

Política de Divulgación de Vulnerabilidades

Última modificación: 23 de julio de 2026

Esta Política de Divulgación de Vulnerabilidades forma parte del compromiso de S.A. Construcciones Industriales («SACI» o la «Compañía») con la seguridad de sus clientes y de la comunidad de internet en general. SACI valora las contribuciones de los investigadores de seguridad y de los usuarios que dedican tiempo y esfuerzo a notificar vulnerabilidades de conformidad con esta política. Asimismo, SACI actuará de buena fe para resolver los hallazgos reportados de acuerdo con lo aquí establecido.

1. Introducción

Este documento describe la política de divulgación de vulnerabilidades de SACI. El objetivo es garantizar la seguridad e integridad de los productos y servicios de la Compañía, al tiempo que se fomenta la colaboración con la comunidad de investigación en ciberseguridad. SACI se compromete a gestionar de forma responsable las vulnerabilidades notificadas. Esta política se aplica a cualquier vulnerabilidad que se pretenda informar a la Compañía, por lo que recomendamos su lectura detenida antes de enviar un reporte.

2. Notificación de Vulnerabilidades

Se anima a los investigadores de seguridad o usuarios que descubran vulnerabilidades en los productos o sistemas de la Compañía a remitirlas por correo electrónico a:

infociber@saci.es

Para que el reporte sea procesado, por favor proporcione los siguientes detalles:

- **Ubicación:** El sitio web, la dirección IP o la página específica donde se observa el problema.
- **Descripción:** Una breve explicación del tipo de vulnerabilidad (por ejemplo: «Vulnerabilidad de acceso en producto XXX»).
- **Pasos para reproducirla:** Una prueba de concepto benigna y no destructiva. Esto permite clasificar el reporte con rapidez y precisión, además de reducir la probabilidad de notificaciones duplicadas o la explotación maliciosa de fallos (como el secuestro de subdominios o *subdomain takeover*).

3. Compromisos de SACI

La Compañía se compromete a actuar sobre las vulnerabilidades notificadas de manera oportuna. Tras recibir un reporte, evaluaremos el problema y tomaremos las medidas necesarias para subsanarlo.

- **Acuse de recibo y clasificación:** La Compañía realizará esfuerzos comercialmente razonables para acusar recibo de los reportes en un plazo

máximo de **5 días hábiles** y completar su evaluación inicial (clasificación) en un plazo de **10 días hábiles**. Todo acuse de recibo por escrito incluirá una valoración preliminar y los pasos a seguir.

- **Priorización:** La prioridad de la subsanación se determinará analizando el impacto, la gravedad y la complejidad de la explotación. Se dará prioridad al manejo de vulnerabilidades críticas para garantizar que se aborden con la urgencia requerida.
- **Seguimiento:** SACI proporcionará actualizaciones periódicas sobre el estado de la gestión, cumpliendo con las obligaciones contractuales aplicables. Como mínimo, se remitirá una actualización de estado **cada dos semanas** hasta la resolución definitiva del problema.

4. Proceso de Resolución

1. **Investigación y Validación:** Tras recibir la notificación, el equipo de seguridad de SACI llevará a cabo una investigación inicial para verificar y validar la existencia de la vulnerabilidad.
2. **Subsanación:** La Compañía diseñará un plan de mitigación para corregir el fallo. Esto puede incluir soluciones temporales (*workarounds*), parches o actualizaciones en nuestros productos o sistemas.

5. Guía de Conducta

Lo que NO debes hacer:

- Infringir ninguna ley o regulación aplicable.
- Extraer, acceder o modificar datos en los sistemas o servicios de la Compañía.
- Utilizar herramientas de escaneo invasivas, agresivas o de alta intensidad.
- Intenta o reportar cualquier forma de denegación de servicio (DoS); por ejemplo, saturando un servicio con un volumen masivo de peticiones.
- Interrumpir la disponibilidad o el correcto funcionamiento de los servicios o sistemas de la Compañía.
- Enviar reportes sobre vulnerabilidades no explotables o que simplemente indiquen que los servicios no siguen «buenas prácticas» teóricas (como la ausencia de determinadas cabeceras de seguridad o *security headers*).
- Enviar reportes sobre debilidades menores en la configuración de TLS, tales como el soporte de algoritmos de cifrado considerados débiles o la compatibilidad con TLS 1.0.
- Comunicar cualquier vulnerabilidad o detalle asociado a través de medios distintos al canal oficial indicado.

- Realizar técnicas de ingeniería social o *phishing* contra la Organización o su personal.
- Exigir cualquier tipo de compensación económica a cambio de divulgar la vulnerabilidad.

Lo que SÍ debes hacer:

- Cumplir siempre con las normativas de protección de datos aplicables y respetar la privacidad de los usuarios, personal, contratistas, servicios y sistemas de la Organización. En ningún caso se permite la extracción de datos.
- Si por error se accediera o extrajera información de nuestros sistemas, **todos los datos obtenidos deben eliminarse de forma segura e inmediata** en el momento de detectarse. Dichos datos no podrán compartirse, redistribuirse ni almacenarse bajo ninguna circunstancia.

6. Contacto

Para solicitar más información o enviar un reporte de vulnerabilidad, póngase en contacto con nosotros a través del correo electrónico: **infociber@saci.es**. Este canal garantiza la confidencialidad de la información compartida.

7. Aspectos Legales

Esta política está alineada con las buenas prácticas habituales de la industria sobre divulgación responsable de vulnerabilidades. Su contenido no concede autorización ni permiso alguno para actuar en contra de la legislación vigente, del código ético aplicable, o de un modo que pueda hacer que la Compañía incumpla sus obligaciones legales.