Política Pública de Segurança da Informação e Cibernética

Objetivo: Resumo das diretrizes para estabelecer os objetivos de Segurança da Informação e Cibernética apropriados ao contexto de negócios e seus riscos inerentes, e em acordo com os objetivos da K&N.

Público-alvo: Todos os funcionários da K&N e partes interessadas.

A K&N deve ser contatada, via e-mail ken@keninfo.com.br, nos casos de:

- Dúvidas sobre as informações tratadas neste documento;
- Falhas ou vulnerabilidades encontradas no processo;
- Necessidade de adequação identificada internamente, ou apresentada por auditoria, por órgão regulador, ou por cliente.

POLÍTICA PÚBLICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA DA K&N

Sumário

A. ESCOPO DESSA POLÍTICA

1. Objetivo

Esta Política de Segurança da Informação e Segurança Cibernética ("Política") tem o objetivo de estabelecer diretrizes que permitem à K&N CONSULTORIA E SISTEMAS LTDA. ("K&N") preservar e proteger as informações de seus clientes, funcionários, prestadores de serviços, partes interessadas e da própria K&N contra ameaças e riscos relacionados à segurança da informação e cibernética, bem como implementar controles e procedimentos que visam a reduzir a vulnerabilidade da K&N a incidentes, e também dispõe sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Esta política é formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

Esta Política é compatível com:

- O porte, o perfil de risco e o modelo de negócio da K&N;
- A natureza das atividades da K&N e a complexidade dos produtos e serviços oferecidos;
- A sensibilidade dos dados e das informações sob responsabilidade da K&N.

A K&N designará diretor responsável por esta Política e pela execução do plano de ação e de resposta a incidentes.

2. Abrangência

A Política se aplica a todos os sócios, diretores (coletivamente "Alta Administração"), funcionários e prestadores de serviço[1] da K&N (coletivamente, denominados simplesmente por "Colaboradores").

[1] Quaisquer terceiros que atuem em nome da K&N, tais como Auditoria Externa, Assessoria Jurídica, Tecnologia da Informação, Infraestrutura de TI, dentre outras.

3. Normas Aplicáveis

- Circular nº 3.909, de 16 de agosto de 2018, do Banco Central do Brasil.
- Norma ISSO/IEC 27001:2013.

4. Aprovação e Revisão

Esta Política foi aprovada e revisada pela Alta Administração e será revisada periodicamente. A Política também será alterada para contemplar quaisquer alterações regulatórias e outras obrigações legais.

5. Definições

- **Ativos**: todas as formas de criação, processamento, armazenamento, transmissão e exclusão de informações. Os Ativos podem ser documentos impressos, sistemas, *softwares*, banco de dados, arquivos digitais, dispositivos móveis etc..
- **Log:** registro de eventos de um sistema.
- **Segurança da Informação:** conjunto de conceitos, mecanismos e estratégias que visam a proteger os Ativos da K&N.
- **Segurança Cibernética:** conjunto de tecnologias e processos desenvolvidos para proteger os sistemas internos, computadores, redes e dados da K&N contra ataques, danos, ameaças ou acesso não autorizado.

B. PRINCÍPIOS

A K&N tem o compromisso garantir a segurança e tratamento adequado das informações. Para tanto, nossas atividades se baseiam nos seguintes princípios:

- **Confidencialidade**: garantia de que somente pessoas autorizadas terão acessos às informações e apenas quando houver necessidade;
- **Integridade**: garantia de que as informações permanecerão exatas e completas e não serão modificadas indevidamente;
- **Disponibilidade**: garantia de que a informação estará disponível às pessoas autorizadas sempre que for necessário.

C. DIRETRIZES GERAIS

Com o objetivo de garantir os objetivos desta Política, os procedimentos de Segurança da Informação e Segurança Cibernética seguirão as seguintes diretrizes:

- Assegurar que não haja acessos indevidos, modificações, destruições ou divulgações não autorizadas das informações. Para tanto, o acesso do Colaborador deve ser pessoal, intransferível e restrito aos recursos necessários para realizar suas atribuições na K&N.

