VTEX

The Enterprise
Digital Commerce
Platform

Postura de seguridad de VTEX

VTEX Security

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. Nuestras prácticas de seguridad están integradas en todas nuestras tecnologías, personal 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 27001:2013 para medir la madurez de nuestros programas de seguridad. Este norma es el estándar y la referencia internacional para la gestión de la seguridad de la información. Utilizamos este marco para evaluar e identificar áreas de mejora.

Nuestros valores

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. ¡Somos fiables, seguros y escalables!

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 que siempre aprende aceptando retos incómodos.

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.

Puedes ver más detalles sobre nuestros procesos de seguridad haciendo clic aquí.

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. La política se revisa anualmente dentro de nuestro proceso de gestión de documentos. Nuestra política de seguridad de la información está orientada a la norma ISO IEC 27001, marcos con las mejores prácticas de seguridad, leyes de protección de datos y otras obligaciones aplicables al contexto de VTEX. Nuestros clientes pueden acceder a nuestra versión pública a través del Portal de Administración de la Tienda. Todos nuestros documentos son revisados dentro de una ventana anual 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 está estructurado y dedicado para apoyar los principales procesos de seguridad. 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; periódicamente estos controles son auditados por empresas externas. Actualmente contamos con las siguientes certificaciones.

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.

Educación y concienciación sobre seguridad

Consideramos que nuestros colaboradores son una línea de defensa fundamental para proteger los datos de nuestra empresa y de nuestros clientes. Contamos con un equipo dedicado que impulsa la concienciación, compromiso y educación de nuestros colaboradores sobre las mejores prácticas de seguridad y la adopción de recursos de seguridad en VTEX. Nuestros programas integrales incluyen la incorporación de nuevos colaboradores y una capacitación anual de seguridad.

Capacitamos a los colaboradores para que identifiquen los vectores de ataque más frecuentes, como los emails de phishing, y que sepan cómo denunciarlos. Esto se aplica a todos los colaboradores y terceros. A través de indicadores de rendimiento, medimos la eficacia de los programas de concienciación de seguridad.

Cada año, establecemos un calendario para nuestro programa de formación y siempre revisamos nuestros contenidos y tomamos en cuenta los escenarios actuales y los vectores de ataque y vulnerabilidades.

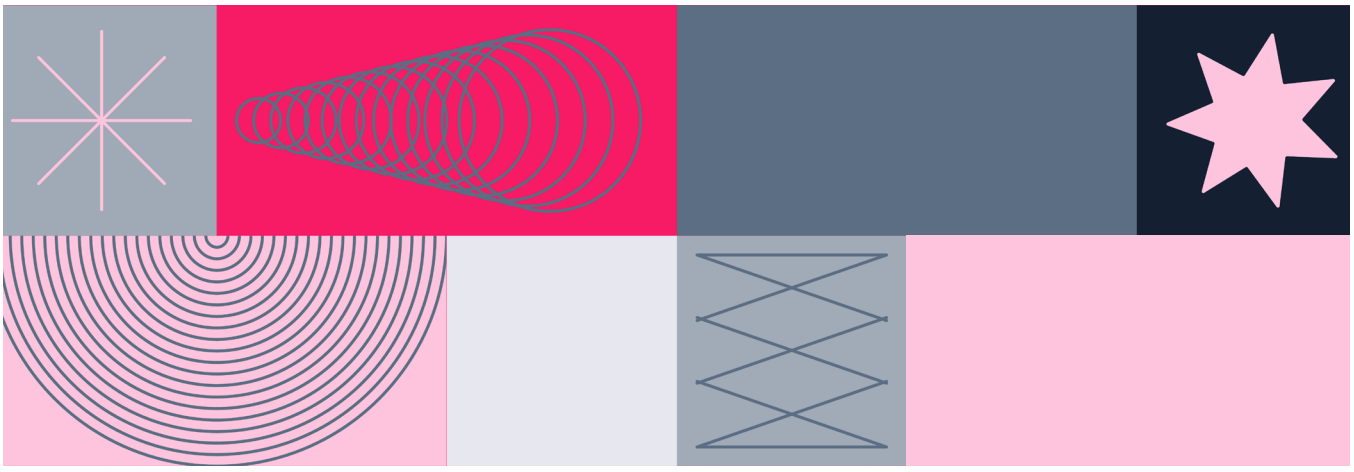
Tenemos un canal ética para denunciar comportamientos inadecuados. Además, tenemos un proceso de sanciones que se aplica a los colaboradores que no cumplen con las políticas y normas de seguridad de la información establecidas.

