Serviço de Resposta a Incidentes da Secretaria-Geral da Economia e do Mar (CSIRT-RMSE)

RFC 2350

Baseado em https://www.ietf.org/rfc/rfc2350.txt

Versão: 1.2

Data: 03/03/2024

1 Informação acerca deste documento

Este documento descreve o serviço de resposta a incidentes de segurança informática da Secretaria-Geral da Economia e do Mar, em conformidade com a RFC2350.

1.1 Data da última atualização

Versão 1.2 publicada em 27/03/2024.

1.2 Listas de distribuição para notificações

A distribuição do documento será feita usando lista específica para o efeito.

1.3 Acesso a este documento

A versão mais recente deste documento está disponível em https://www.sgeconomia.gov.pt/csirt.aspx

1.4 Autenticidade deste documento

Com o objetivo de garantir a validação deste documento, a versão mais recente é disponibilizada em https://www.sgeconomia.gov.pt/csirt.aspx assinada com a chave PGP da Secretaria-Geral da Economia e do Mar, cuja chave pública se encontra no ponto 2.7.

2 Informação de contacto

2.1 Nome da equipa

CSIRT-RMSE - Computer Security Incident Response Team da Rede Multisserviços da Economia.

2.2 Morada

CSIRT-RMSE

Secretaria-Geral da Economia e do Mar

Av. da República, 79
1069-218 Lisboa
Portugal

2.3 Zona horária
Portugal/WEST (GMT+0, GMT+1 in Summer Time)

2.4 Telefone
+351 21 791 16 00

2.5 Outras telecomunicações
Não existentes.

2.6 Endereços de correio eletrónico
O endereço de correio eletrónico para notificação de incidentes relacionados com a cibersegurança é: csirt@sgeconomia.gov.pt

O endereço de correio eletrónico para outros assuntos relacionados com o CSIRT-RMSE: csirt-rmse@sgeconomia.gov.pt

2.7 Chaves públicas e informação de cifra
User ID: csirt-rsme <csirt-rsme@sgeconomia.gov.pt>

Key ID: 0x233A3E53

Key size: 4 096-bit RSA; Expires: 03/11/2026

Fingerprint: 2B90B67397379C7D31B828AF5C285CEB233A3E53

2.8 Membros da equipa
Direção: Ricardo Prieto
Coordenação: Alfredo Ferreira

A informação sobre os membros da equipa apenas está disponível por solicitação.

2.9 Outra informação
Toda a informação relativa ao CSIRT-RMSE pode ser encontrada em https://www.sgeconomia.gov.pt/csirt.aspx

2.10 Meios de contacto

O CSIRT-RMSE dispõe dos seguintes meios de contacto:

Notificação de incidentes relacionados com a cibersegurança: csirt@sgeconomia.gov.pt

Outros assuntos relacionados com o CSIRT-RMSE: csirt-rmse@sgeconomia.gov.pt

+351 21 791 16 00

3 Guião

3.1 Missão

A missão do CSIRT-RMSE é contribuir para a melhoria contínua da segurança dos sistemas de informação e da infraestrutura da Secretaria-Geral da Economia e do Mar e da respetiva Área Governativa, ajudando a prevenir, monitorizar, mitigar e dar resposta a ciberataques e promovendo a partilha de informação em matéria de cibersegurança além de apoiar a validação das políticas internas neste domínio.

3.2 Comunidade servida

O CSIRT-RMSE responde a incidentes de segurança informática no âmbito comunidade da Secretaria-Geral da Economia e do Mar e da respetiva Área Governativa, que engloba os seus utilizadores, sistemas e infraestruturas, representados publicamente pelos seguintes domínios e respetivo endereçamento IP.

Domínios:

Domínio	Entidade	Titular	Entidade Gestora	Name Servers
ani.pt	ANI	ANI	ANI	SGEM
asae.gov.pt	ASAE	ASAE	SGEM	SGEM
asae.pt	ASAE	ASAE	ASAE	SGEM
base.gov.pt	IMPIC	IMPIC	IMPIC	SGEM
comerciocomhistoria.gov.pt	DGAE	DGAE	SGEM	SGEM
consumidor.gov.pt	DGC	DGC	SGEM	SGEM
consumidor.pt	DGC	DGC	DGC	SGEM
dgae.gov.pt	DGAE	DGAE	SGEM	SGEM
dgconsumidor.gov.pt	DGC	DGC	SGEM	SGEM
dgpm.gov.pt	DGPM	SGEM	SGEM	SGEM
dgpm.mm.gov.pt	DGPM	SGEM	SGEM	SGEM
emepc.gov.pt	EMEPC	SGEM	SGEM	SGEM
emepc.mm.gov.pt	EMEPC	SGEM	SGEM	SGEM

