

Eixo Tecnologia da Informação

Conjunto de vocábulos da área de tecnologia da informação e comunicação.

- [Listagem Vocábulos de TIC](#)

- [A](#)
- [B](#)

Listagem Vocábulo de TIC

Listagem de Vocábulo e termos mais utilizados de TIC.

A

AAA: acrônimo de autenticação, autorização e auditoria.

AC: acrônimo de Autoridade Certificadora.

Acordo de Nível de Serviço: acordo entre a unidade responsável pelo provimento de um serviço de TIC e a área responsável pela informação tecnológica, no qual se estabelecem metas de qualidade e de desempenho para o serviço de TIC, considerando-se as necessidades do negócio, o impacto das soluções, o custo e a capacidade de alocação de recursos para o provimento do serviço de TIC.

AC-Raiz: acrônimo de Autoridade Certificadora Raiz.

Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique.

Access Control Lists (ACLs): são regras que auxiliam a tomada de ação baseada em critérios coletados, permitindo ou bloqueando determinados tipos de tráfegos na rede.

Active Directory (AD): é uma implementação de serviço de diretório no protocolo LDAP que armazena informações sobre objetos em rede de computadores e disponibiliza essas informações a usuários e administradores desta rede. É um software da Microsoft utilizado em ambientes Windows, presentes no active directory.

Administrador de Backup: pessoa ou equipe responsável pelos procedimentos de configuração, execução, monitoramento, elaboração de padrões, atendimento avançado de resolução de incidentes e problemas e testes dos procedimentos de backup e restauração, ao qual deve-se requisitar os procedimentos de criação ou restauração de backup.

Administrador de Perfil Institucional: agentes públicos que detenham autorização de responsável pela área interessada para administrar perfis institucionais de um órgão ou entidade da APF, direta e indireta, nas redes sociais.

Administrador da Rede: agente público que administra o segmento de rede correspondente à área de abrangência da respectiva unidade.

Advanced Encryption Standard (AES): criado pelo Instituto Nacional de Padrões e Tecnologia (NIST), tornou-se o padrão efetivo do governo federal americano em 2002, após cinco anos de desenvolvimento. Esse desenvolvimento começou em 1997, quando se verificou que seu antecessor, o data encryption standard (criptografia de dados padrão - DES), não mais atendia os

critérios de segurança. O AES é construído a partir de três cifras de bloco: AES-128, AES-192 e AES-256. Cada uma dessas criptografa e descriptografa os dados em pedaços de 128 bits, usando chaves criptográficas de 128, 192 ou 256 bits. As chaves de 128 bits têm 10 rodadas de processamento, as chaves de 192 bits têm 12 e as de 256 bits 14 rodadas.

Adware: do inglês Advertising Software, é um tipo específico de spyware projetado especificamente para apresentar propagandas. Pode ser usado de forma legítima, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo realizado.

Agente Responsável pela ETIR: agente público incumbido de chefiar e gerenciar a equipe de prevenção, tratamento e resposta a incidentes cibernéticos (ETIR).

Agente Responsável pela Gestão de Continuidade de Negócios: agente público incumbido de gerenciar o processo de gestão de continuidade de negócios em segurança da informação.

Agente Responsável pela Gestão de Mudança: agente público incumbido de gerenciar o processo de gestão de mudanças em aspectos de segurança da informação.

Agente Responsável pelo Mapeamento dos Ativos de Informação: agente público incumbido de gerenciar o processo de mapeamento de ativos de informação.

Agente Responsável pela Gestão de Riscos: agente público incumbido de gerenciar o processo de gestão de riscos de segurança da informação.

Agentes de Tratamento: o controlador ou o operador.

Alerta de ETIR: informação descritiva de um incidente cibernético enviada, de forma reativa, para notificação de usuários.

Algoritmo Criptográfico: função matemática utilizada na cifração e na decifração de informações sigilosas, necessariamente nas informações classificadas.

Algoritmo de Estado: algoritmo criptográfico desenvolvido pelo Estado e não comercializável, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta.

Algoritmo Registrado: função matemática utilizada na cifração e na decifração de informações não classificadas, para uso exclusivo em interesse do serviço de órgãos e entidades da APF, direta e indireta, cujo código fonte e método de processo sejam passíveis de controle e de auditoria.

