

# ZIV

## POLÍTICA DE DIVULGACIÓN DE VULNERABILIDADES

## Contenido


1. INTRODUCCIÓN ..... 3
2. OBJETO Y PRINCIPIOS ..... 3
3. ÁMBITO DE APLICACIÓN ..... 3
4. DIRECTRICES PARA LA INVESTIGACIÓN DE SEGURIDAD DE BUENA FE ..... 4
5. CÓMO COMUNICAR UNA VULNERABILIDAD ..... 5
6. GESTIÓN DE LAS VULNERABILIDADES COMUNICADAS ..... 6
7. DIVULGACIÓN COORDINADA, CONFIDENCIALIDAD Y DATOS ..... 7
8. VULNERABILIDADES EN COMPONENTES DE TERCEROS ..... 8
9. MARCO LEGAL Y RESERVA DE DERECHOS ..... 8

# 1. INTRODUCCIÓN

**ZIV APLICACIONES Y TECNOLOGÍA, S.L.U. (en adelante "ZIV") mantiene un compromiso firme con la ciberseguridad de sus productos y soluciones**. Esta política establece un marco para comunicar, analizar y gestionar de forma responsable vulnerabilidades de seguridad que puedan afectar a productos, soluciones o componentes suministrados por ZIV.

# 2. OBJETO Y PRINCIPIOS

El objetivo de esta política es facilitar la comunicación coordinada de vulnerabilidades de seguridad y establecer unas reglas claras para la investigación de buena fe. ZIV considera que una gestión eficaz de vulnerabilidades contribuye a reducir el riesgo durante el ciclo de vida de los productos y a proteger la confidencialidad, integridad y disponibilidad de los sistemas en los que se integran.

ZIV agradece el tiempo y el esfuerzo de investigadores, clientes, integradores y profesionales de la seguridad que comuniquen vulnerabilidades de forma responsable y de acuerdo con esta política. Salvo que se indique expresamente lo contrario en un programa específico, ZIV no ofrece recompensas económicas por este tipo de comunicaciones.

# 3. ÁMBITO DE APLICACIÓN

Esta política se aplica a productos y soluciones de ZIV que incorporen componentes digitales, software o firmware, incluyendo, entre otros:

- Equipos de protección y control.
- Equipos de medida, supervisión y automatización.
- Equipos de comunicaciones.
- Plataformas, aplicaciones y herramientas software asociadas a productos ZIV.
- Firmware, interfaces de comunicación y servicios digitales suministrados como parte de una solución ZIV.

Quedan fuera del ámbito de esta política los sistemas, servicios o infraestructuras de terceros que no sean propiedad de ZIV ni estén bajo su control. Las vulnerabilidades identificadas en productos, servicios o componentes de terceros integrados en productos o soluciones de ZIV que puedan afectar a la seguridad de éstos deberán comunicarse a ZIV a través del canal establecido en esta política. Cuando la vulnerabilidad afecte exclusivamente a productos, servicios o componentes de terceros no integrados en productos o soluciones de ZIV, se recomienda comunicarla directamente a su fabricante o proveedor correspondiente.

# 4. DIRECTRICES PARA LA INVESTIGACIÓN DE SEGURIDAD DE BUENA FE

ZIV valora y agradece la comunicación responsable de posibles vulnerabilidades de seguridad. Esta política no constituye una autorización general para acceder a sistemas, redes, equipos o información de ZIV, de sus clientes o de terceros. Cualquier investigación deberá realizarse sobre sistemas o equipos propios o para los que se disponga de la correspondiente autorización, respetando los límites establecidos en esta política. Asimismo, solicita a los investigadores y terceros que se abstengan de realizar pruebas o actividades que puedan comprometer la seguridad, disponibilidad o integridad de sus productos, sistemas y servicios, afectar a sus usuarios o provocar la pérdida, alteración o corrupción de datos.

En caso de que, durante una investigación, se identifique una vulnerabilidad que permita acceder a información sensible, como datos personales, información financiera, información confidencial o secretos comerciales de terceros, el investigador deberá interrumpir inmediatamente las pruebas, notificar el hallazgo a ZIV PSIRT y abstenerse de acceder, utilizar, conservar o divulgar dicha información, salvo lo estrictamente necesario para documentar y comunicar la vulnerabilidad de forma segura.

ZIV no tiene intención de emprender acciones legales contra quienes realicen investigaciones de seguridad de buena fe, dentro de los límites establecidos en esta política y sin causar daños ni vulnerar derechos de terceros. Si bien este compromiso se refiere exclusivamente a las acciones que correspondan a ZIV y no limita las facultades de las autoridades ni los derechos de terceros. En todo caso, cualquier actuación de mala fe, así como el incumplimiento de estas directrices o de la legislación aplicable, podrá dar lugar a las responsabilidades legales que correspondan.

# 5. CÓMO COMUNICAR UNA VULNERABILIDAD

Cualquier persona que identifique una posible vulnerabilidad que afecte a un producto o solución de ZIV puede comunicarla al canal de seguridad de producto de ZIV (ZIV PSIRT) indicado a continuación:

| | |
|---|---|
| **Correo electrónico** | product.security@zivautomation.com |
| **Cifrado PGP** | Clave pública PGP Fingerprint: D613 1C19 3134 509B 65C4 2825 E246 25F3 F7D6 3483 |

Se recomienda redactar el informe en castellano o inglés e incluir, siempre que sea posible:

- Identificación del producto o servicio afectado, modelo, versión de firmware/software y cualquier referencia necesaria para identificar de forma inequívoca la versión.
- Descripción técnica de la vulnerabilidad, incluyendo causa probable, impacto, condiciones previas, severidad estimada y resultado observado.
- Pasos de reproducción, herramientas utilizadas y, cuando resulte necesario, una prueba de concepto mínima y no destructiva. Pueden adjuntarse capturas, imágenes, vídeos o trazas de red relevantes.
- Configuración del equipo, topología del escenario de prueba y relación de otros componentes conectados cuando esta información sea necesaria para analizar el caso.
- Datos de contacto, cuando el notificante desee facilitarlos, para permitir el seguimiento de la comunicación y la coordinación de una eventual divulgación. Se admitirán comunicaciones anónimas.

