



CENTRO DE CONFIANZA

Política de divulgación de vulnerabilidades

Cómo reportar un problema de seguridad en los sistemas de Igniten, qué esperar y qué protección tiene quien investiga de buena fe

Versión	Fecha	Vigencia	Acceso	Contacto
1.0	25 de septiembre de 2026	Desde la disponibilidad general	Documento público	security@igniten.io

Vigencia. Este documento describe el servicio Igniten tal como se presta desde su disponibilidad general. Entra en vigor en la fecha en que la plataforma esté disponible comercialmente y rige para cada Cliente desde que celebra el contrato. Hasta entonces se publica solo con fines informativos y no genera obligaciones para ninguna de las partes.

1. Contacto

Si encontró un problema de seguridad en nuestros sistemas, queremos saberlo antes que nadie. Escriba a security@igniten.io. Ese buzón lo atiende directamente el equipo de seguridad de Igniten.

Acusamos recibo, le decimos qué encontramos y en qué plazo pensamos resolverlo, y le avisamos cuando esté corregido.

El contacto también está publicado en <https://igniten.io/well-known/security.txt>, en el formato estándar para este fin (RFC 9116). Aceptamos reportes en castellano y en inglés.

Por favor, no reporte una vulnerabilidad en un canal público (redes sociales, foros, repositorios) antes de que esté corregida.

2. Qué incluir en un reporte

Un buen reporte nos permite reproducir el problema sin tener que pedirle nada más. Incluya, en lo posible:

- una descripción del problema y del sistema o la dirección afectada;
- los pasos para reproducirlo, en orden;
- el impacto que estima: qué podría hacer un atacante y sobre qué datos;
- una prueba de concepto, si la tiene, que demuestre el problema con el mínimo de acceso necesario;
- la fecha en que lo encontró, y si otra persona está al tanto;
- cómo quiere que lo nombremos en el reconocimiento, o si prefiere no ser nombrado.

No hace falta que el reporte esté completo para enviarlo. Si tiene una sospecha fundada, escríbanos igual.

3. Qué puede esperar de nosotros

Etapas	Plazo
Acuse de recibo	Dentro de los 2 días hábiles
Evaluación inicial: le decimos qué encontramos, la severidad que le asignamos y en qué plazo pensamos resolverlo	Dentro de los 5 días hábiles
Corrección de severidad crítica	Dentro de los 7 días corridos
Corrección de severidad alta	Dentro de los 30 días corridos
Corrección de severidad media	Dentro de los 90 días corridos

Etapa	Plazo
Aviso de corrección	Cuando la corrección está desplegada

Durante el proceso lo mantenemos al tanto del avance. Si un plazo no se puede cumplir, se lo decimos antes de que venza y le explicamos por qué.

Si la vulnerabilidad afectó datos de clientes, avisamos a los clientes afectados según nuestros compromisos contractuales, con independencia del proceso con usted.

4. Divulgación coordinada

Le pedimos que no divulgue públicamente la vulnerabilidad hasta que esté corregida, o hasta 90 días corridos desde su reporte, lo que ocurra primero. Si la corrección requiere más tiempo, lo acordamos con usted y le explicamos el motivo. Cuando la corrección esté desplegada, puede publicar su hallazgo; si lo desea, revisamos el texto antes para confirmar que no expone datos de clientes.

5. Puerto seguro para la investigación de buena fe

Consideramos autorizada la investigación de seguridad hecha de buena fe y conforme a esta política. Si usted la respeta:

- no iniciaremos acciones legales ni presentaremos denuncias en su contra por esa investigación;
- si un tercero inicia acciones contra usted por una investigación que cumplió esta política, lo haremos saber públicamente;
- no consideraremos su investigación una violación de nuestros términos de servicio en lo que respecta a las restricciones de uso que la investigación necesariamente requiere.

Investigar de buena fe significa:

- usar solo cuentas propias o cuentas de prueba, y no acceder, modificar ni eliminar datos de otros usuarios u organizaciones;
- si accede sin querer a datos de otra persona u organización, detenerse en ese momento, no conservarlos ni compartirlos, e informarnos;
- demostrar el problema con el mínimo de acceso necesario, y no usarlo para acceder a más sistemas o datos;
- no degradar el servicio para otros usuarios;
- no exigir un pago a cambio de revelar o de no divulgar el hallazgo.

Esta política no autoriza a investigar los sistemas de nuestros proveedores ni de nuestros clientes. Si un hallazgo alcanza a un tercero, se lo comunicamos a ese tercero con su conformidad.

6. Alcance

Están dentro del alcance:

- el sitio público de Igniten y los dominios del producto bajo `igniten.io` ;
- el panel de administración y los canales del asistente (Teams, Slack, Google Chat, WhatsApp) en lo que corresponde a Igniten;
- la imagen publicada del conector que los clientes instalan en su red.

7. Fuera de alcance

- Ataques de denegación de servicio o pruebas de carga.
- Ingeniería social, suplantación o engaño dirigido a personas de Igniten o de sus clientes, y ataques físicos.
- Envío masivo de mensajes o correo no solicitado.
- Sistemas de terceros, aunque el producto se conecte a ellos: Microsoft, Google, Slack, Meta, los proveedores de modelos, la nube y los demás sub-procesadores. Repórtelos directamente a cada proveedor.
- Resultados de herramientas automáticas sin una prueba de impacto.
- Ausencia de cabeceras o configuraciones recomendadas sin un escenario de explotación concreto.
- Configuración de autenticación de correo (registros de remitente y de dominio) sin un escenario de suplantación demostrado.
- Ataques que requieren acceso físico al dispositivo de la víctima, un navegador desactualizado o un dispositivo ya comprometido.
- Problemas que solo afectan a la propia cuenta de quien los provoca, sin impacto sobre otra persona.
- Enumeración de usuarios o límites de frecuencia en funciones sin información sensible.
- Divulgación de versiones o de información de software sin una vulnerabilidad asociada.

Si tiene dudas sobre si algo está dentro del alcance, pregúntenos antes a security@igniten.io.

8. Sin acuerdo de confidencialidad

No exigimos acuerdo de confidencialidad para reportar. Tampoco condicionamos la respuesta, la corrección ni el reconocimiento a que usted firme nada.

9. Reconocimiento

Si lo desea, reconocemos públicamente su contribución cuando la corrección esté desplegada, con el nombre o seudónimo que usted elija y, si quiere, un enlace a su perfil. Si prefiere no ser nombrado, respetamos esa decisión.

Hoy no ofrecemos recompensas en dinero por los reportes.

Responsable: Igniten, sociedad de responsabilidad limitada (LLC) constituida en el Estado de Wyoming, Estados Unidos de América («Igniten»). Contacto de seguridad: security@igniten.io.