Política de divulgación de vulnerabilidades

Notificación responsable, investigación y corrección de vulnerabilidades de seguridad

Versión	Fecha de entrada en vigor	Responsable del documento	Contacto
1.0	Septiembre de 2026	Equipo de Seguridad de SALUS Controls PLC	security@saluscontrols.com

1. Introducción....2
2. Alcance....2
3. Notificación de una vulnerabilidad....3
4. Información que debe incluirse....3
5. Proceso de respuesta....4
6. Corrección basada en el riesgo....4
7. Divulgación coordinada de vulnerabilidades....4
8. Soporte de actualizaciones de seguridad....5
9. Fuera de alcance....5
10. Investigación responsable de seguridad....5
11. Contacto....6
12. Actualizaciones de la política....6
13. Reconocimiento....6

1. Introducción

SALUS Controls PLC se compromete a proteger la seguridad de sus productos, servicios y clientes. Agradecemos las notificaciones responsables de clientes, investigadores de seguridad, socios, desarrolladores y otros miembros de la comunidad de seguridad que identifiquen posibles vulnerabilidades que afecten a productos o servicios de SALUS Controls PLC.

Nuestro objetivo es investigar con prontitud las posibles vulnerabilidades notificadas, mantener una comunicación adecuada con la persona informante durante todo el proceso y aplicar medidas de corrección o mitigación proporcionales para proteger a los usuarios.

Notifique las posibles vulnerabilidades de seguridad de forma privada a security@saluscontrols.com. SALUS Controls PLC confirmará la recepción en un plazo de tres días laborables y, en todos los casos, no más tarde de siete días naturales. Esta confirmación únicamente acredita la recepción de la información y no implica que el problema notificado haya sido confirmado como vulnerabilidad.



2. Alcance

Esta política se aplica a vulnerabilidades de seguridad que afecten a:

- Productos de SALUS Controls PLC
- Firmware y software
- Aplicaciones móviles
- Servicios en la nube
- Aplicaciones web y sitios web de acceso público

Para consultas sobre instalación, configuración, garantía u otros asuntos no relacionados con la seguridad, póngase en contacto con nuestro equipo de Atención al Cliente a través de los canales de soporte habituales.

Aceptamos notificaciones de seguridad relacionadas con productos SALUS independientemente de su estado en el ciclo de vida. Para los productos que se encuentren dentro de su periodo de soporte de seguridad publicado, las vulnerabilidades y actualizaciones de seguridad se gestionarán de conformidad con las obligaciones legales aplicables. Para los productos fuera de dicho periodo, SALUS Controls PLC seguirá evaluando las notificaciones y podrá ofrecer medidas de mitigación, recomendaciones de migración u otras orientaciones en función del riesgo, la viabilidad técnica y las obligaciones aplicables.

3. Notificación de una vulnerabilidad

Si cree que ha identificado una vulnerabilidad de seguridad, notifíquela de forma privada por correo electrónico a **security@saluscontrols.com**. Por favor, informe de las vulnerabilidades sospechadas utilizando esta **plantilla**.

Las notificaciones pueden enviarse de forma anónima. La ausencia de un nombre o de un medio de contacto bidireccional no impedirá la recepción ni la evaluación inicial, pero puede limitar nuestra capacidad para solicitar información adicional, proporcionar actualizaciones de estado u ofrecer reconocimiento público.

Aceptamos una notificación inicial enviada por correo electrónico ordinario o por otro canal. Si fuera necesario intercambiar código de explotación, credenciales, datos personales, configuraciones de clientes u otra información sensible, SALUS Controls PLC ofrecerá un método seguro disponible para continuar la comunicación. La imposibilidad o decisión de la persona informante de no utilizar cifrado no hará, por sí sola, que se rechace la notificación.

4. Información que debe incluirse

Para ayudarnos a investigar su notificación de forma eficiente, incluya, cuando sea posible:

- Nombre y modelo del producto
- Versión del firmware o software
- Descripción de la vulnerabilidad
- Pasos necesarios para reproducir el problema
- Comportamiento esperado y comportamiento real
- Posible impacto en la seguridad
- Capturas de pantalla, registros o prueba de concepto, si están disponibles
- Datos de contacto preferidos para el seguimiento

Evite incluir información personal sensible salvo que sea necesaria para demostrar la vulnerabilidad.

