VELTRIX ENGINE

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Versión: 1.0

Última actualización: Junio de 2026

INTRODUCCIÓN

La seguridad de la información constituye uno de los principios fundamentales de Veltrix Engine.

Nuestro objetivo es proteger la confidencialidad, integridad, disponibilidad y resiliencia de la información procesada por nuestros sistemas, así como reducir los riesgos derivados de amenazas tecnológicas, errores humanos, accesos no autorizados y otros eventos que puedan afectar la continuidad del Servicio.

La presente Política establece los principios generales bajo los cuales Veltrix Engine diseña, opera y mejora continuamente sus controles de seguridad.

Esta Política complementa los Términos y Condiciones, el Aviso de Privacidad, la Política de Uso Aceptable y demás documentos legales de la Plataforma.

---

1. OBJETIVO

El objetivo de esta Política es establecer los principios generales para proteger:

- la información de los Usuarios;
- la infraestructura tecnológica;
- las aplicaciones;
- las bases de datos;
- los servicios en la nube;
- los procesos internos;
- los activos digitales;
- las comunicaciones electrónicas;

- la continuidad operativa de Veltrix Engine.

---

2. ALCANCE

Esta Política aplica a:

- el sitio web oficial;
- la plataforma web;
- el software de escritorio;
- aplicaciones móviles;
- infraestructura en la nube;
- APIs;
- servicios internos;
- herramientas administrativas;
- módulos de inteligencia artificial;
- Radar B2B;
- Vendedor IA;
- servicios de soporte;
- proveedores tecnológicos que participen en la operación del Servicio, cuando resulte aplicable.

---

3. PRINCIPIOS DE SEGURIDAD

Veltrix Engine procura desarrollar sus procesos de seguridad considerando los siguientes principios:

Confidencialidad

La información debe estar disponible únicamente para personas autorizadas.

Integridad

La información deberá mantenerse completa, consistente y protegida contra modificaciones no autorizadas.

Disponibilidad

Los sistemas deberán diseñarse procurando mantener la continuidad del Servicio dentro de límites razonables.

Trazabilidad

Las operaciones relevantes podrán registrarse mediante mecanismos de auditoría cuando resulte apropiado para fines de seguridad.

Mínimo privilegio

Cada usuario, proceso o componente tecnológico deberá disponer únicamente de los permisos necesarios para realizar sus funciones.

Defensa en profundidad

La protección de la Plataforma podrá implementarse mediante múltiples capas de seguridad complementarias.

Mejora continua

Los controles de seguridad podrán actualizarse conforme evolucionen las amenazas, la tecnología y las necesidades operativas de Veltrix Engine.

---

4. MODELO DE RESPONSABILIDAD COMPARTIDA

La seguridad de la información constituye una responsabilidad compartida entre Veltrix Engine y cada Usuario.

Veltrix Engine será responsable de implementar medidas razonables destinadas a proteger la infraestructura bajo su control.

El Usuario será responsable de proteger:

- sus dispositivos;
- sus credenciales;
- las personas autorizadas para acceder a la Cuenta;
- la configuración de sus automatizaciones;
- la información que decida incorporar al Servicio.

La eficacia global de la seguridad dependerá de la colaboración de ambas partes.

---

5. GESTIÓN DE RIESGOS

Veltrix Engine procura identificar, evaluar y gestionar riesgos relacionados con:

- accesos no autorizados;
- pérdida de información;
- errores humanos;
- vulnerabilidades tecnológicas;
- ataques cibernéticos;
- indisponibilidad del Servicio;
- fallas de infraestructura;
- amenazas internas;
- amenazas externas;
- cambios tecnológicos.

La evaluación de riesgos podrá revisarse periódicamente conforme evolucionen las condiciones operativas.

---

6. CLASIFICACIÓN DE LA INFORMACIÓN

Con fines de protección, la información administrada por Veltrix Engine podrá clasificarse conforme a su nivel de sensibilidad.

De manera general, podrán existir categorías como:

Información pública

Información destinada a ser conocida libremente.

Ejemplos:

- documentación pública;
- información del sitio web;
- material promocional.

Información de uso interno

Información utilizada para la operación cotidiana de la Empresa.

Su acceso podrá limitarse al personal autorizado.

Información confidencial

Información cuya divulgación no autorizada podría afectar a Veltrix Engine o a sus Usuarios.

Entre otros ejemplos:

- configuraciones internas;
- registros técnicos;
- procesos administrativos;
- documentación operativa;
- determinados datos comerciales.

