VTEX

The Enterprise
Digital Commerce
Platform

Postura de Segurança da VTEX

VTEX Security

Introdução 03
Estamos comprometidos com a sua tranquilidade 04
Como protegemos nossos clientes e sistemas 05
Programa de segurança da informação 06
Auditoria e Conformidade 07
Educação e Conscientização sobre segurança 08
Gestão de Ativos 09
Acesso, identificação e autenticação 10
Segurança dos Dados 11
Privacidade e Proteção de dados 12
Controles Criptográficos 13
Segurança do datacenter e escritórios 14
Segurança do host 15
Gerenciamento de Mudança 16
Registro e Monitoramento de Segurança 17
Inteligência de Ameaças e Resposta a Incidentes 18
Gestão de Vulnerabilidades 20
Segurança do Perímetro 21
Ciclo de Desenvolvimento Seguro 22
Gestão de Avaliação de Terceiros 23
Gerenciamento de Riscos de Segurança 24
Continuidade de Negócios 25
Maturidade de Segurança 26
Conclusão 27
Recursos 28

Introdução

Com o aumento exponencial do trabalho remoto e do comércio eletrônico, as empresas foram instadas a desenvolver um ambiente online seguro e protegido. Embora a segurança tenha se tornado um tema quente no mercado, menos de um terço das empresas brasileiras têm equipes dedicadas de segurança cibernética.

Aqui na VTEX temos o compromisso de mudar esse cenário. Desenvolvemos uma equipe totalmente dedicada à Segurança da Informação para garantir tranquilidade, bem-estar, segurança e confiança a todos que fazem ou farão parte da nossa comunidade.

Entendemos a importância de adotar práticas de segurança líderes do setor e tecnologias necessárias para proteger os dados dos clientes e essas práticas estão incorporadas em todas as nossas tecnologias, pessoas e processos.

Nossos clientes confiam em nós para fornecer altos níveis de confidencialidade, integridade e disponibilidade de dados. Por mais de duas décadas, trabalhamos com clientes em setores altamente regulamentados, dispostos a confiar seus dados à VTEX.

Compromisso da VTEX

Na VTEX temos o compromisso de seguir as práticas e medidas de segurança mais eficazes, garantindo que os acessos sejam controlados e os dados estejam seguros e protegidos.

Nossas Diretrizes

Para melhorar continuamente nossa postura de segurança, nos baseamos na ISO 27001:2022 para medir a maturidade de nossos programas de segurança e para avaliar e identificar áreas de melhoria. Essa norma é o padrão e a referência Internacional para a gestão da Segurança da informação.

Estamos comprometidos com a sua tranquilidade

Somos a Plataforma de Comércio Digital Empresarial

Tomamos decisões ousadas, colocando-nos em risco pelo sucesso de nossos clientes. Somos uma equipe de alta performance, sempre aprendendo e abraçando desafios fora da nossa zona de conforto.

Somos a espinha dorsal do comércio conectado

Na VTEX entendemos a importância de adotar práticas de segurança e tecnologia necessárias para proteger os dados dos clientes. Nossas medidas de segurança estão incorporadas em toda nossa tecnologia, processos e pessoas.

A VTEX é mais que uma plataforma de comércio

Trazemos harmonia entre negócios e tecnologia. Sabemos que privacidade e segurança são fundamentais para o sucesso em qualquer tipo de negócio.

Nesse documento, iremos abordar uma visão geral sobre a nossa postura de segurança para demonstrar o nosso compromisso com a nossa segurança e dos nossos clientes.

Como protegemos nossos clientes e sistemas

Programa de Segurança da Informação

Na VTEX, temos um programa de Segurança da Informação implementado e gerenciado por uma liderança comprometida em elevar o nível de maturidade de segurança para todo ecossistema VTEX.

Possuímos uma **Política de Segurança da Informação**, que é transmitida para toda a companhia através dos nossos canais de comunicação e revisada anualmente, de acordo com o nosso processo de gestão de documentos.

Nossa Política de Segurança da Informação é orientada pela norma ISO/IEC 27001:2022; frameworks com as melhores práticas de segurança; leis de proteção de dados e outras obrigações aplicáveis ao contexto da VTEX.

Todos os nossos documentos são revisados anualmente e garantimos a gestão deles por meio de uma plataforma de gerenciamento de políticas.

