

## RFC-2350

CSIRT-SC  
SC\_SSI\_0242-C

# Tabela de conteúdos

1	Preâmbulo .....	3
1.1	Sobre este documento .....	3
1.2	Data de lançamento .....	3
1.3	Disponibilidade do documento.....	3
1.4	Identificação e autenticação do documento .....	3
2	Informações de contato .....	3
2.1	Nome da equipe .....	3
2.2	Endereço .....	
2.3	Email .....	3
2.4	Fuso horário .....	3
2.5	Número de telefone .....	4
2.6	Número de fax .....	4
2.7	Site da Internet .....	4
2.8	Chaves públicas e criptografia.....	
2.9	Membros da equipe .....	4
2.10	Horário de funcionamento .....	4
3	Estatuto .....	5
3.1	Declaração de missão .....	5
3.2	Grupo constituinte .....	5
3.3	Afiliação / Organização patrocinadora.....	
3.4	Autoridade .....	5
4	Políticas .....	6
4.1	Tipos de incidentes e nível de suporte .....	
4.2	Cooperação, interação e divulgação de informações.....	
4.3	Comunicação e autenticação .....	6
5	Serviços.....	7
5.1	Serviços proativos .....	7
5.2	Serviços reativos .....	7
6	Formulários de relatório de incidentes.....	8
7	Isenção de responsabilidade .....	8

# 1 Preâmbulo

## 1.1 Sobre este documento

Este documento é a apresentação do CSIRT da Sagemcom de acordo com a RFC2350.

## 1.2 Data de lançamento

Esta versão SC\_SSI\_0242-C foi lançada em 13 de setembro de 2022.

## 1.3 Disponibilidade do documento

O documento pode ser baixado do site da Sagemcom:

<https://www.sagemcom.com/sagemcom-csirt>

O documento pode ser recebido por e-mail enviando uma solicitação para:

[csirt@sagemcom.com](mailto:csirt@sagemcom.com)

## 1.4 Identificação e autenticação do documento

Título : CSIRT-SC – RFC 2350

Versão: SC\_SSI\_0242-C

Data do Documento : 2022-09-13

Expiração: este documento é válido até ser substituído por uma versão posterior

Nível TLP : **TLP:CLEAR**

# 2 Informações de contato

## 2.1 Nome da equipe

Nome Completo : CSIRT-Sagemcom

Nome Curto : CSIRT-SC

## 2.2 Endereço

Sagemcom CSIRT, Franck Bonneville, 4 allée des Messageries, 92270 Bois Colombes, França

## 2.3 Email

[csirt@sagemcom.com](mailto:csirt@sagemcom.com)

Este e-mail é usado tanto para relatar incidentes quanto para contatar o CSIRT-SC.

## 2.4 Fuso horário

GMT+1

## 2.5 Número de telefone

Não disponível

## 2.6 Número de fax

Não disponível

## 2.7 Site da Internet

<https://www.sagemcom.com/sagemcom-csirt>

## 2.8 Chaves públicas e criptografia

CSIRT-SC usa a seguinte chave pública PGP :

ID: 0x99028588872003E9

Impressão digital : 51BC5B3F84ABF12C43F477BE99028588872003E9

A chave está disponível nos seguintes sites:

<https://pgp.circl.lu/>

<http://pgp.mit.edu/>

## 2.9 Membros da equipe

O líder da equipe do CSIRT-SC é Franck Bonneville

A equipe é composta por :

- ⇒ Gerentes e analistas de segurança de TI da equipe de segurança de TI da Sagemcom (DSSI)
- ⇒ Pentester e analista do Laboratório de Segurança de Produtos da Sagemcom (SPSL)
- ⇒ Com o apoio de outras equipes da Sagemcom envolvidas em segurança (Oficiais de Segurança de BU, DSI SOC,...)

## 2.10 Horário de funcionamento

A operação do CSIRT-SC é restrita ao horário comercial (CET 09:00-18:00 de segunda a sexta-feira), durante todo o ano, excluindo feriados bancários e públicos.

## 3 Estatuto

### 3.1 Declaração de Missão

O CSIRT-SC tem como objetivo prevenir, investigar e coordenar qualquer incidente de segurança cibernética e ameaça cibernética que possa impactar as atividades do Grupo Sagemcom.

### 3.2 Grupo constituinte

O CSIRT-SC conduz sua missão em 2 eixos:

- Suporta todas as equipes de sistemas de TI
- Suporta todas as equipes de negócios e produtos (desenvolvimento, fabricação, ...)

Além disso, o CSIRT-SC pode fornecer suporte a todos os funcionários e clientes da Sagemcom.

O suporte pode ser :

- Pesquisa geral
- Sensibilização e treinamento, recomendações,...
- Pesquisa de vulnerabilidades
- Gerenciamento de incidentes, Resposta a Incidentes Digitais e Forense (DFIR)
- Gerenciamento de crise cibernética.

### 3.3 Afiliação / Organização patrocinadora

O CSIRT-SC é um CSIRT industrial privado, de propriedade, operado e financiado pela Sagemcom.

### 3.4 Autoridade

O CSIRT-SC está vinculado ao Departamento de Qualidade, Ética e Riscos da Sagemcom e está sob a autoridade do CISO. O CSIRT-SC trabalha internamente em cooperação com outros departamentos da Sagemcom (TI, P&D, Unidades de Negócios, sites offshore,...). O CSIRT-SC coopera externamente com outros CERT e CSIRT.

