VTEX

The Enterprise
Digital Commerce
Platform

Postura de seguridad de VTEX

VTEX Security

Introducción 03
Estamos comprometidos con tu tranquilidad 04
Cómo protegemos nuestros sistemas y clientes 05
Programa de seguridad de la información 06
Auditoría y cumplimiento 07
Educación y concientización sobre seguridad 08
Gestión de activos 09
Acceso, identificación y autenticación 10
Seguridad de los datos 11
Privacidad y protección de datos 12
Controles Criptográficos 13
Seguridad del centro de datos y las oficinas de VTEX 14
Seguridad del host 15
Gestión de capacidad y cambios 16
Registro y monitoreo de seguridad 17
Inteligencia sobre amenazas y respuesta a incidentes 18
Gestión de vulnerabilidades 20
Seguridad perimetral 21
Ciclo de desarrollo seguro 22
Gestión y evaluación de terceros 23
Gestión de riesgos de seguridad 24
Continuidad de negocio 25
Madurez de la seguridad 26
Conclusión 27
Recursos 28

Introducción

Con el aumento exponencial del trabajo a distancia y el comercio electrónico, se ha instado a las empresas a desarrollar un entorno online seguro. Aunque la seguridad se ha convertido en un tema popular en el mercado, menos de un tercio de las empresas brasileñas cuentan con equipos dedicados a la ciberseguridad.

En VTEX nos comprometemos a cambiar esta situación. Hemos desarrollado un equipo totalmente dedicado a garantizar que proporcionamos a todos los que forman o formarán parte de nuestra comunidad tranquilidad, bienestar, seguridad y confianza en lo que respecta a la seguridad y la privacidad.

Entendemos la importancia de adoptar las prácticas de seguridad más avanzadas del sector y las tecnologías necesarias para proteger los datos de los clientes y estas prácticas se incorporan a todas nuestras tecnologías, personas y procesos.

Nuestros clientes confían en nosotros para proporcionar altos niveles de integridad, confidencialidad y disponibilidad de los datos. Por más de dos décadas, hemos trabajado con clientes de sectores altamente regulados como gobiernos, servicios financieros, salud y servicios públicos, y todos ellos han estado dispuestos a confiar sus datos a VTEX.

Compromiso de VTEX

En VTEX, nos comprometemos a seguir las prácticas y medidas de seguridad más eficaces para garantizar que el acceso esté controlado y los datos estén seguros y protegidos.

Nuestras pautas

Para mejorar continuamente nuestra postura de seguridad, utilizamos la norma ISO 27001:2022 para medir la madurez de nuestros programas de seguridad y evaluar e identificar áreas de mejora. Este norma es el estándar y la referencia internacional para la gestión de la seguridad de la información.

Estamos comprometidos con tu tranquilidad

Somos la plataforma de comercio digital para empresas

Tomamos decisiones audaces y nos arriesgamos por el éxito de nuestros clientes. Somos un equipo de alto desempeño, siempre aprendiendo y aceptando desafíos fuera de nuestra zona de conforto.

Somos el eje principal del comercio conectado

En VTEX, entendemos la importancia de adoptar las prácticas de seguridad y tecnología necesarias para proteger los datos de los clientes. Nuestras medidas de seguridad están integradas en toda nuestra tecnología, procesos y personal.

VTEX es más que una plataforma de comercio

Armonizamos los negocios y la tecnología. Sabemos que la privacidad y la seguridad son fundamentales para el éxito de cualquier tipo de negocio.

En este documento, ofreceremos una visión general de nuestra postura de seguridad que servirá como punto de partida para demostrar nuestro compromiso con nuestra propia seguridad y la de nuestros clientes.

Cómo protegemos nuestros sistemas y clientes

Programa de seguridad de la información

En VTEX contamos con un programa de Seguridad de la Información implementado y gestionado por líderes comprometidos con el aumento del nivel de madurez de la seguridad de todo el ecosistema VTEX.

Disponemos de una **Política de Seguridad de la Información**, que se ha transmitido a toda la empresa a través de nuestros canales de comunicación interna y revisada anualmente de acuerdo con nuestro proceso de gestión de documentos.

