Política Corporativa de Segurança da Informação e Cibernética

Site Institucional

Responsável: Segurança da Informação

Classificação: Público

ÍNDICE

1. OBJETIVO

A Política Corporativa de Segurança da Informação e Cibernética ("política") do Conglomerado Prudencial Genial ("GENIAL") tem por objetivo definir as diretrizes, responsabilidades e princípios relativos à Segurança da Informação e Cibernética, em linha com as práticas de mercado, considerando a natureza e a complexidade dos produtos, serviços, atividades, processos e sistemas e a conformidade com os requerimentos legais e regulatórios do Conglomerado Prudencial Genial. Ela é aplicável a Genial e suas empresas controladas que estão subordinadas às regras do Sistema Financeiro Nacional, assim como a seus administradores, colaboradores e prestadores de serviços terceirizados.

2. PRINCÍPIOS

Entende-se como Segurança da Informação e Cibernética a adoção de um conjunto de medidas com vistas a garantir a continuidade dos negócios. Tais medidas devem impedir o uso, divulgação, alteração ou destruição não autorizada de informações. Devem evitar perdas financeiras e ações que comprometam a imagem da GENIAL, quando relacionadas ou decorrentes das estruturas de tecnologia. Está baseada nos seguintes princípios:

- **Confidencialidade:** É a garantia que todos os meios de processamento e/ou conservação de informação contenham medidas de proteção quanto ao acesso e utilização por pessoa não-autorizada, assegurando que toda informação esteja protegida de revelações acidentais, espionagem industrial, violação da privacidade e outras ações similares.
- **Integridade:** É a garantia que todas as informações processadas, transacionadas ou armazenadas nas bases e sistemas da GENIAL estejam livres de erros e irregularidades de qualquer espécie, assegurando que toda informação processada em cada um dos sistemas de informação e processos transacionais seja necessária, útil e suficiente para o desenvolvimento dos negócios.
- **Disponibilidade:** É a garantia que a informação e sua capacidade de processamento, manual ou automática, sejam resguardadas e recuperadas sempre que necessário, de modo a não impactar significativamente o andamento dos negócios, estando sempre ao dispor da entidade que a solicitar.
- **Conformidade:** É a garantia que toda informação e os meios físicos que a contenham, processem e ou transportem, cumpram com os regulamentos legais vigentes em cada âmbito, e que todos os direitos de propriedade sobre a informação utilizada ou produzida pela GENIAL, no desenvolvimento de suas atividades, estejam adequadamente estabelecidos a favor da empresa.

3. DIRETRIZES

O gerenciamento de Segurança da Informação na GENIAL é formado por uma estrutura compatível com o seu porte, e tem o objetivo de assegurar a eficiência, eficácia e efetividade desse gerenciamento, em linha com a estratégia da GENIAL, contando com áreas responsáveis pela governança, riscos e conformidade de segurança da informação, operação de segurança da informação, continuidade de negócios e prevenção a fraudes.

3.1 Cultura e Conscientização

- É implementado um programa de conscientização sobre segurança cibernética, para disseminação da cultura de segurança, preparar os colaboradores para identificar e reportar e-mails falsos (*phishing*, *spoofing* e *spam*) e *workshops* sobre segurança e planos de ação;
- A GENIAL disponibiliza informativos para seus usuários sobre precauções de segurança da informação durante a utilização de produtos e serviços financeiros.

3.2 Trabalho Remoto

- A GENIAL disponibiliza o trabalho remoto de seus colaboradores, desde que as medidas de segurança necessárias estejam implementadas com o objetivo de proteger as informações e tecnologias.

3.3 Acesso

- São implementados controles para que o acesso aos sistemas, serviços e ambientes tecnológicos da GENIAL sejam limitadas as pessoas identificadas e autorizadas;

3.4 Terceiros

- Os controles a serem adotados por terceiros deverão, minimamente, seguir os mesmos níveis de controles de segurança que a GENIAL;
- Prestadores de serviço, sejam provedores, parceiros ou fornecedores, que armazenam e/ou processam dados contratados pela GENIAL devem ser avaliados sob o ponto de vista de Segurança da Informação, e devem assegurar a adoção de governança corporativa, boas práticas de segurança e aderência às regulamentações, requisitadas pela GENIAL;
- Os fornecedores de serviços contratados devem informar os incidentes relevantes, relacionados as informações da GENIAL processadas ou armazenadas por eles, através do canal csirt@genial.com.vc;
- A contratação ou alteração contratual de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser previamente comunicada ao Banco Central e atender os requisitos da Resolução CMN Nº 5.274.

3.5 Classificação da Informação

- A informação deve ser classificada para indicar a importância, prioridade e nível de proteção, sendo classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade.

3.6 Continuidade do Negócio

- São implementados planos de continuidade para os processos relevantes da GENIAL devem ter Planos de Continuidade de Negócio de acordo com a necessidade ou seu nível de importância, levando em consideração o mapeamento e avaliação de todos os processos classificados como críticos;
- Os testes de continuidade de negócios deverão ser realizados periodicamente, levando em consideração, no mínimo, os cenários de indisponibilidade, mapeados durante o Plano de Continuidade de Negócios (PCN).

3.7 Segurança para Ativos, Perímetro, Infraestrutura e Sistemas

- São implementados mecanismos de proteção contra softwares nos equipamentos e apenas os dispositivos corporativos (gerenciados ou homologados) podem ser conectados à rede corporativa;
- O processo de desenvolvimento e manutenção de aplicações, aplicativos, sistemas e serviços deve garantir a aderência às regras de desenvolvimento seguro e às boas práticas de segurança estabelecidas na GENIAL;
- São realizadas, por meio de testes de segurança, varreduras para identificação de vulnerabilidades no ambiente de tecnologia produtivo, de acordo com prazos e escopo estabelecidos internamente a fim de identificar e reduzir vulnerabilidades nos ativos de informação da GENIAL;
- São implementadas ferramentas e controles contra-ataques para proteção das infraestruturas, sistemas e informações da GENIAL. Os eventos lógicos de sistemas e serviços, bem como os eventos físicos, devem ser devidamente registrados e monitorados.

3.8 Incidentes de Segurança

- A GENIAL implementa controles de prevenção, identificação, registro e resposta a incidentes e crises de segurança do ambiente tecnológico;
- Os incidentes devem ser classificados de acordo com o seu nível de criticidade;
- Anualmente, é elaborado um relatório de resposta a incidentes, contendo os resultados obtidos na implementação de rotinas, processos e tecnologias utilizados na prevenção e reposta a incidentes, assim como incidentes cibernéticos relevantes e os resultados dos testes dos cenários de crise cibernéticas realizados pela GENIAL.

4. DISPOSIÇÕES FINAIS

Este documento é uma versão resumida e pública da Política de Segurança da Informação e Segurança Cibernética da GENIAL e é revisada e aprovada pelo Comitê de Segurança da Informação.

5. VIGÊNCIA

Esta política possui prazo de vigência de 1 (um) ano a partir da data de sua publicação.

www.genialinstitucional.com.br