Política da Segurança da Informação

esg trek

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ESGTREK TECNOLOGIA DA INFORMAÇÃO LTDA

CNPJ: 62.316.392/0001-50 - São Paulo – SP

1. Introdução

A EsgTrek Tecnologia da Informação Ltda, inscrita no CNPJ nº 62.316.392/0001-50, dedica-se ao desenvolvimento de software e soluções digitais para gestão de dados ESG. Neste contexto, informação e dados — incluindo dados ambientais, sociais, governamentais e dados pessoais — constituem ativos estratégicos e essenciais para a continuidade do negócio.

A informação é um dos ativos mais valiosos da EsgTrek Tecnologia da Informação Ltda., sustentando a operação, a confiabilidade dos produtos, a tomada de decisão e a entrega de soluções inovadoras em gestão de dados ESG. Em um contexto de crescente digitalização, expansão de ambientes em nuvem e tratamento intensivo de dados, especialmente dados pessoais e informações estratégicas de sustentabilidade, a proteção desses ativos torna-se essencial para a continuidade do negócio, para a preservação da reputação da empresa e para a conformidade regulatória.

Como provedora de tecnologia voltada ao monitoramento, análise e governança de indicadores ambientais, sociais e de governança, a EsgTrek lida diariamente com dados sensíveis, resultados de auditorias, avaliações de risco, planos de ação, métricas de emissões e demais informações críticas de seus clientes. Por essa razão, a empresa adota uma postura robusta e sistemática de Segurança da Informação, baseada em princípios internacionalmente reconhecidos, práticas consolidadas de mercado e nas exigências legais aplicáveis, como a Lei Geral de Proteção de Dados Pessoais (LGPD).

Esta Política estabelece diretrizes, responsabilidades, papéis e controles necessários para assegurar que todos os colaboradores, parceiros e terceiros atuem de forma alinhada à preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações. Também orienta a criação de normas internas complementares, a gestão de riscos, o uso responsável dos recursos tecnológicos e a adoção de medidas preventivas e reativas para incidentes de segurança.

A Política de Segurança da Informação da EsgTrek representa, portanto, um compromisso institucional com a governança digital, a ética no tratamento de dados e a excelência operacional que sustenta as soluções tecnológicas oferecidas ao mercado ESG.

2. Objetivos

A Política de Segurança da Informação da EsgTrek tem como objetivos:

1. **Proteger os ativos de informação**, assegurando confidencialidade, integridade, disponibilidade e autenticidade.
2. **Estabelecer diretrizes e responsabilidades** para o correto uso, armazenamento, processamento e descarte de informações.
3. **Mitigar riscos tecnológicos, jurídicos e operacionais**, preservando a confiabilidade de dados ESG e pessoais tratados pelas plataformas da empresa.
4. **Alinhar a segurança da informação à estratégia de negócio**, fortalecendo governança e confiança junto a clientes, parceiros e usuários.
5. **Cumprir requisitos legais e normativos**, incluindo LGPD, Marco Civil da Internet e demais regulamentos aplicáveis.
6. **Fomentar cultura interna de segurança e proteção de dados**, por meio de capacitações e comunicação contínua.

3. Escopo

Esta Política aplica-se a:

- Todos os colaboradores, estagiários, sócios, prestadores de serviço, consultores e terceiros.
- Todos os ativos de informação da empresa, físicos ou digitais, incluindo:
    - Sistemas, códigos-fonte, APIs e ferramentas internas
    - Banco de dados e data lakes
    - Infraestrutura em nuvem
    - Dispositivos corporativos
    - Softwares de gestão e monitoramento ESG
- Todas as operações de tratamento de dados pessoais e sensíveis realizadas no contexto dos serviços da empresa.

4. Princípios de Segurança da Informação

1. **Confidencialidade** – acesso somente por pessoas autorizadas.
2. **Integridade** – informações íntegras, atualizadas e protegidas contra alteração indevida.
3. **Disponibilidade** – informações acessíveis quando necessárias.
4. **Autenticidade** – garantia da origem e rastreabilidade das informações.

5. **Legalidade e Conformidade** – aderência à LGPD e demais regulações.
6. **Privacidade por padrão e por concepção (Privacy by Design)**.
7. **Responsabilidade e prestação de contas**.
8. **Minimização de riscos e prevenção de incidentes**.
9. **Alinhamento estratégico com o negócio ESG-TI**.

5. Termos e Definições

- **Ativo de Informação**: qualquer dado, sistema, serviço digital ou recurso de TI crítico para o negócio.
- **Dado Pessoal**: informação relacionada a pessoa natural identificada ou identificável.
- **Dado Pessoal Sensível**: informações definidas no Art. 5º, II da LGPD.
- **Incidente de Segurança**: violação, tentativa de violação ou falha que comprometa SI.
- **Usuário**: qualquer pessoa que utilize recursos tecnológicos da EsgTrek.