Indique también, cuando lo sepa, si el problema es público, está siendo explotado activamente, ha afectado a usuarios o ha sido notificado a otro proveedor, fabricante o coordinador. No es necesario proporcionar todos los elementos solicitados para que podamos aceptar y registrar una notificación.

Durante la divulgación coordinada, el acceso a información no pública sobre vulnerabilidades se restringe según el principio de necesidad de conocimiento. SALUS Controls PLC podrá compartir la información necesaria con equipos de producto, proveedores, coordinadores, partes afectadas o autoridades competentes para la validación, corrección, protección de los usuarios y cumplimiento de obligaciones legales, sujeto a controles adecuados de confidencialidad y protección de datos.

Los datos personales enviados con una notificación de vulnerabilidad se tratan de acuerdo con el aviso de privacidad aplicable de SALUS Controls PLC. Consulte la política de privacidad en: https://saluscontrols.com/es/privacidad-cookies/

5. Proceso de respuesta

Tras recibir su notificación, SALUS Controls PLC:

- Confirmará la recepción en un plazo de tres días laborables y, en todos los casos, no más tarde de siete días naturales; cuando sea posible, incluirá un identificador único del caso e información preliminar sobre su estado.
- Realizará una evaluación inicial en un plazo de siete días laborables
- Validará la vulnerabilidad notificada
- Evaluará su gravedad y posible impacto
- Desarrollará un plan de corrección o una actualización de seguridad cuando proceda
- Le mantendrá informado durante el proceso de investigación y corrección
- Mientras el caso permanezca activo, proporcionará una actualización sustancial del estado al menos una vez cada 30 días naturales y comunicará antes cualquier cambio relevante en el alcance confirmado, el riesgo, el enfoque de corrección o la fecha de divulgación.
- Si se necesita información adicional, podremos ponernos en contacto con usted durante nuestra investigación.

6. Corrección basada en el riesgo

Las vulnerabilidades confirmadas se priorizan según su gravedad técnica, explotabilidad, productos afectados, impacto potencial, exposición de los usuarios, pruebas de explotación activa, medidas de mitigación disponibles y necesidades de despliegue seguro. Una puntuación numérica puede contribuir a la evaluación, pero no determina por sí sola la prioridad de corrección.

SALUS Controls PLC establece un objetivo de corrección específico para cada caso y comunica los cambios relevantes a la persona informante. Cuando no sea posible una corrección inmediata, podrán proporcionarse medidas de mitigación u orientaciones para reducir el riesgo antes de que esté disponible una solución permanente.

7. Divulgación coordinada de vulnerabilidades

SALUS Controls PLC colabora con la persona informante y, cuando sea necesario, con proveedores, coordinadores y otras partes afectadas para establecer una fecha de divulgación específica para cada caso. El calendario podrá revisarse en función de la gravedad, la explotación activa, el riesgo para los usuarios, el progreso de la corrección y el despliegue, las dependencias de la cadena de suministro y las obligaciones legales o reglamentarias aplicables. Los cambios relevantes en la fecha prevista se comunicarán a las partes pertinentes.

SALUS Controls PLC podrá acelerar la notificación a los usuarios o la divulgación pública cuando una vulnerabilidad ya sea pública, esté siendo explotada activamente, represente un riesgo urgente para los usuarios, exista una probabilidad de filtración o cuando la notificación sea exigida por ley. Si todavía no está disponible una solución completa, SALUS podrá proporcionar medidas temporales de mitigación o reducción del riesgo sin facilitar innecesariamente la explotación.

La información sobre vulnerabilidades corregidas se publicará en avisos de seguridad accesibles y legibles para las personas. Los avisos identificarán la vulnerabilidad y los productos afectados, las fechas de publicación y revisión, el impacto y la gravedad potenciales, las medidas de corrección o mitigación disponibles, las acciones necesarias por parte de los usuarios y la

información de contacto. Los avisos relativos a componentes de terceros podrán remitir a información oficial del proveedor original cuando ello permita a los usuarios determinar si los productos SALUS están afectados.

