VTEX

The Enterprise
Digital Commerce
Platform

Postura de Segurança da VTEX

VTEX Security

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 para garantir que fornecemos a todos que fazem ou farão parte da nossa comunidade tranquilidade, bem-estar, segurança e confiança quando o assunto é Segurança & Privacidade. Entendemos a importância de adotar práticas de segurança líderes do setor e tecnologias necessárias para proteger os dados dos clientes. Nossas práticas de segurança estão incorporadas em todas as nossas tecnologias, pessoas e processos. Nossos clientes confiam em nós para fornecer altos níveis de integridade, confidencialidade e disponibilidade de dados. Por mais de duas décadas, trabalhamos com clientes em setores altamente regulamentados, como governos, serviços financeiros, saúde e serviços públicos — cada cliente disposto 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, usamos o ISO 27001:2013 para medir a maturidade de nossos programas de segurança. Essa norma é o padrão e a referência Internacional para a gestão da Segurança da informação. Nós usamos essa norma para avaliar e identificar áreas de melhoria.

Nossos Valores

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. Somos confiáveis, seguros e escaláveis!

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 abraçando desafios desconfortáveis.

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 e servirá como ponto de partida para demonstrar o nosso compromisso com a nossa segurança e dos nossos clientes.

Saiba mais detalhes sobre os nossos processos de segurança clicando aqui.

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 foi transmitida para toda a companhia através dos nossos canais internos de comunicação. A política é revisada anualmente dentro do nosso processo de gestão de documentos. A nossa política de Segurança da Informação é orientada à norma ISO IEC 27001, frameworks com as melhores práticas de segurança, leis de proteção de dados e outras obrigações aplicáveis ao contexto da VTEX. Nossos clientes podem ter acesso a nossa versão pública através do Portal de Administração da Loja. Todos os nossos documentos são revisados dentro de uma janela anual e garantimos a gestão através de uma plataforma de gerenciamento de políticas.

A VTEX possui uma equipe robusta e especializada em Segurança da Informação, nossa equipe é estruturada e dedicada para suportar os principais processos de segurança. Nossa equipe de segurança trabalha em esquema de prontidão, com equipes em diferentes time zones para garantir que tenhamos uma cobertura que vai 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 gerenciar e manter os controles de segurança, periodicamente esses controles são auditados por empresas externas. Atualmente possuímos as seguintes certificações.

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.

Educação e conscientização sobre segurança

Consideramos nossos funcionários uma linha crítica de defesa na proteção dos dados da nossa empresa e dos nossos clientes. Temos uma equipe dedicada que impulsiona a conscientização, o envolvimento e a educação de nossos funcionários sobre as práticas recomendadas de segurança e a adoção de recursos de segurança na VTEX. Nossos programas abrangentes incluem integração de novos funcionários e treinamento anual de segurança.
Treinamos funcionários para identificar vetores de ataque usados com frequência, como e-mails de phishing, e como denunciá-los. Isso se aplica a todos os funcionários e terceiros, através de indicadores de desempenho medimos a eficácia dos programas de conscientização em segurança.

Anualmente estabelecemos um cronograma para o nosso programa de educação e revisamos sempre os nossos conteúdos, considerando os cenários