Domínio	Entidade	Titular	Entidade Gestora	Name Servers
gama.gov.pt	GAMA	SGEM	SGEM	SGEM
gama.mm.gov.pt	GAMA	SGEM	SGEM	SGEM
gee.gov.pt	GEE	GEE	SGEM	SGEM
gisaf.gov.pt	GPIAAF	GPIAAF	SGEM	SGEM
gpiaa.gov.pt	GPIAAF	GPIAAF	SGEM	SGEM
iapmei.pt	IAPMEI	IAPMEI	IAPMEI	SGEM
innovationscoring.pt	IAPMEI	IAPMEI	DMNS	SGEM
ipac.pt	IPAC	IPAC	IPAC	SGEM
ipq.pt	IPQ	IPQ	IPQ	SGEM
min-economia.pt	SGEM	SGEM	SGEM	SGEM
reachhelpdesk.pt	DGAE	DGAE	IAPMEI	SGEM
sgeconomia.gov.pt	SGEM	SGEM	SGEM	SGEM
turismodeportugal.pt	TDP	TDP	DMNS	SGEM

Redes IP: 195.225.180.0/22 (AS202277)

3.3 Filiação

O CSIRT-RMSE faz parte do Núcleo de Gestão de Políticas de Segurança Informática e está integrado na Direção de Serviços de Sistemas de Informação da Secretaria-Geral da Economia e do Mar.

3.4 Autoridade

O Núcleo de Gestão de Políticas de Segurança Informática encontra-se definido no Despacho n.º 11408/2021, publicado no Diário da República, 2.ª série, de 19 de novembro, retificado pela Declaração de Retificação n.º 846/2021, publicada no Diário da República, 2.ª série, de 26 de novembro, e alterado pelo Despacho n.º 5459/2023, de 2 de maio de 2023, com as seguintes competências:

a) Assegurar o desenvolvimento, definição e cumprimento das normas de segurança associadas aos sistemas de informação da área da Economia, de acordo com as melhores práticas internacionais,

b) Assegurar a articulação com os serviços tutelados por outros ministérios, tendo em vista o reforço da segurança das comunicações e dos Sistemas de Informação da Administração Pública;

c) Implementar e garantir políticas de segurança adequadas, quer ao nível das redes, quer dos sistemas de informação, garantindo a segurança, confidencialidade e integridade da informação e das plataformas tecnológicas associadas;

d) Assegurar a defesa e lidar com ameaças de segurança da informação, garantindo a prestação de serviços críticos em situações adversas através de uma adequada gestão do risco e da implementação de mecanismos de confidencialidade, integridade e disponibilidade.

4 Políticas

4.1 Tipos de incidente e nível de suporte

O CSIRT-RMSE responde a todos os tipos de incidente de cibersegurança, enquadrados num dos vetores de disponibilidade, confidencialidade ou integridade, especialmente aqueles que resultam numa violação dos seguintes tipos:

a) Negação de Serviço/Disponibilidade;
b) Código Malicioso;
c) Intrusão/Tentativa de Intrusão;
d) Fraude/Personificação;
e) Conteúdo Abusivo;
f) Vulnerabilidades.

4.2 Cooperação, interação e política de privacidade

A política de privacidade e proteção de dados do CSIRT-RMSE prevê que informação sensível pode ser passada a terceiros, nos termos do RGPD.

4.3 Comunicação e autenticação

O telefone e o correio eletrónico não cifrado são considerados suficientes, de entre os meios de comunicação disponibilizados pelo CSIRT-RMSE, para a transmissão de informação não sensível. No caso da transmissão de informação sensível o uso de cifra PGP é preferencial, sendo o uso de proteção por *password* o recurso para quando o uso de cifra não seja possível.

5 Serviços

5.1 Resposta a Incidentes

A equipa do CSIRT-RMSE, prevê apoiar os administradores de sistemas nos aspetos técnicos e organizacionais do processo de gestão de incidentes, bem como as restantes equipas técnicas e outras áreas de negócio. Em particular, deverá prestar assistência e definir diretivas estratégicas.

5.1.1 Triagem de incidentes

Classificar, avaliar, priorizar e encaminhar um incidente.

