SECURITY WHITEPAPER

1. INTRODUÇÃO

Aqui na **Vantico** desenvolvemos uma nova metodologia para execução de testes de segurança (Pentests) sob demanda e totalmente escalável. Assim, elaboramos esta Política de Segurança da Informação e Cyber Security (Política) para reafirmar o compromisso que temos com a adoção das melhores práticas de segurança da informação e proteção dos dados dos nossos clientes.

2. GESTÃO DE RISCO

Todas as principais mudanças da empresa e da plataforma são através de tickets em nosso sistema de tarefas Jira. Mantemos atividades de segurança separadas no backlog que seguem o mesmo processo e visam aumentar a postura de risco da empresa e da plataforma. Esses itens de backlog podem vir de resultados de testes, feedback, resultados de bug bounty ou análise de nossa segurança baseada em melhores práticas de mercado.

3. CONFORMIDADE

A **Vantico** se esforça para seguir os regulamentos governamentais nos países em que atendemos nossos clientes, seguindo Regulamento Geral sobre a Proteção de Dados (GDPR) e a Lei Geral de Proteção de Dados (LGPD).

4. ARMAZENAMENTO DE DADOS

Todas os nossos bancos de dados e buckets de dados são armazenados de acordo às melhores práticas de provedores de nuvem nas regiões de São Paulo.

Os backups são replicados para outros provedores de nuvem em São Paulo (criptografado) para garantir a disponibilidade. A restauração de backup de produção é testada periodicamente.

5. TESTES DE SEGURANÇA

Depois que o código foi mesclado para staging, o ticket é atualizado e passado para a equipe de Testes de Qualidade (QA) para testes funcionais e não funcionais. Após a aprovação do controle de qualidade, este é passado para nossa própria equipe interna de triagem, que possui ampla experiência em testes de vulnerabilidades.

Depois de executar o teste de segurança black/graybox em cada mudança de ticket, o ticket é devolvido para a segurança equipe que revisará os resultados do teste e aprovará ou negará a release. Após o lançamento da nossa plataforma.

6. PROGRAMA DE DIVULGAÇÃO DE VULNERABILIDADES

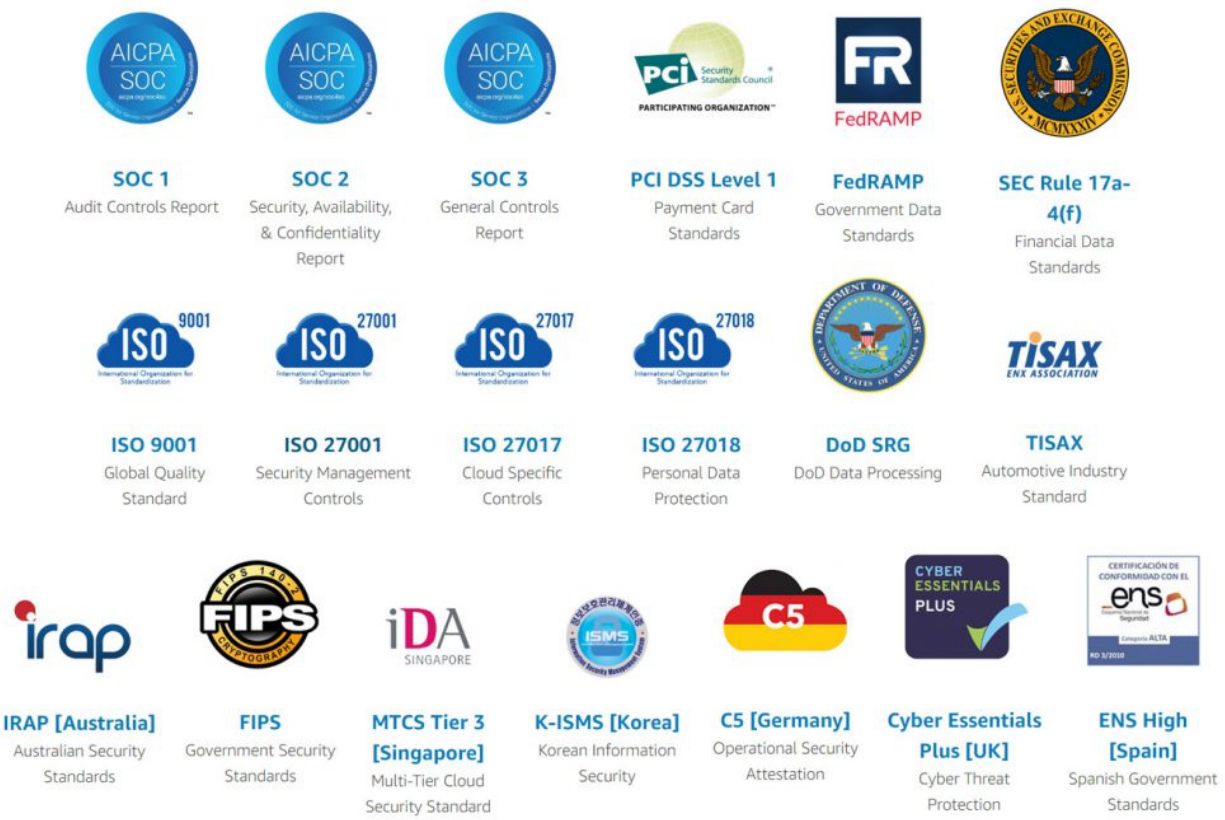
Se você acredita ter descoberto um bug na segurança a **Vantico**, informe-nos através do e-mail security@vantico.com.br. Nossa equipe de segurança investiga prontamente todos os problemas relatados.