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 e 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. También cabe destacar que 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 su ciclo de vida.

AWS utiliza normas rigurosas sobre cómo instalar, mantener y, finalmente, 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 y gestionar los sistemas utilizando únicamente aplicaciones hospedadas a través de un cliente de escritorio remoto seguro: infraestructura de escritorio virtual (VDI).

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; añadir y remover usuarios de la organización forma parte de los procesos de contratación y desvinculación. 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. Después de la desvinculación, se bloquean las cuentas privilegiadas, se terminan las conexiones activas y se remueven los tokens de autenticación de dos factores. 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 datos

Para nosotros, en VTEX, los datos 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: restringido, confidencial o público. Por ejemplo, los siguientes tipos de datos se consideran confidenciales y críticos dentro de nuestra escala de calificación de la información:

- Información sobre tarjetas de pago (PCI-DSS)
- Información personal identificable (PII)

Por ello, se adoptan estrictas medidas de seguridad para la clasificación y protección de estos datos. Nuestra información crítica debe estar siempre encriptada no solo en tránsito, sino también en reposo. Por lo tanto, todos los datos confidencial están encriptados. Los datos en tránsito se encriptan con TLS 1.2 o superior y los datos en reposo con el algoritmo AES-256 o RSA con claves de al menos 2048 bits.

Retención de datos

VTEX no elimina activamente ningún dato propietario de nuestros clientes sin su expresa expresión de voluntad. Esto también incluye casos de terminación del contrato del cliente con VTEX, donde se nos solicita eliminar los datos del cliente, incluidos los datos de identificación personal.

Transferencia segura de datos

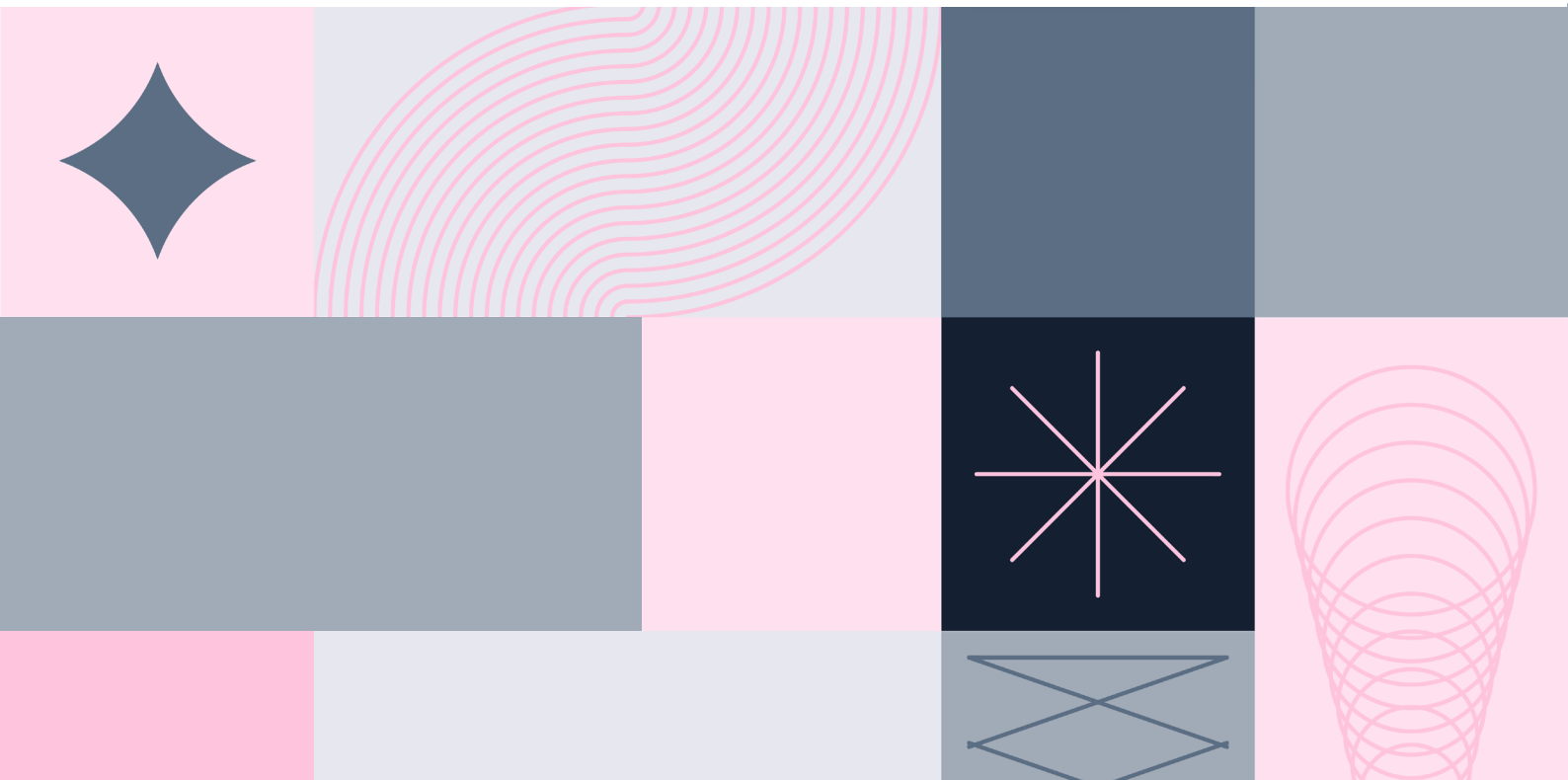
Como ya se ha mencionado, para VTEX, los datos de nuestros clientes son extremadamente valiosos y preservamos su integridad y confidencialidad durante todo su ciclo de vida. Por eso, VTEX no transfiere ni divulga los datos de los clientes, salvo para prestar los servicios y prevenir o resolver problemas técnicos o de servicio, a petición del cliente en relación con cuestiones de soporte o según lo exija la ley. 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).

