VTEX

The Enterprise
Digital Commerce
Platform

VTEX Security Posture

VTEX Security

Introduction

With the exponential increase in remote work and ecommerce, companies have been urged to develop a safe and secure online environment. Although security has become a hot topic in the market, less than one third of Brazilian companies have teams dedicated to cybersecurity.

Here at VTEX, we are committed to changing this scenario. We have developed a team fully dedicated to Information Security, to guarantee peace of mind, security and trust to everyone who is or will be part of our community.

We understand the importance of adopting industry-leading security practices and technologies to protect customer data and these practices are embedded in all our technologies, people, and processes.

Our customers trust us to provide high levels of data integrity, confidentiality, and availability. For more than two decades, we have worked with customers in highly regulated industries, who are willing to entrust their data to VTEX.

VTEX’s Commitment

At VTEX, we are committed to following the most effective security practices and measures, ensuring that access is controlled and data is safe and secure.

Our Guidelines

To continuously improve our security posture, we use the ISO 27001:2022 standard to measure the maturity of our security programs and also to evaluate and identify improvement opportunities.

This standard is the international reference for information security management.

We are committed to your peace of mind

We are the Enterprise Digital Commerce Platform

We make bold decisions, putting ourselves at risk for our clients' success. We are a high-performance team, always learning by embracing uncomfortable challenges.

We are the backbone of connected commerce

At VTEX, we understand the importance of adopting the necessary security and technology practices to protect customer data. Our security measures are embedded throughout our technology, processes, and people.

VTEX is more than a commerce platform

We bring harmony between business and technology. We know that privacy and security are key to success in any business.

In this document, we will provide an overview of our security posture to demonstrate our commitment to our clients' security and our own.

How We Safeguard Our Clients and Systems

Information Security Program

At VTEX, we have an information security program in place, managed by a leadership committed to raising the level of security maturity for the entire VTEX ecosystem.

We have an **Information Security Policy** that has been transmitted to the entire company, reviewed annually, in accordance with our document management process.

Our Information Security Policy is targeted toward the ISO/IEC 27001:2022 standard, frameworks for security best practices; data protection laws; and other obligations applicable to the VTEX context.

All our documents are reviewed annually and and we ensure their management through a policy management platform.

VTEX has a strong and expert Information Security team that is structured and dedicated to supporting key security processes. Our security team works on an on-call basis, with teams in different time zones to ensure we can provide security beyond business hours.

Audit and Compliance

Internal Compliance Audits

Our internal audit team conducts internal compliance audits to prepare for external certification audits.

Our audit team is constantly improving this process and automating control checks to have an active compliance dashboard.

External Compliance Audits

Certification audits are performed by independent companies and monitored by our Internal Audit team. Their results are used to improve internal compliance monitoring processes.

VTEX's Certifications

VTEX has a compliance program to manage and maintain security controls.

Service Organization Controls (SOC 1)

Audit encompassing internal control over financial reporting systems.

Service Organization Controls (SOC 2 e 3)

Audit covering the Security, Availability, Integrity, Confidentiality, and Privacy processes of the platform.

Payment Card Industry Data Security Standards (PCI DSS)

A control validation of cardholder data to reduce credit card fraud.

Learn more about all VTEX's certifications.

PCI DSS - DESV

It's a set of additional procedures that are intended to reaffirm the effective and ongoing maintenance of the controls established by the PCI DSS.

Security education and awareness

We consider our employees a **critical defense line** in protecting the data of our company and our clients. VTEX developed a program dedicated to **awareness and training on security** best practices and the adoption of security resources at VTEX.

The program extends to all employees and third parties through:

- Periodic global meetings;
- Global announcements on emerging issues and security alerts;
- Phishing simulations and training to understand how to recognize and report them;
- Monthly training on security best practices;
- Security onboarding for new employees;
- Security events.