Nuestra Política de Seguridad de la Información está orientada a la norma ISO IEC 27001; frameworks con las mejores prácticas de seguridad; leyes de protección de datos y otras obligaciones aplicables al contexto de VTEX.

Todos nuestros documentos son revisados anualmente y garantizamos la gestión a través de una plataforma de gestión de políticas.

VTEX cuenta con un equipo robusto y especializado en la Seguridad de la Información. Nuestro equipo de seguridad trabaja en modo de espera, con equipos en diferentes zonas horarias para garantizar una cobertura que va más allá del horario laboral.

Auditoría y cumplimiento

Auditorías de Cumplimiento Internas

Las auditorías de cumplimiento internas son realizadas por nuestro equipo de auditores internos y se llevan a cabo periódicamente como preparación para las auditorías de certificación externas.

Nuestro equipo de auditoría trabaja constantemente en la mejora de este proceso y en la automatización de la verificación de los controles, con el objetivo de disponer de un panel de cumplimiento activo.

Auditorías de cumplimiento Externas

Las auditorías de certificación las realizan empresas independientes y son supervisadas por nuestro equipo de Auditoría Interno. Los resultados se utilizan para mejorar los procesos de control de cumplimiento internos.

Certificaciones de VTEX

VTEX cuenta con un programa de cumplimiento para gestionar y mantener los controles de seguridad.

Service Organization Controls (SOC 1)

Auditoría que cubre los controles internos sobre los sistemas de información financiera.

Service Organization Controls (SOC 2 e 3)

Auditoría que cubre los procesos de seguridad, disponibilidad, integridad, confidencialidad y privacidad de la plataforma.

Payment Card Industry Data Security Standards (PCI DSS)

Una validación de los controles en torno a los datos de los titulares de las tarjetas para reducir el fraude con tarjetas de crédito.

Aprende más sobre todas las certificaciones VTEX.

PCI DSS - DESV

Comprende un conjunto de procedimientos adicionales destinados a reafirmar el mantenimiento efectivo y continuo de los controles establecidos por las PCI DSS.

Educación y concientización sobre seguridad

Consideramos que nuestros colaboradores son una línea de defensa fundamental para proteger los datos de nuestra empresa y de nuestros clientes. Es por eso que desarrollamos un programa dedicado a la **concientización y capacitación** sobre las mejores prácticas de seguridad y la adopción de características de seguridad en VTEX.

El programa se extiende a todos los empleados y terceros a través de:

- Reuniones globales periódicas;
- Anuncios globales sobre problemas emergentes y alertas de seguridad;
- Envío de simulaciones de *phishing* y capacitaciones para entender cómo reconocerlos y denunciarlos;
- Capacitación mensual sobre mejores prácticas de seguridad;
- *Onboarding* de seguridad para nuevos empleados;
- Realización de eventos de seguridad.

A través de indicadores de desempeño medimos la efectividad de los programas de concientización en seguridad y el conocimiento de los empleados sobre el tema.

Gestión de activos

Los activos se gestionan de forma centralizada a través de un sistema de gestión de inventario que almacena y monitorea el propietario, ubicación, status, mantenimiento y información descriptiva de los activos. Después de la adquisición, se comprueban y rastrean los activos. Además, los activos en mantenimiento se comprueban y monitorean para dar seguimiento a su propiedad, status y resolución. VTEX opera 100% en la nube y es el mayor socio de AWS (Amazon Web Services) en América Latina. Por lo tanto, no es necesario realizar un inventario de activos físicos de los recursos de la nube AWS. Para el inventario de software, utilizamos el inventario de AWS Systems Manager, que proporciona visibilidad en nuestro entorno informático de AWS.

Los dispositivos de almacenamiento de multimedia utilizados para almacenar los datos de los clientes se clasifican como críticos y se tratan adecuadamente, como de alto impacto, a lo largo de sus ciclos de vida.