VTEX está plenamente comprometido con el cumplimiento de las regulaciones de protección de datos. Por eso, constantemente actualizamos nuestros procedimientos de seguridad y privacidad de datos personales de acuerdo con todas las leyes de protección de datos aplicables en los países donde prestamos servicios.

Controles criptográficos

VTEX maneja datos críticos de los clientes, por lo que la encriptación de la información es esencial. TLS y su predecesor, SSL, son protocolos criptográficos para la comunicación segura a través de redes informáticas. Son la S de HTTPS. Esta tecnología no evita que los delincuentes intercepten la conexión entre el consumidor y la tienda, pero imposibilita la lectura de los datos, que solo pueden ser desencriptados dentro de su servidor con la posesión de la clave privada generada por el sistema. VTEX ha establecido normas de criptografía para todos sus clientes, tanto para los datos en reposo como para los datos en tránsito.

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. Las claves AWS KMS (claves de KMS) son el recurso de AWS KMS. Se puede utilizar una clave de KMS para encriptar, desencriptar y reencriptar los datos. También se puede generar claves de datos que pueden utilizarse fuera de AWS KMS.



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. Antes de elegir un local, AWS realiza una primera evaluación medioambiental y geográfica. 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 solo permite que los colaboradores aprobados tengan acceso físico al centro 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+

VTEX tiene oficinas en todo el mundo. Tenemos un control de seguridad física como monitoreo y control de acceso en todas las oficinas de VTEX. El acceso físico está controlado en los puntos de entrada del edificio por el equipo de seguridad profesional que utiliza sistemas de vigilancia como torniquetes de acceso y otros medios electrónicos. Este equipo registra las salidas y entradas de las personas autorizadas a través de registros.

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 parches 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.
- Monitoreo de los cambios en los archivos de configuración críticos para recibir notificaciones de los cambios en dichos archivos.
- 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 este dominio es definir cómo se controlan los cambios realizados en los sistemas de información. Lo que el dominio quiere es que la organización gestione estos cambios para que no actúen 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. Estas consecuencias no siempre son muy claras y pueden ocultar daños graves. Al realizar este análisis, la organización aumenta las posibilidades de elegir la mejor idea y no la primera y, además, de no verse sorprendida negativamente después.

