acionamento e testes periódicos;
- Estabelecer e monitorar as configurações básicas de segurança nos recursos de tecnologia;
- Assegurar que fornecedores e prestadores de serviços terceirizados estão cientes e aderentes aos requisitos de Segurança Cibernética;
- Definir e divulgar as normas de Segurança Cibernética a serem aplicadas no Safra; e
- Difundir a cultura de Segurança Cibernética para todos os Colaboradores do Safra, prestadores de serviços e clientes.

5. Considerações finais

Casos extraordinários a esta política serão remetidos para apreciação do Diretor responsável pela segurança cibernética e tratados pontualmente envolvendo as alçadas pertinentes.

As violações das regras definidas nesta Política poderão ensejar a aplicação de medidas disciplinares, conforme determinam as normas de conduta do Código de Ética (CS-9.157.012) do Safra.

Os mecanismos de controle e acompanhamento quanto à implementação e efetividade da Política de Segurança Cibernética deverão ser definidos pela Área de Segurança da Informação em conjunto com as demais Áreas de Controles, incluindo a definição de processos, testes e trilhas de auditoria, a definição de métricas e indicadores adequados e mecanismos de identificação e correção de deficiências na implantação.

6. Plano de alçadas

Esta política deve ser aprovada e revisada anualmente pelo Diretor responsável pela segurança cibernética e pelo Conselho de Administração, com recomendação do Comitê Superior de Riscos.