1 Informação acerca deste documento

1.1 Data da última atualização

Versão 1.0 publicada em 2023/09/16.

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 e da sua versão em inglês podem ser encontradas em https://www.ipv.pt/csirt-ipv/#documentos.

1.4 Autenticidade deste documento

Esta versão e a versão em inglês da descrição do CSIRT.IPV encontra-se assinada com a chave PGP, sendo possível consultá-las em https://www.ipv.pt/csirt-ipv/#documentos.

2 Informação de contacto

2.1 Nome da equipa

CSIRT.IPV

2.2 Endereço postal

Avenida Coronel José Maria Vale de Andrade
Campus Politécnico
3504-510 Viseu
Portugal

2.3 Zona horária

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

2.4 Telefone

+351 232 480 700 (horário normal de funcionamento – 09h00-12:30 e 14:00-17h30).

2.5 Fax

Não existente.

2.6 Endereço de correio eletrónico

csirt@sc.ipv.pt

2.7 Outras telecomunicações

Não existentes.

2.8 Chaves públicas e informação de cifra

User ID: CSIRT.IPV csirt@sc.ipv.pt
Key ID: 0x844C654E Key type: RSA
Key size: 4096 Expires: Never
Fingerprint: 2B1D72D5B2F9E1FFEE8F71FE920C3985844C654E
A chave pública (Public Key) pode ser encontrada em https://www.ipv.pt/csirt-ipv/#documentos.

2.9 Membros da equipa

Coordenação: Filipe Caldeira
Membros: João Branco
Pedro Carvalho
Luís Almeida
Carlos Barros
Apoio jurídico: Paula Bettencourt

2.10 Outra informação

Mais informação sobre o CSIRT.IPV pode ser encontrada em https://www.ipv.pt/csirt-ipv.

2.11 Meios de contacto para utilizadores

O CSIRT.IPV dispõe dos seguintes meios de contacto (por ordem de preferência):
Correio eletrónico: csirt@sc.ipv.pt
Telefone: +351 232 480 700

3 Guião

3.1 Missão

O CSIRT.IPV tem como missão a promoção de uma cultura de segurança nos meios informáticos dentro da comunidade académica do Politécnico de Viseu, recorrendo a ações de sensibilização, aconselhamento e dando resposta a incidentes de segurança informática detetados internamente ou reportados por equipas de resposta a incidentes das redes académicas e nacionais.

3.2 Comunidade servida

O CSIRT.IPV responde a incidentes de segurança informática no contexto da comunidade da Instituto Politécnico de Viseu. As gamas de endereços IP abrangidos no âmbito de atuação do CSIRT.IPV são:

IPV4: 193.137.7.0/24
193.137.141.0/24
194.210.123.0/24
IPV6: 2001:690:20C0::/48

3.3 Filiação

O CSIRT.IPV é um centro integrado nos Serviços de Informática do Instituto Politécnico de Viseu.

3.4 Autoridade

O CSIRT.IPV tem autoridade para responder a Incidentes que ocorram dentro do IPV, bem como para responder em nome da organização nos processos resposta a Incidentes em colaboração com entidades externas à mesma.

4 Políticas

4.1 Tipos de incidente e nível de suporte

O CSIRT.IPV responde a incidentes nas áreas de segurança informática, nomeadamente na intrusão ou tentativa de intrusão, código malicioso, disponibilidade, recolha de informação, segurança da informação, fraude, conteúdo abusivo e vulnerabilidades.

4.2 Cooperação, interação e política de privacidade

A política de privacidade e proteção de dados do CSIRT.IPV prevê que informação sensível pode ser passada a terceiros, única e exclusivamente em caso de 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 disponibilizados pelo CSIRT.IPV, o correio eletrónico não cifrado e o telefone 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

O CSIRT.IPV prevê apoiar os administradores de sistemas na gestão dos aspetos técnica e organizacional dos incidentes. Em particular, poderemos providenciar assistência e aconselhamento com os seguimentos aspetos da gestão de incidentes:

5.1.1 Triagem de Incidentes

- Determinar quando um incidente é autêntico.
- Avaliar e priorizar um incidente.

5.1.2 Coordenação de Incidentes

- Determinar as organizações envolvidas.

- Contactar as organizações envolvidas para investigar o incidente e tomar as medidas adequadas.
- Facilitar o contacto com outras partes que podem ajudar na resolução do incidente.
- Enviar relatórios a outros CERTs.
- Vemo-nos como um hub de informação que conhece a instituição e consegue encaminhar os incidentes para ajudar e facilitar a resolução dos incidentes de segurança informática.

5.1.3 Resolução de Incidentes

- Aconselhamento das equipas locais de administração de sistemas das ações apropriadas a adotar.
- Acompanhar o progresso das equipas de administração de sistemas relativamente a questões de segurança.
- Solicitar relatórios.
- Dar resposta às solicitações.

O CSIRT.IPV colecionará ainda estatísticas sobre incidentes no contexto da sua operação.

5.2 Atividades proactivas

O CSIRT.IPV coordena e mantêm os seguintes serviços para expandir os seus recursos:

- Produção de alertas e disseminação de informação relacionada com segurança.
- Monitorizar a infraestrutura, aplicações e sistemas sob a perspetiva de vulnerabilidades de segurança informática.
- Promover Auditorias de segurança ou avaliações.
- Definir, implementar e garantir a execução de normas e procedimentos técnicos nas suas áreas de competência.

6 Formulários de report de incidentes

Não existem disponíveis formulários para o efeito.

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, o CSIRT.IPV não assume qualquer responsabilidade por erros ou omissões, ou por danos resultantes do uso dessa informação.