Política de Divulgação de Vulnerabilidades

Comunicação responsável, investigação e correção de vulnerabilidades de segurança

Versão	Data de entrada em vigor	Responsável pelo documento	Contacto
1.0	Setembro de 2026	Equipa de Segurança da SALUS Controls PLC	security@saluscontrols.com

1. Introdução

A SALUS Controls PLC está empenhada em proteger a segurança dos seus produtos, serviços e clientes. Acolhemos comunicações responsáveis de clientes, investigadores de segurança, parceiros, programadores e outros membros da comunidade de segurança que identifiquem potenciais vulnerabilidades de segurança que afetem produtos ou serviços da SALUS Controls PLC.

O nosso objetivo é investigar prontamente potenciais comunicações de vulnerabilidades, manter uma comunicação adequada com a parte que efetuou a comunicação ao longo do processo e disponibilizar medidas de correção ou mitigação proporcionais para proteger os utilizadores.

Comunique potenciais vulnerabilidades de segurança de forma privada para security@saluscontrols.com. A SALUS Controls PLC confirmará a receção no prazo de três dias úteis e, em qualquer caso, o mais tardar no prazo de sete dias de calendário. Esta confirmação apenas atesta a receção da informação e não significa que o problema comunicado tenha sido confirmado como vulnerabilidade.

2. Âmbito

Esta política aplica-se a vulnerabilidades de segurança que afetem:

- Produtos da SALUS Controls PLC
- Firmware e software
- Aplicações móveis
- Serviços na cloud
- Aplicações Web e websites acessíveis ao público

Para questões relacionadas com instalação, configuração, garantia ou outros assuntos não relacionados com segurança, contacte a nossa equipa de Apoio ao Cliente através dos canais de suporte habituais.

Aceitamos comunicações de segurança relativas a produtos SALUS independentemente do seu estado no ciclo de vida. Para produtos dentro do respetivo período de suporte de segurança publicado, as vulnerabilidades e atualizações de segurança são tratadas em conformidade com as obrigações legais aplicáveis. Para produtos fora desse período, a SALUS Controls PLC continuará a avaliar as comunicações e poderá fornecer medidas de mitigação, aconselhamento sobre migração ou outras orientações de acordo com o risco, a viabilidade técnica e as obrigações aplicáveis.

3. Comunicação de uma Vulnerabilidade

Se considerar que identificou uma vulnerabilidade de segurança, comunique-a de forma privada por email para security@saluscontrols.com.

As comunicações podem ser efetuadas anonimamente. A ausência de um nome ou de um meio de contacto bidirecional não impedirá a receção ou avaliação inicial, mas poderá limitar a nossa

capacidade de solicitar informações adicionais, fornecer atualizações de estado ou oferecer reconhecimento público.

Aceitamos uma comunicação inicial enviada por email normal ou por outro canal. Se for necessário trocar código de exploração, credenciais, dados pessoais, configurações de clientes ou outras informações sensíveis, a SALUS Controls PLC disponibilizará um método seguro disponível para continuar a comunicação. A impossibilidade ou decisão da parte comunicante de não utilizar encriptação não fará, por si só, com que a comunicação seja rejeitada.

4. Informações a Incluir

Para nos ajudar a investigar a sua comunicação de forma eficiente, inclua, sempre que possível:

- Nome e modelo do produto
- Versão do firmware ou software
- Descrição da vulnerabilidade
- Passos necessários para reproduzir o problema
- Comportamento esperado e comportamento real
- Potencial impacto na segurança
- Capturas de ecrã, registos ou prova de conceito, se disponíveis
- Dados de contacto preferenciais para acompanhamento

Evite incluir informações pessoais sensíveis, salvo quando sejam necessárias para demonstrar a vulnerabilidade.

Indique também, quando souber, se o problema é público, está a ser explorado ativamente, afetou utilizadores ou foi comunicado a outro fornecedor, fabricante ou coordenador. Não é necessário fornecer todos os elementos solicitados para que possamos aceitar e registar uma comunicação.