- Cada Colaborador, quando aplicável, receberá uma senha pessoal de acesso e ficará responsável por manter sua senha em sigilo para evitar acesso indevido às informações que estão sob sua responsabilidade.
- Qualquer risco à informação deverá ser imediatamente reportado pelo Colaborador, através do e-mail ken@keninfo.com.br.
- Assegurar que todas as informações sejam tratadas de maneira ética e sigilosa e que sejam adotadas medidas capazes de evitar acessos indevidos, modificações, destruições ou divulgações não autorizadas.
- Assegurar que as informações sejam utilizadas somente para a finalidade para a qual foram coletadas e que o acesso esteja condicionado à autorização.
- Assegurar que os procedimentos e controles adotados para reduzir a vulnerabilidade a incidentes e atender aos demais objetivos de Segurança Cibernética, tais como, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.
- Assegurar que os controles específicos, incluindo os voltados para a rastreabilidade da informação, garantam a segurança das informações sensíveis.
- Assegurar o registro, análise da causa e o impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades de uma empresa de desenvolvimento e suporte de sistemas.
- Definir os procedimentos e controles voltados à prevenção e ao tratamento dos incidentes que devem ser adotados pelos prestadores serviços e terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da K&N;
- Assegurar os mecanismos para disseminação da cultura de segurança cibernética, incluindo:
    - A implementação de programas de capacitação e de avaliação periódica de pessoal;
    - A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos.
- Assegurar o registro, análise da causa e do impacto, bem como o controle dos efeitos de incidentes de informações recebidas de empresas prestadoras de serviços a terceiros.

D. PROCESSO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

A fim de assegurar que todas as diretrizes acima sejam cumpridas e que os princípios de Segurança da Informação e de Segurança Cibernética sejam devidamente seguidos, a K&N adotará políticas e procedimentos para os processos elencados a seguir.

1. Gestão de ativos

Os Ativos devem ser inventariados e protegidos de acessos indevidos ou ameaças que possam comprometer o negócio. Para tanto, o acesso às salas com documentos físicos deve ser limitado, através de mecanismos de autorização de acesso, destinados a impedir o acesso de indivíduos não autorizados.

Os Ativos devem ser utilizados tão somente para a finalidade devidamente autorizada. A K&N deve assegurar proteção aos Ativos durante todo o seu ciclo de vida, a fim de garantir que os princípios da confidencialidade, integridade e disponibilidade sejam cumpridos integralmente.

2. Autenticação

A K&N adotará mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados, levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação.

3. Segmentação de rede

A K&N deve adotar mecanismos internos para a segmentação de rede para proteger seus dados de ataques cibernéticos.

Caso o Colaborador queira criar, alterar ou excluir regras nos *firewall* e ativos de rede deverá enviar uma requisição ao departamento de tecnologia da informação, que fará análise e aprovação.

4. Classificação da Informação

As informações devem ser classificadas segundo sua criticidade e sensibilidade para o negócio e seus clientes. Portanto, a K&N adota a seguinte classificação:

- **Informação Pública**: aquela que pode ser acessada por todos, sem restrição.
- **Informação Interna**: aquela que pode ser acessada somente por Colaboradores da K&N. São exemplos de Informação Interna: normas, procedimentos e formulários da K&N;

- **Informação Restrita**: aquela que pode ser acessada somente por Colaboradores que precisam dela para desempenhar suas atribuições. São exemplos de Informação Restrita: contratos, fórmulas, algoritmos, programas fontes e documentos estratégicos da K&N e de seus clientes.
- **Informação Confidencial**: aquela que pode ser acessada somente por Colaboradores que tenham permissão de acesso ou que necessitem dela para um propósito específico. São exemplos de Informação Confidencial: plano estratégico e informações de clientes.

5. Controle de acesso

A K&N deve adotar controles de acesso em toda infraestrutura para evitar que indivíduos não autorizados tenham acesso aos ambientes segregados e aos sistemas internos. Desta forma, a K&N deve implementar mecanismos para a autenticação de usuários, manutenção de segregação de funções e rastreabilidade de acesso, de forma a garantir procedimentos internos adequados e consistentes.