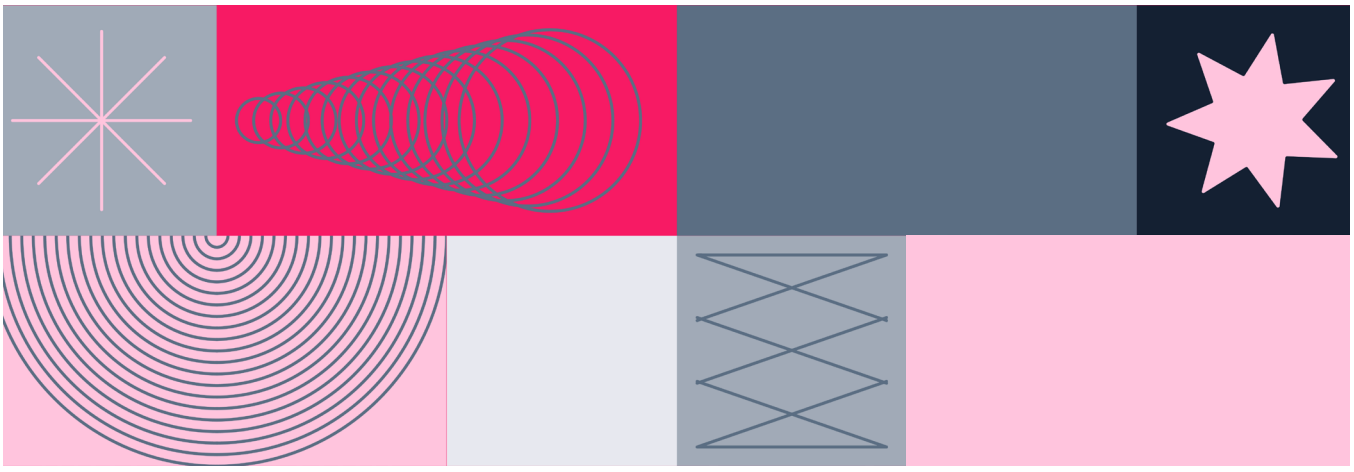
Disponibilizamos um canal de ética para a notificação de comportamento inadequado. Além disso, possuímos um processo de sanções que será aplicado para os funcionários que não cumprem as políticas e padrões de segurança da informação estabelecidos.

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 ativos. 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. Vale ainda ressaltar que 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 em 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 nossa prática do Princípio do Mínimo Privilégio e Segregação de Funções, onde o acesso é concedido com base em necessidade legítima. Funcionários privilegiados da VTEX, como engenheiros de confiabilidade da plataforma, precisam usar várias camadas de autenticação de dois fatores para acessar um ambiente segregado e gerenciar sistemas usando apenas aplicativos hospedados por meio de um cliente de desktop remoto seguro, infraestrutura de desktop virtual (VDI).
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, adicionar e remover usuários da organização faz parte dos processos de contratação e demissão. 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, e muitos mais.

Quando um funcionário é demitido, a notificação de Recursos Humanos aciona um conjunto de tarefas que protegem o acesso ao sistema de produção. Após o encerramento, as contas privilegiadas são bloqueadas, as conexões ativas são encerradas e os tokens de autenticação de dois fatores são removidos. Nossa equipe de controle de acessos revisam o acesso lógico periodicamente e verificam se os usuários encerrados foram removidos dos respectivos sistemas por meio de um sistema de tíquete interno.

Também revisamos as transferências 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. E se ainda 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 dos Dados

Para nós da VTEX os dados devem ser classificados considerando os impactos de confidencialidade, integridade e disponibilidade em alto, moderado e baixo. Essa estrutura resultará em uma das três classificações, respectivamente: restrita, confidencial ou pública. Por exemplo, os seguintes tipos de dados são considerados como confidenciais e críticos dentro da nossa escala de classificação da informação:

- Informações do cartão de pagamento (PCI-DSS)
- Informações de Identificação Pessoal (PII)

Lembre-se, estamos comprometidos em manter seus dados seguros e protegidos. Nossas informações críticas devem sempre ser criptografadas não apenas em trânsito, mas também em repouso. Portanto, todos os dados confidenciais são criptografados.

Retenção dos Dados

A VTEX não exclui ativamente nenhum dado de propriedade dos nossos clientes sem que haja a expressa manifestação de vontade deles. Isso também inclui os casos de rescisão do contrato do cliente junto a VTEX, em que há o pedido para excluirmos os dados do cliente, incluindo dados de identificação pessoal.