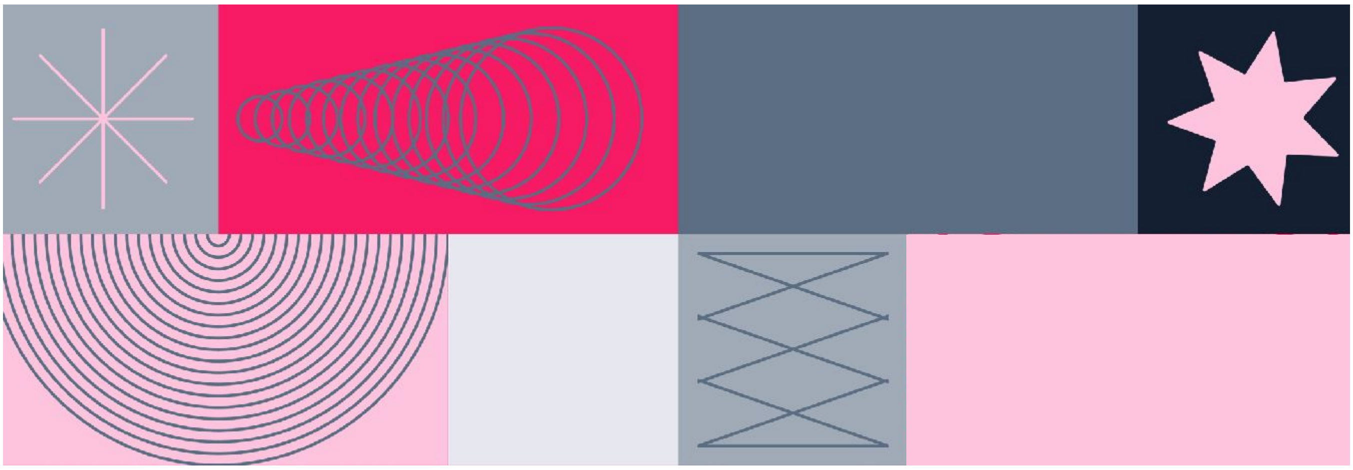
Through performance indicators, we measure the effectiveness of the security awareness programs and the knowledge of employees on the subject.

Asset Management

Assets are centrally managed through an inventory management system that stores and tracks their owner, location, status, maintenance, and descriptive information of the devices. Once acquired, VTEX checks and tracks all assets. VTEX also inspects and monitors for ownership, status, and resolution of assets under maintenance. It is also worth mentioning that VTEX operates 100% in the cloud and is the largest AWS (Amazon Web Services) partner in Latin America. Thus, there is no need for physical asset inventory for the resources in the AWS cloud. VTEX uses the AWS Systems Manager for software inventory, which provides visibility into AWS computing environment.

The media storage devices used to store customer data are classified as critical with high impact and are treated as this throughout their entire life cycles.

AWS uses strict standards on installing, maintaining, and eventually destroying devices when they are no longer useful. When a storage device reaches the end of its useful life, it is decommissioned using techniques detailed in NIST 800-88. The media used to store the client data is not removed from the control until safely deactivated.



Access, Identification, and Authentication

VTEX strictly controls and monitors access to its production environments. Only employees whose job functions require access can qualify for permission to access our systems. This guideline is in accordance with the practice of the Principle of Least Privilege and Segregation of Duties, where access is granted on the basis of legitimate need. Employees with privileged access to VTEX technologies need to use multiple layers of authentication to access a segregated environment.

Administrators with logical access to the systems do not have physical access to the datacenters. Logical access to the systems that provide the service is restricted to the VTEX Site Reliability Engineering team.

The repositories containing the platform's code are private, and adding and removing users from the organization is part of VTEX's hiring and termination processes. Only VTEX Development Engineers have access to the code repositories.

We have adopted secure configurations and a strong password policy for access to our systems, requiring: minimum number of characters, special characters, periodicity for changing passwords, control and session inactivity, and others.

When an employee is terminated, the Human Resources notification triggers a set of tasks and automations that protect access to the production systems.

Our access control team periodically reviews, using a service management system, all logical access and check if all the terminated users have been removed from the systems.

We also review employee transfers to ensure that network, server and database access to production systems is still appropriate for their new job role.

If you want to learn more about the platform's security features, click here and get to know our identity provider, VTEX ID.

Data Security

Information Classification and Protection

For VTEX, information must be classified according to the impacts of confidentiality, integrity and availability in high, moderate and low levels. This procedure results in one of the three information classifications: restricted, confidential or public.

Each classification level has its own handling and storage rules, considering the criticality of each piece of information and the possible impact it may have.

We are committed to keeping yours and your client's information secure. We understand that the proper classification of information is essential to guaranteeing its protection, allowing proper access control and preserving the confidentiality, integrity and availability of data.