A VTEX possui uma equipe robusta e especializada em Segurança da Informação, estruturada e dedicada para suportar os nossos processos de segurança. Nossa equipe de segurança trabalha em esquema de prontidão, com equipes em diferentes fusos horários para garantir que tenhamos uma cobertura além do horário comercial.

Auditoria e Conformidade

Auditorias de Conformidade Internas

As auditorias internas de conformidade são conduzidas por nossa equipe de auditoria interna e ocorrem periodicamente, como preparação para auditorias externas de certificação.

Nossa equipe de auditoria atua constantemente na melhoria deste processo e na automação da verificação dos controles, com o objetivo de ter um painel de conformidade ativo.

Auditorias de Conformidade Externas

As auditorias de certificação são realizadas por empresas independentes e são monitoradas por nossa equipe de Auditoria Interna. Seus resultados são utilizados para melhorar os processos internos de monitoramento de conformidade.

Certificações da VTEX

A VTEX possui um programa de conformidade a fim de adotar os mais elevados padrões de segurança.

Service Organization Controls (SOC 1)

Auditoria que abrange os controles internos sobre os sistemas de relatórios financeiros.

Service Organization Controls (SOC 2 e 3)

Auditoria cobrindo os processos de Segurança, Disponibilidade, Integridade, Confidencialidade e Privacidade da plataforma.

Payment Card Industry Data Security Standards (PCI DSS)

Uma validação de controles em torno dos dados do titular do cartão para reduzir a fraude de cartão de crédito.

Saiba mais sobre todas as certificações VTEX.

PCI DSS - DESV

Compreende um conjunto de procedimentos adicionais que visam reafirmar a manutenção eficaz e contínua dos controles estabelecidos pelo PCI DSS.

Educação e conscientização sobre segurança

Consideramos que nossos funcionários são uma **linha crítica de defesa** na proteção dos dados da nossa empresa e dos nossos clientes. Por isso, desenvolvemos um programa dedicado a **conscientização e treinamento** sobre as práticas recomendadas de segurança e a adoção de recursos de segurança na VTEX.

O programa se estende a todos os funcionários e terceiros por meio de:

- Reuniões periódicas globais;
- Comunicados globais sobre temas emergentes e alertas de segurança;
- Envio de simulações de *phishings* e capacitações para entender com reconhecê-los e denunciá-los;
- Treinamento mensal sobre as melhores práticas de segurança;
- *Onboarding* de segurança para novos colaboradores;
- Realização de eventos de segurança.

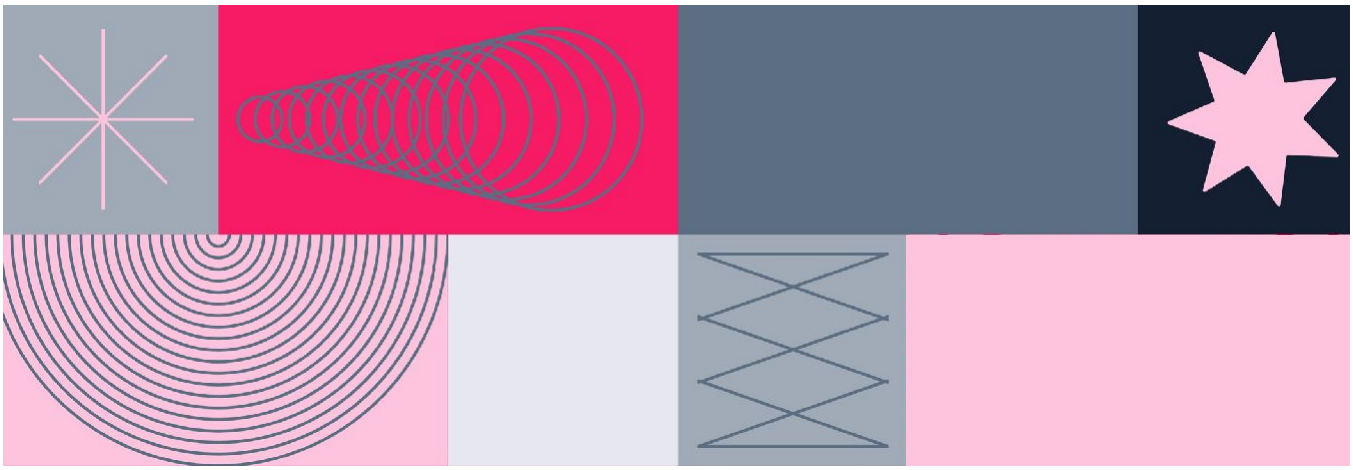
Através de indicadores de desempenho medimos a eficácia dos programas de conscientização em segurança e o conhecimento dos colaboradores sobre o tema.