AWS utiliza normas rigurosas sobre cómo instalar, mantener y, posiblemente, destruir los dispositivos cuando ya no son útiles. Cuando un dispositivo de almacenamiento llega al final de su vida útil, se desactiva utilizando las técnicas detalladas en NIST 800-88. Los dispositivos multimedia utilizados para almacenar los datos de los clientes no se retiran del control hasta que se desactivan de forma segura.

Acceso, identificación y autenticación

VTEX controla y supervisa estrictamente el acceso a nuestros entornos de producción. Solo los colaboradores cuyas funciones de trabajo requieren acceso pueden tener permiso para acceder a nuestros sistemas. Esta pauta se corresponde con nuestra práctica del principio de mínimo privilegio y la segregación de funciones, donde el acceso se concede en función de una necesidad legítima. Los colaboradores con privilegios de VTEX, como los ingenieros de confiabilidad de la plataforma, necesitan utilizar varias capas de autenticación de dos factores para acceder a un entorno segregado.

Los administradores con acceso lógico a los sistemas no tienen acceso físico a los centros de datos. El acceso lógico a los sistemas que prestan el servicio está restringido al equipo de Site Reliability Engineering de VTEX. Los repositorios con los códigos de la plataforma son privados y añadir y remover usuarios de la organización forma parte de los procesos de contratación y desvinculación de VTEX. Solo los ingenieros de desarrollo de VTEX tienen acceso a los repositorios de código.

Adoptamos configuraciones seguras y una política de contraseñas robusta para el acceso a nuestros sistemas que incluye el número mínimo de caracteres y caracteres especiales, la periodicidad del cambio de contraseñas, la no utilización de contraseñas anteriores, el control y la inactividad de la sesión, entre otros.

Cuando un colaborador es despedido, la notificación de Recursos Humanos desencadena un conjunto de tareas que protegen el acceso al sistema de producción.

Nuestro equipo de control de acceso periódicamente revisa los accesos lógicos y verifica que los usuarios desvinculados hayan sido removidos de los respectivos sistemas a través de un sistema de tickets interno.

También revisamos los traslados de colaboradores y nos aseguramos de que los accesos a la red, servidor y base de datos de los sistemas de producción sigan siendo adecuados para su nueva función de trabajo.

Si quieres saber más sobre los recursos de seguridad de la plataforma, haz clic aquí y aprende sobre nuestro proveedor de identidad, VTEX ID.

Seguridad de los datos

Clasificación y protección de la información

Para VTEX, las informaciones deben ser clasificados considerando los impactos de confidencialidad, integridad y disponibilidad en alto, moderado y bajo. Esta estructura da lugar a una de las tres clasificaciones, respectivamente: restringida, confidencial o pública.

Cada nivel de clasificación tiene sus propias reglas de manejo y almacenamiento, considerando la criticidad de cada dato y el posible impacto que genera.

Estamos comprometidos a mantener su informaciones y de sus clientes seguras y protegidas. Entendemos que la adecuada clasificación de la información es fundamental para garantizar su protección, permitiendo un adecuado control de acceso y la preservación de la confidencialidad, integridad y disponibilidad de los datos.

Privacidad y protección de datos

Para VTEX las informaciones de nuestros clientes son extremadamente valiosas y preservamos su integridad y confidencialidad durante todo su ciclo de vida.
Por eso, VTEX no transfiere ni divulga los datos de los clientes y shoppers a terceros.

Cumplimos con las obligaciones de gobernanza bajo una variedad de regulaciones regionales de privacidad y protección de datos, como el Reglamento general de protección de datos de la Unión Europea (GDPR), la Ley general de protección de datos de Brasil (LGPD) y la Ley de privacidad del consumidor de California (CCPA).

El cumplimiento de las leyes y regulaciones de privacidad vigentes es un compromiso fundamental para VTEX. Estamos dedicados a garantizar que todas nuestras operaciones cumplan con las regulaciones aplicables. Tomamos medidas proactivas para proteger todos los datos personales que procesamos.

Esta responsabilidad se refleja en nuestra mejora constante de políticas y procedimientos y controles de seguridad y privacidad, en la búsqueda del cumplimiento y la transparencia.