Privacy and data protection

For VTEX, our customers' information are extremely valuable and we preserve its integrity and confidentiality throughout its life cycle.
For this reason, VTEX does not transfer or disclose customer or shopper data to third parties.

We comply with a variety of regional privacy and data protection regulations, such as the European Union's General Data Protection Regulation (GDPR), Brazil's General Data Protection Law (LGPD) and, the California Consumer Privacy Act (CCPA).

Compliance with privacy laws and regulations is a fundamental commitment for VTEX. We are dedicated to ensuring that all our operations comply with applicable regulations. We take proactive measures to protect all the personal data we process.

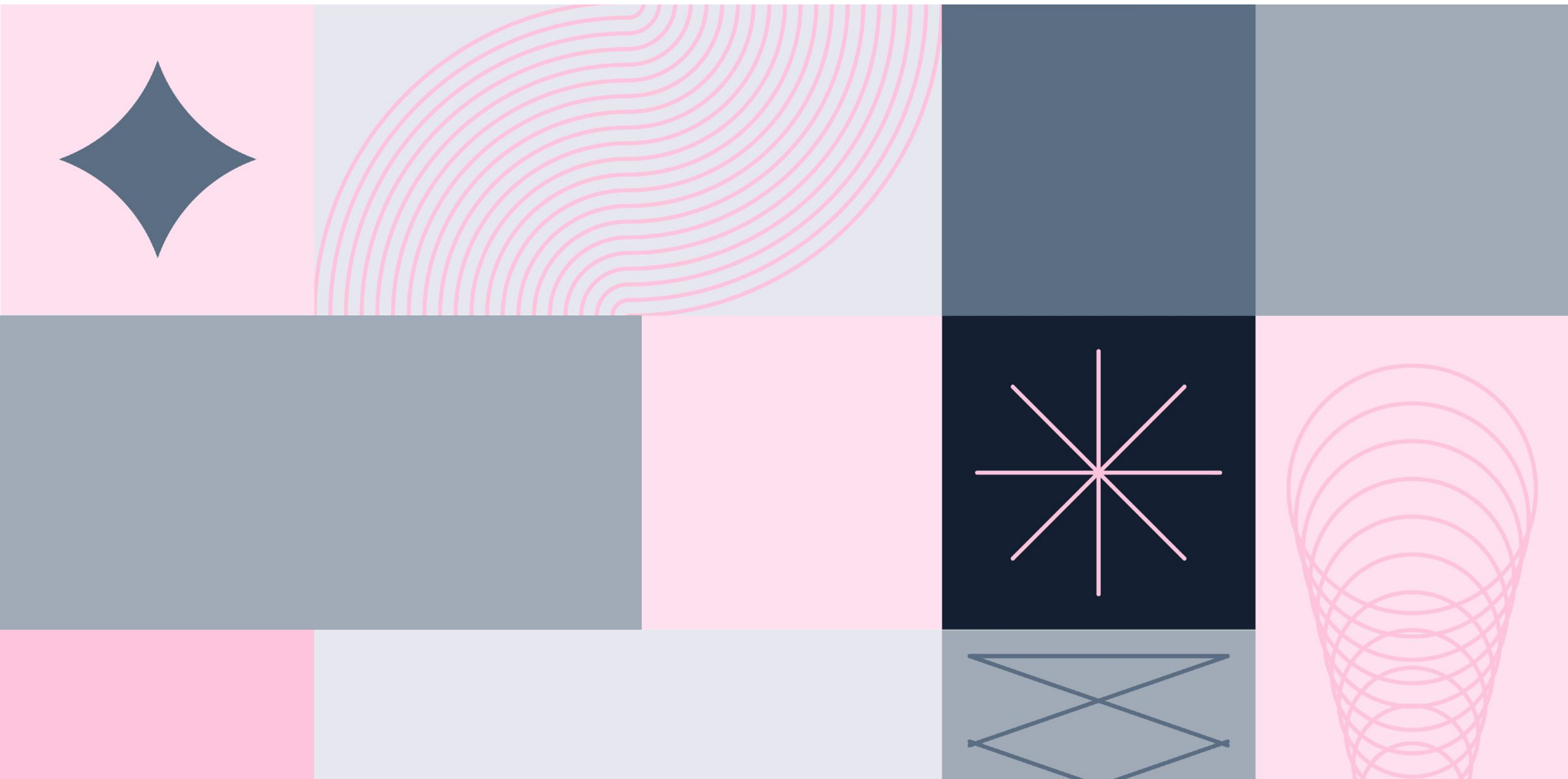
This responsibility is reflected in our constant improvement of security and privacy policies and procedures and controls, seeking for compliance and transparency.