La ausencia de alguno de estos elementos no impedirá comunicar una posible vulnerabilidad. ZIV podrá solicitar información adicional cuando resulte necesaria para su análisis.

Para proteger la información intercambiada, ZIV recomienda mantener la máxima confidencialidad posible durante todo el proceso y utilizar cifrado PGP, empleando la clave pública PGP.

# 6. GESTIÓN DE LAS VULNERABILIDADES COMUNICADAS

ZIV gestionará las vulnerabilidades reportadas mediante un proceso estructurado, adaptado a la naturaleza y criticidad de cada caso:

| Fase | Etapa | Objetivo |
|---|---|---|
| 1 | Recepción y registro | Recepción del reporte, identificación del producto afectado y recopilación de la información inicial. |
| 2 | Verificación y análisis | Reproducción técnica, validación del hallazgo y evaluación preliminar del impacto, alcance y aplicabilidad. |
| 3 | Tratamiento | Definición de mitigaciones, medidas compensatorias, correcciones o actualizaciones en función del riesgo y del ciclo de vida del producto. |
| 4 | Coordinación y comunicación | Intercambio de información con el notificante y las partes afectadas y, cuando proceda, preparación de avisos de seguridad o recomendaciones. |
| 5 | Seguimiento y cierre | Seguimiento de las medidas adoptadas, soporte a su implantación y revisión de información adicional que pueda aparecer tras la comunicación. |
| 6 | Recepción y registro | Recepción del reporte, identificación del producto afectado y recopilación de la información inicial. |
| 7 | Verificación y análisis | Reproducción técnica, validación del hallazgo y evaluación preliminar del impacto, alcance y aplicabilidad. |

La prioridad y los plazos de tratamiento dependerán del riesgo, impacto, explotabilidad, criticidad del producto, disponibilidad de mitigaciones y complejidad de la corrección. ZIV procurará acusar recibo de las comunicaciones y mantener informado al notificante sobre los avances relevantes en su análisis y tratamiento, siempre que se haya facilitado un medio de contacto válido y las circunstancias lo permitan.

# 7. DIVULGACIÓN COORDINADA, CONFIDENCIALIDAD Y DATOS

Se solicita a los notificantes que mantengan confidencial la información sobre la vulnerabilidad mientras ZIV la analiza y hasta que exista una solución, mitigación o fecha de divulgación acordada. ZIV podrá coordinar con el notificante la comunicación con clientes, integradores, proveedores, CERT/CSIRT u otras partes afectadas cuando sea necesario para reducir el riesgo, teniendo en cuenta la gravedad de la vulnerabilidad, las medidas de mitigación disponibles y los riesgos para los usuarios.

ZIV tratará de forma confidencial la identidad y los datos de contacto del notificante y a no divulgar públicamente ni comunicar a terceros datos que permitan identificarle, incluyendo su nombre, datos de contacto u otros elementos identificativos, ni información que permita identificar sus sistemas, redes, direcciones, infraestructura o entorno técnico. El acceso a esta información se limitará al personal y a las partes que necesiten conocerla para gestionar la vulnerabilidad o cumplir obligaciones legales y quedará sujeta a las correspondientes obligaciones de confidencialidad. ZIV no compartirá esta información fuera del ámbito descrito salvo cuando exista consentimiento expreso del notificante o una obligación legal que así lo exija.

Los investigadores deberán limitar la recopilación y conservación de información a lo estrictamente necesario para documentar y comunicar la vulnerabilidad y eliminarla de forma segura cuando deje de ser necesaria, sin perjuicio de las obligaciones legales de conservación.

Si durante la investigación se accede accidentalmente a datos personales, información confidencial o secretos empresariales, las pruebas deberán detenerse inmediatamente, la información no deberá divulgarse ni utilizarse para ningún otro fin y el incidente deberá comunicarse a ZIV.

# 8. VULNERABILIDADES EN COMPONENTES DE TERCEROS

Cuando el hallazgo afecte a un componente de terceros incorporado en una solución ZIV, ZIV podrá coordinar el análisis y la comunicación con el proveedor correspondiente. Si la vulnerabilidad afecta exclusivamente a un producto o servicio de un tercero y no existe impacto específico sobre una solución ZIV, deberá notificarse preferentemente al fabricante o responsable de dicho componente conforme a su propia política de divulgación.

# 9. MARCO LEGAL Y RESERVA DE DERECHOS

Esta política pretende ser compatible con las buenas prácticas de divulgación responsable y coordinada de vulnerabilidades y no autoriza actuaciones contrarias a la legislación aplicable, a obligaciones contractuales, a derechos de terceros o a cualquier otra norma que resulte de aplicación.

Entre otras normas, y cuando resulten aplicables al caso concreto, deberán respetarse la normativa de protección de datos personales, propiedad intelectual y secretos empresariales, así como la regulación nacional y europea en materia de seguridad de redes y sistemas de información.

ZIV se reserva los derechos que legalmente le correspondan cuando exista incumplimiento de esta política, actuación de mala fe, daño intencionado o acceso no autorizado fuera del alcance permitido. ZIV podrá actualizar esta política cuando resulte necesario por cambios legales, técnicos, organizativos o de proceso.