Ambientação: evento que oferece informações sobre a missão organizacional do órgão ou entidade da APF, direta e indireta, bem como sobre o papel do agente público nesse contexto.

Ambiente Cibernético: inclui usuários, redes, dispositivos, software, processos, informação armazenada ou em trânsito, serviços e sistemas que possam ser conectados direta ou

indiretamente a redes de computadores.

Ambiente de Informação: agregado de indivíduos, organizações e/ou sistemas que coletam, processam ou disseminam informação.

Ameaça: qualquer evento que explore vulnerabilidades ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Ameaça Persistente Avançada (APT): operações de longo prazo projetadas para infiltrar ou exfiltrar o máximo possível de dados sem serem descobertas, sendo mais conhecidas pelo seu acrônimo em inglês APT - Advanced Persistent Threat. Possui ciclo de vida mais longo e complexo que outros tipos de ataque, sendo mais elaborados e necessitando de volume significativo de recursos para sua viabilização, o que exige forte coordenação. Em geral, são realizados por grupos com intenção de espionagem ou sabotagem.

Análise De Impacto nos Negócios (AIN): visa estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho dos órgãos ou entidades da APF, bem como as técnicas para qualificar e quantificar esses impactos. Define também a criticidade dos processos de negócio, suas prioridades de recuperação, interdependências e os requisitos de segurança da informação para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.

Análise de Incidentes: consiste em examinar todas as informações disponíveis sobre o incidente, incluindo artefatos e outras evidências relacionadas ao evento. O propósito da análise é identificar o escopo do incidente, sua extensão, sua natureza e quais os prejuízos causados. Também faz parte da análise do incidente propor estratégias de contenção e recuperação.

Análise de Riscos: uso sistemático de informações para identificar e estimar os riscos.

Análise de Vulnerabilidade: verificação e exame técnico de vulnerabilidades, para determinar onde estão localizadas e como foram exploradas.

Análise Dinâmica: tipo de teste de software que verifica seu comportamento externo em busca de anomalias ou vulnerabilidades. A análise dinâmica ocorre por meio de execução do software com dados de teste para examinar as saídas e o comportamento operacional. Ela opera como complemento da análise estática, considerando o código como uma caixa-preta. A principal vantagem da análise dinâmica é evidenciar defeitos sutis ou vulnerabilidades cujas origens são muito complexas para serem descobertas na análise estática. A análise dinâmica pode desempenhar um papel na garantia da segurança, mas seu principal objetivo é encontrar e eliminar erros, o chamado de bug. Após o produto passar por um teste de análise dinâmica, ele tende a ficar mais limpo, o que traz consideráveis melhorias na performance.

Análise Estática: tipo de teste de software que verifica a lógica interna em busca de falhas ou vulnerabilidades. A análise estática ocorre por meio de revisão, análise automatizada ou verificação formal do código-fonte ou dos binários, usando uma abordagem do tipo caixa-branca. Uma ferramenta que executa a análise estática de forma automatizada vai, essencialmente, procurar por erros que possam impedir a execução (run-time errors), erros comuns da linguagem

alvo e código potencialmente malicioso, sendo especialmente eficiente para encontrar erros como a corrupção de memória e estouros de buffer, vazamentos de memória, operações ilegais e inseguras, ponteiros nulos, loops infinitos, código incompleto, código redundante e código morto (absolutamente sem uso) e permitindo também identificar se está sendo chamada uma biblioteca incorretamente ou se a linguagem está sendo utilizada de forma incorreta ou de forma inconsistente.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

ANPD: acrônimo de Autoridade Nacional de Proteção de Dados.

Antimalware/Antivírus: software de proteção utilizado para prevenir, detectar e remover programas maliciosos.

Apetite ao Risco: nível de risco que uma organização está disposta a aceitar.

APF: acrônimo de Administração Pública Federal.

API: acrônimo de Interface de Programação de Aplicações (Application Programming Interface).

Aplicações de TIC: programa de computador (software) que constitui uma parte de um processo de negócio, operacionalizando suas transações ou automatizando suas atividades.

Aplicativos: softwares desenvolvidos ou adquiridos para atendimento de uma necessidade específica.

APT: acrônimo de Ameaça Persistente Avançada (Advanced Persistent Threat).