Cryptographic Controls

VTEX believes that the encryption of its customers' information and data is essential. We have adopted TLS and its predecessor, SSL, as encryption protocols for secure communication over computer networks. This technology makes it impossible to read the data transmitted between consumer and store, and it can only be decrypted inside its server with the private key generated by the system.

The encryption keys are provided by the AWS service. The access keys are stored in a segregated environment with appropriate cryptographic protection.

To manage the cryptographic keys, we use AWS Key Management which stores and protects encryption keys to make them highly available, while at the same time offers strong and flexible access control.



Security of the VTEX data center and offices

Our data and our clients’ data are hosted on Amazon (Amazon Web Services), a public cloud infrastructure service provider. VTEX has agreements with this provider to ensure physical security and environmental protection to run our services.

Before choosing a site, AWS performs initial environmental and geographic assessments. Data center sites are chosen carefully to reduce environmental risks such as flooding, extreme weather conditions, and seismic activity. Our availability zones are designed to be independent and physically separate from each other.

AWS has strict controls when it comes to managing access to its datacenters. All employees who need to access the datacenter must first request access and provide a valid justification for it. It is also important to mention that AWS operates its datacenters in compliance with the Tier III+ guidelines (UpTime Institute).

In all VTEX offices around the world, we have controlled physical security, allowing only authorized people to access our facilities. To do this, physical access is controlled at the building's entry points, by professional security staff using surveillance systems, and by technological equipment that validates visitors' identities.

This equipment records people's exits and entrances and validates their identity.

Our offices have Closed Circuit Television Cameras (CCTV) and their images are stored in accordance with legal and compliance requirements.

We also have power and fire suppression controls that are in line with industry-leading measures to help prevent electrical faults and surges.

Host Security

VTEX services are powered by operating systems configured and implemented according to the industry's security best practices. We create environments using the latest AMI provided by AWS for each deployment service. In doing so, we leverage our security in the protection that AWS already provides for instances deployed by its services. We complement this security practice with the following measures:

- Applying critical security patches to operating systems when they are not provided as an updated AMI by AWS;
- Activating and centralizing system logs not to lose important information from the systems;
- Monitoring changes to critical configuration files to receive notification of changes to these files;
- Activating local firewalls configured only with secure ports, such as HTTPS, TLS 1.2, or higher.
- Removing unnecessary processes, accounts and protocols to reduce the attack surface.
- Installing anti-malware software.

These settings are applied during the deployment of a new environment.
If the new installation module needs to be added to our servers, the baseline installation will automatically be added to the devices.

Capacity and Change Management

Change management in our organization follows a documented process, as required. This process aims to define how VTEX control changes made to information systems. What the domain requires from the organization is to manage these changes so they do not act as improvisations.

However urgent it may be, even if the need appears last minute, the change management process requires our organization to evaluate the change and its consequences, that not always are clear, and may conceal serious damage.

By doing this analysis, VTEX increases the chances of choosing the best idea and not the first one, and, moreover, of not being negatively surprised afterwards.

The VTEX's Change Management process includes a study of the alternatives for making the change and its consequences, and require that every change be authorized by someone who takes responsibility for it.

Security Logging and Monitoring

The information security monitoring system consists of a series of resources and softwares related to Information Technology, used to prevent that important data of the business or its customers are accessed and exploited by third parties. That's why we continuously monitor our resources in our environment on a 24/7 basis.

Our critical services are monitored to identify possible anomalies and cyber threats. Event logs from VTEX's internal infrastructure and infrastructure provided by third parties are collected and centralized by our detection and response system, through the predefined rules.

Alerts are generated through pre-defined rules and using correlated detection logic. When this occurs, our incident response team investigates the causes of these alerts using standard processes and procedures.

VTEX periodically evaluates effectiveness of the monitoring tools, the threat and risk identification process and the resolution process aiming to discover improvements on it, making them increasingly efficient.

