SUMÁRIO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA DO ING Bank - Filial de São Paulo

1. INTRODUÇÃO

Este sumário fornece um resumo dos principais requisitos para atendimento e adequação às exigências regulatórias divulgadas pelo Banco Central referente à Resolução 4.658, com o intuito de divulgar ao público às diretrizes gerais sobre segurança cibernética.

2. ESCOPO E APLICABILIDADE

As políticas e normas contidas neste resumo aplicam-se às seguintes empresas do conglomerado ING no Brasil ("ING"):

- ING Bank N.V., Filial de São Paulo; e
- ING Corretora de Câmbio e Títulos S.A.

3. POLÍTICAS, NORMAS & PROCEDIMENTOS

A **POLÍTICA DE SEGURANÇA CIBERNÉTICA** descreve o programa de segurança cibernética do ING e as respectivas políticas, normas e procedimentos de apoio relacionados.

A segurança cibernética inclui as práticas e os processos para proteção da informação corporativa, incluindo a confidencialidade, a integridade e a disponibilidade de tais informações, bem como, ainda, de danos causados através de meios eletrônicos.

Adicionalmente, este documento de segurança cibernética contempla os controles projetados para se manter a acessibilidade e a resiliência dos sistemas, das redes e dos outros elementos de infraestrutura que suportam a manutenção de informação corporativa do ING.

Este programa é sustentado por um "framework" de governança em tecnologia que inclui diversas políticas, normas e procedimentos, cobrindo disciplinas-chave relacionadas, e também pelo programa de conscientização de segurança cibernética. A seguir seguem os principais requisitos atendidos por tais politicas:

- **Gestão de Continuidade de Negócio:**
  - Treinamento e conscientização dos colaboradores no que tange ao plano de continuidade de negócio;
  - Estratégia de continuidade de negócio com base nos cenários prescritos na norma;
  - Monitoramento das métricas e notificação;
  - Plano e organização de gestão de risco;

- Plano de recuperação de desastres;

- **Resiliência contra Crime Cibernético**:
  - O ING dispõe de Centro de Operações de Segurança Cibernética para Identificação dos problemas, avaliação da criticidade, comunicação dos vetores de riscos e vulnerabilidades e eventual ataque cibernético;
  - Conhecimento de desenvolvimentos pertinentes em relação ao *modus operandi* do Crime Cibernético, vetores de ameaça no ambiente tecnológico no qual o ING opera para fins de melhoria do quesito resiliência em tempo hábil;
  - Recursos aptos para ajudar o ING a lidar com ameaças avançadas e ataques de negação onde são documentados e testados de forma que possam ser utilizados quando necessário para controle de referência (segurança), como por exemplo, gestão de acesso de usuário, segurança de plataforma, monitoramento de segurança e implantação de forma efetiva;
  - Medidas de mitigação para limitar o tempo de inatividade como resultado de ataques de negação, bem como precauções e os controles para impedir que a infraestrutura do ING seja indevidamente usada em terceiros;
  - Compartilhamento da inteligência relacionada a ameaças cibernéticas relevantes e vulnerabilidades com outras instituições financeiras por meio da plataforma FS-ISAC;

- **Gestão de Risco da Informação**:
  - Processos definidos para identificar e controlar os Riscos de Informação em todos os produtos, processos e sistemas, incluindo a absorção em tempo hábil de alterações regulatórias. Todos os colaboradores, prestadores e usuários terceirizados que atuam no ING recebem treinamento de conscientização e atualizações regulares sobre políticas, normas e procedimentos organizacionais relevantes para suas respectivas funções;
  - O processo de monitoramento desenhado para evitar incidentes e limitar os impactos e para garantir que a integridade das configurações de “hardware” e “software” seja gerenciada pelo estabelecimento e manutenção de um repositório de configuração preciso e completo;
  - Avaliação de Impacto de Negócios (BIAs) para avaliar os níveis de classificação para Confidencialidade (C), Integridade (I) e Disponibilidade (A) e nas respectivas medidas de mitigação de risco para garantir que a Informação receba o nível apropriado de proteção;

- **Gestão de Segurança da Informação**:
    - O pilar de Segurança de Rede define as exigências mínimas do controle para serviços e dispositivos de rede visando proteger adequadamente os sistemas e canais de comunicação do ING;
    - O pilar denominado “Cloud” (Computação em Nuvem) objetiva que os ambientes estejam em conformidade com as políticas, normas e procedimentos de defesa da informação do ING;
    - O pilar de Acesso Remoto delineia os controles de proteção da informação exigidos para prover acesso remoto seguro, quando autorizado, a empregados e quando necessário, a prestadores de serviço, a ativos de informação do ING;
    - O Pilar de Antivírus informa os controles para prevenir, conter disseminação, e mitigar o impacto de “software” malicioso na rede do ING, em aplicações e em outros sistemas que poderiam impactar a confidencialidade, a integridade ou a disponibilidade da informação;
    - O pilar de Resposta a Incidente da Segurança da Informação delimita a abordagem do ING para responder aos incidentes cibernéticos, e descreve os papéis das partes interessadas do ING na resposta a potenciais incidentes conforme modelo abaixo:
        - O ING estabeleceu um processo que consiste em análise de evento, monitoramento de possíveis incidentes de segurança, encaminhamento de incidentes para departamentos apropriados e planos de ação para melhorar os controles;
        - A Gestão de Incidente de Segurança é realizada principalmente por meio do serviço centralizado de Monitoramento de Evento de Segurança na Central de Operações de Segurança (SOC) Global, que informa o ING NY sobre qualquer problema identificado ou possível ataque cibernético que possa afetar o negócio;
        - Quando um ataque cibernético ou possível ataque é identificado, um incidente que impacta a entrega do serviço ou uma tolerância a falhas no datacenter é necessária. O SOC ING NY se reúne para realizar as avaliações iniciais;
        - Caso um ataque seja confirmado, ele é registrado no Sistema Service Now (SNOW) para rastreamento e, caso o impacto para os países da América Latina seja confirmado, o ING é convidado a fazer avaliações sobre os impactos e medidas que devem ser realizadas para reduzir, mitigar o incidente, realizar as notificações e conclusão do mesmo.