Controles Criptográficos

VTEX entiende que es fundamental cifrar las informaciones y datos de sus clientes. Adotamos TLS y su predecesor, SSL, como protocolos criptográficos para la comunicación segura a través de redes informáticas.

Esta tecnología imposibilita la lectura de los datos transmitidos entre el consumidor y la tienda, y sólo puede descifrarse dentro de su servidor con la clave privada generada por el sistema.

Las claves de encriptación son proporcionadas por el servicio de AWS. Las claves de acceso se almacenan en un entorno segregado con la debida protección criptográfica. Para realizar la gestión de claves criptográficas, utilizamos AWS Key Management, que almacena y protege las claves de encriptación para que estén ampliamente disponibles a la vez que proporciona un control de acceso fuerte y flexible.

Seguridad del centro de datos y las oficinas de VTEX

Nuestros datos y los de nuestros clientes están hospedados en Amazon (Amazon Web Services), un proveedor de servicios de infraestructura de nube pública. VTEX tiene acuerdos con estos proveedores para garantizar una línea base de seguridad física y protección ambiental para ejecutar nuestros servicios. La selección de los locales de los centros de datos se lleva a cabo con mucho cuidado para reducir los riesgos medioambientales, como inundaciones, condiciones meteorológicas extremas y actividad sísmica. Nuestras zonas de disponibilidad están creadas para ser independientes y estar físicamente separadas unas de otras.

AWS tiene controles estrictos respecto a la gestión de acceso a sus centros de datos. Todos los colaboradores que necesiten acceder al centro de datos primero deben solicitar acceso y presentar una justificación válida. También cabe destacar que AWS opera sus centros de datos de acuerdo con las pautas Tier III+ (UpTime Institute).

En las oficinas de VTEX, repartidas por todo el mundo, tenemos el control de Seguridad física, permitiendo únicamente el acceso a nuestras instalaciones a personas autorizadas. Para ello, el acceso físico es controlado en los puntos de ingreso al edificio, por un equipo de seguridad profesional que utiliza sistemas de vigilancia y por equipos tecnológicos que validan la identidad de los visitantes. Este equipo registra las salidas y entradas de personas, y valida su identidad.

Las oficinas disponen de cámaras de circuito cerrado de televisión (CCTV). Las imágenes se mantienen de acuerdo con los requisitos legales y de cumplimiento.

También disponemos de controles de energía y extinción de incendios que corresponden con las medidas más avanzadas del sector para ayudar a evitar fallos y sobrecargas eléctricas.

Seguridad del host

Los servicios de VTEX están impulsados por sistemas operativos configurados y aplicados según las mejores prácticas de seguridad del sector.
Creamos entornos utilizando la última AMI proporcionada por AWS para cada servicio de implementación. De esta manera, aprovechamos en nuestra seguridad la protección que AWS ya proporciona para las instancias implementadas por sus servicios.
Complementamos esta práctica de seguridad con las siguientes medidas:

- Aplicación de patches de seguridad críticas a los sistemas operativos cuando AWS no las proporciona como una AMI actualizada.
- Activación y centralización de los logs del sistema para no perder información importante de los sistemas;
- Monitoração das alterações nos arquivos críticos de configuração para nos notificar sobre as alterações desses arquivos;
- Activación de firewalls locales configurados solo con puertos seguros, por ejemplo, HTTPS y TLS 1.2 o superior;
- Eliminación de procesos, cuentas y protocolos innecesarios y estándar para reducir la superficie de ataque del equipo.
- Instalación de software antimalware.

Estas configuraciones se mantienen durante la implementación de un nuevo entorno.
Si el nuevo módulo de instalación tiene que ser añadido en nuestros servidores, la instalación de línea base se añadirá a los dispositivos automáticamente.

Gestión de capacidad y cambios

La gestión de cambios en nuestra organización sigue un proceso documentado de acuerdo con los requisitos. El propósito de tener un proceso estandarizado es definir cómo se controlan los cambios realizados en los sistemas de información. Gestionamos los cambios para que no funcionen como improvisaciones.