Aquisição de Evidência: processo de coleta e cópia das evidências de incidente de segurança em redes computacionais.

AR: acrônimo de Autoridade de Registro.

Área de TIC: unidade setorial, seccional ou correlata do SISP, responsável por gerir a Tecnologia da Informação e Comunicação e pelo planejamento, coordenação e acompanhamento das ações relacionadas às soluções de TIC do órgão ou entidade;

Área de Informação: esfera de atividade que envolve a criação, transformação e uso da informação, a infraestrutura de TIC envolvida e a informação propriamente dita.

Área Negocial: unidade responsável pelas atividades finalísticas que podem ou não envolver ativos e serviços de TI.

Áreas e Instalações de Acesso Restrito: áreas e instalações que contenham documento com Informação Classificada, ou que, por sua utilização ou finalidade, demandarem proteção, as quais

tem seu acesso restrito às pessoas autorizadas pelo órgão ou entidade.

Áreas Prioritárias: áreas definidas no Plano Nacional de Segurança de Infraestruturas Críticas para a aplicação da Política Nacional de Segurança de Infraestruturas Críticas, nos termos do disposto no art. 9º, inciso I, do Anexo ao Decreto nº 9.573, de 22 de novembro de 2018.

Área Técnica: unidade responsável pela operação técnica dos ativos e serviços de TI.

Arma Cibernética: software, hardware e firmware projetado ou aplicado especificamente para causar dano através do domínio cibernético. Estão incluídas nessa categoria: ferramentas para acesso não-autorizado, vírus, worms, trojans, DoS, DDoS, botnets e rootkits. Além disso, atividades como a engenharia social também são consideradas armas cibernéticas. Armas cibernéticas podem ser utilizadas individualmente ou em conjunto para aumentar os efeitos desejados.

Arma Cibernética Cinética: software, hardware e firmware projetado ou aplicado especificamente para causar danos físicos, direta ou indiretamente, tanto em pessoas como em equipamentos somente através da exploração de vulnerabilidades dos sistemas e processos de informação.

ARP: acrônimo de Address Resolution Protocol (Protocolo de Resolução de Endereços).

Arquitetura AAA: arquitetura que define uma forma estruturada para integração das funcionalidades de autenticação, autorização e auditoria.

Arquitetura de Aplicações: é a definição de como a aplicação fará o gerenciamento dos dados e o fornecimento de informação tecnológica para as pessoas que executam funções de negócio, possibilitando o acesso ao dado no formato adequado e custo aceitável.

Arquitetura da Informação: conjunto de documentos que descrevem dados e informações corporativas, compreendendo o modelo de dados, o dicionário de dados, as regras de sintaxe, integridade e consistência para os dados, a classificação destes quanto à propriedade, confidencialidade e criticidade e os direitos para acesso, retenção e descarte.

Arquitetura de Negócios: atividades ou tarefas que compõem os processos de negócios necessários para desempenhar a competência organizacional e alcançar a missão e as metas organizacionais.

Arquitetura de Rede: definição de alto nível do comportamento e das conexões entre os nós em uma rede, suficiente para possibilitar a avaliação das propriedades da rede.

Arquitetura de Tecnologia: definição de padrões para tipos de tecnologias ou plataformas que darão suporte ao negócio em ambiente de compartilhamento de dados.

Arquitetura de TIC: é a lógica de organização para aplicações, dados e tecnologia de infraestrutura concretizada em um conjunto de políticas e escolhas técnicas, cujo propósito é viabilizar a estratégia de negócio, compreendendo quatro dimensões: arquitetura de negócios, arquitetura da informação, arquitetura de aplicações e arquitetura tecnológica.

Artefato Malicioso: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas ou redes de computadores.

Assinatura Digital: tipo de assinatura eletrônica que usa operações matemáticas com base em algoritmos criptográficos de criptografia assimétrica para garantir segurança na autenticidade e a integridade das informações constantes no documento, sua autoria e eventuais modificações. É necessário possuir um certificado digital para assinar digitalmente um documento. Entre as principais vantagens do uso de assinatura digital estão o não repúdio, princípio em que não há dúvidas quanto ao remetente, e tempestividade, princípio pelo qual a autoridade certificadora pode verificar data e hora da assinatura de um documento.

