DICIONÁRIO DE REFERÊNCIA DE TI

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 Demandante: servidor público, militar de carreira ou empregado público, ocupantes de cargo efetivo em órgão ou entidade da administração pública federal, direta ou indireta, responsável por uma demanda de serviços endereçadas à área de segurança de informação, devidamente autorizada pela chefia superior.

Agente Público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da APF, direta e indireta.

Agente Público com Dispositivo Móvel Corporativo: agente público, que utilize dispositivo móvel de computação de propriedade dos órgãos ou entidades a que pertence.

Agente Público com Dispositivo Móvel Particular: agente público, que utilize dispositivo móvel de computação de sua propriedade. Os dispositivos particulares que se submetem aos padrões corporativos de software e controles de segurança, e que são incorporados à rede de um órgão ou entidade, são considerados como dispositivos corporativos.

Agente Responsável: agente público que se enquadre em qualquer das opções seguintes: a) possuidor de credencial de segurança; b) incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais; c) incumbido de chefiar ou gerenciar o processo de Inventário e Mapeamento de Ativos de informação; d) incumbido de chefiar e gerenciar o uso de dispositivos móveis; e) incumbido da gestão do uso seguro de redes sociais.

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.

Agente Responsável de Posto de Controle: representante do gestor de segurança e credenciamento de um órgão de registro em um posto de controle, a ele subordinado, podendo ser instituído a critério dos órgãos de registro.

Agente Responsável pelo Uso Seguro de Mídias Sociais: agente público incumbido de gerenciar, de forma contínua, o uso seguro de mídias sociais de sua organização.

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 integro, 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.

C

Cadeia de Custódia: processo que acompanha o movimento de evidência através de sua coleta, salvaguarda e ciclo de análise, documentando cada indivíduo que manuseou a evidência, o momento (data/hora) em que a evidência foi coletada ou transferida, além do propósito de cada transferência.

Cavalo de Tróia ou Trojan: programa que, além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

CDC (Container Data Center): são data centers modulares. Ao invés de construir enormes instalações para acomodar racks de servidores e storage usa-se o container como um modulo completo de processamento. Sua expansão é simples, basta adicionar mais módulos quando necessário. Os containers podem ser empilhados, otimizando o espaço do prédio.

Certificação: atesta a validade de um documento ou entidade.

Certificações Profissionais: processo negociado pelas representações dos setores sociais, pelo qual se identifica, avalia e valida formalmente os conhecimentos, saberes, competências, habilidades e aptidões profissionais desenvolvidos em programas educacionais ou na experiência de trabalho, com o objetivo de promover o acesso, a permanência e a progressão no mundo do trabalho e o prosseguimento ou conclusão de estudos.

Certificado: documento assinado criptograficamente, que é destinado a assegurar para outros a identidade do terminal que utiliza o certificado. Um certificado é confiável se esse certificado é assinado por outro certificado confiável, como uma autoridade de certificação, ou se ele próprio é um certificado confiável.

Certificado de Conformidade: garantia formal de que um produto ou serviço, devidamente identificado, está em conformidade com uma norma legal.

Certificado Digital: conjunto de dados de computador, gerados por uma Autoridade Certificadora, em observância à Recomendação Internacional ITU-T X.509, que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave criptográfica e uma pessoa física, jurídica, máquina ou aplicação.

Chave Criptográfica: valor que trabalha com um algoritmo criptográfico para cifração ou decifração.

Ciclo de Vida da Informação: compreende as fases de criação, manuseio, armazenamento, transporte e descarte da informação, considerando sua confidencialidade, integridade e disponibilidade.

Ciclo de vida do Incidente: conjunto de medidas que são repetidamente aplicadas até o incidente ficar totalmente resolvido.

Cifração: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro por outros ininteligíveis por pessoas não autorizadas a conhecê-la.

Circuito Elétrico Estabilizado: rede elétrica que possui controles necessários para evitar oscilações elétricas que danificam equipamentos.

Classificação da Informação: atribuição, pela autoridade competente, de grau de sigilo, disponibilidade e integridade dado à informação, documento, material, área ou instalação.