Información restringida

Información que requiere un nivel elevado de protección debido a su sensibilidad.

Podrá incluir, entre otros:

- credenciales;
- claves criptográficas;
- configuraciones críticas;

- registros de seguridad;
- información protegida por obligaciones legales.

---

7. CONTROL DE ACCESO

Veltrix Engine procura implementar mecanismos destinados a garantizar que únicamente personas autorizadas accedan a la información correspondiente.

Las medidas podrán incluir:

- autenticación;
- autorización;
- segmentación de privilegios;
- control de sesiones;
- verificación de identidad;
- revocación de accesos cuando resulte necesario.

---

8. GESTIÓN DE CREDENCIALES

Las credenciales utilizadas para acceder a la Plataforma deberán mantenerse bajo estricta confidencialidad.

Veltrix Engine recomienda:

- utilizar contraseñas robustas;
- no reutilizar contraseñas;
- activar mecanismos adicionales de autenticación cuando estén disponibles;
- cambiar credenciales cuando exista sospecha de compromiso;
- evitar compartir accesos.

Las contraseñas nunca deberán enviarse por correo electrónico ni compartirse con terceros no autorizados.

---

9. AUTENTICACIÓN

La Plataforma podrá implementar distintos mecanismos de autenticación dependiendo del tipo de Servicio utilizado.

Entre ellos podrán encontrarse:

- usuario y contraseña;
- autenticación multifactor;
- tokens de acceso;
- sesiones autenticadas;
- claves API;
- certificados digitales.

Veltrix Engine podrá modificar los mecanismos de autenticación cuando resulte necesario para fortalecer la seguridad.

---

10. GESTIÓN DE SESIONES

Con el fin de reducir riesgos asociados al acceso no autorizado, la Plataforma podrá implementar controles relacionados con las sesiones de usuario, incluyendo:

- expiración automática por inactividad;
- cierre de sesiones comprometidas;
- invalidación de sesiones al cambiar credenciales;
- limitación de sesiones simultáneas cuando resulte apropiado;
- monitoreo de accesos inusuales.

---

11. SEGREGACIÓN DE PRIVILEGIOS

Los permisos otorgados a usuarios, procesos internos y componentes tecnológicos procurarán ajustarse al principio de mínimo privilegio.

El acceso a funciones administrativas, configuraciones críticas y herramientas internas será restringido únicamente a quienes requieran dicho acceso para el desempeño de sus funciones.

La asignación y revocación de privilegios podrá revisarse periódicamente.

---

12. GESTIÓN DE IDENTIDADES

Veltrix Engine podrá implementar procesos destinados a administrar el ciclo de vida de las identidades digitales, incluyendo:

- creación de cuentas;
- modificación de permisos;
- suspensión de accesos;
- eliminación de cuentas;
- verificación de identidad cuando resulte necesaria.

Estos procesos tienen como finalidad reducir riesgos derivados de accesos no autorizados o privilegios excesivos.

13. SEGURIDAD DE LA INFRAESTRUCTURA

Veltrix Engine procura diseñar y operar su infraestructura tecnológica siguiendo principios de seguridad por capas (Defense in Depth), resiliencia y reducción de riesgos.

Las medidas implementadas podrán incluir, entre otras:

- segmentación lógica de servicios;
- separación entre ambientes;
- controles de acceso administrativos;
- monitoreo continuo;
- endurecimiento (hardening) de sistemas;
- protección perimetral;
- mecanismos de alta disponibilidad cuando resulten técnicamente viables.

La arquitectura podrá evolucionar conforme cambien las necesidades operativas y los riesgos tecnológicos.

---

14. SEGURIDAD DE SERVIDORES

Los servidores utilizados para operar los servicios de Veltrix Engine podrán incorporar medidas destinadas a reducir la superficie de ataque, incluyendo:

- configuración segura de sistemas operativos;
- eliminación de servicios innecesarios;

- control de privilegios;
- autenticación reforzada;
- monitoreo de integridad;
- revisión de configuraciones críticas;
- actualización periódica de componentes.

Los servidores podrán ser administrados directamente por Veltrix Engine o por proveedores especializados de infraestructura.

---

15. SEGURIDAD EN LA NUBE

Cuando el Servicio utilice infraestructura en la nube, Veltrix Engine procurará seleccionar proveedores reconocidos por la industria que implementen controles de seguridad apropiados para sus servicios.