Durante a divulgação coordenada, o acesso a informações não públicas sobre vulnerabilidades é limitado ao princípio da necessidade de conhecimento. A SALUS Controls PLC poderá partilhar as informações necessárias com equipas de produto, fornecedores, coordenadores, partes afetadas ou autoridades competentes para validação, correção, proteção dos utilizadores e cumprimento de obrigações legais, sujeito a controlos adequados de confidencialidade e proteção de dados.

Os dados pessoais enviados com uma comunicação de vulnerabilidade são tratados de acordo com o aviso de privacidade aplicável da SALUS Controls PLC. Consulte a política de privacidade em: https://saluscontrols.com/pt/politica-privacidade-cookies/.

5. Processo de Resposta

Após receber a sua comunicação, a SALUS Controls PLC irá:

- Confirmar a receção no prazo de três dias úteis e, em qualquer caso, no máximo em sete dias de calendário; sempre que possível, incluir um identificador único do caso e informação preliminar sobre o estado.
- Efetuar uma avaliação inicial no prazo de sete dias úteis
- Validar a vulnerabilidade comunicada
- Avaliar a sua gravidade e potencial impacto
- Desenvolver um plano de correção ou uma atualização de segurança, quando adequado
- Mantê-lo informado durante o processo de investigação e correção

- Enquanto o caso permanecer ativo, fornecer uma atualização substantiva do estado pelo menos uma vez a cada 30 dias de calendário e comunicar mais cedo quando o âmbito confirmado, o risco, a abordagem de correção ou a data de divulgação sofrerem alterações relevantes.
- Se forem necessárias informações adicionais, poderemos contactá-lo durante a investigação.

6. Correção Baseada no Risco

As vulnerabilidades confirmadas são priorizadas de acordo com a gravidade técnica, explorabilidade, produtos afetados, potencial impacto, exposição dos utilizadores, indícios de exploração ativa, medidas de mitigação disponíveis e necessidades de implementação segura. Uma classificação numérica pode contribuir para a avaliação, mas não determina por si só a prioridade de correção.

A SALUS Controls PLC define um objetivo de correção específico para cada caso e comunica alterações relevantes à parte comunicante. Quando não for possível uma correção imediata, poderão ser fornecidas medidas de mitigação ou orientações para redução do risco antes de estar disponível uma correção permanente.

7. Divulgação Coordenada de Vulnerabilidades

A SALUS Controls PLC trabalha com a parte comunicante e, quando necessário, com fornecedores, coordenadores e outras partes afetadas para definir uma data de divulgação específica para o caso. O calendário poderá ser revisto em função da gravidade, exploração ativa, risco para os utilizadores, progresso da correção e implementação, dependências da cadeia de fornecimento e obrigações legais ou regulamentares aplicáveis. Alterações relevantes à data prevista serão comunicadas às partes pertinentes.

A SALUS Controls PLC poderá antecipar a notificação aos utilizadores ou a divulgação pública quando uma vulnerabilidade já for pública, estiver a ser explorada ativamente, representar um risco urgente para os utilizadores, tiver probabilidade de ser divulgada indevidamente ou quando a notificação seja exigida por lei. Quando ainda não estiver disponível uma correção completa, a SALUS poderá fornecer medidas temporárias de mitigação ou redução de risco sem facilitar desnecessariamente a exploração.

As informações sobre vulnerabilidades corrigidas serão publicadas em avisos de segurança acessíveis e legíveis por pessoas. Os avisos identificarão a vulnerabilidade e os produtos afetados, as datas de publicação e revisão, o potencial impacto e gravidade, as medidas de correção ou mitigação disponíveis, as ações necessárias dos utilizadores e os dados de contacto. Os avisos relativos a componentes de terceiros poderão remeter para informações oficiais da fonte quando isso permita aos utilizadores determinar se os produtos SALUS são afetados.