Transferência Segura dos Dados

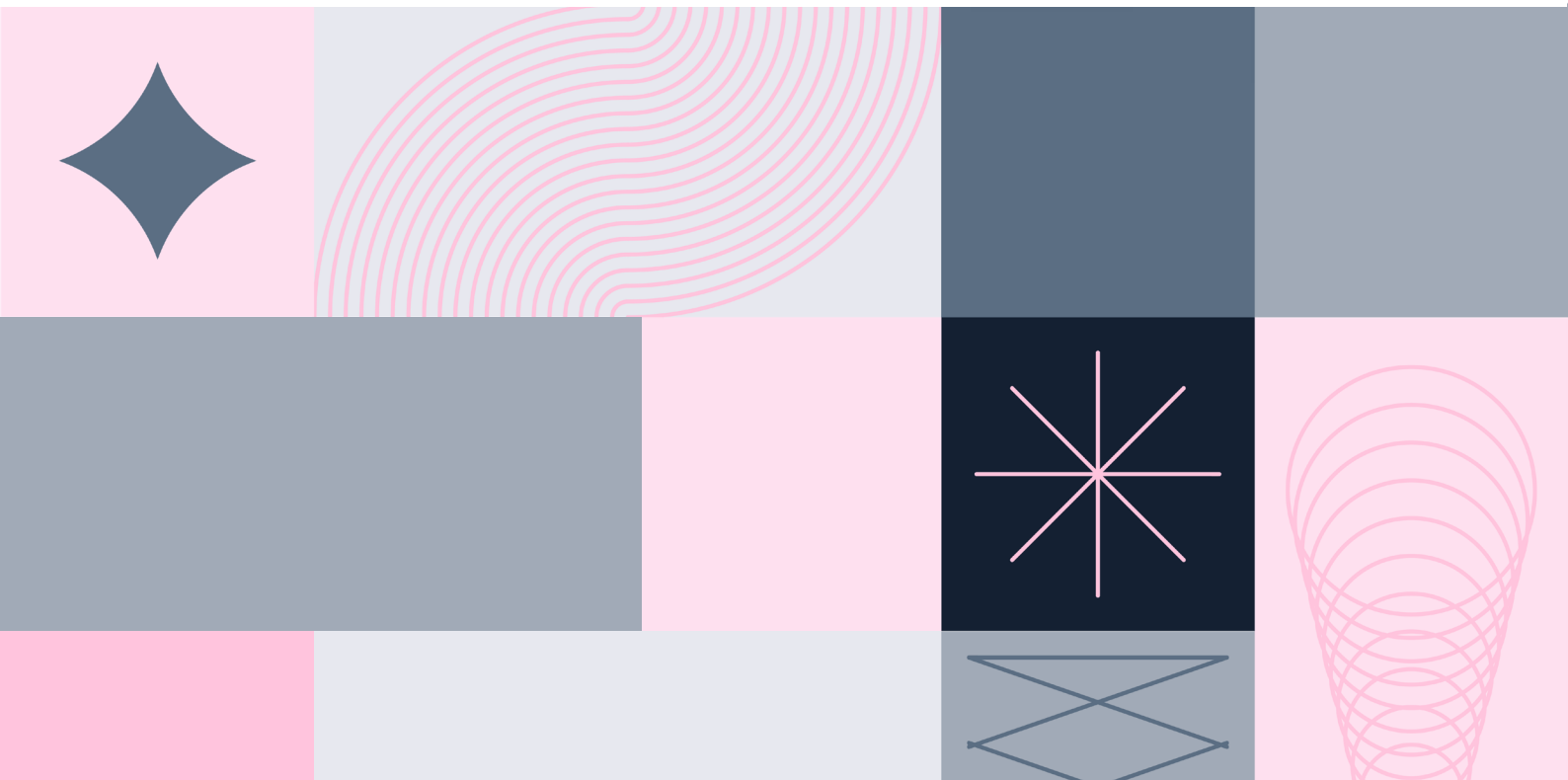
Como já dito anteriormente para a VTEX os dados dos nossos clientes são extremamente valiosos e preservamos sua integridade e confidencialidade durante todo o seu ciclo de vida. Sendo assim, a VTEX não transfere nem divulga dados do cliente, exceto para fornecer os serviços e prevenir ou resolver problemas técnicos ou de serviço, a pedido do cliente em relação a questões de suporte ou conforme exigido por lei. Cumprimos as obrigações de governança sob uma variedade de regulamentações regionais de privacidade e proteção de dados 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 VTEX está totalmente comprometida em cumprir os Regulamentos de Proteção de Dados; é por isso que estamos constantemente atualizando nossos procedimentos de segurança e privacidade de dados pessoais em conformidade com todas as leis de proteção de dados aplicáveis nos países onde prestamos serviços.