Assinatura Eletrônica: nome dado aos mecanismos que permitem a assinatura de documentos virtuais com validade jurídica. A legislação brasileira disciplinou a assinatura eletrônica, de forma ampla, através da Medida Provisória 2002-2/2001.

Ataque: ação que constitui uma tentativa deliberada e não autorizada para acessar/manipular informações, ou tornar um sistema inacessível, não íntegro, ou indisponível.

Ataque Sybil: estratégia baseada na saturação de uma rede blockchain com diversos clones (Sybils) dando apoio a uma determinada decisão de forma a reverter o consenso obtido anteriormente utilizando mecanismos PoW ou PoS. Ataques Sybil são uma extensão do conceito de gastos-duplos.

Atividade: ação ou conjunto de ações executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços.

Atividade Crítica: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.

Atividade Maliciosa: qualquer atividade que infrinja a política de segurança de uma instituição ou que atente contra a segurança de um sistema.

Atividades de TIC: todas as tarefas que utilizam os meios tecnológicos para tratamento da informação ou auxílio na comunicação, incluindo hardware, computadores, rede telemóvel e softwares.

Ativo: aquilo que tem valor – tangível ou intangível - para a organização (tais como informação, software, equipamentos, instalações, serviços, pessoas e imagem institucional).

Ativo Crítico: equipamento físico, unidade de armazenamento e dados que possuem elevada importância para a continuidade das atividades e serviços e concretização dos objetivos da organização.

Ativo de Informação: são os ativos que suportam os meios de armazenamento, transmissão e processamento da informação, tais como: os equipamentos necessários a isso, os sistemas

utilizados para tal, os documentos impressos, os locais onde se encontram esses meios, e os recursos humanos a eles associados.

Ativo de Rede: equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores.

Atos Internacionais: veja Tratados Internacionais.

Atualização Automática: atualizações que são feitas no dispositivo ou sistema sem a interferência do usuário, inclusive, em alguns casos, sem notificação ao usuário.

Atualização Automatizada: fornecem aos usuários a habilidade de aprovar, autorizar e rejeitar uma atualização. Em alguns casos o usuário pode necessitar ter o controle de como e quando as atualizações serão implementadas em função de horário de funcionamento, limite de consumo de dados da conexão, padronização do ambiente, garantia de disponibilidade, entre outros aspectos.

Auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos.

Autenticação: processo que busca verificar a identidade digital de uma entidade de um sistema no momento em que ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo.

Autenticação de Dois Fatores (2FA): processo de segurança que exige que os usuários forneçam dois meios de identificação antes de acessarem suas contas.

Autenticação de Multifatores (MFA): Multifactor Authentication (MFA) é a utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, tokens, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito).

Autenticação Mútua: processo em que duas partes, tipicamente um cliente e um servidor, se autenticam mutuamente. Essa autenticação permite que ambos conheçam a identidade de cada um. Na autenticação mútua, o servidor solicita também um certificado do cliente. Também conhecida como autenticação bidirecional.

Autenticidade: propriedade pela qual se assegura que os dados ou informações são verdadeiros e fidedignos tanto na origem quanto no destino, permitindo, inclusive, a identificação do emissor equipamento, sistema, órgão ou entidade, quando for o caso.

Autoridade Certificadora (AC): entidade responsável por emitir e gerenciar certificados digitais.

Autoridade Certificadora Raiz (AC-Raiz): se situa no topo da hierarquia da cadeia de certificação, sendo a primeira autoridade. Sua função é executar as normas técnicas e operacionais e as políticas de certificados estabelecidas pelo Comitê Gestor da ICP Brasil. Isso significa que a AC-Raiz pode emitir, distribuir, expedir, revogar e gerenciar os certificados das autoridades que estão abaixo de seu nível hierárquico, que são as autoridades certificadoras. A Autoridade Certificadora Raiz da ICP Brasil é o Instituto Nacional de Tecnologia da Informação (ITI).

Autoridade de Registro (AR): estabelece a interface entre o usuário e a Autoridade Certificadora. A AR se vincula à AC e tem como principal objetivo ser o intermediário presencial entre a AC e o interessado pelo certificado digital, recebendo, validando, e encaminhando as solicitações de emissão ou revogação dos certificados digitais, além de identificar seus solicitantes de forma presencial.

