

## Política de divulgación coordinada de vulnerabilidades

### Notificación responsable de vulnerabilidades de ciberseguridad

Otto Martin Maschinenbau GmbH & Co. KG («MARTIN») concede gran importancia a la seguridad de sus máquinas, su software y sus componentes digitales.

A pesar de un desarrollo y unas pruebas minuciosos, pueden surgir vulnerabilidades de ciberseguridad en los productos que contienen elementos digitales. Por ello, agradecemos cualquier información sobre posibles vulnerabilidades que nos faciliten clientes, distribuidores, socios, investigadores de seguridad y otras personas.

Con esta Política de divulgación coordinada de vulnerabilidades (Política CVD) describimos cómo se pueden notificar a MARTIN las posibles vulnerabilidades de ciberseguridad y cómo gestionamos dichas notificaciones.

### 1. Ámbito de aplicación

Esta política se aplica a las vulnerabilidades de ciberseguridad en los productos y componentes digitales de MARTIN, en particular en:

- sistemas de control de máquinas,
- software de control,
- firmware,
- interfaces de usuario,
- interfaces de red y comunicación,
- aplicaciones web y en la nube, siempre que formen parte de un producto MARTIN o sean necesarias para su funcionamiento,
- aplicaciones móviles, en caso de que existan,
- interfaces y API, así como
- componentes de software de terceros integrados por MARTIN.

No forman parte de esta política de CVD las reclamaciones generales sobre productos, los defectos mecánicos, las consultas sobre el manejo u otras solicitudes de servicio que no guarden relación con la ciberseguridad. Para ello, utilice nuestros canales habituales de servicio y contacto.

### 2. Notificación de vulnerabilidades de seguridad

Si detecta una posible vulnerabilidad de ciberseguridad en un producto de MARTIN, le rogamos que nos lo comunique lo antes posible.

#### Punto de contacto central para vulnerabilidades de ciberseguridad

Otto Martin Maschinenbau GmbH & Co. KG

Correo electrónico: [product-security@martin.info](mailto:product-security@martin.info)

Formulario de notificación en línea: <https://martin.info/es/seguridad-de-los-productos/>

Para información confidencial o técnicamente sensible, le rogamos que utilice preferentemente nuestro canal de transmisión específico para ello:

### 3. ¿Qué información necesitamos?

Para que podamos revisar su notificación lo antes posible, le rogamos que nos facilite los siguientes datos, en la medida en que los conozca y estén disponibles:

- producto o tipo de máquina afectado,
- número de serie del producto,
- versión del software o del firmware,
- componente o función afectada,
- descripción de la supuesta vulnerabilidad,
- posibles consecuencias de la vulnerabilidad,
- pasos para reproducir el comportamiento,
- configuración de red o del sistema utilizada,
- si procede, capturas de pantalla, archivos de registro u otras pruebas técnicas,
- información sobre si la vulnerabilidad ya es conocida por terceros o se ha hecho pública,
- información sobre si hay indicios de que la vulnerabilidad se esté explotando activamente,
- sus datos de contacto para cualquier consulta.

Le rogamos que no facilite datos personales, datos de acceso, secretos comerciales ni datos de terceros, salvo que sean necesarios para la investigación de la vulnerabilidad.

### 4. ¿Qué ocurre tras su notificación?

Una vez recibida la notificación de una vulnerabilidad, MARTIN la tramitará en el marco del proceso establecido de gestión de vulnerabilidades.

El proceso comprende, en principio, los siguientes pasos:

1. Confirmación de recepción: le confirmaremos la recepción de su notificación en un plazo razonable.
2. Primera evaluación: Comprobamos si la notificación se refiere a una posible vulnerabilidad de ciberseguridad de un producto de MARTIN.
3. Análisis técnico: Los departamentos especializados correspondientes investigan la vulnerabilidad y evalúan, en particular, sus repercusiones técnicas, su posible explotabilidad y el riesgo resultante.
4. Priorización: El tratamiento posterior se basa en la gravedad, la explotabilidad y las posibles repercusiones de la vulnerabilidad.
5. Medidas correctivas: En la medida en que sea necesario y técnicamente posible, desarrollamos medidas adecuadas para subsanar o reducir el riesgo. Estas pueden consistir, por ejemplo, en actualizaciones de software o firmware, cambios de configuración, medidas de protección técnicas o recomendaciones de actuación.
6. Publicación coordinada: Por norma general, los detalles técnicos no se publicarán hasta que se disponga de medidas correctivas adecuadas o hasta que, por otros motivos, resulte conveniente o necesario realizar una publicación coordinada.
7. Información a los usuarios afectados: En la medida en que sea necesario, informaremos a los clientes, distribuidores o usuarios afectados sobre las medidas correctivas adecuadas y las recomendaciones de seguridad.

