Serviço de Resposta a Incidentes da Secretaria-Geral do Governo (CSIRT-GOV)

RFC 2350

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

Versão: 1.0

Data: 01/04/2026.

1. Informação acerca deste documento

Este documento descreve o serviço de resposta a incidentes de cibersegurança da Secretaria-Geral do Governo e da Rede Interna do Governo, em conformidade com a RFC2350.

1.1 Data da última atualização

Versão 1.0 publicada em 01/04/2026.

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://csirt-gov.sggoverno.gov.pt/"

1.4 Autenticidade deste documento

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

2. Informação de contacto

2.1 Nome da equipa

CSIRT-GOV - Computer Security Incident Response Team da Secretaria-Geral do Governo e Rede Interna do Governo.

2.2 Morada

CSIRT-GOV

Secretaria-Geral do Governo

Campus XXI, Av. João XXI, 63
1000-300 Lisboa
Portugal

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

2.4 Telefone
+351 213 923 412

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@sggoverno.gov.pt

2.7 Chaves públicas e informação de cifra
User ID: CSIRT-GOV <csirt@sggoverno.gov.pt>
Key ID: 518A 14DB 0EE2 D9ED
Key size: 4 096-bit RSA; Expires: 01/04/2027
Fingerprint: BBE0 48D1 5DDC 611F 5933 DD20 518A 14DB 0EE2 D9ED

2.8 Membros da equipa
Direção: Ricardo Prieto
Divisão: Divisão de Cibersegurança e Resiliência Digitais
A informação sobre os membros da equipa apenas está disponível por solicitação.

2.9 Outra informação
Toda a informação relativa à CSIRT-GOV pode ser encontrada em https://csirt-gov.sggoverno.gov.pt/

2.10 Meios de contacto
A CSIRT-GOV dispõe dos seguintes meios de contacto:
Notificação de incidentes relacionados com a cibersegurança: csirt@sggoverno.gov.pt

3. Guião
3.1 Missão

Secretaria-Geral do Governo

A missão da CSIRT-GOV é contribuir para a melhoria contínua da segurança dos sistemas de informação e da infraestrutura da Secretaria-Geral do Governo e da respetiva Área de Ação Governativa, bem como das entidades dependentes das mesmas, 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

A CSIRT-GOV responde a incidentes de segurança informática no âmbito comunidade da Secretaria-Geral do Governo e da Área de Ação Governativa, que engloba os seus utilizadores, identidade, sistemas e infraestruturas, representados publicamente pelos seguintes domínios e respetivo endereçamento IP.

Domínios:

Domínio	Entidade	Titular	Entidade Gestora	Name Servers
acreditacao.media.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
apps.ceger.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
ceger.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
ebupi.mj.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
ecce.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
ecee.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
emce.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
emext.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
emropm.pm.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
esquadra.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
gtre.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
ma.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
maa.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
maac.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
maap.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mact.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
madj.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
maec.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
maen.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mafdr.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
magrim.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
magrip.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mai.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mail.consultalex.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mail.portugal.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mam.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mamb.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
map.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mare.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mate.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mc.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mcjd.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mct.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mctes.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mdn.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
me.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
meci.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mecon.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mect.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
media.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
medu.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mem.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt

Domínio	Entidade	Titular	Entidade Gestora	Name Servers
metd.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mf.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mh.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mi.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mih.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mj.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mjm.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mm.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mmeap.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mne.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mp.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mpcm.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mpi.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mpma.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
ms.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
mtsss.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
oe.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
pcm.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
pm.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
portugal.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
portugaldigital.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
portugalforukraine.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
portugalin.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
scee.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
seap.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
sg.pcm.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
sgeconomia.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
sggov.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
sggoverno.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt
sirp.gov.pt	SGGov	SGGov	SGGov	dns1.gov.pt / a.dns.pt

Redes IP:

193.47.185.0/24 (AS35822)

195.225.180.0/22 (AS202277)

3.3 Filiação

A CSIRT-GOV é parte integrante da Divisão de Cibersegurança e Resiliência Digitais e está inserida na Direção de Serviços da Transformação Digital, da Secretaria-Geral do Governo.

3.4 Autoridade

A Divisão de Cibersegurança e Resiliência Digitais encontra-se definido na Portaria n.º 205-B/2025/1, de 30 de abril, publicado no Diário da República n.º 83/2025, Suplemento, Série I, de 30 de abril, com as seguintes competências:

a) Garantir a conformidade com o quadro legal no âmbito da cibersegurança;