La información sobre vulnerabilidades también se facilitará en un formato legible por máquina ampliamente reconocido, salvo que exista una justificación documentada y aprobada para no hacerlo. La publicación solo podrá retrasarse u omitirse cuando se hayan evaluado, documentado y aprobado las condiciones aplicables.

Cuando lo exija la legislación aplicable o sea necesario para proteger a los usuarios, SALUS Controls PLC informará a los usuarios afectados y proporcionará medidas de mitigación u orientaciones correctivas disponibles a través de canales adecuados y accesibles.

8. Soporte de actualizaciones de seguridad

SALUS Controls PLC proporciona actualizaciones de seguridad durante el periodo de soporte establecido para cada producto aplicable. El periodo de soporte se determina de acuerdo con los requisitos legales aplicables, teniendo en cuenta el periodo de uso esperado del producto, su naturaleza y las expectativas razonables de los usuarios.

El periodo de soporte será de al menos cinco años, salvo que razonablemente se espere que el producto se utilice durante un periodo más corto, y podrá ser más largo cuando lo justifique la vida útil prevista del producto. La fecha de finalización del periodo de soporte aplicable se comunicará a través de la información pertinente del producto.

9. Fuera de alcance

Todas las posibles notificaciones de seguridad se registran y reciben una evaluación inicial. Las cuestiones puramente funcionales, comerciales o relacionadas con el soporte podrán derivarse al canal de soporte adecuado. Si un problema no puede reproducirse inicialmente, SALUS Controls PLC podrá solicitar información adicional y volver a evaluar la notificación cuando haya nuevas pruebas disponibles.

Las cuestiones teóricas, los escenarios con acceso físico, las condiciones de denegación de servicio, los escenarios de ingeniería social y las dependencias de terceros se evalúan según su impacto realista en la seguridad, su explotabilidad y el uso previsto y razonablemente previsible del producto.

Las vulnerabilidades en componentes de terceros integrados en un producto SALUS, suministrados con él o de los que dependa siguen estando sujetas a la evaluación del impacto sobre el producto SALUS.

10. Investigación responsable de seguridad

SALUS Controls PLC apoya la investigación de seguridad responsable realizada de buena fe. Pedimos a los investigadores que:

- Actúen de forma responsable y ética
- Eviten interrumpir productos, servicios u operaciones de clientes
- Eviten acceder, modificar o eliminar datos de clientes
- Notifiquen las vulnerabilidades de forma privada mediante el proceso descrito en esta política

- Concedan a SALUS Controls PLC un tiempo razonable para investigar y corregir el problema antes de su divulgación pública
- Cumplan todas las leyes y normativas aplicables durante la investigación de seguridad

Cuando una persona informante actúe de buena fe, cumpla esta política, evite causar daños y notifique con prontitud, SALUS Controls PLC no tiene intención de iniciar acciones legales únicamente por una investigación de seguridad realizada de conformidad con esta política. Esta declaración no autoriza el acceso a sistemas o datos de terceros, no vincula a terceros ni a autoridades, ni exime a la persona informante de su obligación de cumplir la legislación aplicable y obtener las autorizaciones necesarias.

11. Contacto

Para todas las notificaciones relacionadas con la seguridad o preguntas sobre esta política, póngase en contacto con:

Equipo de Seguridad de SALUS Controls PLC

Correo electrónico: security@saluscontrols.com

12. Actualizaciones de la política

Esta política se revisa al menos una vez al año y tras cambios relevantes en los requisitos legales aplicables, los canales de notificación, el alcance de los productos o los procesos de gestión de vulnerabilidades. La versión actual, la fecha de publicación, la fecha de la última actualización y el responsable de la política se muestran en la política publicada.

13. Reconocimiento

Con el consentimiento de la persona informante, SALUS Controls PLC podrá reconocer el nombre, alias u organización de quien presente una notificación válida de vulnerabilidad y colabore en la divulgación coordinada. Las notificaciones pueden enviarse de forma anónima y renunciar al reconocimiento no afecta a su aceptación, priorización ni corrección.

Esta política no establece un programa de recompensas por vulnerabilidades ni garantiza recompensas económicas o de otro tipo.