Por eso, VTEX ha establecido un procedimiento para controlar los cambios. Este procedimiento incluye un estudio de las alternativas para llevar a cabo el cambio y sus consecuencias. Además, cada cambio debe ser 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 a escala 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; además, 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

Nuestra prioridad es proteger los datos de nuestros clientes y para ello contamos con procedimientos complejos que garantizan el debido monitoreo de nuestros recursos con el objetivo principal de identificar posibles amenazas y actuar ante ellas con rapidez y eficacia. Nuestro equipo de detección y respuesta se dedica a desarrollar inteligencia contra las amenazas a través de la investigación y el análisis relacionados con los incidentes de seguridad. 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 líneas base de seguridad, la actualización de parches, 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

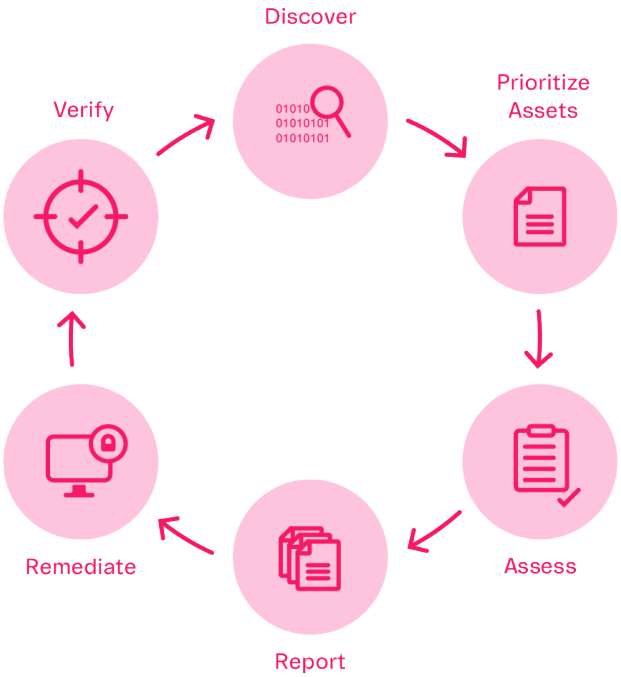
VTEX evalúa rigurosamente los recursos probando e identificando las vulnerabilidades mediante la realización de escaneos y pruebas de penetración en nuestros entornos.

Tenemos un calendario de verificaciones de vulnerabilidad; estas comprobaciones se producen periódicamente y según la criticidad del alcance.

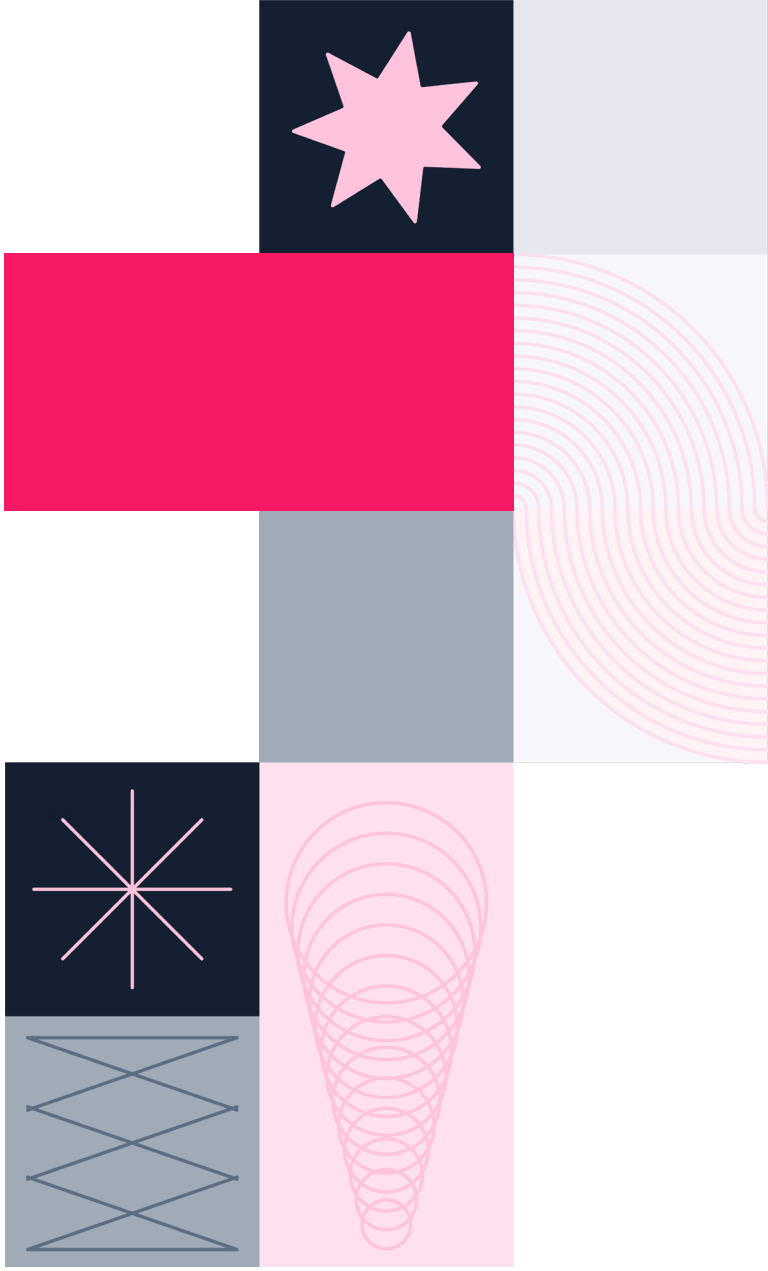
Las vulnerabilidades identificadas se abordan en nuestro proceso de gestión de vulnerabilidades y son debidamente gestionadas a lo largo de su ciclo de vida.

