VELTRIX ENGINE

INCIDENT RESPONSE POLICY (POLÍTICA DE RESPUESTA A INCIDENTES)

Versión: 1.0
Última actualización: Junio de 2026

INTRODUCCIÓN

La presente Política de Respuesta a Incidentes define el marco operativo y técnico mediante el cual Veltrix Engine detecta, clasifica, responde, contiene y recupera incidentes de seguridad, disponibilidad o integridad que afecten sus sistemas, infraestructura o datos.

Este documento establece procedimientos internos y estándares de respuesta ante eventos críticos, con el objetivo de minimizar impacto, preservar la continuidad del servicio y proteger la información del Usuario.

---

1. OBJETO DE LA POLÍTICA

El propósito de esta política es:

- definir qué se considera un incidente;
- establecer procesos de detección y respuesta;
- asignar niveles de severidad;
- estructurar la comunicación interna y externa;
- definir tiempos de respuesta operativa;
- establecer procedimientos de contención y recuperación;
- reducir el impacto en usuarios y sistemas.

---

2. ALCANCE

Esta política aplica a:

- infraestructura cloud de Veltrix Engine;
- base de datos y almacenamiento;
- APIs y servicios backend;
- módulos de IA (Vendedor IA);
- Radar B2B;
- sistemas de autenticación;
- panel web y clientes;
- integraciones con terceros;
- endpoints públicos y privados;
- sistemas de monitoreo y logs.

---

3. DEFINICIÓN DE INCIDENTE

Se considera “incidente” cualquier evento que afecte o pueda afectar:

- la confidencialidad de la información;
- la integridad de los datos;
- la disponibilidad del servicio;
- la seguridad del sistema;
- el rendimiento crítico de la plataforma.

---

4. TIPOS DE INCIDENTES

4.1 Incidentes de seguridad

- acceso no autorizado;
- fuga de datos;
- explotación de vulnerabilidades;
- ataques externos (DDoS, inyección, etc.);
- compromiso de credenciales.

4.2 Incidentes de disponibilidad

- caída total del sistema;
- interrupción de APIs;
- fallas en autenticación;
- degradación severa del servicio.

4.3 Incidentes de integridad de datos

- corrupción de bases de datos;
- pérdida parcial o total de información;
- inconsistencias críticas en registros.

4.4 Incidentes operativos

- fallos de automatización;
- errores en despliegues;
- fallos en integraciones externas;
- comportamiento anómalo del sistema.

---

5. CLASIFICACIÓN DE SEVERIDAD

SEVERIDAD CRÍTICA (P0)

Impacto total o crítico:

- sistema completamente inaccesible;
- fuga de datos sensibles;
- compromiso de seguridad activo.

Respuesta inmediata (prioridad máxima)

SEVERIDAD ALTA (P1)

Impacto severo pero no total:

- fallos en módulos críticos;
- degradación significativa del sistema;
- interrupciones parciales.

SEVERIDAD MEDIA (P2)

Impacto limitado:

- fallos en funcionalidades secundarias;
- errores intermitentes;
- degradación leve.

SEVERIDAD BAJA (P3)

Impacto mínimo:

- bugs menores;
- errores visuales;
- incidencias no críticas.

---

6. DETECCIÓN DE INCIDENTES

Veltrix Engine utiliza mecanismos de detección que pueden incluir:

- monitoreo automatizado de infraestructura;
- alertas en tiempo real;
- logs centralizados;
- sistemas de observabilidad;
- detección de anomalías;
- reportes de usuarios.

---

7. RESPUESTA INICIAL

Al detectarse un incidente:

1. Se valida la existencia del evento.
2. Se clasifica su severidad.
3. Se activa el protocolo de respuesta.
4. Se asigna equipo responsable.
5. Se inicia contención inmediata si aplica.

---

8. CONTENCIÓN

Las acciones de contención pueden incluir:

- aislamiento de servicios afectados;
- desactivación temporal de módulos;
- bloqueo de endpoints comprometidos;
- suspensión de integraciones externas;
- restricción de accesos.

El objetivo es limitar el impacto del incidente.

---

9. INVESTIGACIÓN Y ANÁLISIS

Una vez contenido el incidente:

- se analizan logs del sistema;
- se identifican causas raíz;
- se revisan vectores de ataque o fallo;
- se documenta el impacto técnico;
- se evalúan sistemas afectados.

---

10. RECUPERACIÓN DEL SISTEMA

Las acciones de recuperación pueden incluir:

- restauración desde backups;
- rollback de versiones;
- reinstalación de servicios;
- reconfiguración de infraestructura;
- validación de integridad de datos.

El objetivo es restablecer la operación normal del sistema.

---

11. COMUNICACIÓN DE INCIDENTES

Veltrix Engine podrá comunicar incidentes dependiendo de su severidad:

- notificación interna inmediata;
- actualización a usuarios afectados;
- comunicación pública si es necesario;
- reporte post-incidente.

La comunicación puede variar según el impacto y la sensibilidad del incidente.

---

12. TIEMPOS DE RESPUESTA

Los tiempos objetivo pueden variar según severidad:

- P0: respuesta inmediata / prioritaria
- P1: dentro de 24 horas
- P2: dentro de 48–72 horas
- P3: según disponibilidad operativa

Estos tiempos son objetivos operativos, no garantías absolutas.

---

13. LECCIONES APRENDIDAS

Después de incidentes relevantes, Veltrix Engine podrá realizar:

- análisis post-mortem;
- identificación de mejoras;
- actualización de sistemas;
- fortalecimiento de seguridad;
- ajustes de infraestructura.

---

14. ROLES Y RESPONSABILIDADES

Equipo técnico

- detección y respuesta;
- contención y recuperación;
- análisis forense;

- implementación de correcciones.

Dirección del sistema

- decisiones estratégicas;
- comunicación externa;
- priorización de recursos.

Usuarios

- reporte de incidentes;
- cooperación en diagnóstico;
- mantenimiento de credenciales seguras.

---

15. DEPENDENCIA DE TERCEROS

Algunos incidentes pueden estar relacionados con:

- proveedores cloud;
- APIs externas;
- servicios de mensajería;
- infraestructura de pago.

Veltrix Engine no controla estos sistemas, pero coordina esfuerzos de recuperación cuando es posible.

---

16. LIMITACIÓN DE RESPONSABILIDAD

En la máxima medida permitida por la ley:

- Veltrix Engine no garantiza ausencia de incidentes;
- no se responsabiliza por pérdidas indirectas;
- no garantiza recuperación inmediata en todos los casos;
- el uso del sistema implica aceptación de riesgos inherentes.

---

17. ACTUALIZACIONES DE LA POLÍTICA

Esta política puede actualizarse para:

- mejorar procesos de respuesta;
- adaptarse a nuevas amenazas;
- incorporar nuevas herramientas;
- optimizar tiempos de recuperación.

La versión vigente sustituye a las anteriores desde su publicación.

---

18. CONTACTO

Para reportes de incidentes:

Veltrix Engine
🌐 https://veltrixengine.pro
📧 soporte@veltrixengine.pro
📧 seguridad@veltrixengine.pro
📍 Aguascalientes, México

---

19. ENTRADA EN VIGOR

Esta política entra en vigor desde su publicación y permanece activa mientras los sistemas de Veltrix Engine estén en operación.