SALUS Controls PLC - Formulario de notificación de una posible vulnerabilidad

Utilice este formulario para informar de una posible vulnerabilidad de seguridad que afecte a un producto, aplicación, servicio en la nube o sitio web de SALUS.
Facilite toda la información que le sea posible. No es necesario completar todos los campos para que podamos aceptar su notificación.
Puede enviar la notificación de forma anónima. No obstante, si no facilita datos de contacto, es posible que no podamos solicitar información adicional ni comunicarle novedades sobre su notificación.
Una vez cumplimentado, envíe este formulario a security@saluscontrols.com.
No incluya contraseñas, tokens de autenticación, claves privadas ni datos personales o de clientes que no sean necesarios.
Los campos marcados como «Obligatorio» solo son obligatorios cuando la información esté razonablemente disponible. Aunque no disponga de toda la información, puede enviar la notificación.

Notificación de una posible vulnerabilidad

1. Información de la persona notificante

Campo	Respuesta
Nombre o alias (opcional)	
Organización (opcional)	
Correo electrónico / método de contacto (obligatorio salvo notificación anónima)	
Idioma preferido (opcional)	
¿Desea realizar la notificación de forma anónima?	☐ Sí ☐ No

2. Producto o componente afectado

Campo	Respuesta
Nombre del producto o servicio (obligatorio)	
Modelo (si procede)	
Versión de hardware (si se conoce)	
Versión de firmware / software / aplicación (si se conoce)	
País / región	

Campo	Respuesta
Otra información de configuración pertinente	

3. Descripción de la posible vulnerabilidad

Campo	Respuesta
Título breve (obligatorio)	
Describa el problema de seguridad identificado (obligatorio)	
¿Cuándo detectó el problema por primera vez?	
¿Qué esperaba que ocurriera?	
¿Qué ocurrió realmente?	
¿Puede reproducir el problema?	☐ Sí ☐ No ☐ A veces ☐ Desconocido
Si es posible, describa los pasos necesarios para reproducirlo:	
¿Qué impacto sobre la seguridad cree que podría tener el problema?	
¿Se incluyen archivos adjuntos? Puede aportar capturas de pantalla, registros, vídeos o información de prueba de concepto pertinentes.	☐ Sí ☐ No

Información técnica adicional (opcional, para investigadores de seguridad)

Campo	Respuesta
Tipo de vulnerabilidad (omisión de autenticación, inyección, corrupción de memoria, etc.), si se conoce	
CWE / CVE, si se conoce	
Causa técnica / detalles	
Entorno de prueba / configuración	
Prueba de concepto	

4. Escenario de ataque

El escenario de ataque es distinto del procedimiento de reproducción. Describa cómo podría un atacante realista aprovechar la vulnerabilidad.

Campo	Respuesta
Si se conoce, describa cómo podría alguien aprovechar esta vulnerabilidad	
Acceso del atacante	☐ Red remota ☐ Red adyacente ☐ Local network ☐ Local device ☐ Physical access ☐ Desconocido
Interacción del usuario necesaria	☐ Sí ☐ No ☐ Desconocido
Permisos especiales / cuenta necesarios	☐ Sí ☐ No ☐ Desconocido En caso afirmativo, describa los permisos / la cuenta necesarios:

5. Evaluación del impacto (opcional)

Complete esta sección si puede evaluar el posible impacto.

Área de impacto	Evaluación de la persona notificante
Confidencialidad	☐ None ☐ Bajo ☐ Medio ☐ Alto ☐ Desconocido
Integridad	☐ None ☐ Bajo ☐ Medio ☐ Alto ☐ Desconocido
Disponibilidad	☐ None ☐ Bajo ☒ Medio ☐ Alto ☐ Desconocido
Seguridad física	☐ None ☐ Bajo ☐ Medio ☐ Alto ☐ Desconocido
Privacidad	☐ None ☐ Bajo ☐ Medio ☐ Alto ☐ Desconocido
Impacto en la cadena de suministro o en el ecosistema más amplio	☐ Ninguno ☐ Bajo ☐ Medio ☐ Alto ☐ Desconocido
Gravedad sugerida, si está disponible (opcional)	☐ Bajo ☐ Medio ☐ Alto ☐ Crítico ☐ Desconocido
Vector CVSS, si está disponible (opcional)	