Además, nuestros clientes son libres de realizar pruebas en sus tiendas de forma abierta y transparente. En una solución multiusuario como VTEX, esto significa que toda la plataforma se prueba constantemente a lo largo del año.

Nuestros clientes deben informar de cualquier vulnerabilidad que identifiquen en la plataforma VTEX. Tenemos un proceso para recibir y evaluar los informes de los clientes, y si es confirmado por el equipo de seguridad de VTEX, se aborda internamente para su corrección, siempre observando el nivel de criticidad y riesgo a la plataforma.



Seguridad perimetral



VTEX utiliza un enfoque multicapa para la protección de los 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, tanto en nuestra red interna como en internet. Esta solución es parte de la mitigación de los ataques DDoS. Cuando se identifica un evento asociado a un ataque DDoS, 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.

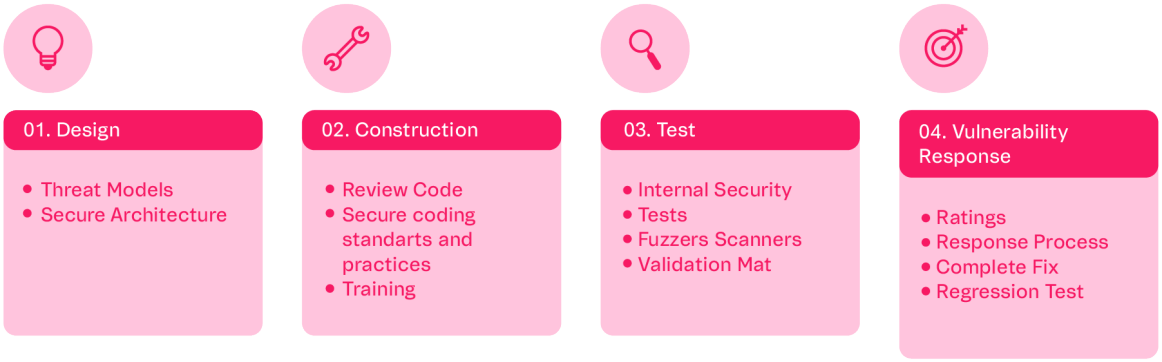
Ciclo de desarrollo seguro

En VTEX, integramos los requisitos de seguridad en todas las fases del ciclo de desarrollo de la plataforma y utilizamos el proceso Secure Software Development Lifecycle (SSDLC).

A través de esta metodología, nuestros ingenieros de desarrollo trabajan con procesos ágiles y toman en cuenta los puntos y preocupaciones de seguridad de nuestros productos. Innovamos teniendo en cuenta las constantes demandas del mercado; un ejemplo de ello es VTEX IO, una plataforma nativa capaz de ayudar en la entrega de soluciones empresariales con más agilidad y seguridad. Aprende más sobre VTEX IO.

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.



Gestión y evaluación de terceros

VTEX garantiza que sus proveedores subcontratados respetan y siguen las mismas políticas de seguridad que VTEX ofrece. Todos nuestros proveedores de infraestructura externos están listados en este link: https://vtex.com/br-pt/subprocessors/.

