# POLÍTICA GLOBAL DE SEGURANÇA DA INFORMAÇÃO

## 1. OBJETIVO

Esta Política de Segurança da Informação estabelece os princípios que regem a segurança da informação dentro da Natura Institucional e a estrutura de políticas dentro do Framework de Gestão de Segurança da Informação (FGSI).

## 2. ABRANGÊNCIA

A Política de Segurança da Informação e a FGSI aplicam-se a todos os colaboradores, fornecedores ou terceiros, contratados e outros, conforme autorizado pela Natura Institucional.

O FGSI aplica-se a todos os ativos de informação e informação da Natura Institucional, incluindo, mas não se limitando a:

- Todas as informações criadas, utilizadas, armazenadas, transferidas e excluídas pelos colaboradores da Natura Institucional.
- Todos os sistemas, aplicativos, bancos de dados e redes operando em ambientes locais e em nuvem que criam, usam, armazenam e transferem informações da Natura Institucional.
- Todos os hardwares e equipamentos de comunicação que suportam sistemas, aplicativos, banco de dados e redes da Natura Institucional.

## 3. DEFINIÇÕES

Não aplicável.

## 4. DESCRIÇÃO

**Princípios de Segurança da Informação da Natura Institucional**

**Assumimos nossa responsabilidade pela proteção de dados extremamente a sério.**

O nosso compromisso com a segurança da informação começa no topo, com uma declaração oficial do Conselho de Administração que dá a maior importância à salvaguarda de produtos, serviços e dados para reduzir o impacto de ataques cibernéticos prejudiciais. A Política de Segurança da Informação é aprovada pela Alta Administração para utilização em todas as Unidades de Negócio. Avaliamos regularmente a estratégia de segurança cibernética e reportamos os riscos à alta administração

**Todos na Natura Institucional entendem e absorvem sua responsabilidade de proteger dados e sistemas de abusos.**

Um programa abrangente de treinamento e conscientização em segurança da informação garante que todas as partes entendam suas obrigações de cumprir os princípios, políticas, padrões e legislações e regulamentações globais de segurança da informação da Natura Institucional.

**Adotamos uma abordagem ativa, baseada em riscos e proporcional à segurança, identificando e protegendo o que mais importa.**

Nossa estrutura de Gestão de Risco garante que o risco de segurança cibernética seja visível e compreendido pelas unidades de negócios proprietárias dos ativos e/ou processos envolvidos. A avaliação regular de riscos é realizada nas operações, ativos e dados associados ao processamento,

armazenamento ou transmissão de informações e funções de negócios. Os riscos são geridos ativamente no nível apropriado. A priorização dos controles cibernéticos de acordo com os riscos do negócio garante a melhor utilização dos recursos.

**Incorporamos segurança e resiliência no design de todos os nossos produtos e serviços e usamos a defesa em profundidade, nunca confiando em apenas um controle para proteger nossos sistemas.**

As medidas de segurança são definidas no início de qualquer projeto tecnológico. Os princípios de "segurança desde a concepção" e "defesa em profundidade" estão no centro de todas as soluções desenvolvidas internamente e externamente. Os proprietários de sistemas em nuvem garantem que todos os provedores de serviços em nuvem cumpram os controles de segurança obrigatórios antes do uso. Os proprietários dos dados implementam controles para garantir a proteção das informações e dos sistemas para atender ao apetite de risco e aos requisitos legais e regulamentares.

**Trabalhamos com nossos fornecedores e parceiros para atender aos mesmos altos padrões de segurança em todo o ecossistema de nossos negócios.**

Todos os terceiros estão sujeitos aos nossos processos de integração e gestão de riscos. Um Adendo de Segurança é necessário para todos os contratos e acordos novos e revisados. São realizadas revisões regulares e proporcionais dos relacionamentos e acordos existentes com fornecedores.

**Gerenciamos o acesso a dados e sistemas, garantindo que as pessoas só tenham o acesso de que precisam para fazer seu trabalho.**

Nosso gerenciamento de acesso é construído em torno de princípios de segurança relacionados ao acesso:

- Necessidade de saber – os usuários ou recursos só terão acesso necessário para cumprir suas funções e responsabilidades,
- Privilégio mínimo – os usuários ou recursos receberão os privilégios mínimos necessários para cumprir suas funções e responsabilidades,
- Segregação de Funções – será seguida a divisão de responsabilidades.

**Mantemos nossos sistemas e processos para reduzir a vulnerabilidade a ataques.**

A Natura Institucional constrói e mantém seus sistemas de TI para reduzir a vulnerabilidade a ataques cibernéticos. Gerenciamos vulnerabilidades por meio de um processo contínuo de avaliação e priorização para manter o risco dentro de níveis aceitáveis.

**Estabelecemos e mantemos a capacidade de monitorar nossos sistemas em busca de sinais de ataque.**

A Natura Institucional monitora continuamente seus sistemas de TI em busca de sinais de ataque. As anomalias são rapidamente identificadas, analisadas e tratadas.

**Preparamo-nos, respondemos e recuperamos de incidentes de forma rápida e eficaz, tendo sempre em conta os interesses dos nossos clientes.**

A Natura Institucional mantém e treina seus planos para lidar de forma eficaz com incidentes cibernéticos. Os planos são amplamente compreendidos e estabelecem funções, responsabilidades e obrigações claras em todos os níveis durante um incidente.

**Cumprimos os regulamentos e leis de segurança em todas as jurisdições em que fazemos negócios.**

A Natura Institucional mantém a conformidade com as leis e regulamentos identificando ativamente os requisitos e garantindo que todos os funcionários sejam treinados e preparados para desempenhar suas funções de forma adequada.

