-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

RFC 2350: CSIRT@UC
Última Revisão: Alexandre Santos

1 Informação acerca deste documento
Este documento descreve o serviço de resposta a incidentes de segurança
informática da Universidade de Coimbra (UC), em conformidade com RFC2350.
É um serviço integrante da Rede Académica de CSIRT.

1.1 Data da última atualização
Versão 1.0 publicada em 2023/05/16.

1.2 Listas de distribuição para notificações
Não existe um canal de distribuição para notificar alterações a este documento.

1.3 Acesso a este documento
A versão atualizada deste documento pode ser encontrada em
+ rfc2350-pt.txt

1.4 Autenticidade deste documento
Esta versão da descrição do RCTS CERT encontra-se assinada com a chave PGP
da equipa CSIRT@UC.

2 Informação de contacto

2.1 Nome da equipa
CSIRT@UC

2.2 Endereço postal
Rua do Arco da Traição
3000-056 COIMBRA

2.3 Zona horária
Portugal/WEST (GMT+0, GMT+1 em horário de verão)

2.4 Telefone
+351 239 24 70 70

2.5 Fax
+351 239 827 994

2.6 Endereço de correio eletrónico
csirt@uc.pt

2.7 Outras telecomunicações
Não existentes.

2.8 Chaves públicas e informação de cifra
A chave PGP da equipa CSIRT@UC tem o KeyID 0x5EEBF0A0FEBDC1A4 e o fingerprint é 9EA8 6FB0 AE40 CBE4 3EEE EB3A 5EEB F0A0 FEBD C1A4. Esta chave pode ser encontrada nos habituais servidores de chaves públicas existentes na Internet, como por
exemplo pgp.mit.edu ou keys.openpgp.org.

2.9 Membros da equipa
Coordenação: Alexandre Santos
Membros: Luis Gonçalves
Apoio jurídico: Gabinete Jurídico da UC

2.10 Outra informação
Mais informação sobre a equipa CSIRT@UC pode ser encontrada em https://ucpages.uc.pt/sgsiic/ncs/csirt

2.11 Meios de contacto para utilizadores
O CSIRT@UC dispõe dos seguintes meios de contacto (por ordem de preferência):
Correio eletrónico para comunicação de incidentes de segurança informática:
csirt@uc.pt
Correio eletrónico para outros assuntos relacionados com segurança informática:
ncs@uc.pt
Telefone
+351 239 24 70 70

3 Guião

3.1 Missão
O CSIRT@UC tem como missão central contribuir para o esforço de cibersegurança da comunidade, nomeadamente através do tratamento e coordenação da resposta a incidentes, na produção de alertas e recomendações de segurança e na promoção de uma cultura de cibersegurança.

3.2 Comunidade servida
O CSIRT@UC responde a incidentes de segurança informática no âmbito comunidade da Universidade de Coimbra, que engloba os seus Sistemas e Infraestruturas, Utilizadores suportados nos seguintes domínios e gamas de endereços IP:

Domínios:

csirt.uc.pt
*.uc.pt;

Redes IP:
192.84.13.0/24
192.84.15.0/24
192.92.144.0/24
193.136.94.0/23
193.136.200.0/22
193.136.204.0/23
193.136.212.0/22
193.136.230.0/23
193.136.236.0/23
193.137.93.0/24
193.137.102.0/24
193.137.200.0/21
193.137.208.0/24
193.137.209.0/24
193.137.210.0/23
193.137.212.0/24
193.137.214.0/23
194.210.160.0/20
194.210.16.0/20
194.210.32.0/20
Redes privadas internas;

3.3 Filiação
O CSIRT@UC é responsável pelo tratamento de incidentes de segurança informática na UC.

3.4 Autoridade
O CSIRT@UC é um serviço integrante do Núcleo de cibyrsegurnaça da Universidade de Coimbra (NCS@UC).
O NCS@UC encontra-se definido em despacho interno, e também com competências definidos em regulamento interno, nas seguintes matérias:
a) Dar resposta a questões legais do DL 65/2021;
c) Propostas de melhorias e acompanhamento da segurança dos sistemas de informação e das infra-estruturas de suporte;
d) Reforço da capacidade para enfrentar incidentes de cibersegurança e ciberataques;
e) Promoção de ações de formação e qualificação de recursos humanos na área da segurança informática;
f) Promoção da adoção de referenciais normativos ao nível das TIC nas áreas da segurança de informação e da cibersegurança.