Threat Intelligence and Incident Response

Our proactive approach to cybersecurity relies on two main lines of defense: threat intelligence and incident response. Threat intelligence is a fundamental pillar for identifying, analyzing and understanding the threats that surround the digital universe. We strive to stay ahead of cybercriminals by actively monitoring the threat landscape, analyzing data, attack patterns and malicious behavior to anticipate hostile actions.

We have a specialized team of security analysts who collect, aggregate and interpret information from different sources, allowing us to identify emerging threats and even the most sophisticated ones, and enabling us to take preventive measures before they can cause significant damage.

Our incident response plan has been structured according to the four main stages of the response process:

Preparation

Before any response plan, our focus must be on incident prevention. This requires environment risk assessment, implementation of security baselines, patch updates, minimum access assurance, perimeter security safeguards, malware prevention and security education campaigns.

Incident Identification

Anomalous behavior is confirmed as an incident if it directly affects the Availability, Integrity and Confidentiality of information, systems and services or if it results from improper access or a attack.

Containment, Eradication and Recovery

Before starting any corrective action, collecting, preserving, protecting, and documenting evidence is essential.

No evidence can be deleted. No asset involved in the incident can be changed or deleted without proper approval.

If the evidence contains confidential information, it must be encrypted. After resolving an incident, VTEX must assess whether other environments are exposed or have already suffered the same type of attack to resolve the problem at its root cause. The team in charge must re-establish uncompromised safeguards.

Post-Incident Activities

This is an important stage of the process, in which learnings and improvements will be collected for the security controls when preparing and managing future incidents. The objective is to analyze what happened, what has been done to intervene and whether the intervention worked properly.

Vulnerability Management

VTEX rigorously evaluates resources by testing and identifying vulnerabilities by performing scans and penetration tests in our environments.

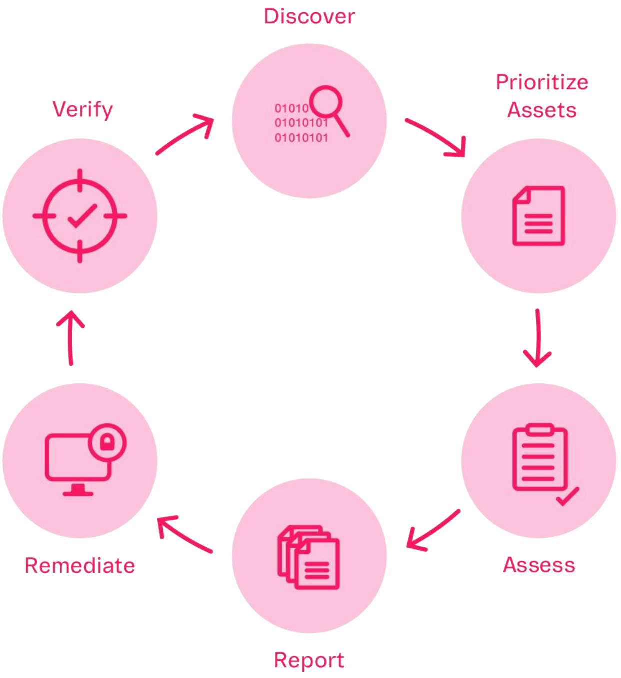
We have a schedule for vulnerability checks that must occur periodically, according to the criticality of the scope.

The vulnerabilities identified are handled and addressed in accordance with our vulnerability management process and are properly managed throughout their lifecycle.

In a multi-tenant solution like VTEX, this means that the entire platform is constantly tested throughout the year.

Customers who wish to carry out their own vulnerability assessment must follow the pre-established process, available on the Help Center.

If a reported vulnerability is confirmed by the VTEX security team, it is addressed internally for correction, always observing its level of criticality and risk for the platform.

