A TRIGO reconhece que o processamento de informações é fundamental para a prestação de seus serviços e que a segurança e a proteção das informações coletadas, tratadas e compartilhadas devem ser mantidas. Nossa gestão está comprometida não apenas em garantir a conformidade com os requisitos aplicáveis (legais, regulamentares e de clientes, fornecedores, colaboradores e outras partes interessadas), mas também em aprimorar continuamente o sistema de gestão para assegurar a disponibilidade, a integridade e a confidencialidade das informações sensíveis.

Para atingir esse objetivo, nos esforçamos para:

- Identificar e gerenciar riscos e oportunidades de segurança da informação.
- Conscientizar os funcionários sobre os riscos e desenvolver uma cultura de segurança da informação por meio de treinamentos, comunicações e compartilhamento de lições aprendidas, para manter todos os funcionários da nossa organização atualizados sobre as boas práticas de segurança.
  - → A TRIGO pretende garantir que pelo menos 90% dos seus funcionários tenham recebido treinamento em cibersegurança até o final de 2027.
- Proteger os dados pessoais em conformidade com nossa obrigação legal.
- Implantar e manter infraestruturas de TI e sistemas digitais estáveis, seguros e altamente disponíveis, apoiados por uma estratégia abrangente de cibersegurança, incluindo o controle de processos terceirizados.
- Detectar, reportar e responder eficazmente a incidentes de segurança da informação.
- Implantar e manter infraestruturas de TI e sistemas digitais estáveis, seguros e altamente disponíveis, apoiados por uma estratégia abrangente de cibersegurança, incluindo o controle de processos terceirizados.
- Monitoramos continuamente nosso ambiente de TI por meio de uma combinação de ferramentas de monitoramento internas e plataformas externas de avaliação de segurança cibernética, proporcionando visibilidade constante sobre nossa exposição a vulnerabilidades e ameaças.
  - → A TRIGO tem como objetivo manter uma classificação mínima de 750 pontos em um total de 1000 nos indicadores de cibersegurança, conforme medido por plataformas independentes de avaliação cibernética, esse resultado reflete um sólido controle sobre sua superfície de ataque externa e um esforço contínuo para identificar e corrigir as vulnerabilidades.
- Realizar auditorias de segurança regulares para garantir a eficácia dos controles implementados e impulsionar a melhoria contínua.
- Testar e manter os planos de recuperação de desastres para nossos sistemas operacionais de TI.

Esta política é elaborada pelo Diretor de Segurança da Informação (Chief Information Security Officer - CISO), em coordenação com o Diretor de Proteção de Dados do Grupo (Group Data

Protection Officer - DPO), e aprovada pelo CEO e pelo Vice-CEO. A implementação desta política é apoiada por diversas políticas complementares, processos e recursos, garantindo sua adequada aplicação e efetividade em toda a organização.
Aplica-se a todas as entidades da TRIGO em todo o mundo, abrangendo todos os nossos colaboradores, prestadores de serviços e terceiros que tenham acesso aos sistemas de informação da TRIGO.

Sua implementação se baseia em um modelo de responsabilidade compartilhada:

- A função de TI do Grupo é responsável por definir, implementar e manter as infraestruturas globais de TI, as medidas de cibersegurança, as atividades de monitorização e as capacidades de recuperação de desastres.
- As entidades locais e os usuários são responsáveis por cumprir as regras definidas, proteger os ativos de informação e contribuir para a gestão dos riscos e incidentes de segurança da informação.

Portanto, embora alguns controles sejam gerenciados centralmente em nível de Grupo, o Gerente Geral de cada entidade é responsável por garantir a correta aplicação desta política dentro de sua área de atuação e responsabilidade.

O Grupo também promove a melhoria contínua através do monitoramento de indicadores relevantes e da implementação de ações corretivas quando necessário.

Esta política está sujeita a uma revisão anual como parte do processo de Análise de Gestão. Esta revisão leva em consideração questões internas e externas, eventos e impactos significativos em matéria de segurança e a direção estratégica do Grupo, a fim de garantir a relevância, a eficácia e a melhoria contínua da política.

Contamos com todos os nossos colaboradores para adotar os comportamentos adequados e contribuir para o melhoria contínua de nossas práticas de segurança, compartilhando e apresentando ideias de melhoria por meio dos canais apropriados.

Matthieu Rambaud
CEO

Benoît Leblanc
Vice-CEO

Versão #	Data de aplicabilidade (mm/dd/ aa)	Página(s)	Descrição da(s) alteração(ões)
A	15/07/2026	Todos	Conteúdo inicialmente incluído no documento PR.MAN.WW. 09.PT -A Segurança da informação (versão de 3 de abril de 2023). Este novo documento também introduz metas quantitativas.