5.1.2 Coordenação de incidentes

Identificar e contactar as entidades envolvidas, aplicar e gerir os procedimentos previstos para a resolução de incidentes nas ações de cada organismo, entidade ou equipa.
Agilizar os canais de comunicação, bem como assegurar a apresentação de relatórios do incidente ao CERT.

5.1.3 Resolução de incidentes

Coordenação operacional junto das equipas locais de IT nas ações previstas a adotar e acompanhamento do progresso da resolução do incidente, gerindo a informação decorrente das operações, produzindo relatórios e respondendo a solicitações.

5.2 Atividades proactivas
O CSIRT-RMSE coordena e mantém os seguintes serviços para expandir os seus recursos:

Monitorização e alarmística;
Desenvolvimento, implementação e manutenção de soluções de segurança sobre sistemas, aplicações e infraestruturas;
Auditorias de segurança e deteção de intrusão;
Divulgação de informação estruturada sobre segurança;
Avaliação da evolução tecnológica e adoção de novas soluções.

6 Formulários de notificação de incidentes
Formulário disponível através da plataforma de *ticketing* ou, em alternativa, na área restrita do *site*. Para notificações através de e-mail devem ser utilizados os contactos indicados em 2.6.

7 Salvaguarda de responsabilidade
O Núcleo de Políticas de Segurança Informática não poderá assumir qualquer responsabilidade por erros ou omissões, ou por danos resultantes do uso da informação divulgada quer no portal Internet, quer através das listas de distribuição, contrárias a políticas aprovadas, embora tome todas as precauções na sua preparação.

8 Chave pública PGP
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGVEO/ABEACpmjHDT0Bpktbc/w+jNtr++B4KmRiHFZDzV7cK6SE+skGQFZCP
AHmc7Xgptvc6NODr6jA2MBXlCL/sIT358vMIA1xbYO5kPYWzMsQb4eMFSmbJUEiq
0ybsXQI5VuXxnhXYTj0JxZsocDpC7W/75Qqm9mhSKuLRa+58x37Smjh/DAlDdtkr
qUYIduUVPHS5kFE7i4v2NPPRQ/b163kzZSmsRNTN/KMrCh4Ublx1o5RHz/2LNnpO
7Nqwdzsgjjf20BnsEW49Gy/xYzWLK2MiVpq+q73kbSeF35mlMKSzruYoFJuemjr1
4DwuSAaUYVNkwD9/rqNiSYuCxyLf24MMQgB8ji2xJ7PuagenMPMY+6VoieG8mbg0
7xNy2zNlyTe5wkVZWqGTnXuCwq4xoB3k2aGe59NVA5LB2zQ3XVmK10uJs6gKTLxN
Ysc04KuUqs2udgJNlkRowYlUVeNPs8VHFCn2JtwQ7rShTRs3ekGP6KlPdKFrFklY
aPOMUuCUeoxXrzNfTTInrUvO+l7g0m5fDA8UJJWAl6XTNkHf91ckpeXwGGR5wUn8
Mjo31+hC8jk51qleCxTvQrH3M5YxR804ETCtyDjPWnlf952ew3zAi4IxYa5yCzMP
gITNYB/AcdXJ6oLIhqSPm3ZH3T/dJb2WgOREtbgtAQRyhQtgRW2CUl2RpQARAQAB
tCljc2lydC1yc21lIDxjc2lydC1yc21lQHNnZWNvbm9taWEuZ292LnB0PokCVwQT
AQgAQRYhBCuQtnOXN5x9Mbgor1woXOsjOj5TBQJlRDvwAhsDBQkFpZDQBQsJCAcC
AiICBhUKCQgLAgQWAgMBAh4HAheAAAoJEFwoXOsjOj5TnYkP/j4dtIx/BTdVamP6

