Política de segurança e cibersegurança dos sistemas de informação

Políticas Corporativas 2025

Índice

01

Objetivo

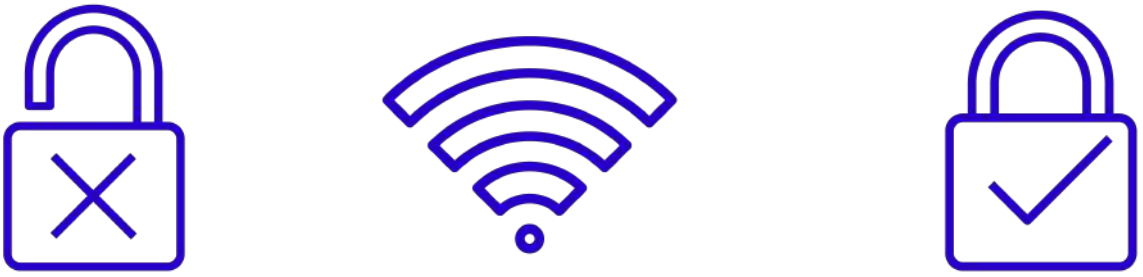
O objetivo da presente Política de Segurança e Cibersegurança dos Sistemas de Informação (doravante, a «Política»), que faz parte da Política-Quadro de Conformidade, é estabelecer e divulgar as normas básicas e gerais da Konecta, grupo multinacional de empresas especializadas na prestação de serviços e soluções digitais de gestão de clientes (doravante, «Konecta», a «Empresa», a «Sociedade» ou a «Companhia»), para garantir a integridade, privacidade e confidencialidade das informações, em conformidade com a legislação vigente na matéria, ponderando os riscos e fazendo uma utilização eficiente dos recursos, sempre com base em critérios de proporcionalidade na gestão.

O uso massivo das tecnologias da informação e telecomunicações (TIC) em todos os âmbitos da sociedade criou um novo espaço, o ciberespaço, onde podem ocorrer conflitos e agressões, e existem ciberameaças que podem afetar a Konecta e as suas diferentes empresas.

A presente Política estabelece um quadro de referência que define os princípios para garantir a proteção dos sistemas de informação da Konecta contra acessos não autorizados, perda ou danos durante o processamento da informação ou outro tipo de ameaças cibernéticas, garantindo a disponibilidade, integridade e confidencialidade da informação dos dados geridos pela Konecta.

Esta Política foi concebida para estabelecer o quadro de referência para os grupos de interesse internos da Konecta (funcionários, acionistas, investidores, diretores) e externos (clientes, fornecedores, auditores, governos, entidades reguladoras, meios de comunicação, concorrentes e entidades financeiras), reforçando a confiança nos sistemas de informação da empresa, garantindo o cumprimento escrupuloso da regulamentação em vigor em cada país, dos seus próprios requisitos e das normas internacionais.

Esta Política estará disponível no site corporativo (konecta.com) para que possa ser consultada por todas as partes interessadas.



02

Âmbito de aplicação

A presente Política está incluída no âmbito de aplicação da Política-Quadro de Conformidade e estende-se a todas as entidades da Konecta, apoiada pela direção-geral da empresa.

Consequentemente, o seu conteúdo é de cumprimento obrigatório para todos os funcionários da Konecta, independentemente do cargo ou função que ocupem dentro da organização ou da sua localização geográfica.

Sem prejuízo do acima exposto, o seu âmbito de aplicação poderá ser ampliado, quando necessário e possível devido à natureza da relação, a todas as pessoas singulares e/ou coletivas ligadas à Konecta por uma relação comercial ou profissional e que não seja de trabalho: fornecedores, empreiteiros e funcionários da cadeia de abastecimento e parceiros comerciais.

Uma vez que muitas das empresas da Konecta estão sediadas fora da União Europeia, o regulamento interno será adaptado às regulamentações específicas de cada Estado, respeitando e garantindo os princípios básicos aqui enunciados.

03

Princípios gerais de atuação

A Política de Segurança e Cibersegurança dos Sistemas de Informação reflete o compromisso expresso da Empresa em determinar e estabelecer as diretrizes e o suporte adequado para a administração da segurança da informação que gere, de acordo com os seus próprios requisitos e com as leis e regulamentos em vigor.

A Konecta zela por garantir «uma utilização segura das redes e dos sistemas de informação através do reforço das nossas capacidades de prevenção, defesa, deteção, análise, investigação, recuperação e resposta a ciberataques» que possam ocorrer.

A Konecta defende o uso seguro dos sistemas de informação e telecomunicações, mantendo-se sempre alinhada com a estratégia e os objetivos do negócio e, nessa linha, estabeleceu entre os seus objetivos específicos os seguintes, em conformidade com o contexto em que as atividades da empresa se desenvolvem:

- Impulsionar a segurança e a resiliência das redes e sistemas de informação utilizados.
- Sensibilizar todo o pessoal da empresa para os riscos decorrentes do ciberespaço.
- Capacitar e manter os conhecimentos, competências, experiência e capacidades tecnológicas para suster os objetivos da Konecta em matéria de cibersegurança.