COBIT 2019: Control Objectives for Information and Related Technology - Framework e governança empresarial de TI que oferece um modelo de referência

para governança da TI e do negócio, objetivos de controle, mapas de auditoria, ferramentas para a sua implementação e principalmente, técnicas de gerenciamento.

Código de Indexação: código alfanumérico que indexa documento com informação classificada em qualquer grau de sigilo.

Código fonte: é o conjunto de palavras ou símbolos escritos de forma ordenada, contendo instruções em uma das linguagens de programação existentes, de maneira lógica.

Código malicioso: programa, ou parte de um programa de computador, projetado especificamente para atentar contra a segurança de um sistema e/ou redes de computadores, normalmente através de exploração de alguma vulnerabilidade de sistema.

Coleta de Evidências de Segurança em Redes Computacionais: processo de obtenção de itens físicos que contêm uma potencial evidência, mediante a utilização de metodologia e de ferramentas adequadas. Esse processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou a coleção de dados que contenham evidências do incidente.

Comitê de Controle de Mudanças - CCM: Grupo de profissionais responsáveis por áreas técnicas de TIC e de negócio, técnicos com sólidos conhecimentos em operação de infraestrutura de TIC ou desenvolvimento de sistemas, líderes de projeto, pontos focais das coordenações-gerais, coordenadores e outros colaboradores necessários para a correta avaliação das propostas de mudanças.

Comitê de Segurança da Informação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da APF.

Comitê de Gestão de Riscos: tem caráter consultivo, deliberativo e permanente, que tem como competência orientar, monitorar e revisar estruturas, sistemas, processos e políticas de governança, gestão de riscos e integridade da instituição, propondo diretrizes e fomentando melhores práticas compatíveis com seus objetivos estratégicos.

Comitê Governança Digital (CGD): órgão de caráter consultivo e deliberativo, de atuação permanente, que tem por objetivo o estabelecimento de políticas e diretrizes sobre os assuntos relativos à implementação das ações de governo digital e ao uso de recursos de tecnologia da informação e comunicação - TIC.

Comitê Gestor da ICP Brasil: vinculado à Casa Civil da Presidência da República, o Comitê Gestor da ICP-Brasil tem como principal competência determinar as políticas que a AC-Raiz executará. O comitê é composto por cinco representantes

da sociedade civil, integrantes de alguns setores afetos ao tema e representantes de órgãos da APF.

Computação em Nuvem: modelo computacional que permite acesso, por demanda e independente da localização, a conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços.

Comprometimento: perda de segurança resultante do acesso não autorizado.

Comunicação de Dados: transmissão, emissão ou recepção de dados ou informações de qualquer natureza por meios confinados, por radiofrequência ou por qualquer outro processo eletrônico ou eletromagnético ou ótico.

Comunicação do Risco: troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas.

Comunidade da ETIR: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais. Também chamado de Público-alvo da ETIR.

Confidencialidade: propriedade que garante acesso à informação somente a pessoas autorizadas, assegurando que indivíduos, sistemas, órgãos ou entidades não autorizados não tenham conhecimento da informação, de forma proposital ou acidental.

Conformidade: ser conforme, análogo ou similar; estar de acordo com determinadas normas, regras ou preceitos.

Conscientização: atividade que tem por finalidade orientar sobre o que é SI levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade. O objetivo dessa atividade é proteger o ativo de informações do órgão ou entidade para garantir a continuidade dos negócios, minimizar os danos e reduzir eventuais prejuízos financeiros.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Contas de Serviço: contas de acesso à rede corporativa de computadores necessários a um procedimento automático (aplicação, script etc.), sem qualquer intervenção humana no seu uso.

Contato Técnico de Segurança: pessoa ou equipe a ser acionada em caso de incidente de segurança envolvendo a organização, com atribuições eminentemente técnicas sobre a questão.

Contêiner dos Ativos de Informação: local onde "vive" o ativo de informação. Geralmente, um contêiner descreve algum tipo de ativo tecnológico - hardware, software ou sistema de informação (mas também pode se referir a pessoas ou mídias como papel, CD-ROM ou DVD-ROM). Portanto, um contêiner é qualquer tipo de ativo no qual um ativo de informação é armazenado, transportado ou processado. Ele pode ser um único ativo tecnológico (como um servidor), uma coleção de ativos tecnológicos (como uma rede) ou uma coletânea de mídias digitais, entre outros.