Controles Criptográficos

A VTEX lida com dados críticos dos clientes, sendo assim, é imprescindível a criptografia dessas informações TLS e seu predecessor, o SSL, são protocolos de criptografia para segurança da comunicação sobre redes de computadores. Eles são o S do HTTPS. Essa tecnologia não evita que criminosos interceptem a conexão entre consumidor e loja, mas torna impossível a leitura desses dados, que só podem ser desembaralhados dentro do seu servidor com posse da chave privada gerada pelo sistema. A VTEX possui padrões de criptografia definidos para todos os seus clientes tanto para dados em repouso quanto para dados em trânsito.

Chaves de criptografia são providas pelo serviço da AWS. Chaves de acesso são armazenadas em ambiente segregado com devida proteção criptográfica. Para realizar a gestão das chaves criptográficas utilizamos a AWS Key Management que armazena e protege as chaves de criptografia para torná-las altamente disponíveis e, ao mesmo tempo, oferece controle de acesso forte e flexível. AWS KMS keys (chaves do KMS) são o recurso principal no AWS KMS. É possível usar uma chave do KMS para criptografar, descriptografar e recriptografar dados. Ela também pode gerar chaves de dados que você pode usar fora do AWS KMS.



Segurança do data center e escritórios da VTEX.

Os nossos dados e dos nossos clientes estão hospedados na Amazon (Amazon Web Services) um provedor de serviços de infraestrutura em nuvem pública, A VTEX tem acordos com esses fornecedores para garantir uma linha de base de 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 permite que apenas funcionários aprovados tenham acesso físico ao datacenter. 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).

A VTEX possui escritórios espalhados pelo mundo inteiro, possuímos controle de segurança física, tais como monitoramento e controle de acessos em todos os escritórios da VTEX. O acesso físico é controlado nos pontos de entrada do edifício pela equipe de segurança profissional que utiliza sistemas de vigilância, como catracas e outros meios eletrônicos. Esses equipamentos registram as saídas e entradas das pessoas autorizadas através dos registros.

Os escritórios possuem Câmera de Televisão de Circuito Fechado (CFTV). As 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 importante 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 deste domínio é definir como as mudanças feitas nos sistemas de informação são controladas. O que o domínio quer é que a organização gerencie essas mudanças, para que elas não funcionem como improvisos. Por mais urgente que seja, mesmo que a necessidade apareça na última hora, a Gestão de Mudança quer que a organização avalie a mudança e suas consequências. Nem sempre essas consequências são tão claras, e podem esconder sérios prejuízos. Ao fazer essa análise a organização aumenta as chances de escolher a melhor ideia e não a primeira e, além disso, de não ser surpreendida negativamente depois.

Por isso, a VTEX estabeleceu um procedimento para controlar mudanças. Esse procedimento inclui um estudo das alternativas para realizar a mudança e suas consequências. Além disso, toda mudança deve ser autorizada por alguém que se responsabilize por ela. Para comprovar que esse procedimento está sendo seguido, a VTEX arquiva as conclusões sobre cada avaliação e quem é o responsável por autorizar a mudança.

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 de um negócio ou dos seus clientes sejam acessados e explorados por terceiros. Por isso na VTEX monitoramos continuamente os nossos recursos em nosso ambiente em uma escala 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 e utilizando lógica de detecção correlacionada são gerados alertas, quando isso ocorre a nossa equipe de resposta a incidentes investiga as causas desses alertas usando processos e procedimentos padrão.

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

Inteligência de ameaças e Resposta a Incidentes

A nossa prioridade é proteger os dados dos nossos clientes e para isso, temos procedimentos complexos que garantem o devido monitoramento dos nossos recursos, com o principal objetivo de identificar potenciais ameaças e para atuar na resposta dessas ameaças de forma rápida e eficaz. Nossa equipe de detecção e resposta é dedicada a desenvolver inteligência contra as ameaças por meio de pesquisas e análises relacionadas a incidentes de segurança. Nosso plano de resposta a incidente foi estruturado de acordo com as quatro principais etapas do processo de resposta:

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 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 na causa raiz. A equipe responsável deverá restaurar salvaguardas não comprometidas.