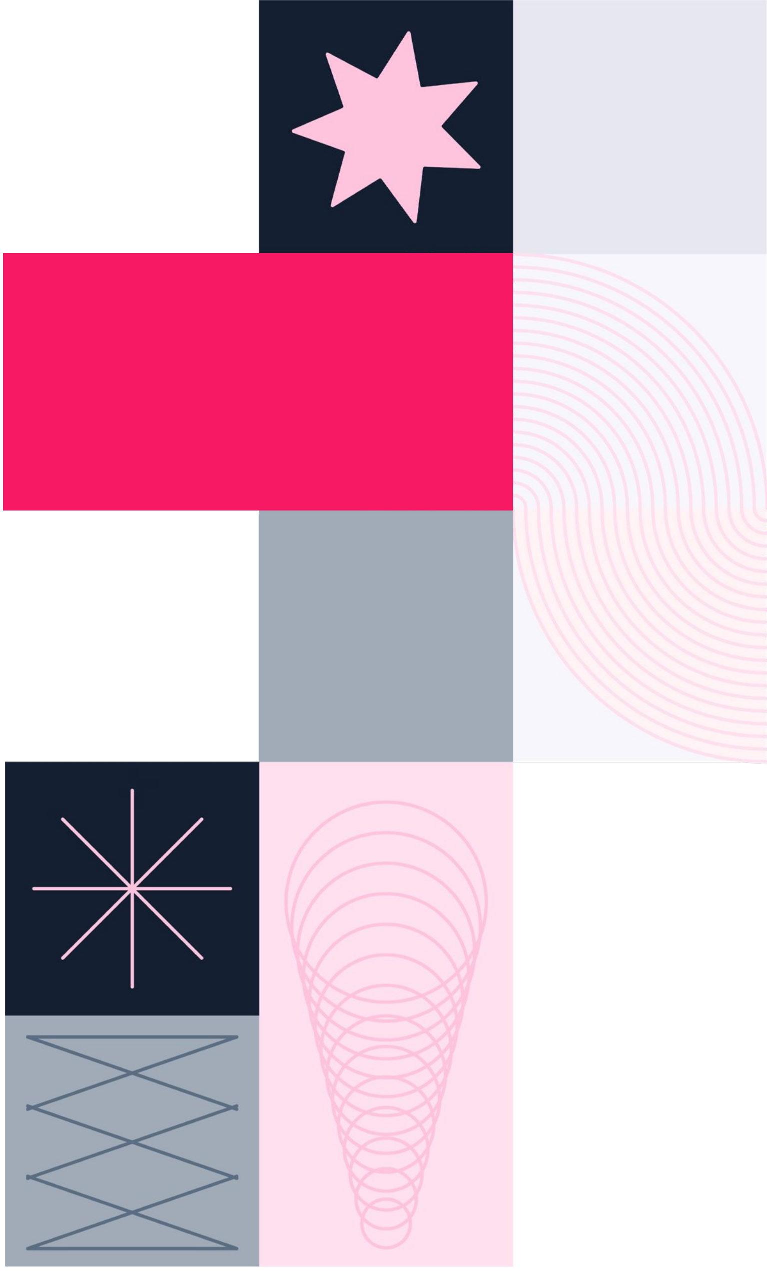


Perimeter Security

VTEX uses a multi-layered approach to protect resources, adopting processes such as network segregation, firewalls, and edge routers as the mechanism for perimeter and network protection.

We have an **IDS (Intrusion Detection System)** and **IPS (Intrusion Prevention System)** solution as network layer protection. We continuously monitor network traffic for anomalies.

This solution acts in the mitigation of DDoS attacks, redirecting the traffic, to ensure that it is clean and clients can continue their operations as usual.



Our clients' information are contained in a store account and it is isolated from different accounts by the VTEX process and storage implementation. There is no integrated method of accessing data from different accounts, even for internal VTEX use. The only ways to access the data require the explicit indication of a specific account.

Secure Development Cycle

At VTEX, we integrate security requirements into every stage of the platform development cycle, using the Secure Software Development Lifecycle (SSDLC) process.

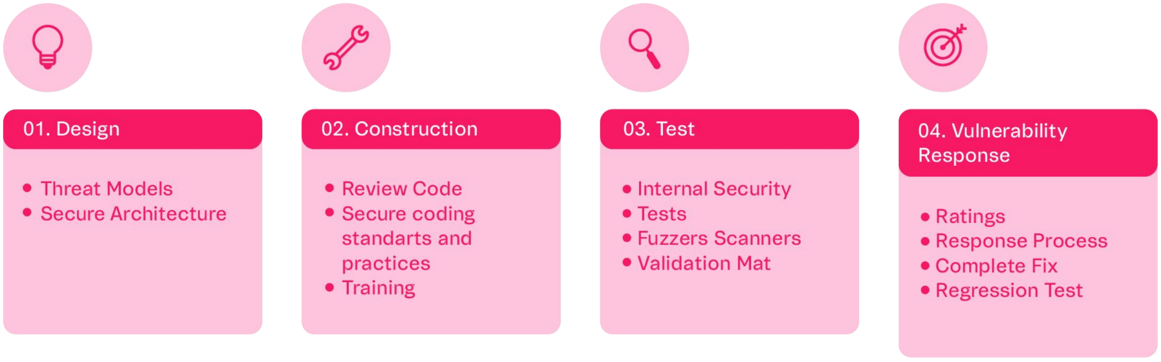
Through this methodology, our development engineers work with agile processes, taking into account our products' security issues and concerns.