Gestão de Ativos

Os ativos são gerenciados centralmente por meio de um sistema de gerenciamento de inventário que armazena e rastreia o proprietário, a localização, o status, a manutenção e as informações descritivas dos dispositivos. Após a aquisição, os ativos são verificados e rastreados, além disso, os ativos em manutenção são verificados e monitorados quanto à propriedade, status e resolução. A VTEX opera 100% na nuvem e é a maior parceira da AWS (Amazon Web Services) na América Latina. Assim, não há necessidade de inventário de ativos físicos para os recursos na nuvem da AWS. Para inventário de software, usamos o inventário do AWS Systems Manager, que fornece visibilidade através do nosso ambiente de computação da AWS.

Os dispositivos de armazenamento de mídia usados para armazenar dados do cliente são classificados como críticos e tratados adequadamente, como de alto impacto, ao longo de seus ciclos de vida.

A AWS utiliza padrões rigorosos sobre como instalar, fazer manutenção e, eventualmente, destruir os dispositivos quando eles não forem mais úteis. Quando um dispositivo de armazenamento chega ao fim de sua vida útil, ele é desativado usando técnicas detalhadas no NIST 800-88. A mídia utilizada para armazenar os dados do cliente não é removida do controle até que seja desativada com segurança.



Acesso, Identificação, e autenticação

A VTEX controla e monitora rigorosamente o acesso aos nossos ambientes de produção. Somente os funcionários cujas funções de trabalho exigem acesso, podem se qualificar com a permissão para acessar nossos sistemas. Esta diretriz está alinhada com a prática do Princípio do Privilégio Mínimo e Segregação de Funções, onde acessos são concedidos com base em necessidades legítimas. Funcionários com acessos privilegiados as tecnologias da VTEX precisam usar várias camadas de autenticação de dois fatores para acessar um ambiente segregado.

Os administradores com acesso lógico aos sistemas não têm acesso físico aos datacenters. O acesso lógico aos sistemas que fornecem o serviço é restrito à equipe de Site Reliability Engineering da VTEX.
Os repositórios com os códigos da plataforma são privados, e adicionar e remover usuários da organização faz parte dos processos de contratação e desligamento da VTEX.
Apenas os Engenheiros de Desenvolvimento da VTEX têm acesso aos repositórios de código.

Adotamos configurações seguras e política de senha robusta para o acesso aos nossos sistemas, tais como, quantidade mínima de caracteres e caracteres especiais, periodicidade para alteração das senhas, não utilização das últimas senhas, controle e inatividade de sessão, entre outros.

Quando um funcionário é desligado, a notificação de Recursos Humanos aciona um conjunto de tarefas e automações que protegem o acesso ao sistema de produção.

Nossa equipe de controle de acessos revisa o acesso lógico periodicamente e verifica se os usuários encerrados foram removidos dos respectivos sistemas por meio de um sistema de chamados.

Também revisamos as transferências e movimentações de funcionários e garantimos que os acessos à rede, servidor e banco de dados aos sistemas de produção ainda sejam apropriados para sua nova função de trabalho.

Se quiser saber mais sobre os recursos de segurança da plataforma clique aqui e conheça nosso provedor de identidade, o VTEX ID.

Segurança dos Dados

Classificação e Proteção da Informação

Para a VTEX, as informações devem ser classificadas considerando os impactos de confidencialidade, integridade e disponibilidade em alto, moderado e baixo. Essa estrutura resulta em uma das três classificações da informação: restrita, confidencial ou pública.

Cada nível de classificação possui suas próprias regras de manuseio e armazenamento, considerando a criticidade de cada dado e o possível impacto gerado por ele.

Estamos comprometidos em manter suas informações e de seus clientes seguras e protegidas. Entendemos que a classificação adequada da informação é essencial para garantir sua proteção, permitindo o controle de acesso adequado e a preservação da confidencialidade, integridade e disponibilidade dos dados.

