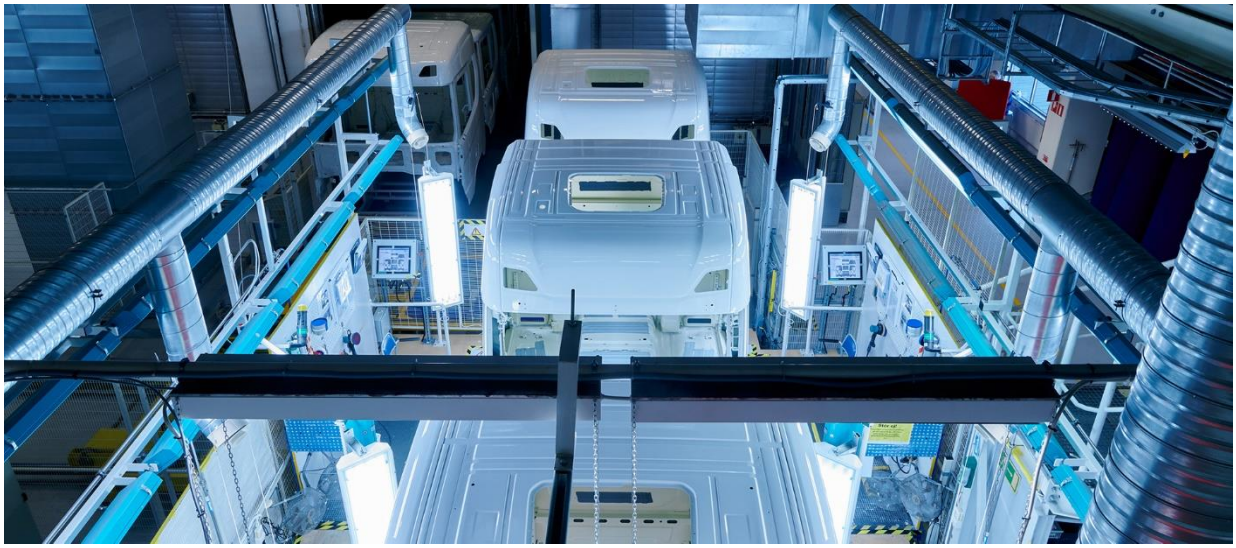
# POLÍTICA DE SEGURANÇA CIBERNÉTICA



Dezembro, 2022

# ÍNDICE

## 1. INTRODUÇÃO

Esta política visa atender a Resolução CMN n. 4.893/2021 do Banco Central e nova Lei de Proteção de Dados - LGPD.

## 2. OBJETIVO

Estabelecer as diretrizes para compor um programa completo e consistente de segurança da informação e gestão de riscos cibernéticos sempre se utilizando das políticas padrões do Grupo Scania aplicáveis ao Conglomerado Prudencial (Scania Banco S.A. e Scania Administradora de Consórcios Ltda.), visando:

- Proteger o valor e a reputação;
- Garantir a confidencialidade, integridade e disponibilidade das informações e de informações de terceiros por elas custodiadas, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;
- Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros;
- Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;
- Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;
- Conscientizar, educar e treinar os colaboradores por meio de Política Corporativa de Segurança Cibernética, normas e procedimentos internos aplicáveis as suas atividades diárias.

## 3. PRINCÍPIOS

A proteção e privacidade de dados dos clientes refletem os valores do Conglomerado Prudencial e reafirmam o seu compromisso com a melhoria contínua da eficácia do processo de Proteção de Dados.

Quanto às informações de nossos clientes, são obedecidas as seguintes determinações:

- São coletadas de forma ética e legal, para propósitos específicos e devidamente informados;
- Somente serão acessadas por pessoas autorizadas e capacitadas para o seu uso adequado;
- Poderão ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossas diretrizes de segurança e privacidade de dados;

- As informações constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais, somente serão fornecidas aos próprios interessados, mediante a solicitação formal, seguindo os requisitos legais vigentes.

## 4. DIRETRIZES CORPORATIVAS

O cumprimento da Política de Segurança Cibernética é de responsabilidade de todos os colaboradores e dos prestadores de serviços do Conglomerado Prudencial, os quais devem obedecer às seguintes diretrizes:

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;
- Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade;
- Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas;
- Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas de negócios;
- Atender às leis que regulamentam atividades do Conglomerado Prudencial e seu mercado de atuação;
- Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;
- Comunicar imediatamente à área de Segurança, quaisquer descumprimentos da Política Corporativa de Segurança Cibernética.

## 5. ESTRUTURA DE GERENCIAMENTO

O gerenciamento de procedimentos e controles de Segurança Cibernética objetivam assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e mantidos ou modificados de acordo com os objetivos estabelecidos pela Política de Segurança Cibernética em conformidade com a Politicas Globais do Grupo Scania e principalmente com o *ISec Code of Conduct* (Código de Conduta de Segurança da Informação).

### 5.1 Gestão de acessos às informações

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente com a aprovação do gestor do responsável e o da informação, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço conforme Política de Gerenciamento de Acesso.

## 5.2 Classificação da Informação

A classificação é um modo para decidir como a informação deve ser tratada e protegida, indicando a necessidade e prioridade para proteção. O dono da informação é responsável por avaliar o valor da informação e classifica-la de acordo, e é normalmente a pessoa que cria e / ou aprova a informação.

Dessa forma, todos são responsáveis por manusear a informação de acordo com sua respectiva classe de confidencialidade conforme o *ISec Code of Conduct* (Código de Conduta de Segurança da Informação).

## 5.3 Proteção do ambiente

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes conforme políticas *standards* do Grupo Scania ***Information Security Incident Management***, ***Malware Protection, NetworkSecurity*** e ***Cryptography***, para minimizar o risco de falhas e a administração segura de redes de comunicações, incluindo a gestão de serviços contratados de processamento e armazenamento de dados e informações em nuvem.

Testes de penetração são anualmente executados na rede do Conglomerado Prudencial e vulnerabilidades encontradas são tratadas conforme ***SLA ISEC Risk mang***.

Todo o acesso à informação do Conglomerado Prudencial somente pode ser realizado por pessoas autorizadas por meio da rede Scania ou por VPN se utilizando de tecnologias Juniper ou Citrix com *two factor authentication*.

O compartilhamento dos incidentes de Segurança Cibernética do Conglomerado Prudencial devem ser anualmente disponibilizados ao BACEN conforme Resolução 4.658/2018.

## 5.4 Segurança Física e Lógica

Os equipamentos e instalações de processamento de informação críticas ou sensíveis são mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais conforme ***ISec Stantard Physical Security***. Os requisitos de segurança de sistemas de informação são identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, integridade e disponibilidade. Os colaboradores do Conglomerado Prudencial deverão ser treinados periodicamente em encontros anuais sobre os conceitos de Segurança da Informação, através de

um programa efetivo de conscientização, e os prestadores de serviços de processamento e armazenamento de dados, devem ser seguir os procedimentos e controles necessários para garantir a segurança das informações.

### 5.5 Continuidade de Negócios

O processo de gestão de continuidade de negócios relativo a segurança da informação, é implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações identificados através do nosso BIA (Business Impact Analysis), funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços de processamento de dados contratados e os testes previstos para os cenários descritos em nosso PCN (Plano de Continuidade de Negócios).

## 6. RESPONSABILIDADE

A Alta Administração do Conglomerado Prudencial se compromete com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os quais devem ser objetos de pautas recorrentes em Comitês internos da empresa.