We innovate considering the constant market demands. An example of this is VTEX IO, a native platform that provides enterprise solutions with more agility and security.

We care about following the best market guidelines for secure development. That's why VTEX engineers follow OWASP Top 10 methods to prevent any malicious code.

In addition, VTEX has a code scanning system in the repository that acts by catching possible vulnerabilities and errors within the software development cycles.

Learn more about VTEX IO in the diagram below:



01. Design

- Threat Models
- Secure Architecture

02. Construction

- Review Code
- Secure coding standarts and practices
- Training

03. Test

- Internal Security
- Tests
- Fuzzers Scanners
- Validation Mat

04. Vulnerability Response

- Ratings
- Response Process
- Complete Fix
- Regression Test

Third-Party Management

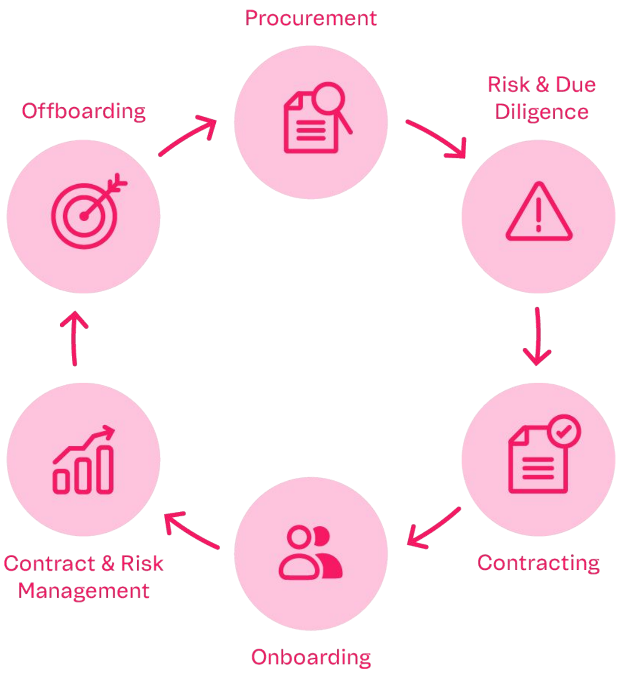
VTEX ensures that its outsourced providers respect and follow the same security policies offered by VTEX.

VTEX has an established security risk assessment process to evaluate suppliers that will handle personal data, sensitive data or that will interact with VTEX infrastructure or technologies.

We assess these vendors' security maturity and posture in order to understand and ensure that companies maintain an adequate level of protection and care regarding the data and information we share with them.

Only after all the necessary assessments and upon presentation of an adequate level of maturity do we proceed with hiring.

All of our third-party infrastructure providers can be found at this link.



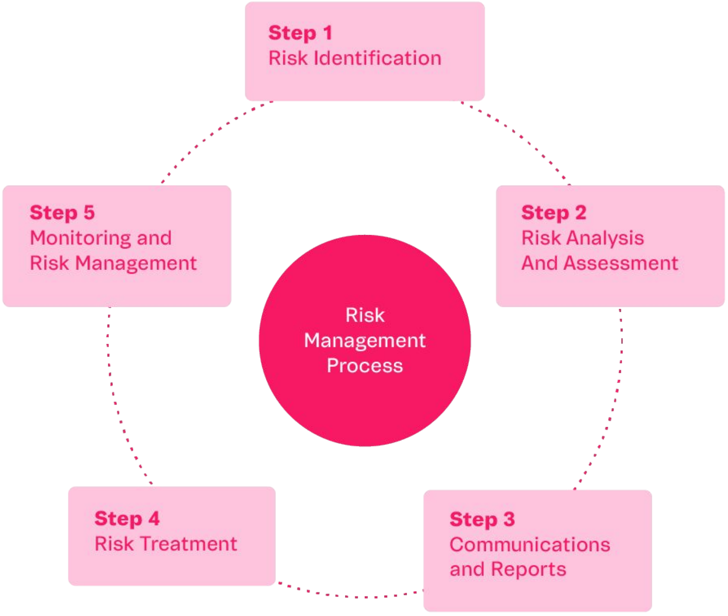
Security Risk Management

Our risk management program provides visibility into potential security threats and helps us make decisions aimed at corporate objectives.