Continuidade de Negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

Contrato Sigiloso: ajuste cujo objeto ou execução implique tratamento de informação classificada.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação.

Controle de Acesso à Informação Classificada: realizado através de credencial de segurança e da demonstração da necessidade de conhecer.

Controles de Segurança: medidas adotadas para evitar ou diminuir o risco de um ataque. Exemplos de controles de segurança são: criptografia, funções de hash, validação de entrada, balanceamento de carga, trilhas de auditoria, controle de acesso, expiração de sessão e backups, entre outros.

Coordenação-Geral (CG): a Subsecretaria de Tecnologia é composta por coordenações destinadas a atender as segmentações da TI, sejam elas: Infraestrutura de TI, desenvolvimento e soluções digitais, sustentação de sistemas, padrões arquiteturais e qualidade, ciência de dados, governança e gestão de TIC e soluções meteorológicas.

Credenciais ou Contas de Acesso: permissão, concedida por autoridade competente após o processo de credenciamento, que habilitam determinada

pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como um crachá), ou lógica (como a identificação de usuário e senha).

Credencial de Segurança: certificado que autoriza pessoa para o tratamento de informação classificada.

Credenciamento: processo pelo qual o usuário recebe credenciais de segurança que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer.

Credenciamento de Segurança: processo utilizado para habilitar órgão ou entidade pública ou privada ou para credenciar pessoa, para o tratamento de informação classificada.

Crime Cibernético: ato criminoso ou abusivo contra redes ou sistemas de informações, seja pelo uso de um ou mais computadores utilizados como ferramentas para cometer o delito ou tendo como objetivo uma rede ou sistema de informações a fim de causar incidente, desastre cibernético ou obter lucro financeiro.

Criptografia: arte de proteção da informação através de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem.

Criptografia Assimétrica: veja criptografia de chave pública.

Criptografia de Chave Pública: também conhecida como criptografia assimétrica, é qualquer sistema criptográfico que usa pares de chaves: chaves públicas, que podem ser amplamente disseminadas, e chaves privadas que são conhecidas apenas pelo proprietário. Isto realiza duas funções: autenticação, onde a chave pública verifica que um portador da chave privada parelhada enviou a mensagem, e encriptação, onde apenas o portador da chave privada parelhada pode decriptar a mensagem encriptada com a chave pública.

Criticidade: grau de importância da informação para a continuidade das atividades e serviços.

CSIRT (Computer Security Incident Response Team): acrônimo internacional para designar um grupo de resposta a incidentes de segurança, responsável por tratar incidentes de segurança para um público-alvo específico.

CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (APF).

Custódia: consiste na responsabilidade de se guardar um ativo para terceiros. A custódia não permite automaticamente o acesso ao ativo e nem o direito de conceder acesso a outros.

Custodiado: recursos computacionais e/ou de comunicações ou informações que estejam sob a responsabilidade do órgão. Todavia, não são de sua propriedade.

Custodiante do Ativo de Informação: qualquer indivíduo ou estrutura de órgão ou entidade da APF, direta e indireta, que tenha responsabilidade formal de proteger a informação que não lhe pertence e aplicar os níveis de controles de segurança em conformidade com as exigências de SI comunicadas pelo proprietário da informação.

D

Dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador.

Dado Anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Dado em Repouso: informação armazenada. A proteção dos dados em repouso não deve ser subestimada, pois informações valiosas podem não ser transmitidas por canais de comunicação, mas apenas serem imóveis.

Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável.

Dado Pessoal Sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Dados Processados: dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação.

Datagrama (Pacote de Dados): trata-se de dados encapsulados, ou seja, dados aos quais são acrescentados cabeçalhos com informações sobre o seu transporte (como o endereço IP de destino). Os dados contidos nos datagramas são

analisados e eventualmente alterados pelos switches(roteadores) que permitem o seu trânsito. Os dados circulam na Internet na forma de datagramas.