6. Gestão de riscos

A K&N deve possuir processo para análise de vulnerabilidades, ameaças e impactos sobre os Ativos de informação para, diante de um incidente, adotar as medidas adequadas para minimizar os danos causados.

7. Gestão de fornecedores

A K&N deve verificar o grau de comprometimento com relação a controles de Segurança da Informação e Segurança Cibernética de todos os seus prestadores de serviços, fornecedores, provedores e parceiros que processam e armazenam dados da K&N, com a finalidade de verificar o nível de maturidade dos controles de segurança e o plano de tratamento de incidentes adotados.

A K&N disponibiliza o e-mail ken@keninfo.com.br para que seus prestadores de serviços, fornecedores, provedores e parceiros comuniquem incidentes de Segurança da Informação e Segurança Cibernética que estejam relacionados às informações da K&N.

8. Segurança física do ambiente

A K&N deve implementar sistema para controle de acesso dos Colaboradores, prestadores de serviços, fornecedores, provedores e parceiros aos locais restritos. Os equipamentos e instalações de processamento de informação crítica ou sensível devem são mantidos em áreas seguras.

9. Backup e gravação de LOG

A K&N adota uma rotina de backup e restauração de dados para assegurar a disponibilidade das informações relevantes para o pleno funcionamento de suas atividades.

10. Proteção contra vírus, arquivos e softwares maliciosos

A K&N adota mecanismos para prevenir que vírus e outros tipos de software e condutas maliciosas (e.g., *phishing*, *spam* etc.) se propaguem nos computadores, sistemas e servidores internos ou exponham a K&N a vulnerabilidades. Para tanto, os softwares de segurança, como o antivírus, estão instalados e atualizados em toda a rede interna da K&N.

11. Testes de varredura para detecção de vulnerabilidade

A K&N se preocupa em identificar e eliminar as vulnerabilidades de seus sistemas e servidores para assegurar a integridade do ambiente dos processos de negócio. Para tanto, promove monitoramento constante e condução de testes e varredura para detecção de vulnerabilidades, avaliação de riscos e determinação de medidas de correção adequadas.

12. Criptografia

Os Ativos de informação da K&N devem possuir criptografia adequada, a fim de se garantir proteção em todo o ciclo de vida da informação, em conformidade com os padrões de segurança dos órgãos reguladores.

13. Plano de continuidade

A K&N realiza plano de continuidade dos serviços prestados a partir da adoção de um conjunto preventivo de estratégias para garantir que os serviços essenciais da K&N sejam devidamente identificados e preservados após a ocorrência de uma contingência.

14. Incidentes de segurança

a) Classificação de relevância dos incidentes

A K&N classifica os incidentes de segurança segundo sua relevância e conforme a classificação das informações envolvidas e o impacto na continuidade dos negócios da K&N.

b) Gestão de incidentes

Todos os incidentes ou suspeita de incidentes identificados por um Colaborador, cliente, prestador de serviços, fornecedor, provedor ou parceiro devem ser imediatamente comunicados à área responsável. A comunicação deve ser feita através do e-mail ken@keninfo.com.br.

Os incidentes reportados serão classificados segundo o risco que representam para a K&N e o impacto na continuidade dos negócios da K&N. Além disso, devem ser devidamente registrados, tratados e comunicados.

A K&N adotará procedimentos para mitigar os efeitos dos incidentes relevantes e a interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados.

c) Plano de compartilhamento de incidentes

Sem prejuízo do dever de sigilo e da livre concorrência, a K&N adota iniciativas para o compartilhamento de informações sobre incidentes relevantes com seus clientes.

d) Plano de ação e resposta a incidentes

A K&N deve estabelecer plano de ação e de resposta a incidentes visando à implementação desta Política, que abrange, minimamente:

- As ações a serem desenvolvidas para adequar as estruturas organizacional e operacional às diretrizes desta Política;
- As rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes.

15. Mecanismos de rastreabilidade

A K&N deve adotar controles específicos para promover a rastreabilidade da informação, principalmente que busquem garantir a segurança das informações sensíveis.