Por muy urgente que sea, aunque la necesidad aparezca en el último momento, la Gestión de Cambios plantea que la organización evalúe el cambio y sus consecuencias, que no siempre son muy claras y pueden ocultar daños graves.

Al realizar este análisis, VTEX aumenta las posibilidades de elegir la mejor idea y no la primera y, además, de no verse sorprendida negativamente después.

El procedimiento para controlar los cambios de Gestión de Cambios además de incluir un estudio de las alternativas para llevar a cabo el cambio y sus consecuencias exige que cada cambio sea autorizado por alguien que asuma la responsabilidad.

Para demostrar que se sigue este procedimiento, VTEX archiva los resultados de cada evaluación y quién es el responsable de autorizar el cambio.

Registro y monitoreo de seguridad

El sistema de monitoreo de la seguridad de la información consiste en una serie de recursos, softwares vinculados a la tecnología de la información, que sirven para evitar que terceros accedan a los datos importantes y los usen. Por eso, en VTEX monitoreamos continuamente los recursos de nuestro entorno en una escala ininterrumpida (24/7).

Nuestros servicios críticos son monitoreados para identificar posibles anomalías y ciberamenazas. Los logs de eventos de la infraestructura interna y de los proveedores de infraestructura de VTEX se recopilan y centralizan en nuestro sistema de detección y respuesta a través de reglas predefinidas. Utilizando una lógica de detección correlacionada, se generan alertas, en cuyo caso nuestro equipo de respuesta a incidentes investiga las causas de las alertas mediante procesos y procedimientos estándar.

Además, evaluamos periódicamente la eficacia de la identificación y resolución de amenazas y riesgos, lo que produce mejoras en nuestros procesos automatizados, haciéndolos cada vez más eficaces.

Inteligencia sobre amenazas y respuesta a incidentes

Nuestro enfoque proactivo hacia la ciberseguridad se basa en dos líneas principales de defensa: inteligencia contra amenazas y respuesta a incidentes. La inteligencia de amenazas es un pilar fundamental para identificar, analizar y comprender las amenazas que rodean el universo digital. Nos esforzamos por adelantarnos a los ciberdelincuentes monitoreando activamente el panorama de amenazas, analizando datos, patrones de ataque y comportamiento malicioso para anticipar acciones hostiles.

Contamos con un equipo especializado de analistas de seguridad que recopilan, agregan e interpretan información de diferentes fuentes, permitiéndonos identificar amenazas emergentes e incluso las más sofisticadas, y tomar medidas preventivas antes de que puedan causar daños importantes.

Nuestro plan de respuesta a incidentes se estructuró según las cuatro etapas principales del proceso de respuesta:

Preparación

Antes de cualquier plan de respuesta, los esfuerzos deben centrarse en la prevención de incidentes. Esto requiere una evaluación de riesgos de los entornos, la aplicación de baselines de seguridad, la actualización de patches, la garantía de acceso mínimo, las garantías de seguridad perimetral, la prevención contra el malware y las campañas de educación de seguridad.

Identificación de incidentes

Un comportamiento anómalo se confirma como incidente si afecta directamente la disponibilidad, integridad y confidencialidad de la información, sistemas y servicios o si se deriva de un acceso indebido o un ataque explícito.

Contención, erradicación y recuperación

Antes de iniciar cualquier acción de tratamiento es esencial recopilar, preservar, proteger y documentar las pruebas. No se puede excluir ninguna prueba. Ningún activo involucrado en el incidente puede ser modificado o eliminado sin la aprobación correspondiente.
Si las pruebas contienen información confidencial, deben estar encriptadas.
Después de contener un incidente, se debe evaluar si otros entornos están expuestos o ya han sufrido el mismo tipo de ataque para resolver el problema en la causa raíz. El equipo encargado debe restablecer las salvaguardas no comprometidas.