As informações sobre vulnerabilidades serão também disponibilizadas num formato legível por máquina amplamente reconhecido, salvo se existir uma justificação documentada e aprovada para não o fazer. A publicação só poderá ser adiada ou omitida quando as condições aplicáveis tiverem sido avaliadas, documentadas e aprovadas.

Quando exigido pela legislação aplicável ou necessário para proteger os utilizadores, a SALUS Controls PLC informará os utilizadores afetados e fornecerá medidas de mitigação ou orientações corretivas disponíveis através de canais adequados e acessíveis.

8. Suporte de Atualizações de Segurança

A SALUS Controls PLC fornece atualizações de segurança durante o período de suporte definido para cada produto aplicável. O período de suporte é determinado de acordo com os requisitos legais

aplicáveis, considerando o período esperado de utilização do produto, a sua natureza e as expectativas razoáveis dos utilizadores.

O período de suporte será de, pelo menos, cinco anos, salvo se for razoável esperar que o produto seja utilizado por um período inferior, podendo ser superior quando tal se justifique pela vida útil prevista do produto. A data de fim do período de suporte aplicável será comunicada através das informações relevantes do produto.

9. Fora do Âmbito

Todas as potenciais comunicações de segurança são registadas e recebem uma avaliação inicial. Questões exclusivamente funcionais, comerciais ou relacionadas com suporte poderão ser encaminhadas para o canal de suporte adequado. Se um problema não puder ser inicialmente reproduzido, a SALUS Controls PLC poderá solicitar informações adicionais e reavaliar a comunicação quando surgirem novas evidências.

Questões teóricas, cenários com acesso físico, condições de negação de serviço, cenários de engenharia social e dependências de terceiros são avaliados de acordo com o seu impacto realista na segurança, explorabilidade e utilização prevista e razoavelmente previsível do produto.

As vulnerabilidades em componentes de terceiros integrados, fornecidos com ou dos quais um produto SALUS dependa continuam sujeitas à avaliação do impacto no produto SALUS.

10. Investigação Responsável de Segurança

A SALUS Controls PLC apoia a investigação de segurança responsável realizada de boa-fé. Pedimos aos investigadores que:

- Atuem de forma responsável e ética
- Evitem perturbar produtos, serviços ou operações dos clientes
- Evitem aceder, modificar ou eliminar dados dos clientes
- Comuniquem vulnerabilidades de forma privada através do processo descrito nesta política
- Concedam à SALUS Controls PLC tempo razoável para investigar e corrigir o problema antes da divulgação pública
- Cumpram todas as leis e regulamentos aplicáveis durante a investigação de segurança

Quando uma parte comunicante atua de boa-fé, cumpre esta política, evita causar danos e comunica prontamente, a SALUS Controls PLC não pretende iniciar ações judiciais apenas devido a investigação de segurança realizada em conformidade com esta política. Esta declaração não autoriza o acesso a sistemas ou dados de terceiros, não vincula terceiros ou autoridades e não elimina a obrigação da parte comunicante de cumprir a legislação aplicável e obter as autorizações necessárias.

11. Contacto

Para todas as comunicações relacionadas com segurança ou questões sobre esta política, contacte:

Equipa de Segurança da SALUS Controls PLC

Email: security@saluscontrols.com

12. Atualizações da Política

Esta política é revista pelo menos anualmente e após alterações relevantes aos requisitos legais aplicáveis, canais de comunicação, âmbito dos produtos ou processos de tratamento de vulnerabilidades. A versão atual, a data de publicação, a data da última atualização e o responsável pela política são apresentados na política publicada.

13. Reconhecimento

Com o consentimento da parte comunicante, a SALUS Controls PLC poderá reconhecer o nome, pseudónimo ou organização de uma parte que apresente uma comunicação válida de vulnerabilidade e apoie a divulgação coordenada. As comunicações podem ser efetuadas anonimamente e a recusa de reconhecimento não afeta a aceitação, priorização ou correção.

Esta política não constitui um programa de recompensas por vulnerabilidades nem garante recompensas financeiras ou de outra natureza.