6. Estado de explotación y divulgación

Campo	Respuesta
¿La vulnerabilidad ya es pública?	☐ No ☐ Sí ☐ Desconocido En caso afirmativo, indique la URL y la fecha:
¿Existe una prueba de concepto pública?	☐ No ☐ Sí ☐ Desconocido En caso afirmativo, indique la URL y la fecha:
¿Se conoce o sospecha una explotación activa?	☐ No ☐ Sí ☐ Desconocido En caso afirmativo, facilite los detalles:
¿Se ha contactado con otro fabricante, proveedor, CERT o coordinador?	☐ No ☐ Yes ☐ Desconocido En caso afirmativo, indique la entidad, el identificador del caso y la fecha:
¿Tiene previsto comentar o publicar el problema después de su corrección?	☐ No ☐ Sí ☐ Desconocido En caso afirmativo, facilite los detalles:
Fecha preferida para la divulgación coordinada, si procede	

Nota sobre divulgación coordinada:
Mantenga confidencial la información no pública sobre la vulnerabilidad hasta la fecha de divulgación acordada. Si cambia el riesgo, se observa una explotación activa o resulta probable una divulgación pública, póngase en contacto de inmediato con security@saluscontrols.com para que pueda reevaluarse el plan de divulgación.

7. Medidas correctivas o de mitigación sugeridas (opcional)

- Corrección sugerida de la causa raíz, si se conoce: _____
- Medida de mitigación temporal o solución alternativa sugerida, si se conoce: _____
- Práctica sectorial, regla defensiva o referencia pertinente: _____

8. Preferencia de reconocimiento

Opción	Respuesta
¿Podemos reconocer públicamente su contribución si se publica un aviso?	☐ Sí ☐ No
Nombre público, alias u organización	
Perfil o enlace de referencia preferido, si la política lo permite	

9. Archivos adjuntos e información adicional

Enumere los archivos incluidos con la notificación. No incluya contraseñas, tokens de autenticación, claves privadas ni datos personales o de clientes que no sean necesarios.

Campo	Respuesta
¿Hay archivos adjuntos a esta notificación?	☐ Sí ☐ No
Tipo de archivos adjuntos	☐ Capturas de pantalla ☐ Registros ☐ Vídeo ☐ Prueba de concepto ☐ Captura de paquetes ☐ Otro
Descripción de los archivos adjuntos	
Información adicional pertinente para la notificación	
Requisitos de confidencialidad o tratamiento	

Si incluye registros, capturas de pantalla, vídeos, capturas de paquetes o material de prueba de concepto, elimine antes de enviar la notificación los datos personales o de clientes innecesarios, contraseñas, tokens de autenticación, claves privadas u otra información sensible.

10. Confirmación de buena fe

Al enviar esta notificación, la persona notificante confirma, según su leal saber y entender, que:

☐ La notificación es exacta y se ha elaborado en el marco de una investigación de seguridad realizada de buena fe.
☐ Las pruebas se limitaron a sistemas, dispositivos, cuentas y datos que pertenecen a la persona notificante o para los que estaba autorizada a realizar pruebas.
☐ Se evitó el acceso, la conservación o la divulgación innecesarios de datos no públicos.
☐ La persona notificante coordinará la divulgación de conformidad con la política publicada, con sujeción a la legislación aplicable y a cualquier cambio urgente en el riesgo para los usuarios.
☐ Confirmo que no he incluido intencionadamente contraseñas, tokens de autenticación, claves privadas ni datos personales o de clientes innecesarios.

Fecha de envío: _____

Nombre o alias de la persona notificante, si se facilita:

_____

Cómo enviar esta notificación

Envíe el formulario cumplimentado por correo electrónico a: security@saluscontrols.com
También puede informar de una posible vulnerabilidad directamente por correo electrónico sin utilizar este formulario. Se recomienda utilizarlo porque ayuda a SALUS Controls PLC a recopilar la información necesaria para evaluar la notificación de forma eficiente.