Actividades posteriores al incidente

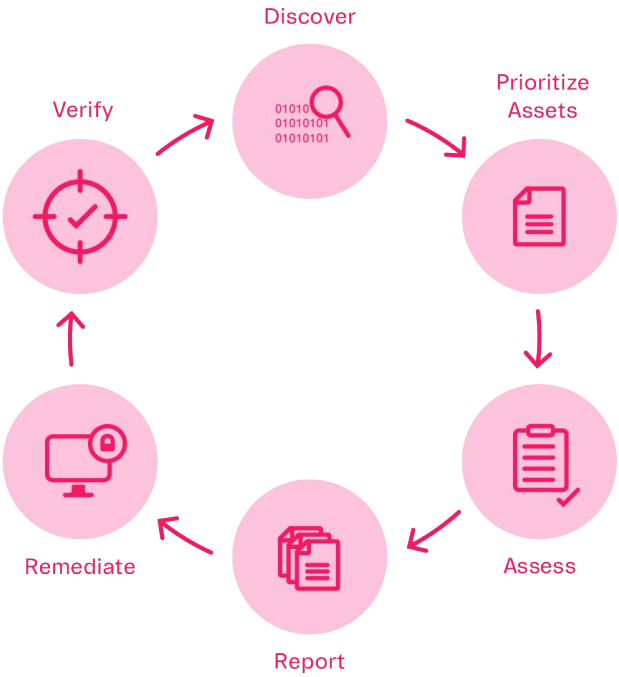
Esta es una etapa importante del proceso donde se recogerán los aprendizajes y mejoras para los controles de seguridad que se aplicarán en la etapa de preparación y gestión de futuros incidentes. El objetivo es analizar lo sucedido, lo que se ha hecho para intervenir y si la intervención funcionó correctamente.

Gestión de vulnerabilidades

VTEX evalúa rigurosamente los recursos probando e identificando las vulnerabilidades mediante la realización de escaneos y pruebas de penetración en nuestros entornos.

Tenemos un calendario de verificaciones de vulnerabilidad, donde las comprobaciones se producen periódicamente y según la criticidad de cada alcance.

Las vulnerabilidades identificadas se abordan en nuestro proceso de gestión de vulnerabilidades y son debidamente gestionadas a lo largo de su ciclo de vida.



En una solución multiusuario como VTEX, esto significa que toda la plataforma se prueba constantemente a lo largo del año.

Los clientes que desean realizar una evaluación de vulnerabilidad deben seguir el proceso preestablecido, disponible en Help Center.

Si una vulnerabilidad reportada es confirmada por el equipo de seguridad de VTEX, se aborda internamente para su corrección, observando siempre su nivel de criticidad y riesgo para la plataforma.

Seguridad perimetral

VTEX utiliza un enfoque de múltiples capas para la protección de recursos y adopta procesos como la segregación de la red, firewalls y enrutadores de borde como mecanismo de protección del perímetro y la red.

Disponemos de una solución **IDS (Intrusion Detection System)** y **IPS (Intrusion Prevention System)** como protección de la capa de red y monitoreamos continuamente el tráfico de la red en busca de anomalías.

Esta solución es parte de la mitigación de los ataques DDoS, en que el tráfico es redirigido para garantizar que esté limpio y que los clientes puedan continuar sus operaciones con normalidad.

La información del cliente está contenida en una cuenta de tienda y está aislada de las diferentes cuentas por el proceso de VTEX y la implementación del almacenamiento. No hay ningún método integrado de acceso a los datos que traspase los límites de las diferentes cuentas, ni siquiera para el uso interno de VTEX. Las únicas formas de acceder a los datos requieren la indicación explícita de una cuenta específica.