Atividades pós incidente

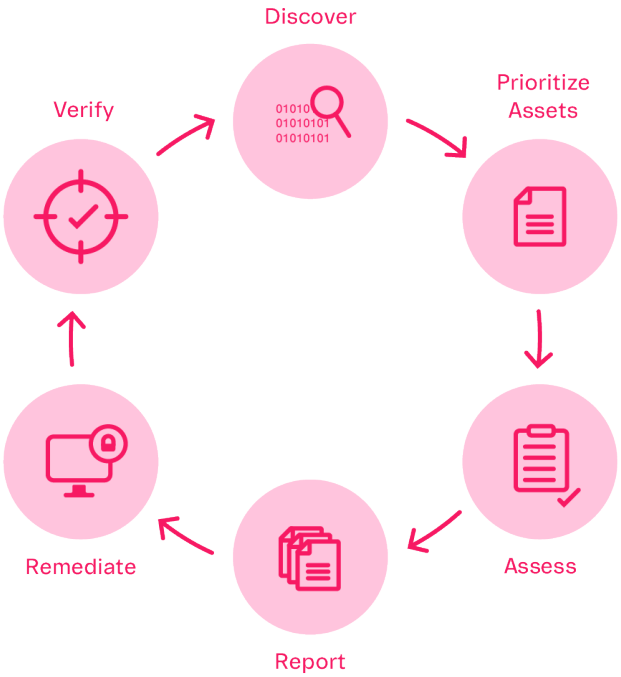
Etapa importante do processo onde serão colhidos os aprendizados e melhorias para os controles de segurança a serem aplicados na etapa de Preparação e gerenciamento de futuros incidentes. O objetivo é analisar o que ocorreu, o que foi feito para intervir e se a intervenção funcionou adequadamente.

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, essas verificações ocorrem periodicamente e de acordo com a criticidade do escopo.

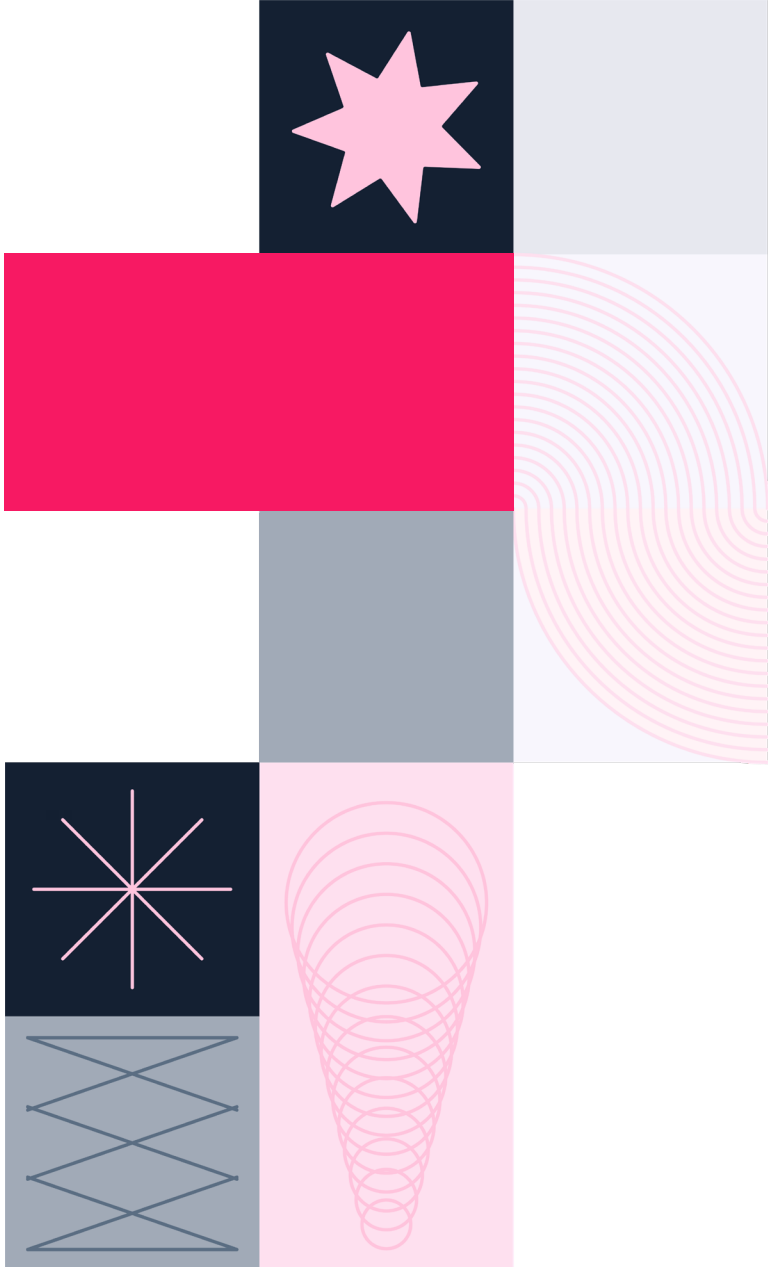
As vulnerabilidades identificadas são tratadas e endereçadas no nosso processo de gestão de vulnerabilidades e serão devidamente gerenciadas durante todo o seu ciclo de vida.