La seguridad física de los centros de datos, la infraestructura subyacente y determinados controles de red podrán ser responsabilidad del proveedor correspondiente, conforme al modelo de responsabilidad compartida.

---

16. CIFRADO DE INFORMACIÓN

Veltrix Engine procura utilizar mecanismos criptográficos apropiados para proteger la información durante su transmisión y, cuando resulte técnicamente viable, durante su almacenamiento.

Dependiendo del servicio y la naturaleza de la información, podrán utilizarse mecanismos como:

- cifrado de comunicaciones mediante protocolos seguros;
- almacenamiento cifrado;
- protección de credenciales;
- gestión segura de claves;
- funciones criptográficas para verificación de integridad.

Los algoritmos y mecanismos utilizados podrán modificarse conforme evolucionen las prácticas recomendadas por la industria.

---

17. PROTECCIÓN DE CONTRASEÑAS

Veltrix Engine no almacena contraseñas de usuarios en texto plano.

Las credenciales de autenticación se procesan utilizando mecanismos diseñados para reducir el riesgo de divulgación en caso de acceso no autorizado a los sistemas.

Los procesos internos procuran evitar la exposición innecesaria de información relacionada con la autenticación de los Usuarios.

---

18. SEGURIDAD DE BASES DE DATOS

Las bases de datos utilizadas por Veltrix Engine podrán protegerse mediante diversas medidas técnicas y administrativas, incluyendo:

- autenticación;
- autorización;
- segmentación de accesos;
- monitoreo;
- respaldos;
- registros de actividad;
- controles de disponibilidad;
- mecanismos de recuperación.

El acceso directo a las bases de datos se limitará al personal y procesos autorizados.

---

19. COPIAS DE SEGURIDAD (BACKUPS)

Veltrix Engine podrá realizar copias de seguridad destinadas a facilitar la recuperación de información ante incidentes tecnológicos.

Los respaldos podrán realizarse considerando:

- periodicidad adecuada;
- redundancia;
- protección contra modificaciones no autorizadas;
- verificación de consistencia;
- almacenamiento seguro.

La existencia de respaldos no constituye una garantía absoluta de recuperación de toda la información en cualquier circunstancia.

20. RECUPERACIÓN ANTE INCIDENTES

Veltrix Engine procura mantener procedimientos internos destinados a facilitar la recuperación de los servicios cuando se presenten incidentes tecnológicos relevantes.

Estos procedimientos podrán incluir:

- restauración de respaldos;
- recuperación de servicios;
- verificación de integridad;
- validación de configuraciones;
- monitoreo posterior a la recuperación.

Los tiempos efectivos de recuperación dependerán de la naturaleza y complejidad del incidente.

---

21. GESTIÓN DE VULNERABILIDADES

Veltrix Engine procura identificar y atender vulnerabilidades de seguridad mediante procesos internos de evaluación y mejora continua.

Las actividades podrán incluir:

- revisión de configuraciones;
- análisis de componentes;
- evaluación de dependencias;
- actualización de bibliotecas;
- corrección de vulnerabilidades conocidas;
- seguimiento de alertas de seguridad.

La prioridad de atención dependerá del nivel de riesgo identificado.

---

22. ACTUALIZACIONES Y PARCHES

Los componentes tecnológicos utilizados por Veltrix Engine podrán actualizarse periódicamente para:

- corregir vulnerabilidades;
- mejorar estabilidad;
- fortalecer la seguridad;
- incorporar nuevas funcionalidades;
- mantener compatibilidad con tecnologías soportadas.

Cuando resulte posible, las actualizaciones se planificarán procurando minimizar el impacto sobre los Usuarios.

---

23. MONITOREO DE SEGURIDAD

Veltrix Engine podrá implementar procesos automatizados y manuales destinados a detectar eventos relevantes para la seguridad del Servicio.

El monitoreo podrá incluir:

- intentos de acceso no autorizado;
- actividad anómala;
- consumo inusual de recursos;
- errores críticos;
- disponibilidad de servicios;
- eventos relacionados con autenticación;
- comportamiento potencialmente malicioso.

El monitoreo tiene como finalidad proteger la infraestructura y mejorar la capacidad de respuesta ante incidentes.

---

24. REGISTROS DE AUDITORÍA (LOGGING)

Con fines de seguridad, diagnóstico y cumplimiento, Veltrix Engine podrá generar registros relacionados con la operación de la Plataforma.