b) Assegurar o estudo de sistemas de informação de utilização comum para os gabinetes dos membros do Governo, com especial enfoque na segurança, garantindo a proteção e resiliência das infraestruturas tecnológicas, bem como a confidencialidade, integridade e disponibilidade da informação governamental;
c) Prestar apoio de consultoria aos membros do Governo e respetivos gabinetes, em matérias de segurança eletrónica;
d) Definir e elaborar um sistema de gestão de riscos para as tecnologias de informação e tecnologias operacionais, visando garantir a conformidade com os preceitos legais de âmbito;
e) Definir, elaborar e implementar um sistema de gestão e segurança da informação e de gestão da informação, assegurando o planeamento estratégico e operacional de sistemas de informação, respetiva monitorização, avaliação e promoção do alinhamento;
f) Assegurar a representação no Conselho para o Digital na Administração Pública;
g) Assegurar as funções que lhe sejam cometidas no âmbito do Sistema de Certificação Eletrónica do Estado - Infraestrutura de Chaves Públicas (SCEE), assim como, atuar na qualidade de entidade certificadora de outros serviços, organismos e entidades públicas, sempre que tais funções lhe sejam especialmente cometidas por lei ou convenção;
h) Assegurar o desenvolvimento da política e ambiente de segurança e resiliência digital, garantindo a consolidação de competências digitais e a sensibilização para a segurança e resiliência digitais.
i) Assegurar o desenvolvimento do modelo de governação de sistemas de informação e arquitetura empresarial corporativa, de acordo com as arquiteturas de referência;
j) Promover a orientação para harmonização no desenvolvimento das próprias normas e políticas, garantindo uma arquitetura coerente e integrada assegurando a promoção de ações de conformidade e assessoria para cumprimento de normas e requisitos obrigatórios e recomendados na área de sistemas de informação e segurança e resiliência digital;
k) Promover a inovação e partilha de conhecimento na área de sistemas de informação e uniformização da governação de dados, bem como a promoção de reutilização de dados;
l) Assegurar a gestão integrada do ciclo de vida dos ativos do ecossistema aplicacional da SG-Gov, assim como no âmbito da gestão integrada da operação, exploração e monitorização.

4. Políticas

4.1 Tipos de incidente e nível de suporte

A CSIRT-GOV 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) Código Malicioso;
b) Disponibilidade;
c) Recolha de Informação
d) Intrusão;
e) Tentativa de Intrusão;
f) Segurança da Informação;
g) Fraude;
h) Conteúdo Abusivo;
i) Vulnerabilidades.

4.2 Cooperação, interação e política de privacidade

A política de privacidade e proteção de dados da CSIRT-GOV 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 pela CSIRT-GOV, 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 CSIRT-GOV, 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

A CSIRT-GOV coordena e mantém os seguintes serviços para expandir os seus recursos:

a) Monitorização e alarmística;
b) Desenvolvimento, implementação e manutenção de soluções de segurança sobre sistemas, aplicações e infraestruturas;
c) Auditorias de segurança e deteção de intrusão;
d) Divulgação de informação estruturada sobre segurança;
e) 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