- **Monitoramento de Segurança**:

- Processos e procedimentos padronizados para a identificação e administração eficiente, eficaz e em tempo hábil de (possíveis) pontos fracos e vulnerabilidades nos sistemas de informação, incidentes e eventos de segurança;
- Análise continua dos processos e procedimentos de monitoramento de segurança para garantir que eles sejam implantados e mantidos de acordo com as expectativas e os padrões definidos;
- Os colaboradores são informados de que suas ações são registradas e monitoradas;

- **Gestão de Identidade e Acesso**:
  - Os acessos aos sistemas de informação restritos aos usuários autorizados e/ou aos processos de sistemas que tenham necessidade de usar os ativos. Os usuários acessam somente dados aos quais tiveram acessos explicitamente concedidos;
  - Os direitos de acesso são periodicamente revistos com base no nível de risco relacionado e devem ser revogados e/ou desabilitados quando não forem mais necessários;
  - À concessão de privilégios de acesso é assegurada a segregação básica de funções;
  - Os pedidos de acessos não devem ser submetidos e aprovados pelo mesmo indivíduo para o seu próprio usuário, nem para nenhum identificador de sistema para qual o indivíduo é o responsável;
- **Plataforma de TI**:
  - Os ativos de TI são ativamente gerenciados ao longo dos diferentes estágios do ciclo de vida, do projeto, da construção à produção e descontinuidade;
  - A arquitetura corporativa do Banco ING contém os Princípios da Arquitetura Corporativa de Segurança, tais como segurança por projeto, defesa em profundidade, segurança por padrão, segurança contra falha, segurança em implantação e usabilidade & gestão (confidencialidade, integridade e disponibilidade dos Ativos de TI);
  - Todos os ativos de TI são registrados e gerenciados por meio de um repositório que fornece suporte para Processos de Gestão de Serviço de TI Local e supervisão do Banco e incorporam os requisitos de auditoria e garantia da plataforma durante as operações;
  - Todas as conexões externas estão em conformidade com os critérios de revisão harmonizada. O acesso não autorizado aos ativos de TI e redes através do uso indevido de instalações de manutenção remota é evitado e monitorado;
  - O uso de dispositivos que não são de propriedade do ING, conhecidos como BYOD (Traga Seu Próprio Dispositivo), não comprometem a segurança do Ecossistema de TI do ING;

- **Risco Não Financeiro**:

- Processos em vigor para solicitar, revisar, aprovar e/ou rejeitar exceções às políticas e normas de proteção da informação e cibernética;
- Critérios a serem utilizados para identificar os sistemas e a infraestrutura do ING que são escopo para a avaliação de riscos de tecnologia, e respectivos processos padronizados de avaliação de risco da segunda linha de defesa;

- **Terceirização**:
  - A governança com relação a iniciativas de terceirização definidas e em vigor para identificar, medir, responder, monitorar e gerenciar iniciativas de compras durante seu ciclo de vida;
  - A tomada de decisão adequada em relação às atividades de compras e a aplicação do processo de QF (Qualificação do Fornecedor);
  - Os novos acordos e existentes são avaliados periodicamente com a contribuição de todos os envolvidos;
  - Os riscos e as medidas de mitigação necessárias nas iniciativas de terceirização são identificados através de uma avaliação de risco prévia, incluindo:
    - A adequação da capacidade do prestador de serviço;
    - Se a iniciativa de terceirização é permitida pelos reguladores e/ou lei local;
    - Todos os outros riscos locais ou específicos pertinentes;
  - A gerência responsável tem uma estratégia para garantir a continuidade e a qualidade dos serviços fornecidos, caso a prestação do serviço seja (repentinamente) encerrada por qualquer que seja o motivo; e
  - Informação ao regulador quando da aquisição/contratação de serviços relevantes;

4. CONTATO

Caso tenha alguma dúvida referente a este documento, por favor, entre em contato pelo formulário de comunicação do site institucional do Banco ING abaixo:

https://www.ingwb.com/network-offices/americas/brasil

5. AVISO LEGAL

Com o objetivo de manter a Confidencialidade, Integridade e Disponibilidade das informações do Banco ING, os colaboradores (permanentes ou não) e os terceiros (prestadores de serviços) devem respeitar a política de Segurança Cibernética e quaisquer procedimentos, diretrizes ou então procedimentos correlatos.

Em determinação do Banco Central do Brasil, o Banco ING deverá armazenar as informações por um período de 5 (cinco) anos.

Este documento foi produzido pelo Banco ING com caráter informativo apenas. O mesmo não deve ser reproduzido integralmente ou parcialmente por qualquer pessoa e/ou empresa sem a devida autorização formal do Banco ING.