For risk mapping, we measure the likelihood of the risk materializing and the impact it may have on VTEX's operation.

Identifying risks allows us to improve our monitoring and notification systems to deal with an eventual risk materialization. This can be done by notifying the people handling risks or triggering automated actions to mitigate or eliminate these risks.

The management process that addresses the entire risk lifecycle, ensuring that identified risks are addressed, mitigated and communicated, according to their relevance.



Business Continuity

We have a definitive commitment to our clients to prove that we are a safe and reliable platform. That is why we have implemented a **Business Continuity Plan** designed to prepare the company to deal with the effects of an emergency. Our goal is that following the steps set out in the plan will provide the basis for a quick and easy return to the day-to-day operation of our business in case of any interruption.

Our **Disaster Recovery Plan** focuses on ensuring continuity of operations and the availability of critical resources in the event of a disaster. It contains instructions on what actions to take and how to respond to unplanned incidents characterized as crisis, that can be related to natural disasters, cyber attacks, and any other disruptive event.

This plan is periodically tested by several VTEX teams, aiming to ensure its effectiveness and validity.

Security Maturity

To continuously improve our security posture, we use the ISO 27001 Standard to measure the maturity of our security programs. ISO:IEC 27001 is the International standard and benchmark for Information Security management.

The adoption of the ISO:IEC 27001 standard aims to ensure that the organization adopts an adequate Information Security Management System (ISMS) that can be improved and monitored.

This information security management system (ISMS) is, according to the principles of ISO:IEC 27001, a holistic approach to security that is independent of brands and technology manufacturers.

We perform self-assessments periodically using the ISO 27001 controls as guidelines, and based on the gaps identified, we build a roadmap for implementation and adaptation.

We've also defined a metric to measure the current level of security maturity, which allows us to quantify and track the overall maturity of our security posture.

Conclusion

VTEX is committed to providing security and confidence to all our customers. We place security as one of the fundamental pillars of our operations, aiming to protect data and information of everyone who uses our products and services.

Furthermore, the trust placed in us is a privilege that we value immensely. We seek to earn our customers' trust on a daily basis by delivering high-quality, safe products and services that meet expectations and help our customers to innovate, driving mutual growth.

By choosing VTEX, you are choosing a reliable partner dedicated to the security of your interests. Your peace of mind and satisfaction are our reward, and we will continue to work tirelessly to maintain that relationship of trust. We are here for you, protecting what matters the most.

Companies choose us as a strategic partner to accelerate digital commerce transformation and deliver revenue generating initiatives.

Even after 20 years and all the impact we've delivered to the ecommerce ecosystem, we still keep the mindset that got us here from day one.

We are on a never-ending journey of connecting the world through the way people trade, We invite you to step into our future and be a part of that journey!

#WeAreTrusted.

Resources

Security Help Center

This site is a public channel that serves as a help desk for VTEX clients and prospects. It provides solutions to a variety of questions and has a broad information base.

VTEX Trusthub

The VTEX Trust Hub is our public site for addressing concerns involving legal, compliance, privacy and security issues.

Security FAQ

This space is the only private one. Only VTEX clients can access it using their login and password. This is a reserved portal where we provide our answers to the most frequently asked security questions to support the resolution of doubts and the completion of the Risk Assessment.

VTEX Healthcheck

VTEX HealthCheck is a public page to monitor the status of our platform’s services. The Healthcheck has over 100 tests running per minute. In this dashboard, you can track the health of each module in real time.

Status VTEX

In VTEX Status, you can track the platform’s stability in real time and access the entire history of incidents. Our team reports events whenever our automatic monitoring system identifies an instability in the platform modules.

See more at: vtex.com

VTEX

The Enterprise
Digital Commerce
Platform