Q3A52EjAQlmk7PdX1KAJnHqLSWvhtke+JJvkuBU4kCx5P4wnOUwZ4UwEqDM7YcPn
n/rQeNCTpfUQddz2DsyXhpxPhnzsOF/bJn53AQL4lhwvadk4MW/iOD15VzlkBDBu
+9j8D5jToqY8mFTkyle8dquaWYoY5zJUMCjOURwX5Hng5SV/rXjEcchoS/9NS/bo
ZQyiDgxWMwtJ/MhUm2x8h2JBQ9mZuXI1J4Lcp8eyfK7PZSpbwVSkATxkmXUjYuol
RctHzmkJFIsFTBuo0UY6pB5xjA17nqdUfYbQ7LpbWok6HL5W94LMNk3368eU27G+
djJSfXvdjQCTQ35YIwBB/1fjY9yj4P8g8IL1jZfrsw3iAXPc4TQfVSaDTRUAo2C2
PhJxqZFVivdMq+EMGie5GMYTiOKCFDb7SO5XMMUBS4o3nZLo43zEYbzEwXTM3uhW
FPY2Nax+Wu6RY+779G78ZLvikiFevY0vdQBS1fFsZsu3tTxwNcBmqVivKEHiI8DG
+Tf8jWJRgqJRxn+/o7Dwmd1bVvN4ND7s0WuXc3oJ8hMt+U26e4Z+FJHLbeL1JSVb
GhKulRWh75Yl8LYdsrTcA9WXkJ2MyQp4kYLQOmq2LhoqfZ4p4mLIgeh2adFDix4n
L+sMEOq4voAHugDqJssizFtKuUs5uQINBGVEO/ABEADjYv9guiQh2yzFDeC5S4WS
RlPP3LhaUJJb/12VJxz2G2NnAwx7WYE6hMo9kFVcOt3K/mbHSzuUjJqw7oBOP1bI
vJMmdb3SQdcEW5wwVDtQKeOWRp55eMozOPG2FI1dGe0+zy8jx5iWx6a2J8d9tc53
iu1CrDTQl+r7xlKuWTBWnfrvbd0RrmwlmfeqoVE+hKps6IWcIsJLus4qBYslHLe8
Sv6kbSk5sicVBWol7r7y6AAM2wp5zkk7/yXg1a+6mMDLpZMPbcEfIdDc4GuCyzTt
D17UZFEaN9NrGyMl8kgwC1KNKFetB+0hKWwEPvEDAh0LqjYOZzSf5NBzAsiY5DID
xhU9B94VSUt8l0zmxLW9m0Q1bZQ5h5kEBYWS9ajw+NXPjMjwNXHi/+LyhZ/NlRvq
lOJw6lV6qRbF9DsRqgpYBT1b/+MjgiBNrAVAyPb0mQfM8ezmWATL0/qC0wTry1b5
86Rv5NI/pVVf10PbLWQ7IrC4/RJ03B3d68lZVx56Qr6BBAYo65LnD0aSfaUU/hbH
SfwIW2dnknjPHcZBKe+QLe0d3MXlY3SWH6cRS7Ev6zFmKlPUI9zLXgprXzIWBLP5
I/J4cMTLqZ4DiPvpRBwaqM53pTkqwZ5RMNCeUxsrOK2cZrHS6zqaNZYHUvkD91wN
HQvivAfCIJUYB/upwGSnbwARAQABiQI8BBgBCAAmFiEEK5C2c5c3nH0xuCivXChc
6yM6PlMFAmVEO/ACGwwFCQWlkNAACgkQXChc6yM6PlM4UBAApJmxRTl9Q9J6ZWw7
RyKWqz46yFQEniZbIbd+M04yBUEO62Fmcrh0ZYg0sDR4Z/2tZmX3BePclESCFV1U
15fJQcdn9P0+B06bV8KD4VhMYWqY04pvutV8BZDneBrzP2EQ8BMLrvVntzo2rgNo
lw4Fy2uz4O8ajwJFjKceDg/fRkMNM4RPRErB7AuaNVcpCmy6SVst03xQYwS0k6fH
xmIQX2Lelbav4ihVYcSJuTgJgGlE6srHABov8OrKFkLGLt6ko7BY71BYWjRrofQP
ZQAC0CLHEtiCwIAxf0QO9WmDpO0f5rxP9EmwaT1BWMB6xpYNxWHoOxOgu82jOmxA
BxI4VcGsTn1YaMI7Omg2LCZUDXTcRCh6EHxg/VIbRxYrxuh9QNFkPtfTUoIwTOmt
aoCuCyC4IIw+qpsY6R70rt1ncbUq028vK2WX8uIuPWynK1drVVVyAyfHwcKGZevq
bk+WWlUKPGhXl0zRIvho24lUSklrzODSJP3/XVPllbimX3D4uuEcb8fDCS9yYTUc
Y8ku8U1RcebFyLEMhKLDYulW8fvIZeO4C5DLDUv/J7e514CkkI+FYT/I6xxouq6u
p19IxAleSe20BvIk8pbWUthrEnf90U/WPNISs6wsgs0Rvx2K21WjFGNwDkcbNbv0
fuo2VmGmYhwrlhxoCN+3xnK0UXc=
=9SyK
-----END PGP PUBLIC KEY BLOCK-----