Ciclo de desarrollo seguro

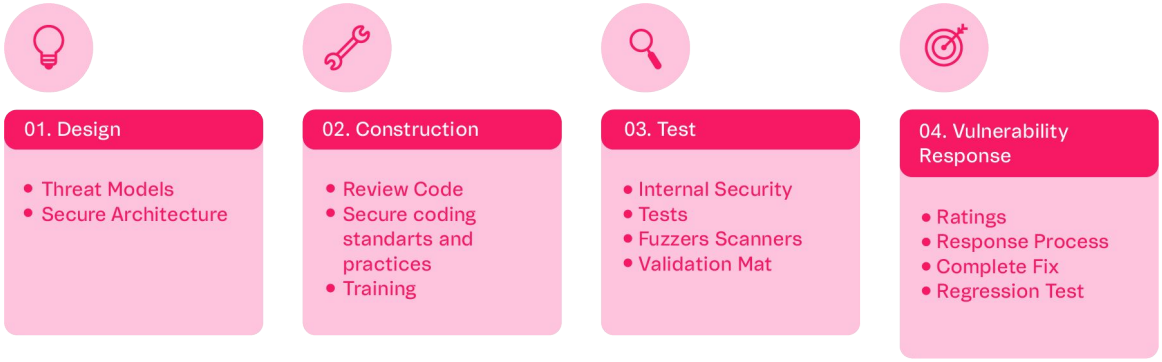
En VTEX, integramos los requisitos de seguridad en todas las fases del ciclo de desarrollo de la plataforma, utilizando el proceso Secure Software Development Lifecycle (SSDLC). A través de esta metodología, nuestros ingenieros de desarrollo trabajan con procesos ágiles, considerando los problemas y preocupaciones de seguridad de nuestros productos.

Innovamos considerando las constantes exigencias del mercado. Un ejemplo de esto es VTEX IO, una plataforma nativa capaz de ayudar en la entrega de soluciones empresariales con más agilidad y seguridad.

Nos preocupamos por seguir las mejores pautas del mercado cuando se trata del desarrollo seguro. Por eso, los ingenieros de VTEX desarrollan siguiendo los métodos OWASP Top 10 para evitar cualquier código malicioso.

Además, VTEX cuenta con un sistema de escaneo de código en el repositorio que captura posibles vulnerabilidades y errores dentro de los ciclos de desarrollo del software.

Conozca más sobre VTEX IO en el siguiente diagrama:



Gestión y evaluación de terceros

VTEX garantiza que sus proveedores subcontratados respetan y siguen las mismas políticas de seguridad que VTEX ofrece.

VTEX tiene establecido un proceso de análisis de riesgos de seguridad para los proveedores que procesarán datos personales, datos sensibles o que interactuarán con la infraestructura o tecnologías de VTEX.

Evaluamos la madurez y la postura de seguridad de estos proveedores para garantizar que las empresas mantengan un nivel adecuado de protección y cuidado en relación con los datos e información que compartimos con ellas.

Sólo después de todas las evaluaciones necesarias y previa presentación de un nivel de madurez adecuado procedemos a la contratación.

Todos nuestros proveedores de infraestructura externos se pueden encontrar en este link.

Gestión de riesgos de seguridad

Nuestro programa de gestión de riesgos brinda visibilidad a las posibles amenazas de seguridad y nos ayuda a tomar decisiones orientadas a los objetivos corporativos.

Para el mapeo de riesgos, medimos la probabilidad de que el riesgo se materialice y el impacto que tendrá en la operación de VTEX.

La identificación de riesgos resulta en la mejora de nuestros sistemas de monitoreo y notificación para hacer frente a su eventual materialización, ya sea notificando a las personas capaces de gestionarlos o activando acciones automatizadas que puedan mitigarlos o eliminarlos.

El proceso de gestión aborda todo el ciclo de vida del riesgo, garantizando que los riesgos identificados se aborden, mitiguen y comuniquen, de acuerdo con su relevancia.

Etapas do Processo de Gerenciamento de Riscos

Continuidad de negocio

Tenemos un compromiso definitivo con nuestros clientes para demostrar que somos una plataforma segura y confiable. Por eso hemos implementado un **Plan de Continuidad de Negocio**, diseñado para preparar a la empresa para hacer frente a los efectos de una emergencia. Creemos que seguir los pasos establecidos en el plan nos proporciona base para un retorno relativamente rápido y fácil al funcionamiento cotidiano de nuestro negocio, en caso de cualquier interrupción.