DC: acrônimo de documento controlado.

Decifração: ato de decifrar, mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original.

Deepfake: forma de vídeo manipulado, utilizando técnicas de síntese de imagem humana, que criam renderizações artificiais hiper-realistas de um ser humano. Esses vídeos geralmente são criados pela mistura de um vídeo já existente com novas imagens, áudio e vídeo, para criar a ilusão da fala. Esse processo é realizado por meio de redes contraditórias generativas (GAN). A consequência mais perigosa da popularidade dos deepfakes é que eles podem facilmente convencer as pessoas a acreditarem em uma determinada história ou teoria, o que pode resultar em comportamentos com grande impacto na vida política, social ou financeira.

Defesa Cibernética: ações realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente.

Desastre: evento, ação ou omissão, repentino e não planejado, que tenha permitido acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica, causando perda para toda ou parte da organização e gerando sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação.

Descarte: eliminação correta dos dados, unidades de armazenamento e acervos digitais.

Descredenciamento de Segurança: processo utilizado para desabilitar órgão ou entidade, pública ou privada, ou para revogar a credencial de pessoal natural, para o tratamento da informação classificada.

Desenvolvimento: compreende as atividades de desenvolvimento e evolução (manutenções evolutivas, perfectivas, adaptativas e integrativas) de aplicações de software em plataformas web, desktop e mobile, que englobam a análise e o levantamento de requisitos, a construção e atualização de artefatos de

documentação e do código-fonte da aplicação, bem como a execução de testes funcionais.

Direito de Acesso: privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo.

Disponibilidade: garantia de que o dado esteja acessível e utilizável sob demanda de pessoa ou entidade devidamente autorizada.

Dispositivos Móveis de Comunicação: equipamentos móveis computacionais, tais como notebooks, netbooks, smartphones, tablets, ou qualquer outro equipamento de transmissão de dados e voz que seja de fácil mobilidade.

DLT: acrônimo de tecnologia de registro distribuído (Distributed Ledger Technology).

DLP: acrônimo de prevenção de perda de dados (Data Loss Prevention).

DMZ: acrônimo de zona desmilitarizada (Demilitarized Zone).

Documento: unidade de registro de informações, qualquer que seja o suporte ou o formato.

Documentos Classificados: documentos que contenham informação classificada em qualquer grau de sigilo.

Documentos Controlados: documentos que contenham informação classificada em qualquer grau de sigilo e que, a critério da autoridade classificadora, requerem medidas adicionais de controle.

Documento Preparatório: documento formal utilizado como fundamento da tomada de decisão ou de ato administrativo, a exemplo de pareceres e notas técnicas.

Domínio: é um nome que serve para localizar e identificar conjuntos de redes computadores.

Domínio Cibernético: domínio de processamento de informações (dados) eletrônicas composto de uma ou mais infraestruturas de TI.

Download: ação de copiar um arquivo ou documento de outro computador, através da Internet para o seu computador local.

E

E-mail: acrônimo de Electronic Mail (correio eletrônico).

Ecossistema Cibernético: infraestrutura de informação interconectada de interações entre pessoas, processos, dados e tecnologias da informação e comunicações, juntamente com o ambiente e as condições que influenciam essas interações. Engloba diversos participantes - governo, firmas privadas, organizações não-governamentais, indivíduos, processos e dispositivos cibernéticos - que interagem com propósitos diversos.

Eficácia: qualidade daquilo que cumpre com as metas planejadas, ou seja, uma característica pertencente as pessoas que alcançam os resultados esperados.

Eficiência: qualidade daquilo ou de quem é competente, que realiza de maneira correta as suas funções.

Eliminação: exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Emissão de Alertas e Advertências: serviço que consiste em divulgar alertas ou advertências imediatas como uma reação diante de um incidente de segurança em redes de computadores, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema.

Empresa Estratégica de Defesa (EED) do Setor De Tecnologia De Informação E Comunicação (TIC): toda pessoa jurídica do setor de TIC devidamente credenciada pelo Ministério da Defesa mediante o atendimento cumulativo das condições previstas no inciso IV do art. 2º da Lei 12.598, de 22 de março de 2012.

Encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

Endereço IP (Internet Protocol): conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores.

Engenharia Social: técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto da SI, é considerada uma prática de má-fé, usada por indivíduos para tentar explorar a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes.

Equipe de Coordenação Setorial: equipe de prevenção, tratamento e resposta a incidentes cibernéticos das agências reguladoras, do Banco Central do Brasil ou da Comissão Nacional de Energia Nuclear ou das suas entidades reguladas responsáveis por coordenar as atividades de segurança cibernética e de centralizar as notificações de incidentes das demais equipes do setor regulado.

Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

Equipes Principais: equipes de prevenção, tratamento e resposta a incidentes cibernéticos de entidades, públicas ou privadas, responsáveis por ativos de informação, em especial aqueles relativos a serviços essenciais, cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade, nos termos do disposto no parágrafo único, inciso I, do art. 1º do Anexo ao Decreto nº 9.573, de 22 de novembro de 2018.

Escritório de Gerenciamento de Programas e Projetos de TIC (EGPP-TI): função responsável pelo controle e monitoramento dos programas e projetos de TIC, atribuída segundo entendimento da direção de TIC.

Esfera de Informação: ambiente onde a informação existe e flui, de forma estruturada ou randômica, e onde fatos ou conhecimento residem e são representados ou transmitidos por uma sequência particular de símbolos, impulsos ou caracterizações.

Espaço Cibernético: espaço virtual composto por um conjunto de canais de comunicação da internet e outras redes de comunicação que garantem a interconexão de dispositivos de TIC e que engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo além de todas as ações, humanas ou automatizadas, conduzidas através desse ambiente.

Espaço de Informação: qualquer meio através do qual a informação seja criada, transmitida, recebida, armazenada, processada ou descartada.

Espalhamento: uma função de espalhamento (hash) transforma uma chave k num endereço. Esse endereço é usado como base para o armazenamento e para a recuperação de registros, sendo bastante similar à indexação, pois associa a chave ao endereço relativo a um registro. No espalhamento os endereços parecem aleatórios, não existindo conexão óbvia entre a chave e o endereço.

Espionagem Cibernética: atividade que consiste em ataques cibernéticos dirigidos contra a confidencialidade de sistemas TIC com o objetivo de obter dados e informações sensíveis a respeito de planos e atividades de um governo, instituição, empresa ou pessoa física, sendo geralmente lançados e gerenciados por serviços de inteligência estrangeiros ou por empresas concorrentes.

Estimativa de riscos: processo utilizado para atribuir valores à probabilidade e consequências de determinado risco.

Estratégia de Continuidade de Negócios: abordagem de um órgão ou entidade que garante a recuperação dos ativos da informação e a continuidade das atividades críticas ao se confrontar com um desastre, uma interrupção ou com outro incidente maior.

Ética: conjunto de normas que dizem respeito a conduta dos agentes públicos dentro de seu serviço.

ETIR: acrônimo para Equipe de Prevenção, Tratamento e Resposta à Incidentes Cibernéticos.

Evento: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falta de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Evento de Segurança: qualquer ocorrência identificada em um sistema, serviço ou rede que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida que possa se tornar relevante em termos de segurança.

Evidência Digital: informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento.

Evitar o Risco: forma de tratamento de risco na qual a alta administração decide não realizar a atividade, a fim de não se envolver, ou agir de forma a se retirar de uma situação de risco.

Exclusão de Acesso: processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e de perfil de acesso.

Exfiltração de Dados: é um movimento não autorizado de dados, também chamado de data exfil, exportação de dados, extrusão de dados, vazamento de dados e roubo de dados.

Exploit (Exploração de Vulnerabilidade): programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um programa de computador.

Exploração de Dia Zero ou Zero-Day Exploit: ataque digital que faz uso das "Vulnerabilidades de Dia Zero" para instalar software malicioso em um aparelho. É considerada uma ameaça grave, pois é impossível de reconhecer uma vez que a

falha não é conhecida. Ela pode ser mitigada, e algumas vezes evitada, por meio de ferramentas de segurança que monitorem o comportamento do tráfego e acesso aos equipamentos para identificar atividades suspeitas ou maliciosas.