Privacidade e proteção de dados

Para a VTEX as informações dos nossos clientes são extremamente valiosas e preservamos sua integridade e confidencialidade durante todo o seu ciclo de vida.
Por isso, a VTEX não transfere nem divulga dados do cliente e shoppers a terceiros.

Cumprimos as obrigações de governança sob uma variedade de regulamentações regionais de privacidade e proteção de dados, tais como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a Lei Geral de Proteção de Dados (LGPD) do Brasil, a Lei de Privacidade do Consumidor da Califórnia (CCPA).

A observância das leis e regulamentos de privacidade vigentes é um compromisso fundamental para a VTEX. Nos dedicamos a garantir que todas as nossas operações estejam em conformidade com os regulamentos aplicáveis. Adotamos medidas proativas para proteger todos os dados pessoais que processamos.

Essa responsabilidade se reflete em nosso constante aprimoramento de políticas e procedimentos e controles de segurança e privacidade, na busca de conformidade e transparência.

Controles Criptográficos

A VTEX entende que é imprescindível a criptografia dessas informações e dados de seus clientes.
Adotamos o TLS e seu predecessor, o SSL, como protocolos de criptografia para segurança da comunicação sobre redes de computadores. Essa tecnologia torna impossível a leitura dos dados transmitidos entre consumidor e loja, e só podem ser desencriptados dentro do seu servidor com posse da chave privada gerada pelo sistema.

As chaves de criptografia são providas pelo serviço da AWS. As chaves de acesso são armazenadas em ambiente segregado com devida proteção criptográfica. Para realizar a gestão das chaves criptográficas utilizamos o AWS Key Management que armazena e protege as chaves de criptografia para torná-las altamente disponíveis, e, ao mesmo tempo, oferecendo controle de acesso forte e flexível.

Segurança do data center e escritórios da VTEX

Nossas informações e de nossos clientes estão hospedadas na Amazon (Amazon Web Services) um provedor de serviços de infraestrutura em nuvem pública. A VTEX tem acordos com esses fornecedores que garantem a segurança física e proteção ambiental para executar nossos serviços. Antes de escolher um local, a AWS faz avaliações ambientais e geográficas iniciais. A seleção dos locais dos datacenters é feita com muito cuidado para reduzir riscos ambientais, como enchentes, condições meteorológicas extremas e atividades sísmicas. Nossas zonas de disponibilidade são criadas para ser independentes e estar fisicamente separadas umas das outras.

A AWS possui controles rigorosos quanto a gestão dos acessos aos seus datacenters. Todos os funcionários que precisam acessar o datacenter primeiro devem solicitar o acesso e fornecer uma justificativa válida. Vale ainda ressaltar que a AWS opera seus datacenters em conformidade com as diretrizes do Tier III+ (UpTime Institute).

Nos escritórios VTEX, espalhados pelo mundo inteiro, possuímos controle de segurança física, permitindo que somente pessoas autorizadas tenham acesso a nossas instalações. Para isso, o acesso físico é controlado nos pontos de entrada do edifício, pela equipe de segurança profissional que utiliza sistemas de vigilância, e pelos equipamentos tecnológicos que validam a identidade dos visitantes. Esses equipamentos registram as saídas e entradas das pessoas, e validam sua identidade.

Nossos escritórios próprios possuem Câmera de Televisão de Circuito Fechado (CFTV) e suas imagens são mantidas de acordo com os requisitos legais e de conformidade.

Também possuímos controles de energia e supressão de incêndio que estão alinhados com as medidas líderes do setor para ajudar a evitar falhas e surtos elétricos.

Segurança do Host

Os serviços da VTEX são alimentados por sistemas operacionais configurados e reforçados de acordo com as práticas de segurança recomendadas do setor.
Criamos ambientes usando a AMI mais recente fornecida pela AWS para cada serviço de implantação. Ao fazer isso, aproveitamos nossa segurança na proteção que a AWS já oferece para instâncias implantadas por seus serviços.
Complementamos essa prática de segurança com as seguintes medidas:

- Aplicação de patches de segurança críticos nos sistemas operacionais quando eles não são fornecidos como uma AMI atualizada pela AWS;
- Ativação e centralização de logs do sistema, para não perdermos informações importantes dos sistemas;
- Monitoração das alterações nos arquivos críticos de configuração para nos notificar sobre as alterações desses arquivos;
- Ativação dos firewalls locais configurados apenas com portas seguras, por exemplo HTTPS e TLS 1.2 ou superior.
- Remoção de processos, contas e protocolos desnecessários e padrão para redução da superfície de ataque do equipamento.
- Instalação do software antimalware.

