SCANIA

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Scania Serviços Financeiros

Scania Banco | Scania Administradora de Consórcios | Scania Corretora | Scania Locadora

Índice

SCANIA

Introdução

A Política de Segurança Cibernética tem como objetivo estabelecer as diretrizes para compor um programa completo e consistente de segurança da informação e gestão de riscos cibernéticos, visando:

- Proteger o valor e a reputação da nossa organização;
- 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.

1. Abrangência

As diretrizes contidas nesta Política se aplicam às empresas do Conglomerado Prudencial Scania.

2. Diretrizes Corporativas

O cumprimento da Política de Segurança Cibernética é de responsabilidade de todos os colaboradores, incluindo também, nossos prestadores de serviços e parceiros de negócios, 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 Compliance, quaisquer descumprimentos da Política de Segurança Cibernética.

3. 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).

3.1 Gestão de Acesso 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.

3.2 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.

As classes de classificações da Scania são:

- Pública
- Interna
- Confidencial
- Secreta - reservada para decisão da alta diretoria

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).

3.3 Proteção ao 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 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 as diretrizes do

SLA ISEC Risk Mangement.
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 autenticação de dois fatores.

O compartilhamento dos incidentes de Segurança Cibernética do Conglomerado Prudencial devem ser anualmente disponibilizados ao BACEN conforme Resolução 4.893/2021.

3.4 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.

3.5 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).

3.6 Manutenção de Cópias de Segurança de Dados e Informações

Objetivando garantirmos a integridade, disponibilidade e confidencialidade dos dados e informações críticas são realizados backups dos dados da Scania Serviços Financeiros regularmente conforme o disposto e detalhado na Política de Backup vigente.
A eficácia dos backups é testada regularmente através de recuperação de dados (*restores*), para assegurar que os dados podem ser restaurados de forma íntegra.

3.7 Definição de Parâmetros para Avaliação da Relevância dos Incidentes

Incidentes de segurança serão classificados com base em parâmetros como: impacto na continuidade do serviço, sensibilidade e volume dos dados comprometidos, número de clientes afetados, e possível dano à reputação da instituição. Os incidentes serão categorizados em níveis de severidade (por exemplo, baixo, médio, alto e crítico).

Critérios de avaliação: a relevância de um incidente será avaliada considerando:

- Impacto financeiro: potencial perda financeira decorrente do incidente.
- Impacto na reputação: possíveis danos à imagem e credibilidade da instituição perante o mercado e clientes.
- Impacto na continuidade: extensão da interrupção dos serviços essenciais.
- Conformidade regulatória: violação de obrigações regulatórias e legais.
- Volume e sensibilidade dos dados: quantidade e natureza dos dados afetados pelo incidente.

Incidentes considerados críticos deverão ser reportados imediatamente à área de Compliance e Gestão de Riscos, alta gestão e às autoridades competentes.

3.8 Prestação de Informação aos Clientes e Usuários

A Instituição compromete-se a disponibilizar, de forma clara, acessível e contínua, informações e orientações aos clientes e usuários sobre os cuidados necessários para a utilização segura dos produtos e serviços financeiros disponibilizados. Tais informações visam mitigar riscos relacionados a fraudes, vazamento de dados, engenharia social e demais ameaças cibernéticas.

As ações de comunicação incluem, mas não se limitam a:

- Divulgação de boas práticas de segurança digital, como a importância de senhas fortes, atualizações de sistemas e verificação da autenticidade de canais de atendimento;
- Alertas periódicos sobre golpes recorrentes no mercado financeiro, especialmente aqueles relacionados ao ambiente digital (phishing, smishing, malwares, etc.);
- Orientações quanto à responsabilidade do cliente no uso adequado das plataformas digitais, incluindo o uso de dispositivos seguros e a não divulgação de dados sensíveis;
- Disponibilização de conteúdo educativo nos canais oficiais da Instituição, como website, aplicativo, e-mails e redes sociais;
- Atendimento a dúvidas e incidentes por meio de canais de suporte preparados para orientar sobre segurança digital.

Essas medidas têm como objetivo promover a conscientização do cliente e do usuário final, fortalecendo a cultura de segurança cibernética e contribuindo para a prevenção de incidentes que possam comprometer a integridade, a confidencialidade e a disponibilidade das informações e dos serviços financeiros.