Nesse sentido, a Konecta compromete-se a alcançar os seguintes objetivos:

- Considerar a informação e os sistemas que a suportam como ativos estratégicos. Assim, a Konecta manifesta a sua determinação em atingir os níveis de segurança necessários para garantir os requisitos de confidencialidade, integridade e disponibilidade da informação processada na organização, bem como dos recursos dos sistemas de informação que a processam, armazenam ou distribuem.

- Garantir a divulgação da regulamentação definida como suporte desta Política, com o objetivo de incutir nos colaboradores da Konecta um nível de sensibilização e formação em matéria de segurança da informação que garanta a aplicação de práticas adequadas, como elemento inerente ao desempenho das suas funções.

- Promover que a obtenção dos níveis de segurança da informação exigidos seja desenvolvida como um processo contínuo de melhoria e progresso constante, sustentado na definição dos objetivos e requisitos a cumprir, na implementação dos processos e medidas adequados, na verificação da sua efetividade, eficácia e eficiência, e na adoção das correções e modificações que se revelarem adequadas.

- A presente Política deve ser a principal ferramenta para garantir a adequada Segurança da Informação, promovendo e assegurando o seu cumprimento nos diferentes serviços.

- Zelar pela existência dos mecanismos necessários que assegurem a continuidade das atividades críticas da empresa que se baseiam nos sistemas de informação, permitindo a sua recuperação num período de tempo aceitável.

- Maximizar a qualidade dos serviços prestados.

- Reduzir ou eliminar, na medida do possível, os perigos e riscos nos ativos, processos e serviços que a Konecta fornece.

- Determinar medidas essenciais de segurança da informação que a Konecta deve adotar para se proteger adequadamente contra ameaças que possam afetar de alguma forma a confidencialidade, integridade e disponibilidade da informação.

Os objetivos da presente Política serão implementados com base numa estratégia de longo prazo. As atividades para atingir os objetivos devem ser mantidas ao longo do tempo.

No que diz respeito aos riscos de segurança, os planos de ação devem ser definidos e ajustados anualmente (controlos de segurança, definição de projetos de segurança, monitorização contínua, etc.).

Serão estabelecidos os planos de transição necessários para reduzir qualquer impacto nas atividades e/ou recursos da Konecta e, da mesma forma, esta zelará para que os funcionários:

- ... conheçam e apliquem os procedimentos internos e protocolos em matéria de segurança da informação da Konecta.
- ... disponham de ferramentas que lhes permitam aceder facilmente aos procedimentos operacionais internos (Intranet); adicionalmente, serão utilizados canais de comunicação alternativos para a comunicação de determinados processos, medidas especiais ou atualização de procedimentos.
- ... estejam cientes de que devem processar apenas as informações para as quais foram autorizados e usar os ativos da Konecta apenas para o desempenho das suas funções profissionais. Os funcionários devem cumprir as normas básicas de acesso a aplicações e/ou equipamentos com acesso a dados de carácter pessoal.
- … conheçam os procedimentos existentes na empresa para saber como agir perante qualquer atividade ou ameaça que possa afetar a segurança da informação, devendo informar o Departamento de Tecnologia e o Diretor de Segurança da Informação (CISO).

Conscientes de que cada país em que o Grupo opera tem um contexto social e necessidades diferentes, a presente Política é articulada através de planos e ações relacionados com os princípios nela contemplados, adaptados à realidade de cada uma das suas operações locais.