Essas configurações são mantidas durante a implantação de um novo ambiente.
Caso o novo módulo de instalação precise ser adicionado em nossos servidores, a instalação do baseline será adicionado aos dispositivos de forma automática.

Gerenciamento de mudanças

O Gerenciamento de Mudanças em nossa organização segue um processo documentado, conforme exigido. A finalidade de possuirmos um processo padronizado é definir como as mudanças feitas nos sistemas de informação são controladas. Nós gerenciamos as mudanças para que elas não funcionem como improvisos.

Por mais urgente que seja, mesmo que a necessidade apareça na última hora, executar o processo de Gestão de Mudança nos permite avaliar a mudança e suas consequências, que nem sempre são tão claras, e podem esconder sérios prejuízos.

Ao fazer essa análise, a VTEX aumenta as chances de escolher a melhor ideia e não a primeira e, além disso, de não ser surpreendida negativamente posteriormente.

O processo de gestão de Mudanças da VTEX além de incluir um estudo das alternativas para realizar a mudança e suas consequências, exige que toda mudança seja autorizada por alguém que se responsabilize por ela.

Para comprovar que esse procedimento está sendo seguido, a VTEX armazena as conclusões sobre cada avaliação e documenta quem é o responsável conceder tais autorizações.

Registro e Monitoramento de Segurança

O sistema de monitoramento de segurança da informação consiste em uma série de recursos, softwares ligados à Tecnologia da Informação, empregados para prevenir que dados importantes do negócio ou dos seus clientes sejam acessados e explorados por terceiros. Por isso, na VTEX monitoramos continuamente os nossos recursos em nosso ambiente numa escala ininterrupta (24/7).

Os nossos serviços críticos são monitorados visando identificar possíveis anomalias e ameaças cibernéticas. Os logs dos eventos da infraestrutura interna e dos provedores de infraestrutura da VTEX são coletados e centralizados pelo nosso sistema de detecção e resposta, através das regras pré definidas. Utilizando lógica de detecção correlacionada, são gerados alertas, acionando a nossa equipe de resposta a incidentes. A equipe então investiga as causas desses alertas, utilizando processos e procedimentos padronizados.

Além disso, avaliamos periodicamente a eficácia dos nossos processos de identificação e resolução das ameaças e riscos, desencadeando a melhoria dos nossos processos, tornando-os cada vez mais eficazes.

Inteligência de ameaças e Resposta a Incidentes

Nossa abordagem proativa para segurança cibernética se baseia em duas principais linhas de defesa: inteligência de ameaças e resposta a incidentes. A inteligência de ameaças é um pilar fundamental na identificação, análise e compreensão das ameaças que rondam o universo digital. Buscamos estar sempre à frente dos criminosos cibernéticos, monitorando ativamente o cenário de ameaças, analisando dados, padrões de ataque e comportamentos maliciosos para antecipar ações hostis.

Contamos com uma equipe especializada de analistas de segurança que coletam, agregam e interpretam informações de diversas fontes, nos permitindo identificar ameaças emergentes e até mesmo as mais sofisticadas, e que possibilitando que tomemos medidas preventivas antes que elas possam causar danos significativos.

Nossa abordagem de resposta a incidentes é guiada por um plano estruturado baseado nas as quatro principais etapas do processo:

Preparação

Antes de qualquer plano de resposta, devem-se concentrar esforços na prevenção de incidentes. Para isso é requerida uma avaliação de riscos dos ambientes, aplicação de *baselines* de segurança, atualização de patches, garantia de mínimo acesso, garantias de segurança de perímetro, prevenção contra malwares e campanhas de educação em segurança.

Identificação do Incidente

O comportamento anômalo é confirmado como incidente caso impacte diretamente a Disponibilidade, Integridade e Confidencialidade das informações, sistemas e serviços, ou quando for proveniente de um Acesso Indevido ou Ataque Explícito.