F

Ferramenta de Gerenciamento de Backup: ferramenta cuja finalidade é a entrega de cópias de segurança empresariais, com a integridade como princípio maior.

Fiscal Administrativo do Contrato: servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos;

Fiscal Requisitante do Contrato: servidor representante da Área Requisitante da solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista de negócio e funcional da solução de TIC;

Fiscal Setorial do Contrato: servidor representante de setores distintos ou em unidades desconcentradas de um órgão ou uma entidade, indicado pela autoridade competente dessa área para o acompanhamento da execução do contrato nos aspectos técnicos ou administrativos;

Fiscal Técnico do Contrato: servidor representante da Área de TIC, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato;

Firewall: recurso destinado a evitar acesso não autorizado a uma determinada rede, ou um a conjunto de redes, ou a partir dela. Podem ser implementados em hardware ou software, ou em ambos. Cada mensagem que entra ou sai da rede passa pelo firewall, que a examina a fim de determinar se atende ou não os critérios de segurança especificados.

Forense Digital: aplicação da ciência da computação e procedimentos investigativos para a identificação, exame e análise de dados com a devida preservação da integridade da informação e mantendo uma estrita cadeia de custódia para os dados.

Formulário Individual de Dados para Credenciamento (FIDC): formulário de preenchimento obrigatório para que pessoa natural seja submetida ao processo de credenciamento de segurança.

Função de Resumo Criptográfico: resultado da ação de algoritmos que fazem o mapeamento de bits de tamanho arbitrário para uma sequência de bits de tamanho fixo menor - conhecida como resultado hash - de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash (resistência à

colisão) e que o processo reverso também não seja realizável (utilizando-se apenas o hash não é possível recuperar a mensagem que o gerou).

G

GAN: acrônimo de redes contraditórias generativas (generative adversarial networks).

Gastos-Duplos: ato de usar o mesmo dado mais de uma vez em diferentes transações em uma rede blockchain.

Gerenciamento de Operações e Comunicações: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suportem.

Gestão de Ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada de seu controle.

Gestão de Conformidade: conjunto de medidas que asseguram que uma entidade está em conformidade com as normas vigentes, ou seja, se está cumprindo todas as obrigatoriedades dos órgãos de regulamentação, dentro de todas as políticas exigidas para a execução da sua atividade.

Gestão de Continuidade de Negócio: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado.

Gestão de Incidentes Cibernéticos: processo que realiza ações sobre qualquer evento adverso relacionado à segurança cibernética dos sistemas ou da infraestrutura de computação.

Gestão de Riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

Gestão de Riscos em Segurança da Informação: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

Gestão de Segurança da Informação: ações e métodos que visam à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.

Gestão de TIC: compreende o uso racional de meios (pessoas e recursos de TIC) para alcançar as metas organizacionais, mediante o planejamento, organização, coordenação, monitoramento e controle das atividades operacionais e dos projetos, considerando um dado período de tempo.

Gestor de Contrato: servidor com atribuições gerenciais, preferencialmente da Área Requisitante da solução, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente;

Gestor de Mudanças: responsável pelo planejamento e implementação do processo de mudanças no âmbito do órgão ou entidade da APF.

Gestor da Informação: é o agente público responsável pela administração das informações geridas nos processos de trabalho sob sua responsabilidade.

Gestor de Segurança da Informação: responsável pelas ações de SI no âmbito do órgão ou entidade da APF.

Gestor de Segurança e Credenciamento (GSC): responsável pela segurança da informação classificada em qualquer grau de sigilo nos Órgãos de Registro e Postos de Controle, devidamente credenciado.

Governança de TIC: conjunto de princípios, diretrizes, normas, processos, estruturas organizacionais e instrumentos de controle que visam assegurar que as decisões e as ações relacionadas à gestão e ao uso de TIC estejam integradas e coerentes com as necessidades institucionais, contribuindo, assim, para o cumprimento da missão e o alcance das metas organizacionais.