Além disso, os nossos clientes possuem liberdade para realizar testes nas suas lojas de maneira aberta e transparente.
Em uma solução multi-tenant como a VTEX, isso significa que toda a plataforma está constantemente sendo testada durante todo o ano.

Nossos clientes devem reportar qualquer vulnerabilidade que identifiquem na plataforma da VTEX. Possuímos um processo para receber e avaliar os relatórios dos clientes, e caso seja confirmada pelo time de segurança da VTEX, a mesma 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, tanto em nossa rede interna quanto na Internet. Essa solução atua na mitigação de ataques DDoS, e quando ocorre a identificação de um evento associado a um ataque DDoS, o tráfego será redirecionado 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.

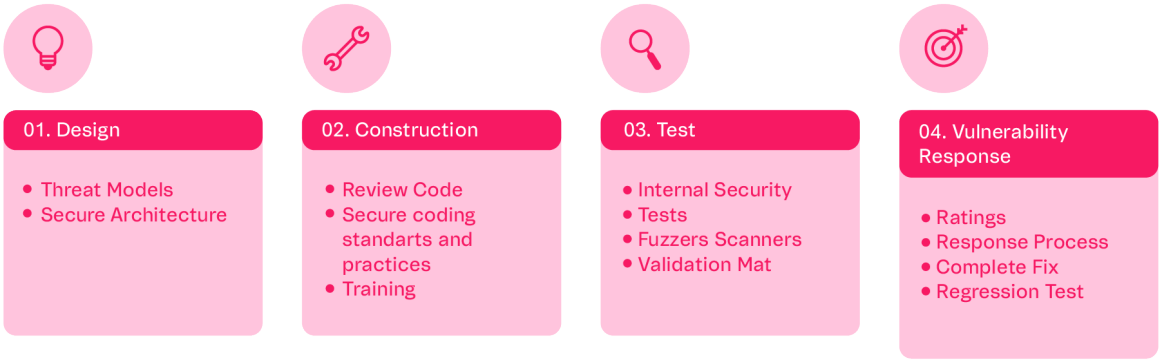
Ciclo de Desenvolvimento Seguro

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 a constante 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. Saiba mais sobre VTEX IO.

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.



Gestão e Avaliação de Terceiros

A VTEX garante que seus provedores subcontratados respeitem e seguem as mesmas políticas de segurança oferecidas pela VTEX. Todos os nossos provedores terceiros de infraestrutura podem ser encontrados neste link.

A VTEX possui um processo estabelecido de análise de risco de segurança para fornecedores críticos, ou seja, aqueles que irão manusear dados sensíveis.

Avaliamos a maturidade e postura de segurança desses fornecedores com o objetivo de entender quais são os riscos e lacunas e direcionar essas questões para as devidas tomadas de decisões internas. Além disso, todos os fornecedores passam pelo fluxo de avaliação de risco para a aderência às leis de proteção de dados e análise de risco do negócio, somente após todas as avaliações necessárias e com um nível de maturidade adequado seguimos com a contratação.

Gerenciamento de Riscos de Segurança

Nosso programa de gerenciamento de risco traz visibilidade das potenciais ameaças de segurança e nos ajudam a tomar decisões visando os objetivos corporativos. Consideramos processos de mapeamento de risco para a avaliação da probabilidade e impacto das ameaças que podem afetar nossa capacidade estratégica.

Além disso, 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, seja acionando ações automatizadas que possam mitigá-los ou eliminá-los.

Utilizamos um processo de gerenciamento que aborda todo o ciclo de vida do risco, garantindo que os riscos identificados sejam tratados, mitigados e comunicados, de acordo com a relevância , nosso processo abrange cinco principais etapas.