Contenção, Erradicação e Recuperação

Antes de iniciar qualquer ação de tratamento é indispensável coletar, preservar, proteger e documentar evidências. Nenhuma evidência pode ser excluída. Nenhum ativo envolvido no incidente pode ser alterado ou excluído sem a devida aprovação.
Caso as evidências contenham informações confidenciais, as mesmas devem ser criptografadas. Após um incidente ser contido, deve-se avaliar se outros ambientes estão expostos ou já sofreram o mesmo tipo de ataque para resolver o problema em sua causa raiz. A equipe responsável deverá restaurar salvaguardas não comprometidas.

Atividades pós incidente

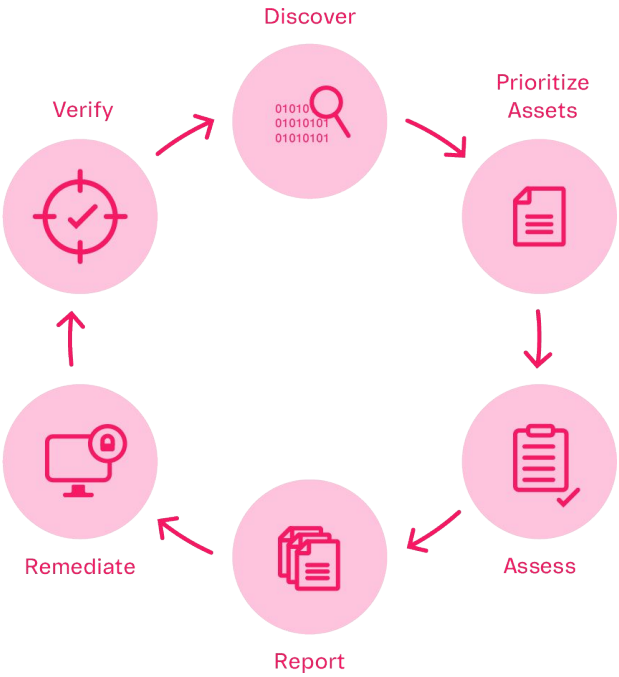
Etapa do processo onde serão colhidos os aprendizados e melhorias para os controles de segurança a serem aplicados na etapa de Preparação e gerenciamento de futuros incidentes. O objetivo é analisar o que ocorreu, o que foi feito para intervir e se a intervenção funcionou adequadamente.

Gestão de Vulnerabilidades

A VTEX, avalia rigorosamente os recursos testando e identificando as vulnerabilidades realizando scans e testes de penetração em nossos ambientes.

Possuímos um cronograma para as verificações de vulnerabilidade, onde as verificações ocorrem periodicamente, de acordo com a criticidade de cada escopo.

As vulnerabilidades identificadas são tratadas e endereçadas de acordo com nosso processo de gestão de vulnerabilidades e são devidamente gerenciadas durante todo o seu ciclo de vida.



Em uma solução multi-tenant como a VTEX, isso significa que toda a plataforma está constantemente sendo testada durante todo o ano.

Os clientes que desejam realizar a sua própria avaliação de vulnerabilidade, devem seguir o processo pré estabelecido, disponível no Help Center.
E caso uma vulnerabilidade reportada seja confirmada pelo time de segurança da VTEX, ela é endereçada internamente para correção observando sempre o seu nível de criticidade e risco para a plataforma.

Segurança do Perímetro

A VTEX usa uma abordagem de várias camadas para proteção dos recursos, adotando processos como segregação de rede, firewalls e roteadores de borda como mecanismo para a proteção do perímetro e rede.

Possuímos uma solução de **IDS (Intrusion Detection System)** e **IPS (Intrusion Prevention System)** como proteção da camada de rede e monitoramos continuamente o tráfego de rede em busca de anomalias.

Essa solução atua na mitigação de ataques DDoS, redirecionando o tráfego, para garantir que ele esteja limpo e os clientes possam continuar suas operações normalmente.

As informações do cliente estão contidas em uma conta de loja e são isoladas de diferentes contas pelo processo da VTEX e pela implementação de armazenamento.
Não existe nenhum método integrado de acesso a dados que ultrapasse as fronteiras de diferentes contas, mesmo para uso interno da VTEX. As únicas formas de acesso aos dados requerem a indicação explícita de uma conta específica.