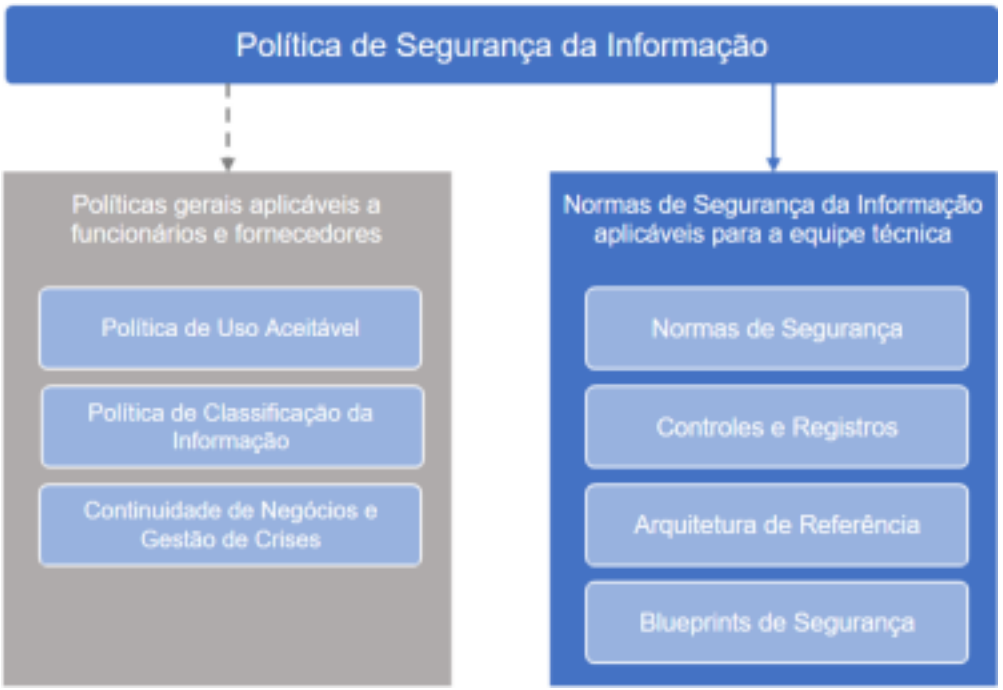
**Estrutura de Gestão de Segurança da Informação (FGSI) da Natura Institucional**

O FGSI da Natura Institucional estabelece a hierarquia de documentos, incluindo Políticas, Padrões, Processos, Controles e Registros, Referências de Arquitetura e Modelos que se baseiam nos Princípios de Segurança da Informação.

Natura Institucional FGSI adapta o NIST CSF (National Institute of Standards and Technology Cybersecurity Framework), garantindo uma abordagem abrangente e bem estruturada à segurança cibernética.

Os tópicos de segurança cibernética estão intimamente ligados a outras funções corporativas de gestão e operacionais. O diagrama a seguir apresenta políticas que, além de elementos de segurança da informação, abrangem áreas relacionadas a questões jurídicas, privacidade de dados e operações comerciais. A Cyber Security é proprietária e responsável por essas políticas; no entanto, outras funções têm contribuições significativas e devem aprovar tais documentos:

- Política de Utilização Aceitável,
- Política de Classificação de Dados,
- Continuidade de Negócios e Gestão de Crises.




A Política de Segurança da Informação estabelece princípios que são traduzidos em requisitos específicos de segurança através de três tipos de documentos:

- Normas de segurança
- Arquitetura de Referência
- Modelos de segurança

Os requisitos e configurações contidos nestes documentos devem ser seguidos em todas as Unidades de Negócio da Natura Institucional. A não conformidade pode resultar em aumento de risco e exposição desnecessária a ameaças externas.

As Normas de Segurança são baseados na análise de categorias relevantes da Estrutura de Segurança Cibernética do NIST e controles relacionados descritos na SP800, Publicação Especial do NIST. Os Padrões de Segurança estabelecem expectativas técnicas detalhadas e um conjunto rastreável de requisitos de segurança para a organização.

Os documentos de Arquitetura de Referência fornecem um padrão arquitetônico abrangente a ser seguido no projeto de novos sistemas de TI. Através de quatro perspectivas (Motivação, Estratégia, Negócios, Desenvolvimento) direcionam o desenho de soluções para melhorar a segurança. Seguir essas referências permite que novos sistemas e serviços sejam aderentes ao FGSI da Natura Institucional e alcancem resultados de negócios, mantendo a conformidade de segurança.

Os Modelos de Segurança estabelecem especificações técnicas para serviços ou componentes de segurança de TI usados com frequência. Seguir os modelos garante que os componentes de segurança dos produtos empresariais permaneçam atualizados.

**Frequência de Revisão**

As políticas dentro da Estrutura de Gestão de Segurança da Informação devem ser avaliadas anualmente para garantir a relevância contínua e o cumprimento de todos os requisitos legislativos, regulatórios e contratuais aplicáveis à Natura Institucional.

A revisão dos documentos que suportam auditorias e certificações é realizada de acordo com os prazos estabelecidos nesses documentos; no entanto, a validade dos padrões de segurança é revisada pelo menos uma vez a cada três anos.

Os modelos de segurança contendo requisitos técnicos são validados pelo menos uma vez por ano.

**Conformidade com Políticas e Normas de Segurança**

A conformidade com políticas e padrões é monitorada; a não conformidade é avaliada e quaisquer ações corretivas ou controles compensatórios devem ser aprovados pelas partes interessadas relevantes.

Qualquer funcionário ou contratado que tenha violado esta política poderá estar sujeito a ações disciplinares, conforme definido no Código de Conduta da Natura Institucional.