Los registros podrán incluir información como:

- autenticaciones;
- cambios relevantes de configuración;
- operaciones administrativas;
- eventos de seguridad;
- errores del sistema;

- actividad de APIs;
- incidentes técnicos.

Los registros podrán conservarse durante el tiempo que resulte razonablemente necesario conforme a las políticas internas y la legislación aplicable.

---

25. SEGURIDAD DE LAS APIS

Las interfaces de programación (APIs) ofrecidas por Veltrix Engine podrán incorporar controles de seguridad como:

- autenticación;
- autorización;
- validación de solicitudes;
- limitación de velocidad (rate limiting);
- monitoreo;
- registros de actividad;
- controles contra abuso.

Veltrix Engine podrá modificar o restringir el acceso a APIs cuando resulte necesario para preservar la seguridad o estabilidad del Servicio.

---

26. SEGURIDAD DE LAS INTEGRACIONES

Cuando el Usuario conecte servicios externos con Veltrix Engine, dichas integraciones se realizarán utilizando los mecanismos autorizados por cada proveedor.

Veltrix Engine no controla la seguridad implementada por servicios de terceros y no puede garantizar la disponibilidad, integridad o continuidad de sus plataformas.

El Usuario será responsable de administrar adecuadamente las autorizaciones concedidas a dichos servicios.

---

27. SEGURIDAD DE LA INTELIGENCIA ARTIFICIAL

Las funcionalidades basadas en inteligencia artificial podrán implementar controles destinados a reducir riesgos relacionados con:

- generación de contenido inapropiado;
- abuso de automatizaciones;
- acceso indebido a información;
- utilización maliciosa de modelos;
- uso contrario a la legislación aplicable.

No obstante, ningún sistema de inteligencia artificial puede garantizar resultados completamente libres de errores, sesgos o inexactitudes.

El Usuario deberá revisar siempre las respuestas generadas antes de utilizarlas para la toma de decisiones.

---

28. DESARROLLO SEGURO (SECURE SDLC)

Veltrix Engine procura incorporar prácticas de seguridad durante el ciclo de desarrollo del Software.

Estas prácticas podrán incluir:

- revisión de código;
- validación de entradas;
- manejo seguro de errores;
- control de excepciones;
- pruebas funcionales;
- pruebas de regresión;
- actualización de dependencias;
- control de versiones;
- revisión de cambios antes de su publicación.

La incorporación de controles de seguridad durante el desarrollo tiene como finalidad reducir vulnerabilidades antes de que las funcionalidades sean puestas a disposición de los Usuarios.

---

29. GESTIÓN DE DEPENDENCIAS

Veltrix Engine podrá utilizar componentes, bibliotecas y herramientas desarrolladas por terceros.

Cuando resulte razonablemente posible, se procurará:

- mantener versiones soportadas;
- revisar vulnerabilidades conocidas;
- actualizar componentes críticos;
- sustituir dependencias obsoletas;
- minimizar riesgos derivados de software de terceros.

---

30. PRUEBAS ANTES DE LA PUBLICACIÓN

Las nuevas funcionalidades podrán someterse a procesos internos de validación antes de su liberación.

Dependiendo de la naturaleza del cambio, podrán realizarse:

- pruebas funcionales;
- pruebas de integración;
- validaciones de estabilidad;
- pruebas de compatibilidad;
- verificaciones de seguridad;
- revisión de rendimiento.

El alcance de estas pruebas podrá variar según la complejidad de cada actualización.

31. GESTIÓN DE INCIDENTES DE SEGURIDAD

Veltrix Engine procura mantener procedimientos internos destinados a identificar, analizar, contener, mitigar y documentar incidentes que puedan afectar la seguridad de la Plataforma o de la información procesada por ella.

Cuando resulte apropiado, un incidente podrá gestionarse mediante etapas como:

- detección;
- clasificación;
- análisis;
- contención;
- erradicación;
- recuperación;
- verificación;
- documentación;
- revisión posterior al incidente.

Cada incidente será evaluado considerando su naturaleza, impacto potencial y nivel de riesgo.

---

32. REPORTE DE INCIDENTES

Los Usuarios que detecten actividades sospechosas o posibles vulnerabilidades deberán comunicarlo tan pronto como sea razonablemente posible utilizando los canales oficiales de Veltrix Engine.