GSI/PR: acrônimo de Gabinete de Segurança Institucional da Presidência da República.

Guerra Cibernética: atos de guerra utilizando predominantemente elementos de TIC em escala suficiente por um período específico de tempo e em alta velocidade em apoio a operações militares através de ações tomadas exclusivamente no espaço cibernético de forma a abalar ou incapacitar as atividades de uma nação inimiga, especialmente pelo ataque aos sistemas de comunicação, visando obter

vantagem operacional militar significativa. Tais ações são consideradas uma ameaça à Segurança Nacional do Estado.

H

Habilitação de Segurança: condição atribuída a um órgão ou entidade pública ou privada, que lhe confere a aptidão para o tratamento da informação classificada em determinado grau de sigilo.

Hardware: é a parte física do computador, ou seja, é o conjunto de componentes eletrônicos, circuitos integrados e placas, que se comunicam através de barramentos.

Hash: resultado único e de tamanho fixo, gerado por uma função de resumo. O hash pode ser utilizado, entre outras possibilidades, para verificar a integridade de arquivos e gerar assinaturas digitais. Ele é gerado de forma que não é possível realizar o processamento inverso para recuperação da informação original. Além disso, qualquer alteração na informação original produzirá um hash distinto. Apesar de ser teoricamente possível que informações diferentes gerem hashes iguais, a probabilidade de isso ocorrer é bastante baixa.

Hipótese Legal de Sigilo: quando uma informação sigilosa é definida por lei específica, diversa da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Honeynet: ferramenta de pesquisa, que consiste em uma rede projetada especificamente para ser comprometida, e que contém mecanismos de controle para prevenir que seja utilizada como base de ataques contra outras redes. Trata-se de um tipo de honeypot de alta interatividade, projetado para pesquisa e obtenção de informações dos invasores, também conhecido como honeypot de pesquisa.

Honeypot: recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido. Existem dois tipos de honeypots: os de baixa interatividade e os de alta interatividade. Em um honeypot de baixa interatividade são instaladas ferramentas para emular sistemas operacionais e serviços com os quais os atacantes irão interagir; desta forma, o sistema operacional real deste tipo de honeypot deve ser instalado e configurado de modo seguro, para minimizar o risco de comprometimento. Nos honeypots de alta interatividade, os atacantes interagem com sistemas operacionais, aplicações e serviços reais.

HSM: acrônimo de módulo de segurança em hardware (Hardware Security Module).

HTTP Strict Transport Security (HSTS): mecanismo de política de segurança web que ajuda a proteger websites contra ataques do tipo degradação de protocolo e sequestro de cookies. Ele permite que os servidores web determinem que os browsers (ou outros mecanismos de acesso) devem interagir com eles utilizando apenas conexões seguras HTTPS. O HSTS é um padrão IETF e está especificado na RFC 6797.

Hypertext Transfer Protocol (HTTP): protocolo de comunicação entre sistemas de informação, o qual permite a transferência de dados entre redes de computadores, principalmente na World Wide Web (Internet). Para que esta transferência de dados ocorra, o protocolo HTTP necessita estar agregado a outros dois protocolos de rede, TCP e IP, os quais possibilitam a comunicação entre a URL e o servidor web que armazenará os dados, a fim de que a página HTML solicitada pelo usuário seja enviada.

Hypertext Transfer Protocol Secure (HTTPS): extensão do HTTP utilizada para comunicação segura pela rede de computadores. No HTTPS, o protocolo de comunicação é criptografado usando o TLS ou o seu predecessor, o SSL. A principal motivação para o uso do HTTPS é a autenticação do site acessado e a proteção da privacidade e integridade dos dados trocados durante o tráfego de informações.

Hypervisor: também conhecido como monitor de máquina virtual, é um software, firmware ou hardware que cria e roda máquinas virtuais.

I

IaaS: acrônimo de infraestrutura como serviço (Infrastructure as a Service).

IaC: acrônimo de infraestrutura como código (Infrastructure as Code).

IBE: acrônimo de criptografia baseada em identidade (Identity-based Encryption).

Identidade Digital: representação unívoca de um indivíduo dentro do espaço cibernético.