O NCS@UC articula-se e partilha recursos com os serviços do Serviço de Gestão de Sistemas e Infraestruturas de Informação e Comunicação (SGSIIC) para uma melhor resposta aos incidentes de segurança.

3.4 Responsabilidades do CSIRT@UC
O serviço de segurança CSIRT@UC assegura a monitorização das operações de rede, a coordenação da reação a incidentes de segurança, incluindo as ações de corte total ou parcial, temporário ou definitivo, de serviço, quando estas se afigurem necessárias para a proteção da Instituição, da RCTS ou da internet em geral, ou ainda a gestão de vulnerabilidades dentro da Instituição que venha a ter

conhecimento.

4 Políticas

4.1 Tipos de incidente e nível de suporte
O CSIRT@UC responde a todos os tipos de incidente de segurança, sendo que adota a taxonomia da Rede Nacional CSIRT, disponível em: https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf
O nível de suporte dado pelo CSIRT@UC varia consoante o tipo, gravidade e âmbito dos incidentes em curso e os recursos disponíveis para o seu tratamento.

4.2 Cooperação, interação e política de privacidade
A política de privacidade e proteção de dados do CSIRT@UC estabelece que informação sensível pode ser transmitida a terceiros, única e exclusivamente em caso de real necessidade e com a autorização prévia expressa do indivíduo ou entidade a quem essa informação diga respeito.

4.3 Comunicação e autenticação
Dos meios de comunicação disponibilizadas pelo CSIRT@UC, o telefone e o mail não cifrado são considerados suficientes para a transmissão de informação não sensível. Para a transmissão de informação sensível é obrigatório o uso de cifra PGP.

5 Serviços

5.1 Tratamento de incidentes de segurança
Entende-se por incidente de segurança informática qualquer ação ou conjunto de ações desenvolvidas contra um computador ou rede de computadores e que resulta, ou pode resultar, na perda da confidencialidade, integridade ou desempenho de uma rede de comunicação de dados ou sistema informático, designadamente, o acesso não autorizado, a alteração ou remoção de informação, a interferência ou a negação de serviço em sistema informático.
O CSIRT@UC trata incidentes de segurança informática no contexto da comunidade académica e Organismos, ou seja, incidentes onde a origem ou o alvo dos ataques é a Instituição.

5.2 Disseminação de alertas
O CSIRT@UC propõe-se reunir um conjunto de informação recebida de várias fontes bem conhecidas, avaliar o grau de severidade e traduzi-la para língua portuguesa. Dependendo do seu grau de severidade a informação analisada pode resultar num alerta de segurança, numa recomendação ou numa simples notícia publicada no portal http://www.uc.pt/csirt, ou na subscrição de uma lista para distribuíção de informação.

5.3 Campanhas de awareness Anti-Phishing
O CSIRT@UC em conjunto com o NCS@UC sensibiliza e treina os

colaboradores da instituição a lidar com situações de fraude através de mensagens de correio electrónico, simulando uma campanha de phishing e realizando posteriormente uma sessão de sensibilização.

6 Formulários de reporte de incidentes

https://uc360.uc.pt/forms/notificacao-de-incidentes-de-seguranca

7 Salvaguarda de responsabilidade

Embora todas as precauções sejam tomadas na preparação da informação divulgada quer no portal Internet, quer através das listas de distribuição,
a equipa do Núcleo de Cibersegurança da Universidade e Coimbra não assume qualquer
responsabilidade por erros ou omissões, ou por danos resultantes do uso dessa informação.

-----BEGIN PGP SIGNATURE-----

-----END PGP SIGNATURE-----