## 4 Políticas

### 4.1 Tipos de incidentes e nível de suporte

O CSIRT-SC processará qualquer incidente de segurança relacionado à sua missão. O nível de suporte do CSIRT-SC será ajustado para fornecer um nível de resposta adaptado a qualquer ameaça, vulnerabilidade, análise de incidentes (avaliação, impacto, remediação).

O CSIRT-SC fará os esforços razoáveis para fornecer sua resposta no mesmo dia útil durante o horário comercial ou no próximo dia útil.

### 4.2 Cooperação, interação e divulgação de informações

#### Internal communication:

As informações relacionadas à segurança são compartilhadas dentro da equipe do CSIRT-SC. Por padrão, as informações são categorizadas como confidenciais e não podem ser compartilhadas fora da equipe sem autorização do gerente do CSIRT-SC. Um nível específico de confidencialidade pode ser atribuído às informações relacionadas à segurança, caso a caso e sujeito ao procedimento aplicável dentro do Grupo Sagemcom. O gerente do CSIRT-SC fornecerá uma lista de casos de uso específicos aprovados pelo CISO do Grupo Sagemcom para os quais o nível de confidencialidade será menor.

#### External communication:

Por padrão, a comunicação externa é limitada a uma lista de parceiros aprovados pelo CISO do Grupo Sagemcom; tipicamente, outros CSIRT e CERT ou grupos de trabalho orientados para a segurança (CLUSIF, CESIN, InterCERT France).

A comunicação externa segue o nível de confidencialidade baseado no TLP (Protocolo de Semáforo versão 2.0) conforme definido pela FIRST (<https://first.org/tlp/> )

### 4.3 Comunicação e autenticação

O CSIRT-SC é o ponto de contato único para tópicos de segurança cibernética da Sagemcom, seja relacionado a produtos ou TI.

Para contatar o CSIRT, envie um e-mail para: [csirt@sagemcom.com](mailto:csirt@sagemcom.com)

Para troca de informações seguras, a seguinte chave PGP pode ser usada:

ID: 0x99028588872003E9

Impressão digital: 51BC5B3F84ABF12C43F477BE99028588872003E9

## 5 Serviços

O CSIRT-SC fornece serviços relacionados aos seguintes aspectos:

- Pesquisa geral: tecnologia, ameaça, produto, proteção de IP de marca
- Sensibilização, treinamento, recomendações
- Pesquisa de vulnerabilidades, auditorias, pentest
- Resposta a Incidentes, forense, gerenciamento de crise

Alguns serviços são proativos, e alguns são reativos.

### 5.1 Serviços proativos

- Pesquisa técnica
- Inteligência de ameaças e IoC
- Pesquisa, avaliação e notificação de vulnerabilidades
- Sensibilização e treinamento de pessoal
- Recomendações
- Auditoria técnica e pentest
- Proteção de provas e forense
- Organização de exercícios cibernéticos
- Desenvolvimento de ferramentas
- Melhoria da detecção de intrusão
- Comunicação geral interna sobre segurança cibernética
- Compartilhamento de informações (CERT/CSIRT) e workshop

### 5.2 Serviços reativos

- Avaliação de ameaças
- Avaliação e prioridade de vulnerabilidades
- Análise de alertas e suporte ao SOC
- Avaliação de incidentes baseada na análise de incidentes (triagem)
- Coordenação de incidentes (prioridade, rastreabilidade, notificação, acompanhamento)
- Suporte à resolução de incidentes, remediação e recuperação
- Ponto de contato único
- Suporte ao gerenciamento de crises cibernéticas

## 6 Formulários de relatório de incidentes

Nenhum formulário de relatório foi desenvolvido para relatar incidentes ao CSIRT-SC. Para relatar um incidente fora da organização Sagemcom, forneça as seguintes informações:

- Detalhes de contato (nome/e-mail e opcionalmente número de telefone).
- Data da descoberta do incidente
- Descrição geral do incidente
- Ativo afetado
- Informações técnicas sujeitas à viabilidade técnica e legal.

O formulário de relatório de incidentes é enviado por e-mail para : [csirt@sagemcom.com](mailto:csirt@sagemcom.com)  
Informações sensíveis podem ser criptografadas usando a chave PGP do CSIRT-SC.

## 7 Isenção de responsabilidade

O CSIRT-SC tomará todas as precauções necessárias e aplicará sua melhor competência e esforço na execução de seus serviços. No entanto, o CSIRT-SC não se responsabiliza por erros, omissões ou danos resultantes do uso das informações fornecidas. Os serviços fornecidos pelo CSIRT-SC não são projetados ou destinados a abordar todas as questões de qualidade, segurança, desempenho ou condição de qualquer produto, material, serviços, sistemas ou processos. O CSIRT-SC e a Sagemcom Broadband SAS excluem expressamente todas as garantias, condições e outros termos implícitos por estatuto ou por lei (incluindo, mas não se limitando a quaisquer garantias implícitas de comercialização e adequação para o propósito). Todos os direitos de propriedade intelectual em quaisquer relatórios, documentos, gráficos, tabelas, fotografias ou qualquer outro material (em qualquer meio) produzidos pelo CSIRT-SC na execução de seus serviços, incluindo todos os direitos em conceitos, ideias e invenções que possam surgir, pertencerão à Sagemcom Broadband SAS.

FIM DO DOCUMENTO