Los reportes podrán incluir, entre otros:

- accesos no autorizados;
- intentos de fraude;
- comportamiento inusual del sistema;
- posibles vulnerabilidades;
- errores críticos;
- exposición accidental de información;
- actividad potencialmente maliciosa.

La pronta notificación contribuye a reducir el impacto de los incidentes y facilita su investigación.

---

33. NOTIFICACIÓN DE INCIDENTES RELEVANTES

Cuando un incidente de seguridad pueda afectar significativamente la confidencialidad, integridad o disponibilidad de la información de los Usuarios, Veltrix Engine procurará realizar las notificaciones que resulten apropiadas conforme a:

- la legislación aplicable;

- la naturaleza del incidente;
- la información disponible al momento;
- las recomendaciones de las autoridades competentes, cuando corresponda.

Las notificaciones podrán realizarse mediante correo electrónico, avisos dentro de la Plataforma o cualquier otro medio razonablemente adecuado.

---

34. CONTINUIDAD DEL NEGOCIO

Veltrix Engine procura mantener procesos orientados a favorecer la continuidad de sus operaciones ante eventos que puedan afectar la prestación del Servicio.

Estos procesos podrán contemplar:

- recuperación de infraestructura;
- restauración de servicios;
- continuidad operativa;
- redundancia de componentes cuando resulte viable;
- procedimientos internos de contingencia;
- priorización de servicios críticos.

La continuidad del negocio dependerá de diversos factores, incluyendo la naturaleza del incidente y la disponibilidad de servicios de terceros.

---

35. RECUPERACIÓN ANTE DESASTRES

Veltrix Engine podrá mantener procedimientos destinados a facilitar la recuperación del Servicio frente a eventos extraordinarios que afecten la infraestructura tecnológica.

Estos procedimientos podrán incluir:

- restauración de respaldos;
- recuperación de configuraciones;
- reconstrucción de infraestructura;
- validación de integridad;
- restablecimiento gradual de servicios;
- monitoreo posterior a la recuperación.

La existencia de un plan de recuperación no constituye garantía de restauración inmediata ni de recuperación absoluta de toda la información.

---

36. SEGURIDAD DEL PERSONAL

Las personas autorizadas para administrar componentes críticos de Veltrix Engine deberán actuar conforme a los principios de confidencialidad, integridad, responsabilidad y protección de la información.

Cuando resulte apropiado podrán implementarse medidas como:

- asignación limitada de privilegios;
- autenticación reforzada;
- registros de actividad administrativa;
- revisión periódica de permisos;
- revocación de accesos cuando dejen de ser necesarios.

---

37. SEGURIDAD DE PROVEEDORES

Veltrix Engine podrá utilizar servicios prestados por proveedores especializados para apoyar la operación de la Plataforma.

Siempre que resulte razonablemente posible, se procurará seleccionar proveedores que implementen prácticas adecuadas de seguridad para los servicios que proporcionan.

Cada proveedor será responsable de los controles implementados dentro de su propia infraestructura y del cumplimiento de las obligaciones asumidas frente a Veltrix Engine.

---

38. GESTIÓN DE CAMBIOS

Las modificaciones relevantes realizadas sobre la infraestructura, aplicaciones o componentes tecnológicos podrán someterse a procesos internos de revisión antes de su implementación.

Dependiendo de la naturaleza del cambio, podrán realizarse:

- evaluación técnica;

- análisis de riesgos;
- validación funcional;
- pruebas de compatibilidad;
- revisión de seguridad;
- documentación del cambio.

El objetivo es reducir el riesgo de introducir vulnerabilidades o afectar la estabilidad del Servicio.

---

39. DOCUMENTACIÓN Y AUDITORÍA

Veltrix Engine podrá mantener documentación relacionada con sus procesos de seguridad, incluyendo:

- procedimientos internos;
- registros técnicos;
- configuraciones relevantes;
- historial de cambios;
- reportes de incidentes;
- evidencia de mantenimiento;
- registros de auditoría.

La documentación podrá utilizarse para fines de mejora continua, cumplimiento normativo, investigación de incidentes y fortalecimiento de la seguridad.

---

40. MEJORA CONTINUA

La seguridad constituye un proceso permanente.

Veltrix Engine podrá revisar periódicamente sus procesos, controles y mecanismos tecnológicos con el propósito de:

- fortalecer la protección de la información;
- adaptarse a nuevas amenazas;
- incorporar mejores prácticas de la industria;
- mejorar la resiliencia operativa;
- optimizar procesos internos.

