



Ministério da Justiça e Segurança Pública- MJSP
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 - www.cade.gov.br

PORTARIA CADE Nº 404, DE 20 DE MAIO DE 2019.

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

O **PRESIDENTE DO CADE**, no uso da atribuição que lhe é conferida pelo disposto no artigo 10, inciso IX, da Lei nº 12.529/2011, no artigo 21, inciso IX, do Decreto nº 9.011/2017, e no artigo 60, inciso IX, do Regimento Interno do Cade, aprovado pela Resolução nº 20, de 7 de junho de 2017,

RESOLVE:

Art. 1º Alterar o Glossário da Política de Segurança da Informação e Comunicação do Cade, instituído pela Portaria Cade nº 403, de 20 de maio de 2019.

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.

ALEXANDRE BARRETO DE SOUZA

Presidente

(assinado eletronicamente)

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, 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. atividades remotas: atividades realizadas pelo Cade fora dos domínios do prédio, como: operações, reuniões externas, congressos, conferências ou quaisquer outros eventos que o servidor esteja a serviço e utilizando computadores do Cade.
- III. 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;
- IV. ativos de infraestrutura: equipamentos ou *softwares* utilizados para manter a infraestrutura de redes do Cade em funcionamento, como: *switches*, *firewalls*, *storages*, servidores, etc;
- V. autenticidade: propriedade que a informação tenha sido produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por determinado sistema, órgão ou entidade;
- VI. backup completo: cópia de segurança de todos os dados de um a pasta, sistema ou unidade de disco;
- VII. backup incremental: cópia de segurança com a função de complementar um backup completo com dados que foram adicionados ou modificados;
- VIII. backup sintético: cópia de segurança que atualiza um backup completo com as atualizações e modificações dos arquivos;
- IX. backup diário crítico: realização de cópia de segurança de dados ou sistemas críticos para o funcionamento do Cade em ambiente apartado do armazenamento utilizado em produção;
- X. *bring Your Own Device (BYOD)*: utilização de dispositivos pessoais para realizar atividades profissionais no Cade;
- XI. 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;
- XII. colaborador: pessoa física contratada pelo Cade por meio de processos de consultoria, serviços de suporte técnico junto ao fabricante e demais prestadores de serviços por contrato de terceirização;
- XIII. 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;
- XIV. criptografia: método de ocultação de informações mediante técnicas matemáticas, no armazenamento ou transmissão de dados, a fim de manter a confidencialidade dos dados;
- XV. 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;
- XVI. disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade;

- XVII. dispositivos móveis: dispositivos portáteis com capacidade de processamento de dados, como *tablets* e *smartphones*;
- XVIII. 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;
- XIX. estação de trabalho: computador utilizado para atividades funcionais. Computador de mesa (desktop), computador portátil (laptop/notebook) ou computador especializado (workstation);
- XX. 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;
- XXI. foto funcional: registro de imagem utilizada para fins de registro no Cade, para controle de gestão de pessoas e acesso físico nas dependências da autarquia.
- XXII. 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.
- XXIII. 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;
- XXIV. 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;
- XXV. incidente de SIC: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
- XXVI. 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;
- XXVII. integridade: propriedade de que a informação não foi modificada ou destruída de maneira culposa ou dolosa;
- XVIII. intercambista: pincadista ou servidor estrangeiro;
- XXIX. legalidade: observância dos parâmetros legais e regulamentares na implementação das ações de SIC;
- XXX. mapa de recursos mínimos: documento ou conjunto de documentos elaborados para definir os recursos mínimos de *software*, acessos a serviços internos e liberações de acessos para internet no Cade. Este mapa será criado e mantido pela CGTI em conjunto com cada unidade administrativa do Cade a nível de Coordenação Geral ou superior;
- XXXI. mídia digital: conjunto de dados armazenados em mídias físicas;
- XXXII. mídia eletrônica de armazenamento: dispositivo físico que armazena dados, como dispositivos móveis, discos rígidos, memórias de impressoras, *scanners*, multifuncionais, CDs e DVDs, *pendrives* dentre outros;
- XXXIII. pincadista: pessoa física participante do programa de intercâmbio PinCade;
- XXIV. 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;
- XXXV. raspagem de dados (*web scraping*): técnica de extração de dados automatizada em redes;

- XXVI. redes de registro distribuído (*blockchain*): redes descentralizadas com validação e auditoria de registros descentralizadas entre os participantes da rede;
- XXVII. 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;
- XVIII. sanitização de mídia: procedimento de sobrescrita a fim de tornar os dados da mídia irrecuperáveis;
- XXIX. segurança da informação: proteção dos ativos de informação contra perda, corrupção, destruição, acesso, uso e alteração indevidos ou não autorizados;
- XL. servidor: pessoa física regida pelo regime da Lei 8.112/90 ou equivalente, efetivo ou ocupante de cargo em comissão, em exercício no Cade;
- XLI. servidor estrangeiro: servidor de agências de defesa da concorrência de outras jurisdições e organismos internacionais participantes do Programa de Intercâmbio Internacional do Cade;
- XLII. termo de conduta, confidencialidade e não repúdio: comprometimento do servidor, colaborador ou estagiário sobre a obediência das normas internas do Cade, sigilo das informações que tenha acesso e não repúdio das regras da autarquia.
- XLIII. termo de custódia: acordo para cessão de equipamentos disponibilizados pelo Cade;
- XLIV. termo de uso: acordo para cessão de softwares ou serviços disponibilizados pelo Cade;
- XLV. 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;
- XLVI. tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle de informação, inclusive as sigilosas;
- XLVII. túnel criptográfico: técnica de criptografia para ocultar os dados transitados entre uma origem a um destino;
- XLVIII. unidades físicas de armazenamento: discos magnéticos, óticos ou eletrônicos para armazenamento de dados digitais. Mídias físicas de armazenamento; e
- XLIX. 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 **Alexandre Barreto de Souza, Presidente**, em 20/05/2019, às 19:10, 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?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0616604** e o código CRC **980CBBE2**.

Referência: Processo nº 08700.000342/2014-58

SEI nº 0616604