Instrução nº 1

Notificação de Incidentes de Cibersegurança e de Violação de Dados Pessoais no IPV

Aprovo

O Presidente do IPV

Assinado por: **JOSÉ DOS SANTOS COSTA**
Num. de Identificação: 03968707
Data: 2022.06.08 09:06:27+01'00'

Cibersegurança

O Regime Jurídico da Segurança do Ciberespaço, constitui a lei-quadro que estatui o cumprimento das normas técnicas e organizativas destinadas à promoção da cibersegurança e, bem assim, os requisitos de notificação de incidentes

A Administração Pública, deve notificar o CNCS (Centro Nacional de Cibersegurança-CNCS) da ocorrência de incidentes de cibersegurança com impacto relevante ou substancial, devendo para esse efeito implementar todos os meios e os procedimentos necessários à detecção e avaliação do impacto dos mesmos.

Por cada incidente com impacto relevante ou substancial, as entidades devem submeter ao CNCS uma notificação inicial (enviada logo que a entidade possa concluir que existe ou possa vir a existir impacto relevante ou substancial e até duas horas após essa verificação), uma notificação de fim de impacto relevante ou substancial (deve ser submetida ao CNCS logo que possível, dentro do prazo máximo de duas horas após a perda de impacto relevante ou substancial) e uma notificação final (enviada no prazo de 30 dias úteis a contar do momento em que o incidente deixou de se verificar).

Nos casos em que o incidente seja resolvido de forma imediata, nas primeiras duas horas após a sua deteção, as entidades podem enviar diretamente a notificação final com todos os campos de informação devidamente preenchidos, ficando dispensadas do envio das restantes notificações.

As notificações devem incluir informação diversa, consoante o caso, nomeadamente acerca do impacto do incidente, do número de utilizadores afetados pela perturbação do serviço, da duração e da área geográfica afetada e eventual impacto transfronteiriço, assim como a descrição do incidente, com indicação da categoria da causa raiz e dos efeitos produzidos. Devem ser igualmente indicadas as medidas adotadas para mitigar o incidente.

Os incidentes podem ter, como causa raiz, uma falha de sistema, um fenómeno natural, um erro humano, um ataque malicioso ou uma falha no fornecimento de bens ou serviços por terceiro. Estas causas podem dar lugar aos seguintes efeitos do incidente, as quais devem ser objeto de notificação à CNCS: infeção por malware; disponibilidade; recolha de informação; intrusão; tentativa de intrusão; segurança da informação; fraude; conteúdo abusivo.

A resposta a incidentes de segurança informática, em particular a contenção da ameaça e o restabelecimento da funcionalidade, deve ter o cuidado de preservar as evidências que ajudem a determinar e comprovar os sistemas e a informação afetados pelo incidente.

Para o efeito, todos os incidentes de segurança informática devem ser reportados ao Responsável de Segurança, do IPV pelo endereço de **email** **rs.ciber@sc.ipv.pt**, com conhecimento dos Pontos de Contato Permanente, através da lista de distribuição **pc.ciber@sc.ipv.pt** e DPO, **dpo@sc.ipv.pt**, sem demora injustificada, para registo, avaliação das medidas a tomar e eventual notificação ao Centro Nacional de Cibersegurança- CNCS.

A avaliação do risco deve ser feita em conjunto com o DPO.

Enquadramento Legal: Lei n.º 46/2018, de 13 de agosto e Decreto-Lei n.º 65/2021, de 30 de junho, Regulamento nº 183/2022 de 27 de fevereiro.

Após análise do incidente, este é reencaminhado para o interlocutor da Unidade Orgânica responsável pelo sistema informático, utilizador ou IP que originou o incidente, para notificação do mesmo através do **Formulário de Notificação de Incidente de Cibersegurança da CNCS (https://www.cncs.gov.pt/pt/notificacao-incidentes/)**

Simultaneamente, deve ser dado conhecimento da evolução do tratamento do incidente, ao Responsável de Segurança, com conhecimento dos Pontos de Contato Permanente e DPO.

Mediante a severidade do incidente e do seu impacto, escalar o conhecimento e tomada de decisão ao Presidente da Instituição.

Rede de Interlocutores: https://site.ipv.pt/rgpd/redeipv.htm

Dados pessoais

Uma das principais medidas introduzidas no novo RGPD é o Artigo 33º -Violação de Dados, que consiste numa falha de segurança acidental ou ilícita e que pode levar à destruição, perda, alteração, divulgação não autorizada e ao acesso não autorizado dos dados pessoais.

Com isto, é obrigatório reportar certos tipos de violação de dados à Autoridade de Controlo(Comissão Nacional de Proteção de Dados- CNPD) e aos Titulares dos Dados afetados da seguinte forma:

- **Responsável pelo Tratamento (Presidência IPV),** por intermédio do DPO**,** fica obrigado a notificar a **CNPD** da violação de dados pessoais, sem demora injustificada, através do **Formulário de notificação de Incidente de Cibersegurança e Violação de Dados Pessoais em https://www.cnpd.pt/databreach/?AspxAutoDetectCookieSupport=1),** sempre que possível até 72 horas após ter tido conhecimento da mesma. Se o prazo não for cumprido, é necessário apresentar os motivos do atraso com a notificação;
- **Titular dos Dados**, em caso de um elevado risco na violação dos dados pessoais, o responsável pelo tratamento tem a responsabilidade de notificar os titulares afetados (RGPD-art.º 34º);
- **Subcontratante,** deve notificar o responsável pelo tratamento sem demora injustificada, após ter conhecimento de uma violação de dados.

Para o efeito, todas as violações de dados pessoais, têm de ser comunicadas ao Encarregado da Proteção de Dados (DPO), por email para o endereço **dpo@sc.ipv.pt.** sem demora injustificada, para registo, avaliação das medidas a tomar e eventual comunicação à Comissão Nacional de Proteção de Dados e aos Titulares dos Dados.

A notificação, deve, pelo menos e se possível:

- Descrever a natureza da violação dos dados pessoais incluindo, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;
- Descrever as consequências prováveis da violação de dados pessoais;
- Descrever as medidas adotadas ou propostas para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos;

Mediante a severidade da violação de dados pessoais e do seu impacto, escalar o conhecimento e tomada de decisão ao Presidente da Instituição.

Quando a sensibilidade da informação o justifique deve ser cifrada e a chave que a decifre enviada ao DPO por canal diferente do email.

Rede de Interlocutores: https://site.ipv.pt/rgpd/redeipv.htm .