



Ministério da Justiça - MJ

Conselho Administrativo de Defesa Econômica - CADE

SEPN 515 Conjunto D, Lote 4 Ed. Carlos Taurisano, 1º andar - Bairro Asa Norte, Brasília/DF, CEP 70770-504

Telefone: (61) 3221-8552 e Fax: (61) 3326-9733 - www.cade.gov.br

PORTARIA CADE Nº 92, DE 12 DE ABRIL DE 2016.

Institui o Glossário da Política de
Segurança da Informação e Comunicações
– POSIC no âmbito do Conselho
Administrativo de Defesa Econômica –
Cade.

O PRESIDENTE DO CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA, no uso da atribuição que lhe é conferida pelo disposto no artigo 10, inciso IX, da Lei nº 12.529/2011, no artigo 22, inciso IX, do Anexo I do Decreto nº 7.738/2012, e no artigo 11, inciso IX, do Regimento Interno do Cade, aprovado pela Resolução nº 1, de 29 de maio de 2012, tendo em vista o disposto no inciso VII do art. 5º da Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008, na Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 30 de junho de 2009, e no Art. 6º da Portaria Cade nº 88, de 12 de abril de 2016, que cria a POSIC-Cade, resolve:

Art. 1º Aprovar o Glossário da Política de Segurança da Informação e Comunicações do Cade;

Art. 2º Publicar o arquivo do Glossário em formato PDF no sítio do Cade no endereço eletrônico www.cade.gov.br e na sua intranet;

Art. 3º Esta Portaria entra em vigor na data da sua publicação.

VINICIUS MARQUES DE CARVALHO

Presidente

GLOSSÁRIO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

CAPÍTULO I

Seção I

Dos objetivos

Art. 1º Esta norma estabelece definições utilizadas no arcabouço normativo do Cade quanto à segurança da informação e comunicações, conforme disposto no Art. 6º da POSIC.

CAPÍTULO II

Seção I

Dos conceitos e definições

Art. 2º No âmbito da POSIC e suas normas complementares, considera-se:

- I. Agente responsável pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR: servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal – APF - incumbido de chefiar e gerenciar a ETIR;
- II. Ativo de informação: meio de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
- III. Autenticidade: propriedade que a informação tenha sido produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por determinado sistema, órgão ou entidade;
- IV. Classificação da Informação: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;
- V. Comitê de Segurança Institucional do Cade – CSIC: colegiado deliberativo responsável por sustentar as estratégias de Gestão de Segurança da Informação, das Instalações e das Comunicações no Cade;
- VI. Informação sigilosa – informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;
- VII. Custodiante de ativo de informação: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;
- VIII. Disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade;
- IX. Equipe de Tratamento e Resposta a Incidentes em Redes de Computadores – ETIR: colegiado com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em redes de computadores no âmbito do Cade;
- X. Ética: observância à Lei nº8.112 de 11 de dezembro de 1990 – que dispõe sobre o regime jurídico dos servidores públicos da União, das autarquias e das fundações públicas federais - ao Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto nº 1.171, de 22 de junho de 1994, à Resolução nº16 de 9 de setembro de 1998 –

- que disciplina e orienta o comportamento ético dos servidores do Cade – e a demais regras de conduta normativamente delimitadas para os agentes públicos;
- XI. Gestão de Segurança da Informação e Comunicações – GSIC: ações e métodos que visam integrar as atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, táticos e operacionais, não se limitando, portanto, no âmbito da tecnologia da informação e comunicações.
- XII. Gestor de SIC: servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da APF designado pelo Presidente do Cade como responsável pela GSIC no âmbito do Cade;
- XIII. Incidente de SIC: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
- XIV. Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independente do suporte em que resida ou da forma pela qual seja veiculado;
- XV. Integridade: propriedade de que a informação não foi modificada ou destruída de maneira culposa ou dolosa;
- XVI. Legalidade: observância dos parâmetros legais e regulamentares na implementação das ações de SIC;
- XVII. Segurança da informação: proteção dos ativos de informação contra perda, corrupção, destruição, acesso, uso e alteração indevidos ou não autorizados;
- XVIII. Privacidade: proteção do direito individual da pessoa à inviolabilidade de sua intimidade e vida privada e do sigilo de suas comunicações, observando o disposto no Art. 5º da Constituição Federal de 1988, Art.31 da Lei nº 12.527, de 18 de novembro de 2011, e nos Arts. 55 a 62 do Decreto nº 7.724, de 16 de maio de 2012;
- XIX. Risco de SIC: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
- XX. Tratamento de incidentes: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança da informação, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;
- XXI. Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle de informação, inclusive as sigilosas; e
- XXII. Vulnerabilidade: fragilidade de um ativo ou grupo de ativos de informação que pode ser explorada por uma ou mais ameaças.

CAPÍTULO III

Disposições Finais

Art. 3º O CSIC é responsável por manter este glossário atualizado e aderente à legislação e normas.

Art. 4º Esta norma será revisada sempre que se fizer necessário.



Documento assinado eletronicamente por **Vinícius Marques de Carvalho, Presidente**, em 12/04/2016, às 18:39, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.



A autenticidade deste documento pode ser conferida no site
[http://sei.cade.gov.br/sei/controlador_externo.php?](http://sei.cade.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)
[acao=documento_conferir&id_orgao_acesso_externo=0](http://sei.cade.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador
0185361 e o código CRC **5D86DD3A**.