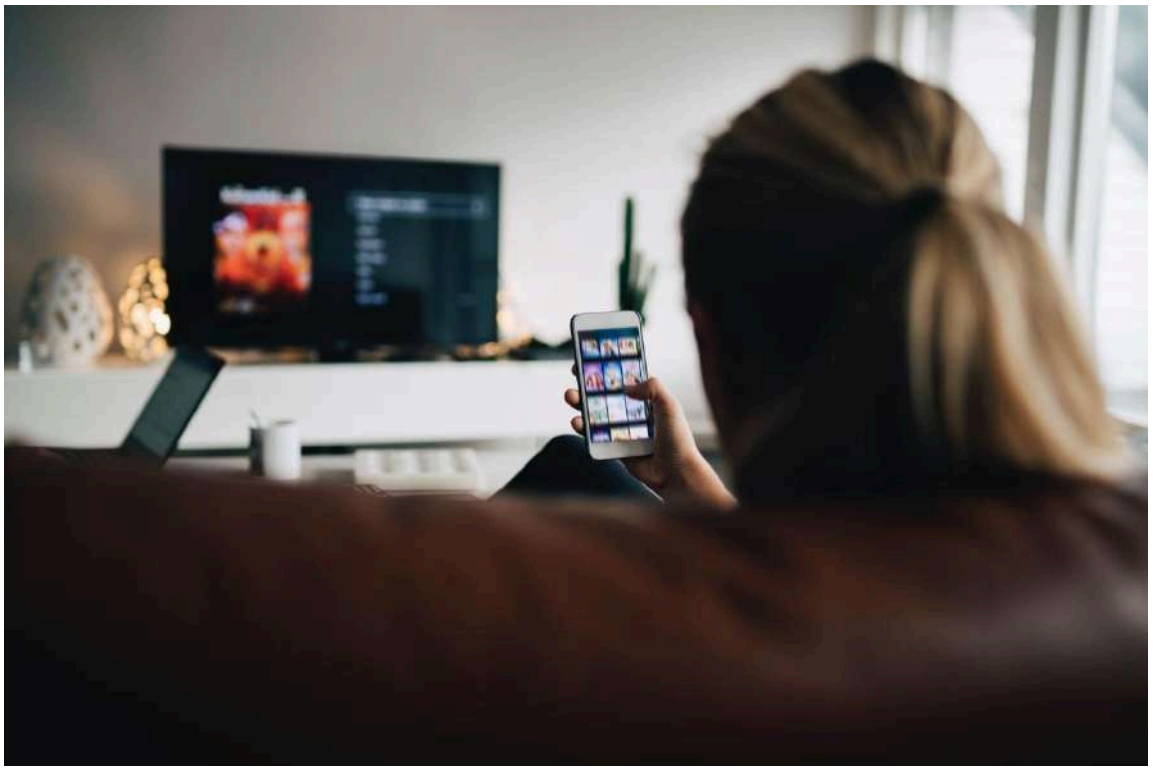
Estes princípios de atuação respondem aos impactos, riscos e oportunidades (IRO) decorrentes das questões materiais aplicáveis: segurança da informação; transformação digital; conformidade e ética corporativa; e gestão de fornecedores.

Tanto os funcionários como quaisquer terceiros que suspeitem da existência de qualquer potencial incumprimento relacionado com a presente Política ou com o Código de Ética, podem transmitir as suas informações, dúvidas ou preocupações sobre este assunto, de forma confidencial e sem receio de represálias, através dos Canais de Informação disponíveis no site corporativo da Konecta

(https://konecta.integrityline.com), de acordo com a natureza da situação, em conformidade com o procedimento PG COR 26 Canais de Informação, disponível no mesmo espaço, que especifica os diferentes canais disponíveis e a natureza da comunicação que pode ser realizada através dos mesmos.

Este canal está disponível 24 horas por dia, 7 dias por semana. Não será tolerada qualquer represália contra quem, de boa-fé, comunicar factos que possam constituir uma violação desta política, sendo aplicadas aos denunciantes as garantias e proteções estabelecidas pela regulamentação e legislação aplicáveis.

O incumprimento da presente política estará sujeito às medidas disciplinares correspondentes, de acordo com as normas e procedimentos internos, sem prejuízo das sanções administrativas ou penais que, se for o caso, também daí possam resultar e que sejam impostas pela autoridade competente.



04

Atualização e revisão

A presente Política estabelece as bases para o cumprimento das seguintes normas:

- ISO/IEC 27001:2022 Tecnologia da informação - Técnicas de segurança - Sistema de gestão da segurança da informação - Requisitos.
- ISO/IEC 27701 - Extensão da ISO 27001 para a gestão da privacidade.
- ISO/IEC 27002:2022 Tecnologia da informação - Técnicas de segurança – Boas práticas para gestão de segurança da informação.
- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE).
- Leis em matéria de Proteção de Dados Pessoais aplicáveis em cada país.

A Política de Segurança e Cibersegurança dos Sistemas de Informação será revista periodicamente ou sempre que necessário, para se ajustar às mudanças no modelo de negócio, à aprovação de novos regulamentos ou às melhores práticas internacionais, garantindo a sua eficácia e conformidade contínua.

NOTA: A presente Política foi revista e aprovada a 16 de dezembro de 2025 pelo órgão máximo de governança e substitui qualquer versão anterior da mesma, sendo válido apenas este documento a partir da data.

Controle de revisões

Edição	Data de revisão	Revisto	Validada	Aprovada	Motivo da alteração
2	22/06/2021	TI - Segurança da Informação Organização e Procedimentos	Assessoria Jurídica	Conselho de Administração	Revisão geral da política
3	19/12/2022	TI - Segurança da Informação Organização e Procedimentos	Assessoria Jurídica	Conselho de Administração	Revisão geral da política
4	16/12/2025	TI - Segurança da Informação Organização e Procedimentos	Assessoria Jurídica	Conselho de Administração	Adaptação aos requisitos legais Adequação ao novo formato e à marca