Esto no afecta a las obligaciones legales de notificación e información, en particular las establecidas en la Ley de Resiliencia Cibernética.

## 5. Divulgación coordinada

Rogamos a quienes notifiquen una vulnerabilidad que den a MARTIN una oportunidad razonable para investigar y subsanarla antes de que los detalles técnicos se hagan públicos o se comuniquen a terceros.

El plazo concreto se acordará entre MARTIN y la persona que haya notificado la vulnerabilidad, en función del tipo, la complejidad y la gravedad de la misma.

La divulgación pública deberá coordinarse, en particular, de tal forma que los usuarios afectados tengan tiempo suficiente para aplicar las actualizaciones de seguridad disponibles u otras medidas de protección.

En caso de que una vulnerabilidad ya se esté explotando activamente o suponga un riesgo grave e inmediato, puede ser necesario un procedimiento acelerado.

## 6. Expectativas respecto a los investigadores de seguridad y a quienes notifican las vulnerabilidades

Les rogamos que actúen de forma responsable al investigar posibles vulnerabilidades.

En particular, les pedimos que

- que investiguen únicamente aquellos sistemas y productos para los que estén autorizados a hacerlo,
- no consulten, modifiquen ni eliminen datos de otras personas o empresas sin autorización,
- no utilicen software malicioso,
- no llevar a cabo medidas que afecten al funcionamiento normal de máquinas, sistemas informáticos o redes,
- no realice ataques de denegación de servicio ni pruebas de carga similares contra sistemas en producción,
- no llevar a cabo ataques de ingeniería social contra empleados, clientes, distribuidores o socios comerciales de MARTIN,
- no aprovechar las vulnerabilidades detectadas más allá de lo necesario para su verificación,
- tratar de forma confidencial la información obtenida y
- conceder a MARTIN una oportunidad razonable para investigar y subsanar los problemas antes de publicar detalles técnicos.

En el caso de las máquinas y las instalaciones, las inspecciones no deben dar lugar, en particular, a que se anulen las funciones de protección ni a que se ponga en peligro a personas, máquinas, piezas de trabajo u otros bienes materiales.

## 7. Comunicación con la persona que realiza la notificación

Siempre que nos facilite sus datos de contacto, nos esforzaremos por mantenerle informado de los avances significativos que se produzcan durante la investigación.

Podremos ponernos en contacto con usted, en particular, si:

- se necesite más información técnica,
- se haya podido reproducir la vulnerabilidad,
- se haya desarrollado una medida correctiva o
- se haya previsto una publicación coordinada.

Tenga en cuenta que, por motivos de seguridad, protección de datos o confidencialidad, es posible que no podamos revelar todos los resultados de nuestra investigación interna.

## 8. Reconocimiento

MARTIN agradece las notificaciones responsables de vulnerabilidades de ciberseguridad. Se podrá hacer pública la identidad del informante, previo acuerdo, siempre que así se desee y no existan motivos legales, de seguridad o contractuales que lo impidan. Esta política de CVD no da derecho a ninguna compensación económica ni a ninguna otra recompensa por las vulnerabilidades notificadas.

## 9. Notificaciones legales

Independientemente de la comunicación con el denunciante, MARTIN comprueba, en el caso de cada vulnerabilidad relevante, si existen obligaciones legales de notificación o de información.

Esto se refiere, en particular, a las vulnerabilidades explotadas activamente y a los incidentes de seguridad graves en el ámbito de aplicación del Reglamento (UE) 2024/2847 —Cyber Resilience Act (CRA)—.

En la medida en que sea necesario, se realizarán las notificaciones correspondientes a los organismos competentes previstos a tal efecto.

## 10. Protección de datos

Los datos personales que se nos transmiten en relación con una notificación de vulnerabilidad los tratamos exclusivamente en la medida necesaria para la tramitación, documentación y seguimiento de la notificación, así como para el cumplimiento de las obligaciones legales.

Encontrará más información sobre la protección de datos en:

[Enlace a la política de privacidad]

## 11. Modificaciones de esta política

Esta Política de divulgación coordinada de vulnerabilidades se revisa periódicamente y, en caso necesario, se adapta a los avances técnicos, organizativos o legales.

Fecha: 09/2026

Otto Martin Maschinenbau GmbH & Co. KG  
Langenberger Str. 6  
87724 Ottobeuren  
Alemania

Contacto para seguridad de los productos: [product-security@martin.info](mailto:product-security@martin.info)  
Página web: [www.martin.info](http://www.martin.info)

|              |                                |            |                                    |
|--------------|--------------------------------|------------|------------------------------------|
| Versión: 1.0 | Fecha: 7 de septiembre de 2026 | Autor: MüM | Nivel de confidencialidad: público |
|--------------|--------------------------------|------------|------------------------------------|