Ciclo de Desenvolvimento Seguro

Na VTEX integramos os requisitos de segurança em todas as etapas do ciclo de desenvolvimento da plataforma, usando o processo Secure Software Development Lifecycle (SSDLC).

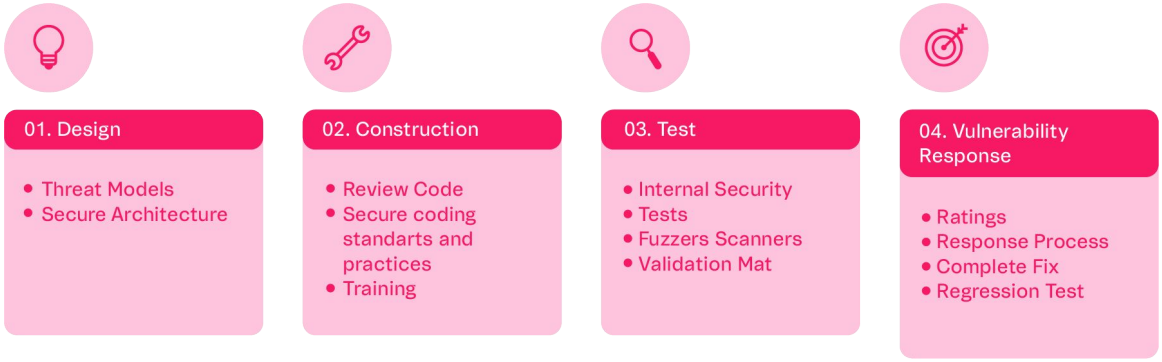
Através dessa metodologia, nossos engenheiros de desenvolvimento atuam com processos ágeis, considerando as questões e preocupações de segurança dos nossos produtos.

Inovamos considerando as constantes demandas do mercado. Um exemplo disso é o VTEX IO, uma uma plataforma nativa capaz de ajudar a entrega de soluções de negócio com mais agilidade e segurança.

Nos preocupamos em seguir as melhores diretrizes do mercado quando o assunto é Desenvolvimento Seguro, por isso os engenheiros da VTEX desenvolvem seguindo os métodos OWASP Top 10, a fim de prevenir qualquer código malicioso.

Além disso, a VTEX possui um sistema de escaneamento de código no repositório que age captando possíveis vulnerabilidades e erros dentro dos ciclos de desenvolvimento de Software.

Saiba mais sobre VTEX IO no diagrama abaixo:



Gestão e Avaliação de Terceiros

A VTEX garante que seus provedores subcontratados respeitem e sigam os mesmos requisitos de segurança oferecidas pela VTEX.

A VTEX possui um processo estabelecido de análise de risco de segurança para avaliar fornecedores que irão tratar dados pessoais, dados sensíveis ou que irão interagir com a infraestrutura ou tecnologias da VTEX.

Avaliamos a maturidade e postura de segurança desses fornecedores com o objetivo de entender de garantir que as empresas mantenham um nível adequado de proteção e cuidado em relação aos dados e informações compartilhamos com elas.

Somente após todas as avaliações necessárias e mediante a apresentação de um nível de maturidade adequado seguimos com a contratação.

Todos os nossos provedores terceiros de infraestrutura podem ser encontrados neste link.

Gerenciamento de Riscos de Segurança

Nosso programa de gerenciamento de riscos traz visibilidade das potenciais ameaças de segurança e nos ajudam a tomar decisões visando os objetivos corporativos.

Para o mapeamento de riscos, medimos a probabilidade de concretização do risco e impacto que terá na operação da VTEX.

A identificação de riscos desencadeia o aprimoramento de nossos sistemas de monitoramento e notificação para lidar com sua eventual materialização, seja notificando as pessoas aptas a tratá-los ou por meio de ações automatizadas que possam mitigá-los ou eliminá-los.

O processo de gerenciamento aborda todo o ciclo de vida do risco, garantindo que os riscos identificados sejam tratados, mitigados e comunicados, de acordo com sua relevância.

Etapas do Processo de Gerenciamento de Riscos

Continuidade de Negócios

Temos um compromisso definitivo com nossos clientes de comprovar que somos uma plataforma segura e confiável. Por isso, temos implementado um **Plano de Continuidade de Negócios**, elaborado para preparar a companhia para lidar com os efeitos de uma emergência. Acreditamos que seguir as etapas definidas no plano nos fornece a base para um retorno relativamente rápido e indolor à rotina comum de funcionamento dos nossos negócios em caso de eventual interrupção.