Continuidade de Negócios

Temos um compromisso definitivo com nossos clientes a fim de provarmos que somos uma plataforma segura e confiável. Por isso temos implementado um plano de continuidade de negócios que foi elaborado para preparar a companhia para lidar com os efeitos de uma emergência. Pretende-se que seguir as etapas definidas no plano forneça a base para um retorno relativamente rápido e indolor à rotina comum de funcionamento dos nossos negócios, independentemente da causa.

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, contendo instruções sobre quais ações e como responder a incidentes não planejados e caracterizado como uma crise, esses incidentes podem estar relacionados a desastres naturais, ataques cibernéticos e quaisquer outros eventos disruptivos.

Maturidade de Segurança

Para melhorar continuamente nossa postura de segurança, usamos com base a norma ISO/IEC 27001 para medir a maturidade de nossos programas de segurança, essa norma é o padrão e a referência Internacional para a gestão da Segurança da informação. Nós usamos essa norma para avaliar e identificar áreas de melhoria. A estrutura da norma é baseada em domínios e foi desenvolvida em 1992 por um departamento do governo Britânico que estabelecia um código de práticas relativas à gestão da Segurança da Informação.

Ao longo dos anos, milhares de profissionais contribuíram com o seu know-how e experiência para o estabelecimento de um Standard estável e maduro, mas que certamente continuará a evoluir ao longo dos tempos.

A adoção da norma SI/IEC 27001 serve para que as organizações adotem por um modelo adequado de estabelecimento, implementação, operação, monitorização, revisão e gestão de um Sistema de Gestão de Segurança da Informação.

Este Sistema de Gestão de Segurança da Informação (SGSI) é, de acordo com os princípios da norma ISO 27001, um modelo holístico de abordagem à Segurança e independente de marcas e fabricantes tecnológicos.

Periodicamente realizamos Self Assessment usando como direcionamento os controles da ISO 27001 e a partir dos gaps identificados construímos um roadmap de implementação e adequação. Também foi possível definir uma pontuação ao nosso estado atual de maturidade. Ao avaliar as pontuações atuais e desejadas da ISO 27001, podemos quantificar e acompanhar a maturidade geral de nossa postura de segurança ao longo do tempo.

Conclusão

Na VTEX, nosso maior compromisso é a Segurança dos nossos clientes. Somos líderes na aceleração da transformação do comércio digital na América Latina e estamos expandindo globalmente. Nossa plataforma é projetada para padrões e funcionalidades de nível empresarial, com aproximadamente 80% de nosso GMV vindo de grandes empresas de primeira linha (ou seja, clientes com mais de US$ 10 milhões de GMV por ano). Temos a confiança de mais de 2.000 clientes com mais de 2.500 lojas online ativas em 32 países para se conectar com seus consumidores de maneira significativa. Somos confiáveis, escaláveis e seguros. Entendemos que nossos clientes dependem da segurança, desempenho e transparência de nossos sistemas e serviços da VTEX.

Oferecemos serviços ricos em segurança que ajudam nossos clientes a inovar para atender às demandas do mercado, o que, por sua vez, impulsiona o crescimento mútuo. Para apoiar o sucesso de nossos clientes, também compartilhamos e incentivamos as melhores práticas de segurança com eles usando uma variedade de canais, incluindo nosso site, blogs, mídias sociais, ferramentas e funcionalidades.

As empresas nos escolhem como um parceiro estratégico para acelerar a transformação do comércio digital e entregar iniciativas de geração de receita. Entregamos nossa plataforma por meio de um modelo de receita de assinatura que inclui componentes variáveis fixos e baseados em GMV.

O que representa todo esse sucesso? 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!

Então lembre-se, #WeAreTrusted

Recursos

Security Help Center
Esse site é um canal público que funciona como uma central de ajuda para clientes e potenciais clientes VTEX. Ele traz soluções sobre questionamentos variados e possui um banco de informações bem grande.

VTEX Trusthub
O VTEX TrustHub é nosso site público para tratar de preocupações envolvendo 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. É um portal reservado onde disponibilizamos nosso FAQ de segurança para apoiar a resolução de dúvidas e o preenchimento de Risk Assessment.

VTEX Healthcheck
O HealthCheck da VTEX é 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