OBJETIVO

O documento estabelece as regras e os princípios da Política de Segurança da Informação e Cibernética, que deve nortear as ações dos parceiros da NicolaSEC. Esta é uma versão resumida para divulgação pública da Política Interna.

PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação abrange três pilares básicos, destacados nos princípios a seguir:

• Confidencialidade: Garante que a informação seja acessível somente pelas pessoas autorizadas e durante o período necessário.

• Disponibilidade: Garante que a informação esteja disponível para as pessoas autorizadas sempre que se fizer necessário aos processos de negócio ou a clientes da NicolaSEC.

• Integridade: Garante que a informação esteja completa e íntegra, bem como não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

ESCOPO DA POLÍTICA

Este documento está embasado nos principios fundamentais de segurança da informação e cibernética da empresa NicolaSEC, cujo escopo abarca os seguintes requisitos:

- Classificação e utilização das informações;
- Acesso lógico;
- Segurança de rede;
- Cópias de segurança (Backup);
- Logs e trilhas de auditoria;
- Dispositivos e controles de mídias;
- Uso de equipamentos;
- Mesa e tela limpa;
- Proteção e combate à vírus;
- Uso de Internet e Correio Eletrônico;
- Criptografia;
- Redes sociais;
- Gestão de vulnerabilidades;
- Incidentes de segurança da informação e cibernética;
- Gestão de riscos;
- Plano de Continuidade de Negócios;
- Plano de Ação e de Resposta a Incidentes;

DIRETRIZES GERAIS

Na NicolaSEC a Segurança da Informação e Cibernética é uma responsabilidade coletiva, em especial:

i) Colaboradores e parceiros;

ii) Privacidade de Dados: As informações da NicolaSEC dos clientes e do público em geral, são tratadas em conformidade com as determinações da regulamentação vigente e de forma alguma são manuseadas por pessoas não autorizadas pela empresa.

São diretrizes que regem a interpretação e a implementação da Política: a confidencialidade, a integridade, a conformidade e a disponibilidade.

As diretrizes expressas nesta Política aplicam-se a todas as informações pertinentes a NicolaSEC, que estiverem sob sua direta gestão ou custódia de terceiros.

As informações geridas são utilizadas apenas para os propósitos definidos pela NicolaSEC não sendo permitido a qualquer momento ou sob qualquer pretexto a apropriação ou utilização dessas informações em benefício próprio.

Todos os colaboradores e parceiros da NicolaSEC deverão se cientificar sobre a presente Política e recebem treinamento anual e adequado para utilizar as informações do negócio.

As informações geradas e manuseadas no âmbito da NicolaSEC possuem classificações que consistem no nível de proteção e cuidado que cada dado deve receber.

Os Colaboradores deverão, com base no tipo de ativo (informação), efetuar a classificação:

- Informação Pública;
- informação de Uso Interno;
- Informação de Uso Restrito, e;
- informação Confidencial;

Informações classificadas como internas, restritas ou confidenciais não devem ser divulgadas em ambiente público de internet, redes sociais, fóruns, grupos de discussão ou semelhantes.

As informações geradas pela NicolaSEC são de propriedade intelectual exclusiva e não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas, inferidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho.

A utilização dos sistemas de informação, rede corporativa, servidores e bancos de dados ocorre por meio da identificação de credencial de acesso individual, que é confidencial e não deve ser revelada em hipótese alguma, mesmo para outros Colaboradores.

Informações confidenciais não devem ficar expostas nas mesas e nos armários e os gaveteiros deverão ser trancados quando não utilizados, se os Colaboradores se ausentarem de suas mesas devem bloquear suas estações de trabalho.

Os incidentes de Segurança da Informação e cibernética da NicolaSEC são registrados, sua causa raiz e impacto são analisados e os fatores de criticidade são definidos, para que posteriormente sejam reportados à Diretoria e devidamente acompanhados pelos seus Colaboradores.

A NicolaSEC garantirá a continuidade do negócio, em caso de incidentes que possam comprometer o funcionamento normal de suas atividades. Para tanto, utilizará o seu PCN – Plano de Continuidade de Negócios, o qual é periodicamente revisado com o objetivo contínuo de melhoria.

A NicolaSEC possui um rigoroso processo de segurança em relação ao acesso físico, aos ativos físicos e lógicos, conforme preconizam as melhores práticas do mercado.

Exige-se dos parceiros o mesmo rigor em relação a proteção dos ativos físicos e lógicos, mediante formalização desta em nossos contratos que disciplinam a prestação dos serviços.

Regulamentação Aplicável:

- NBR ISO/IEC 27001:2013 - Sistemas de Gestão da Segurança da Informação;
- NBR ISO/IEC 27002:2013 - Código de Prática para Controles da Segurança da Informação;
- NBR ISO/IEC 27005:2019 – Gestão de Riscos de Segurança da Informação;
- Marco Civil da Internet – Lei N° 12.965, de 23 de abril de 2014 – Leis n° 12.735 e 12.737;
- Lei Geral de Proteção de Dados (LGPD) – Lei Nº 13.709, de 14 de agosto de 2018;