Nuestro **Plan de Recuperación ante Desastres** se centra en asegurar la continuidad de las operaciones y la disponibilidad de recursos críticos en caso de desastre. El contiene instrucciones sobre qué acciones tomar y cómo responder a incidentes no planificados y caracterizados como crisis, que pueden estar relacionados con desastres naturales, ciberataques y cualquier otro evento disruptivo.

Este plan es probado periódicamente por los más diversos equipos de VTEX, con el objetivo de garantizar su eficacia y validez.

Madurez de la seguridad

Para mejorar continuamente nuestra postura de seguridad, utilizamos la norma ISO 27001:2022 como base para medir la madurez de nuestros programas de seguridad. Esta norma es el estándar y referencia internacional para la gestión de la seguridad de la información.

La adopción de la norma ISO:IEC 27001 tiene como objetivo garantizar que la organización adopte un Sistema de Gestión de Seguridad de la Información (SGSI) adecuado que pueda mejorarse y monitorearse.

Este SGSI es, según los principios de la norma ISO:IEC 27001, un modelo holístico para abordar la seguridad que es independiente de marcas y fabricantes de tecnología.

Periódicamente realizamos una autoevaluación utilizando los controles de la norma ISO 27001 como guía y, a partir de las lagunas identificadas, construimos un plan de trabajo para la implementación y adecuación. También ha sido posible establecer una puntuación a nuestro estado de madurez actual, en que podemos cuantificar y seguir la madurez general de nuestra postura de seguridad.

Conclusión

VTEX está comprometida a brindar seguridad y confianza a todos nuestros clientes. Colocamos la seguridad como uno de los pilares fundamentales de nuestras operaciones, con el objetivo de proteger los datos y la información de todas las personas que utilizan nuestros productos y servicios.

Además, la confianza depositada en nosotros es un privilegio que valoramos inmensamente. Buscamos ganarnos la confianza de nuestros clientes todos los días ofreciendo productos y servicios seguros y de alta calidad que cumplan con las expectativas y ayuden a nuestros clientes a innovar, impulsando el crecimiento mutuo.

Al elegir VTEX, está eligiendo un socio confiable y dedicado a la seguridad de sus intereses. Su tranquilidad y satisfacción son nuestra recompensa y seguiremos trabajando incansablemente para mantener esa relación de confianza. Estamos aquí para usted, protegiendo lo más importante.

Las empresas nos eligen como socio estratégico para acelerar la transformación del comercio digital y ofrecer iniciativas generadoras de ingresos.

Incluso después de 20 años y de todo el impacto que hemos generado en el ecosistema del comercio electrónico, todavía conservamos la mentalidad del primer día que nos trajo hasta aquí.

¡Estamos en un camino sin fin para conectar al mundo a través de la forma en que las personas comercian y te invitamos a entrar en nuestro futuro y ser parte de esta jornada!

Siempre recuerda: #WeAreTrusted.

Recursos

Security Help Center

Este sitio es un canal público que actúa como un servicio de ayuda para los clientes y prospectos de VTEX. Ofrece soluciones a una gran variedad de preguntas y cuenta con una base de información muy amplia.

VTEX Trusthub

Es nuestro sitio público para abordar las preocupaciones relacionadas con asuntos legales, cumplimiento, privacidad y seguridad.

Security FAQ

Este espacio es el único que es privado, al que solo tienen acceso los clientes VTEX a través de su nombre de usuario y contraseña. Se trata de un portal reservado en el que proporcionamos nuestras respuestas a las preguntas de seguridad más frecuentes para apoyar la resolución de dudas y completar el *Risk Assessment*.

VTEX Healthcheck

Es una página pública que tiene como objetivo monitorear el status de los servicios de nuestra plataforma. En HealthCheck, se realizan más de 100 pruebas por minuto. A través de este dashboard, puedes seguir el estado de cada módulo en tiempo real.

Status VTEX

En VTEX Status, puedes seguir la estabilidad de la plataforma en tiempo real, así como acceder a todo el historial de incidentes. Nuestro equipo informa los eventos cada vez que nuestro sistema de monitoreo automático identifica una inestabilidad en los módulos de la plataforma.

Vea más en: vtex.com

VTEX

The Enterprise
Digital Commerce
Platform