Las medidas implementadas podrán evolucionar conforme avance la tecnología y cambien las necesidades del Servicio.

41. CUMPLIMIENTO NORMATIVO

Veltrix Engine procura operar conforme a la legislación aplicable en materia de:

- protección de datos personales;
- comercio electrónico;
- propiedad intelectual;
- seguridad informática;
- obligaciones fiscales;
- demás disposiciones que resulten aplicables a la prestación de sus servicios.

Cuando resulte necesario, las políticas internas podrán actualizarse para reflejar cambios regulatorios.

---

42. RESPONSABILIDAD COMPARTIDA

La protección efectiva de la información requiere la colaboración tanto de Veltrix Engine como del Usuario.

Veltrix Engine implementa medidas razonables para proteger la infraestructura bajo su control.

El Usuario es responsable, entre otros aspectos, de:

- proteger sus dispositivos;
- mantener actualizados sus sistemas;
- utilizar contraseñas robustas;
- proteger sus credenciales;
- revisar las automatizaciones configuradas;
- controlar el acceso de su personal autorizado;
- cumplir las políticas de seguridad aplicables.

---

43. LIMITACIONES DE SEGURIDAD

Aunque Veltrix Engine procura implementar controles técnicos y organizacionales adecuados, ningún sistema informático puede garantizar seguridad absoluta.

En consecuencia, no puede garantizarse que los servicios permanezcan permanentemente libres de:

- vulnerabilidades;
- ataques informáticos;
- interrupciones;
- errores de software;
- eventos derivados de terceros;
- incidentes imprevisibles;
- circunstancias de fuerza mayor.

Veltrix Engine continuará realizando esfuerzos razonables para reducir dichos riesgos y responder oportunamente cuando se presenten.

---

44. MODIFICACIONES A ESTA POLÍTICA

Veltrix Engine podrá actualizar la presente Política cuando resulte necesario para:

- incorporar nuevas tecnologías;
- fortalecer controles de seguridad;
- adaptarse a cambios regulatorios;
- mejorar procesos internos;
- responder a nuevas amenazas;
- reflejar cambios en los servicios ofrecidos.

La versión vigente estará disponible en el sitio web oficial y sustituirá a cualquier versión anterior desde su fecha de publicación.

---

45. DOCUMENTOS RELACIONADOS

La presente Política debe interpretarse conjuntamente con los siguientes documentos de Veltrix Engine:

- Términos y Condiciones.
- Aviso de Privacidad.
- Política de Uso Aceptable (AUP).
- Política de Cookies.
- Acuerdo de Procesamiento de Datos (DPA).
- Acuerdo de Nivel de Servicio (SLA).

En caso de discrepancia, prevalecerá la interpretación que resulte más adecuada conforme a la legislación aplicable y al conjunto de documentos contractuales.

---

46. LEGISLACIÓN APLICABLE

La presente Política se regirá e interpretará conforme a las leyes de los **Estados Unidos Mexicanos**.

---

47. JURISDICCIÓN

Cualquier controversia relacionada con esta Política será sometida a los tribunales competentes de **Aguascalientes, Aguascalientes, México**, salvo disposición legal imperativa en contrario.

---

48. CONTACTO

Para consultas relacionadas con seguridad de la información o para reportar incidentes de seguridad, puede comunicarse con Veltrix Engine a través de los siguientes medios oficiales:

Veltrix Engine

Sitio web oficial

https://veltrixengine.pro

Correo de soporte

soporte@veltrixengine.pro

Correo para asuntos de privacidad y cumplimiento

privacidad@veltrixengine.pro

Domicilio comercial

Aguascalientes, Aguascalientes, México.

49. ENTRADA EN VIGOR

La presente Política de Seguridad de la Información entra en vigor a partir de su fecha de publicación y permanecerá vigente hasta que sea sustituida por una versión posterior.

El uso continuo de los servicios de Veltrix Engine después de la publicación de una nueva versión implicará la aceptación de las modificaciones, en la medida permitida por la legislación aplicable.

DECLARACIÓN FINAL

En Veltrix Engine entendemos que la seguridad no es un estado permanente, sino un proceso continuo de mejora.

Por ello, procuramos fortalecer de manera constante nuestros controles técnicos, administrativos y organizacionales para proteger la información, mantener la confianza de nuestros Usuarios y ofrecer un servicio confiable, resiliente y orientado a las mejores prácticas de la industria.

© VELTRIX ENGINE

Todos los derechos reservados.