Autoridade Nacional de Proteção De Dados (ANPD): órgão da APF responsável por zelar, implementar e fiscalizar o cumprimento da Lei 13.709, de 14 de agosto de 2018.

Autorização: processo que ocorre após a autenticação e tem a função de diferenciar os privilégios atribuídos ao usuário que foi autenticado. Os atributos de autorização normalmente são definidos em grupos mantidos em uma base de dados centralizada, sendo que cada usuário herda as características do grupo a que ele pertence. Portanto, autorização é o direito ou permissão de acesso a um recurso de um sistema.

Avaliação de Conformidade em Segurança da Informação: exame sistemático do grau de atendimento dos requisitos relativos à SI com legislações específicas.

Avaliação de riscos: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

B

Backdoor: dispositivo, em um programa malicioso, que permite acesso a um computador comprometido. Normalmente esse programa é colocado no computador alvo de forma a não ser notado.

Backend as a Service (BAAS): serviço de computação em nuvem que serve como middleware. Fornece aos desenvolvedores uma forma para conectar suas aplicações mobile e web a serviços na nuvem a partir de APIs e SDKs, abstraindo completamente a infraestrutura do lado do servidor.

Backup ou Cópia de Segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação em caso de perda das originais. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada.

Backup Completo (Full): modalidade de backup em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último backup.

Backup Diferencial: modalidade de backup em que são salvaguardados apenas dados novos ou modificados desde o último backup completo efetuado.

Backup Incremental: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup – seja ele completo, diferencial ou incremental – são salvaguardados.

Banco de Dados: base de dados ou coleção de dados inter-relacionados, armazenando informações sobre um domínio específico. São conjuntos de registros organizados que se relacionam de forma a criar algum sentido (informação) e dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento.

Banco de Dados Pessoais: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

BIA: acrônimo de Análise de Impacto de Negócios (Business Impact Analysis).

Big Data: conjuntos de dados extremamente amplos e que, por este motivo, necessitam de ferramentas especialmente preparadas para lidar com grandes volumes, de forma que toda e qualquer informação nesses meios possa ser encontrada, analisada e aproveitada em tempo hábil.

Biometria: verificação da identidade de um indivíduo por meio de uma característica física ou comportamental única, através de meios automatizados.

Blacklist: lista de itens aos quais é negado o acesso a certos recursos, sistemas ou protocolos. Utilizar uma blacklist para controle de acesso significa garantir o acesso a todas as entidades exceto àquelas incluídas na blacklist.

Blindagem: também chamada de hardening, trata-se de um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco em infraestrutura, com o principal objetivo de torná-la preparada para enfrentar tentativas de ataque.

Blockchain: base de dados que mantém um conjunto de registros que cresce continuamente - novos registros são apenas adicionados à cadeia existente e nenhum registro é apagado.

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

Bloqueio de Acesso: processo que tem por finalidade suspender temporariamente o acesso.

Bot: tipo de código malicioso. Programa que, além de incluir funcionalidades de worms, dispõe de mecanismos de comunicação com o invasor que permitem que seja controlado remotamente. O processo de infecção e propagação do bot é similar ao do worm, ou seja, o bot é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

Botnet: rede formada por diversos computadores zumbis (infectados com bots). Permite potencializar as ações danosas executadas pelos bots e ser usada em ataques de negação de serviço, esquemas de fraude, envio de spam etc.

Bring Your Own Device (BYOD): trata-se de uma política de segurança de uma organização, que permite que os dispositivos pessoais dos funcionários sejam usados nas atividades corporativas. Uma política BYOD estabelece limitações e restrições sobre se um dispositivo pessoal (como um notebook, smartphone ou tablet) pode ou não ser conectado pela rede corporativa.

BUILD: desenvolvimento de software, build é o termo usado para identificar uma versão compilada de um programa, ou seja, quando as linhas de código escritas em linguagem de alto nível são traduzidas para linguagem de máquina, que um computador é capaz de entender. A build pode ser completa (software inteiro) ou parcial (partes dele).

Business Intelligence (BI): conjunto de metodologias implementadas por meio de softwares que vão, em última análise, coletar informações e organizá-las em conhecimentos úteis para ajudar na tomada de decisão.