6. Diretrizes Gerais

6.1 Classificação da Informação

- **Pública**
- **Interna**
- **Restrita**
- **Confidencial** (inclui dados pessoais e dados estratégicos de clientes)

6.2 Controle de Acesso

- Acesso individual, intransferível e com autenticação multifator (MFA).
- Senhas fortes e renovação periódica.
- Mínimo privilégio e segregação de funções.
- Proibição de compartilhamento de contas.

6.3 Infraestrutura Tecnológica

- Todos os ambientes são hospedados em **infraestrutura cloud segura**, com criptografia em trânsito e repouso, conforme modelos analisados.
- As integrações via API devem seguir padrões OAuth2/SAML conforme recomendações de segurança.

6.4 Desenvolvimento Seguro de Software

- **Configuração segura de acesso a dados** por meio de regras de privacidade, políticas de acesso por linha (RLS) ou controles equivalentes, garantindo que usuários e integrações acessem apenas o que lhes é autorizado.
- **Implementação de lógica sensível no backend**, evitando exposição indevida de fluxos críticos no front-end e assegurando que APIs, automações e serviços internos operem com autenticação e autorização robustas.
- **Aplicação de princípios de DevSecOps**, com revisões de segurança a cada alteração significativa, testes periódicos de integridade e vulnerabilidade em endpoints e monitoramento contínuo do comportamento dos sistemas.
- **Rastreabilidade das alterações** através de versionamento, registros de mudanças e auditoria de eventos, garantindo visibilidade sobre configurações, permissões, workflows e operações críticas.

6.5 Gestão de Riscos

- Avaliações de risco periódicas.
- Registros, priorização e tratamento documentado.
- Relatórios apresentados ao Comitê de Segurança.

6.6 Tratamento de Incidentes

- Procedimentos para identificação, contenção, erradicação e recuperação.
- Comunicação ao DPO e, quando aplicável, à ANPD e aos titulares.
- Registro em trilhas de auditoria.

6.7 Uso Aceitável dos Recursos

- Proibido uso inadequado, ilegal, discriminatório ou que viole direitos autorais.
- Proibida a instalação de softwares não homologados pela TI.

7. Proteção de Dados Pessoais e Privacidade

1. **Todos os dados pessoais tratados são considerados confidenciais**.
2. Aplicação dos princípios da LGPD: finalidade, adequação, necessidade, transparência etc.
3. Implementação de:
    - Privacy by Design
    - Privacy by Default

- Registro de Operações de Tratamento
- Plano de Resposta à Violação de Dados
- Criptografia de dados pessoais

4. Toda coleta deve estar vinculada a **base legal válida e documentada**.
5. O Encarregado DPO (Karine Almeida de Paula) atua como ponto de contato com titulares e ANPD.

8. Governança e Responsabilidades

8.1 Alta Administração

- Aprovar esta política e garantir recursos.
- Promover cultura de segurança da informação.

8.2 Comitê Interno de Segurança e Privacidade

- Analisar riscos, incidentes e exceções.
- Aprovar normas complementares.
- Acompanhar indicadores de segurança.

8.3 DPO – Encarregada de Dados

- Nomeada: **Karine Almeida de Paula**.
- Funções conforme Carta de Nomeação e Art. 41 da LGPD.

8.4 TI e Segurança da Informação

- Gerenciar infraestrutura, controles e monitoramento.
- Realizar testes de vulnerabilidade e pentests.

8.5 Usuários

- Cumprir a PSI.
- Zelar pelos ativos sob sua responsabilidade.
- Reportar violações ou suspeitas imediatamente.

9. Monitoramento e Auditoria

- A EsgTrek poderá monitorar ambientes, registros de acesso, logs e uso de recursos, respeitando LGPD e proporcionalidade.

- Auditorias periódicas serão realizadas para garantir conformidade.

10. Gestão de Continuidade e Backups

- Backups criptografados e testes de restauração periódicos.
- Plano de Continuidade de Negócios para garantir disponibilidade dos sistemas ESG.

11. Disposições Finais

- Violações à Política estão sujeitas a medidas disciplinares.
- A política será revisada anualmente ou diante de mudanças relevantes.
- Casos omissos serão avaliados pelo Comitê de Segurança.

Histórico de Revisões

Versão	Data	Descrição das Alterações	Responsável pela Alteração
[001/2025]	[03/12/2025]	[Versão inicial]	[Káritas Ribas]

esg trek

Gestão ESG **simplificada, eficiente e estratégica** para sua empresa