VTEX tiene establecido un proceso de análisis de riesgos de seguridad para los proveedores críticos, es decir, los que tratarán datos confidenciales.

Evaluamos la madurez y la postura de seguridad de estos proveedores para entender cuáles son los riesgos y las lagunas y abordar estos puntos para una adecuada toma de decisiones interna. Además, todos los proveedores pasan por un proceso de evaluación de riesgos para garantizar el cumplimiento de las leyes de protección de datos y el análisis de riesgos comerciales, y solo después de todas las evaluaciones necesarias, y con un nivel de madurez adecuado, se procede a la contratación.

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. Consideramos los procesos de mapeo de riesgos para evaluar la probabilidad y el impacto de las amenazas que pueden afectar nuestra capacidad estratégica.

Además, 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.

Utilizamos un proceso de gestión que aborda todo el ciclo de vida del riesgo y que garantiza que los riesgos identificados se traten, mitiguen y comuniquen, según la relevancia. Nuestro proceso abarca cinco pasos principales.

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. El objetivo es que el seguimiento de los pasos establecidos en el plan proporcione la base para un retorno relativamente rápido y fácil al funcionamiento cotidiano de nuestro negocio, independientemente de la causa.

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; contiene instrucciones sobre qué acciones tomar y cómo responder a incidentes no planificados y caracterizados como crisis. Estos incidentes pueden estar relacionados con desastres naturales, ciberataques y cualquier otro evento disruptivo.

Madurez de la seguridad

Para mejorar continuamente nuestra postura de seguridad, utilizamos la norma ISO 27001:2013 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. Utilizamos este marco para evaluar e identificar áreas de mejora. La estructura de la norma está basada en dominios y fue desarrollada en 1992 por un departamento del gobierno británico que estableció un código de prácticas relacionado con la gestión de la seguridad de la información.

A lo largo de los años, miles de profesionales han contribuido con sus conocimientos y experiencia al establecimiento de una norma estable y madura, pero que sin duda seguirá evolucionando con el tiempo.

La adopción de la norma ISO 27001 sirve para que las organizaciones adopten un modelo adecuado para establecer, implementar, operar, monitorear, revisar y gestionar un sistema de gestión de la seguridad de la información.

Este sistema de gestión de la seguridad de la información (SGSI) es, según los principios de la norma ISO 27001, un modelo holístico para abordar la seguridad que es independiente de marcas y fabricantes de teconología.

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. Al evaluar las puntuaciones actuales y deseadas de la norma ISO 27001, podemos cuantificar y seguir la madurez general de nuestra postura de seguridad a lo largo del tiempo.

Conclusión

En VTEX, nuestro mayor compromiso es la seguridad de nuestros clientes. Somos líderes en la aceleración de la transformación del comercio digital en América Latina y nos estamos expandiendo globalmente. Nuestra plataforma está diseñada para estándares y funcionalidades de nivel empresarial, y aproximadamente el 80 % de nuestro GMV proviene de grandes empresas de primer nivel (es decir, clientes con un GMV de más de USD 10 millones al año). Más de 2000 clientes con más de 2500 tiendas online activas en 32 países confían en nosotros para conectarse con sus consumidores de forma significativa. Somos fiables, escalables y seguros. Entendemos que nuestros clientes dependen de la seguridad, el rendimiento y la transparencia de nuestros sistemas y servicios VTEX.

Ofrecemos servicios de alta seguridad que ayudan a nuestros clientes a innovar para satisfacer las demandas del mercado, lo que a su vez impulsa el crecimiento mutuo. Para apoyar el éxito de nuestros clientes, también compartimos y fomentamos las mejores prácticas de seguridad con ellos utilizando una variedad de canales, incluyendo nuestro sitio web, blogs, medios sociales, herramientas y funcionalidades.

Las empresas nos eligen como partner estratégico para acelerar la transformación del comercio digital y ofrecer iniciativas de generación de ingresos. Ofrecemos nuestra plataforma a través de un modelo de ingresos por suscripción que incluye componentes fijos y variables basados en el GMV.

¿Qué representa todo este éxito? Incluso después de 20 años y de todo el impacto que hemos aportado al ecosistema del comercio electrónico, seguimos manteniendo la mentalidad del primer día que nos ha traído 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
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
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.

See more at: vtex.com

The Enterprise
Digital Commerce
Platform