7. SEGURANÇA DE INFRAESTRUTURA

Contamos fortemente com os princípios GitOps e Cloud-Native para execute nossa plataforma em nosso provedor de nuvem. Quaisquer práticas recomendadas são levadas em consideração (como **NIST, CIS Benchmarks, OWASP** e recomendações de fornecedores) para fortalecer nossa infraestrutura baseada no Princípio de **Defesa em Profundidade.**

Cada implantação acontece a partir de nosso repositório de código, que exigirá uma verificação de qualidade antes de implantar em um ambiente de contêiner segregado, que vive por trás de vários controles como um Firewall de rede, Web Application Firewall e Virtual Private Cloud (VPCs).

Todas os serviços da **Vantico** são hospedados na infraestrutura de cloud da Amazon (AWS), seguindo os melhores controles de segurança do mercado.



8. SEGURANÇA NO DESENVOLVIMENTO

O acesso ao nosso repositório de códigos é estritamente controlado por meio de nossa política de acesso. Os desenvolvedores trabalham com um forte modelo de permissões em nosso repositório de código que os força a criar solicitações de pull antes de poder mesclar as alterações em nosso Github. A solicitação pull requer revisão de pelo menos um desenvolvedor sênior que verificará a qualidade do código, melhor práticas e diretrizes de segurança.

Uma solicitação pull também acionará nossos testes automatizados que nos informam sobre quaisquer falhas de desenvolvimento ou vulnerabilidades estáticas.

9. SEGURANÇA DE APLICAÇÃO

Autorização e autenticação são tratadas por testes no código e componentes. Além disso, construímos uma forte estrutura de autorização que explicitamente define e verifica regras de autorização específicas por objeto e conta.

Além disso, todos os dados de envio confidenciais são criptografados com uma chave criptográfica específica para esse cliente, além à criptografia em repouso que fazemos na camada de armazenamento. Esta garante que qualquer risco na camada de armazenamento (seja físico, como roubar um servidor ou obter acesso ao nosso banco de dados) é mitigado pelo fato de que o invasor não tem acesso à chave do cliente para descriptografar esses dados.

Tentativas automatizadas de explorar nossa plataforma serão, em na maioria dos casos, bloqueados por nosso Web Application Firewall (WAF) que aciona alertas para a equipe e pode permitir banimento automático de endereços IP. Qualquer outro suspeito ou inválido as ações também serão alertadas pelo aplicativo e serão desencadear uma investigação mais aprofundada.

10. SEGURANÇA NA PLATAFORMA

Os itens a seguir fornecem uma visão geral das principais medidas importantes que tomamos para garantir uma operação segura na plataforma.

Segurança no front-end

Todas as entradas do usuário são classificadas como entradas não confiáveis e tratadas como tal. Estamos em fase de implementação do Angular, que lida com a codificação de saída com reconhecimento de contexto para prevenir ataques Cross-Site Scripting (XSS). Qualquer novo front-end é testado antes para garantir as melhores práticas.

Segurança no back-end

Nosso back-end é executado em contêineres linux reforçados que são protegidos por meio de configuração e monitoramento de ameaças. Seguimos as melhores práticas conforme definido pelo projeto OWASP. Essas estruturas incluem os itens do ASVS e WSTG. Os servidores que executam nossos contêineres são mantidos atualizados em um cronograma de atualização e possuem medidas de proteção aplicadas de acordo com as recomendações do CIS.

Autenticação

Nossa Autenticação Multi-Factor é habilitada por padrão em todas as contas. Cada solicitação autenticada para a plataforma é verificada para uma sessão existente. As sessões são armazenadas para o usuário em um cookie de host seguro específico ao nosso domínio na plataforma. Atualmente, temos uma vida útil de sessão de 90 minutos.

Dados em trânsito

Cada solicitação para a plataforma é feita atrás de Transport Layer Security (TLS) para garantir que nenhum dado possa ser lido por partes não autorizadas. Os protocolos e listas de cifras são mantidos de perto para garantir nossa Rede De Entrega De Conteúdo (CDN). Cada solicitação não criptografada é redirecionada para seu endereço seguro correspondente e criptografado.

Monitoramento

Nossa aplicação está atrás de um Web Application Firewall (WAF) da Cloudflare que bloqueia vetores de ataque populares e possui um conjunto de regras básico. Todos os alertas do WAF são registrados e podem acionar uma ação de bloqueio para nossa plataforma. O WAF também nos protege contra Ataques De Serviço (DoS) até a Camada 7 (HTTP).

11. RESPOSTA A INCIDENTES

Todos os incidentes são registrados por meio de um fluxo de trabalho central em nosso sistema de gerenciamento de tickets que manterá as informações mais vitais como detalhes, timestamps, ações tomadas e, posteriormente, uma análise de causa raiz.

12. COMUNICAÇÃO

Em caso de dúvida, questão ou preocupação em relação a este documento, entre em contato através de **security@vantico.com.br**.

13. REVISÕES

Versão	Data	Revisão	Aprovação	Conteúdo Revisado
1.0	24/01/2023	Kaique Bonato	Diretoria	Criação do documento
1.1	05/06/2023	Kaique Bonato	Diretoria	Atualização de layout e adições no tópico “Segurança de Infraestrutura”
1.2	26/03/2024	Kaique Bonato	Diretoria	Atualização de layout
1.3	20/04/2024	Kaique Bonato	Diretoria	Atualização do Jira