Nosso **Plano de Recuperação de Desastres** é focado em garantir a continuidade das operações e a disponibilidade de recursos críticos em caso de um desastre. Nele há instruções sobre quais ações tomar e como responder a incidentes não planejados e caracterizados como uma crise, que podem estar relacionados a desastres naturais, ataques cibernéticos e quaisquer outros eventos disruptivos.

Este plano é periodicamente testado, pelos mais diversos times da VTEX, objetivando assegurar sua eficácia e validade.

Maturidade de Segurança

Para melhorar continuamente nossa postura de segurança nos amparamos na norma ISO:IEC 27001, que mede a maturidade de nossos programas de segurança. A ISO:IEC 27001 é um padrão internacional reconhecido mundialmente como eficaz na gestão da Segurança da Informação.

A adoção da norma ISO:IEC 27001 tem como objetivo garantir que a organização adote um Sistema de Gestão de Segurança da Informação (SGSI) adequado e que possa ser aprimorado e monitorado.

Este SGSI é, de acordo com os princípios da norma ISO:IEC 27001, um modelo holístico de abordagem à segurança independente de marcas e fabricantes tecnológicos.

Periodicamente realizamos um *Self-Assessment*, baseado nos controles da ISO:IEC 27001, e a partir dos gaps identificados construímos um roadmap de implementação e adequação.

Também definimos uma métrica para medir o atual nível de maturidade de segurança, que nos permite quantificar e acompanhar a maturidade geral de nossa postura de segurança.

Conclusão

A VTEX está comprometida em proporcionar segurança e confiança a todos os nossos clientes. Colocamos a segurança como um dos pilares fundamentais das nossas operações, visando proteger dados e informações de todos que utilizam nossos produtos e serviços.

Além disso, a confiança depositada em em nós é um privilégio que valorizamos imensamente. Buscamos conquistar a confiança de nossos clientes diariamente, entregando produtos e serviços de alta qualidade, seguros, que atendam às expectativas e que ajudam nossos clientes a inovar, impulsionando o crescimento mútuo.

Ao escolher a VTEX, você está escolhendo um parceiro confiável e dedicado à segurança dos seus interesses. Sua tranquilidade e satisfação são a nossa recompensa, e continuaremos a trabalhar incansavelmente para manter essa relação de confiança. Estamos aqui para você, protegendo o que é mais importante.

As empresas nos escolhem como parceiro estratégico para acelerar a transformação do comércio digital e entregar iniciativas de geração de receita.

Mesmo depois de 20 anos e todo o impacto que entregamos ao ecossistema de comércio eletrônico, ainda mantemos nossa mentalidade do primeiro dia que nos trouxe até aqui. Estamos em uma jornada interminável de conectar o mundo pela maneira como as pessoas fazem comércio. Convidamos você a entrar em nosso futuro e fazer parte dessa jornada!

#WeAreTrusted

Recursos

Security Help Center

Canal público que funciona como uma central de ajuda para clientes e potenciais clientes VTEX. Nele há um grande banco de respostas para questionamentos variados sobre segurança.

VTEX Trusthub

Site público destinado a tratar de questões legais, de conformidade, privacidade e segurança.

Security FAQ

Esse espaço é o único privado, no qual apenas clientes VTEX possuem acesso através do seu login e senha. Nele, disponibilizamos nosso FAQ de segurança para apoiar na resolução de dúvidas e no preenchimento de *Risk Assessments*.

VTEX Healthcheck

Uma página pública que tem por objetivo monitorar o status dos serviços de nossa plataforma. No Healthcheck, temos mais de 100 testes rodando por minuto. Por esse dashboard, pode acompanhar a saúde de cada módulo em tempo real.

Status VTEX

No Status VTEX , você pode acompanhar a estabilidade da plataforma em tempo real, assim como acessar todo o histórico de incidentes. Os eventos são reportados pela nossa equipe sempre que nosso sistema automático de monitoramento identifica uma instabilidade nos módulos da plataforma.

See more at: vtex.com

The Enterprise
Digital Commerce
Platform