A Divisão de Cibersegurança e Resiliência Digitais 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-----
mQINBGnWiZ4BEACn5Ox10QNxVzrMYE+Lno7Ema469fzD+5t0iVo1hL5H8yszlYaX
Nr+7TV7szw0X/BqkIJ5Npnu9V+mhKi7yDDwpkbdlSF9yTcfPuVLUMg/knZ7VQHtQ
9KJ/ez3YUNX7USDXk6y7J0fc+WlgdixLM9LJryCJ7aKYjL4Y/+BrP35zEQfM6ycl
utTjHaEruEwnDh1rjPSflA4G6sAF8wy/5V6bIqHNxpJqsGVlywDPq5DezTTd3fBu
vpLvoyK2PsZhXTeLx6E5vAy0Mb4lf+gxaGksQXN+gQvHC8upumsbE+5eg1e+KdF7
IyTkJ6iSgVqq98UKxQaBKOfXQzX+MVOPo79psimbrowH+ZD/uXOiop57ASEXXnEy
Ka4PyAnSbXZxlY2/t4VnT/vwe6cdR2dtnREYJEdHeMEipLudZ2rT4cbS9tJYoxlB
TptEj3MHrJPwTgTRPn1nzKowhiyTx0HzR4aFaAXt6HAzjrv7difaKts9TLUNS1FP
4pNTJj/ku8oVra96/uJb9stepQEagQ/+HZzdxqvHa7hbyWamg5M+mQBSh8w0Gvcc
ukUxIMjyG5hom/R6OYLXsYREPU+66Dl3Zvpa4elEjNj42SwS459Otxc1c9lvbsy3
+PYFYh09uFCQ95BF23JwceYRsxsQM+pSvHZiMGGOnBfHyAK+82SN/TT1EQARAQAB
tCJDU0lSVC1HT1YgPGNzaXJ0QHNnZ292ZXJuby5nb3YucHQ+iQJzBBMBCABdGxSA
AAAAAAQADm1hbnUyLDIuNSsxLjEyLDIsMQIbAwULCQgHAgIiAgYVCgkICwIEFgID
AQIeBwIXgBYhBLvgSNFd3GEfWTPdIFGKFNsO4tntBQJp1orpBQkB2E0VAAoJEFGK
FNsO4tntrgsQAKGa/f9LK8Dd1eaHbh8g9utzuWDkBMtwsEuJW8b0kZ5OqE0KBK+g
EbCa3Nf/HA52yyb6Tw8nBQn29JJsJ0txFSEdaYYmaDhRYQ07NjCg24Bpz4KjREm3
2WjBto7AGAiNkJqSrulyqVsaXDRYKdj9yJdBysXMJUMJIcmkaWMUZS9ESXmCf1lw
LvZ1uvT48Or0UfQM+II4RNktRE0M5gwW0GcryFuZhS+jvm/7EfE8eYan8u5MKznx
aHxRO6NIfWdv4WuoB3EvEhuTA/zCnhGEiFS1/ZYZ4g6n2K7foGkWW/AM3Qzx4p3X
7/GY8btXjlEqOv1jv3VaEB4kYKP4HUeNuGAmX4lY/uYAVbFj359+sJcOiuSbfFsz
BGMX9j8pZf0H6mI/HXyDz3rl/uDMqe6+REgS7KBHTzYnfemrI10owWAFbAk0Yi6b
z3cjeppVOKQTnSlebk8FPKFO1Npt0Fqts5KEmRybvBi1ioHT8sxOo7nbJcYKpGS5
L/cOvmhpTTKDuiZMOpYpCSXCR9WT/F3GHkKTGetN82wKFKyUDrtJqTD6KkVkP/Df
jZ61b5ogBg2z0Ic6i11uLgXLYno4BCxBnhImHF0gkD2GT1oxMXO8YnaQTSpBBBkX
0XH+VZZw8YwNezgayrVJ57HM5haMgP9aoQUKPEs+P1W1/eTgnjotauSmuQINBGnW
iZ4BEACrbg0IK2ha30ZszKpoIrOmJd61CJr6RzgNC1Y5g26IsCWHwB1dmgseYgm3
tyfosVSSJH5SxY6vCrpq/X6sidmLsCoMxD6ZzuGfVG3g4y+zypBJOOAH8o2pBVrJ
MfnMvJ3DLxk2BEX99I8UnDOLlrqQlcyHAZ5BbTCCeQPgeRy1dSvZ3dVXxi6odNbz
x+4XzZiy9oynK3d/wY1+vOtlMUqkMtEtymVDzsvk5EdTWeDYG4QD4otoItsoIL76
9u//yTTA4NhfS3xy+v4i0Dxqtrp5Ia5Hxko6OXJwoVyw5e9vNyvD4R7kODSxVQ4W
H/038jf0heP3YNzVlCLX+SrWi7qI0x4Eckqu7MOKiAkGWO4i7k2x/+lGYxS/cvPY
osh2DlLe2vioQBI+2dSHBdQQOwcfjo5AJgc65duAeAjCPg/H+YU8tJJt6Dinz2oM
rL6hK4M8xt68by/hcslHZJ2teNg8Rqqu/2eFtCGQwUvunB2e2uXs8OSRuz2ytN/n
SursV3RgShlmKOg6b6pJgQaSzFZ88MINmYqJ9RemtiMV0U9OT0ub7eMwITxsxGbZ
sE3alj7qAnCrrxP6QA9lt289rH1O/J0eeXKuEEeqLpxvEXl2/+tvwZJiQrhGgn+1
EKO+ult+OAW73W7j+g2C175NmfYMXW+b/RL34z7/FOmUzu7GGwARAQABiQJYBBgB
CABCGxSAAAAAAAQADm1hbnUyLDIuNSsxLjEyLDIsMQIbDBYhBLvgSNFd3GEfWTPd
IFGKFNsO4tntBQJp1oryBQkB2E0eAAoJEFGKFNsO4tnte28P/1wfn3sQDEbNKbiD

Secretaria-Geral
do **Governo**

dY6dz5b/RaEvzgjKU8r411hYpqNHi2ouObWqCkRdvb8aqfs0/h7gJd2WpoC5fxKw
LvasVBD2rTVjRm3MoCrXSqdxXtwHirw8BxZQAQzI0Fa8mpnkRsj/vgW75+LPJa3e
E3WVNgqHwifZuqxWP228OSOsdE1XKNnHg/rIMYstaG8w/XhZbpUSeQ3xRCpwz1Xy
UhZvo01+sUGghMiEWiE3hV7Xkyu8Rvr3ffBHwvt73+zCCv/poQOa2f/MAt47Wg82
bFtFrVTBsjUYJdyV6nQ7u0scZPLVBbP8tSvrNGFNK5z9JxhJqPsQV7oRCByRVmAS
RLxXlUlSKfQuhCdq3+8uH/Yj73bfRsOltnoGVX7f6Au8i4y+Z0qcXeWGUp+mHm0s
gG/OwnKgz/fm5odWxSlizfi9P1ihMnAjAdfXgdm6JW7nPqNNTLSwxv/OIgP0s8aF
ruAM4/JN3XS348uHpkiTawlZUdz4G05j4DqGyC8KU4lc0cC/mcqLlUkSI3esoz6E
F44iDsLkFBkJJxrHM9k8LP0PoDy/JbB59PTrzfHq+oRxSGexKrQXTOjFFJgXBg20
ffG5dsaaRXm0JTV72ME7lcYYZpnj7dp2AbmJFtkHc0qo6esmBHXP7srOncZ5yddD
Ow5vCRCDuf8FHI+XfpXm/bPqChyX
=qT9a
-----END PGP PUBLIC KEY BLOCK-----