16. Registro de impacto

A K&N deve realizar registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da K&N, que devem abranger inclusive informações recebidas de empresas prestadoras de serviços à terceiros.

17. Treinamentos e conscientização

A K&N preza por uma cultura de Segurança da Informação e Segurança Cibernética. Dessa forma, devem ser adotados políticas e procedimentos para a difusão dos princípios e diretrizes integrantes desta Política, garantindo-se a capacitação e conscientização para todos os seus Colaboradores.

Além disto, a Alta Administração da K&N deverá difundir a cultura de Segurança da Informação e Segurança Cibernética para promover melhorias contínuas em seus processos internos, a fim de evitar quaisquer incidentes relacionado à Segurança da Informação e Segurança Cibernética.

18. Contratação de serviços de processamento e armazenamento de dados e computação em nuvem

    a. Seleção de terceiros

O processamento e armazenamento de dados e computação em nuvem será realizado por meio de terceiros localizados no Brasil ou no exterior. A contratação de terceiros deve ser realizada por meio da aferição da capacidade do prestador de serviço para realizar as atividades em cumprimento com a legislação e regulamentação aplicável. Desta forma, a K&N deve adotar procedimentos para verificação da capacidade do potencial prestador de serviço de forma a assegurar:

- O cumprimento da legislação e da regulamentação em vigor;
- O acesso da K&N aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
- A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
- A aderência do prestador de serviço a certificações exigidas pela K&N para a prestação do serviço a ser contratado;
- O acesso da K&N aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
- O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A identificação e a segregação dos dados dos usuários finais da K&N por meio de controles físicos ou lógicos;
- A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da K&N.

Na avaliação da relevância do serviço a ser contratado, a K&N também deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a

serem processados, armazenados e gerenciados pelo contratado. Todos os procedimentos devem ser documentados.

Ademais, a K&N deve adotar recursos e medidas necessários para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso dos recursos providos pelo potencial prestador de serviços.

b. Execução de aplicativos pela internet

No caso da execução de aplicativos por meio da internet, a K&N deve assegurar que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades.

c. Serviços de computação em nuvem

Os serviços de computação em nuvem disponibilizados à K&N, sob demanda e de maneira virtual, deverão incluir um ou mais serviços conforme descritos abaixo:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à K&N implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela K&N ou por ela adquiridos;
- Implantação ou execução de aplicativos desenvolvidos pela K&N, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços;
- Execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

A K&N é responsável, em conjunto com o prestador de serviços, pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

d. Arquivamento de informações

A K&N deve armazenar, pelo prazo de 5 anos, as seguintes informações:

- O documento relativo à política de Segurança Cibernética;
- A ata de reunião da Diretoria da K&N;
- A documentação sobre os procedimentos desta Política;
- Os contratos de prestação de serviços mencionados nesta Política;
- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e controle, a partir da implementação dos mecanismos mencionados.

E. DECLARAÇÃO DE RESPONSABILIDADE

Os Colaboradores e prestadores de serviço da K&N devem aderir formalmente a um termo em que se comprometem a agir de acordo com esta Política. Ademais, todos os contratos da K&N devem possuir cláusula que assegure a confidencialidade das informações.

F. DISPOSIÇÕES GERAIS

Esta Política está acompanhada de um Termo de Adesão à Política de Segurança da Informação e Segurança Cibernética e Termo de Adesão às Alterações da Política de Segurança da Informação e Segurança Cibernética, que deverão ser assinados por todos os Colaboradores, prestadores de serviços, fornecedores, provedores e parceiros.

Esta Política está disponível em local acessível a todos Colaboradores, em linguagem clara e acessível. É possível acessá-la no site www.keninfo.com.br.

ANEXO I

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Eu, _____, inscrito no CPF sob o n. _____, declaro ter conhecimento desta Política Segurança da Informação e Segurança Cibernética, bem como das diretrizes contidas nas demais políticas, normas e procedimentos internos da K&N.

Declaro ainda ter conhecimento de que, diante de um incidente de segurança ou ameaça de incidente, devo comunicar imediatamente à área responsável por meio do e-mail ken@keninfo.com.br.

_____ /_____ /_____

Data

_____

Assinatura