Identidade Federada: modelo federado está fundamentado sobre a distribuição da tarefa de autenticação dos usuários por múltiplos provedores de identidade, estando esses dispostos em diferentes domínios administrativos, tais como empresas, governos e academia. Em cada domínio administrativo há diversos usuários, um único provedor de identidade e vários provedores de serviços, sendo que os provedores de identidade estabelecem relações de confiança, de forma que uma identidade emitida por um provedor de identidade de um determinado domínio seja reconhecida por provedores de serviços de outros domínios.

Identidade Sintética: tipo de fraude de identidade na qual os golpistas usam uma mistura de credenciais reais e fabricadas, para criar a ilusão de uma pessoa real. É bastante popular, pois os criminosos podem facilmente criar identidades sintéticas com apenas alguns dados verdadeiros (como nome e número de um documento de identificação), sendo normalmente utilizada com o objetivo de abrir contas fraudulentas e realizar aquisições.

Identificação de riscos: processo para localizar, listar e caracterizar elementos do risco.

IDS: acrônimo de detecção de intrusão (Intrusion Detection System).

Imagem: cópia idêntica do sistema operacional ou aplicações utilizadas para restauração e/ou instalação otimizada de um ambiente padrão em um recurso computacional.

Imagem de Backup: arquivo gerado pela solução/ferramenta de backup, não necessariamente no mesmo formato dos arquivos que contém os dados salvaguardados.

Imagem de Máquina Virtual: abrange a definição completa do armazenamento de uma máquina virtual, contendo o disco do sistema operacional e todos os discos de dados, capturando as propriedades do disco (como cache de host) necessárias para implantar uma Virtual Machine em uma unidade reutilizável.

Implantação: compreende as atividades de preparação de ambientes de aplicação de software, além das atividades de inserção desse sistema no rol soluções de aplicações, tais como planejamento, parametrizações, configurações, treinamentos técnicos, funcionais e operacionais, além de apoio na intermediação das evoluções, apoio no endomarketing e na elaboração de materiais de apoio à utilização do sistema (manuais, vídeos, orientações etc.).

Incidente: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

Incidente Cibernético: ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que

caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso. De maneira geral, os tipos de atividade comumente reconhecidas como incidentes cibernéticos são: a) tentativas de obter acesso não-autorizado a um sistema ou a dados armazenados; b) tentativa de utilização não-autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados; c) mudanças não-autorizadas de firmware, hardware ou software em um ambiente computacional; d) ataques de negação de serviço (DoS); e e) demais ações que visem afetar a disponibilidade ou integridade dos dados. Um incidente de segurança cibernética não significa necessariamente que as informações já estão comprometidas; significa apenas que a informação está ameaçada.

Incidente de Segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

Indicadores Estratégicos: instrumentos dinâmicos de gestão essenciais para pôr em prática a obtenção dos objetivos estratégicos, permitindo monitorar e avaliar continuamente o cumprimento das metas, identificando seus avanços ou deficiências com vistas a sua melhoria contínua.

Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado.

Informação Atualizada: informação que reúne os dados mais recentes sobre o tema, de acordo com sua natureza, com os prazos previstos em normas específicas ou conforme a periodicidade estabelecida nos sistemas informatizados que a organizam.

Informação Classificada: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada conforme procedimentos específicos de classificação estabelecidos na legislação vigente.

Informação Custodiada: informação sob a guarda e responsabilidade do órgão.

Informação Pessoal: informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem.

Informação Sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

Informação Sigilosa Protegida por Legislação Específica: informação amparada pelo sigilo bancário, fiscal, comercial, profissional ou segredo de justiça.

Infraestrutura Cibernética: sistemas e serviços de informação e comunicações compostos por todo o hardware e software necessários para processar, armazenar e transmitir a informação, ou qualquer combinação desses elementos. O processamento inclui a criação, acesso, modificação e destruição da informação. O armazenamento engloba qualquer tipo de mídia na qual a informação esteja armazenada. A transmissão é composta tanto pela distribuição como pelo compartilhamento da informação, por qualquer meio.

Infraestrutura como Código (IaC): processo de gerenciamento e provisionamento de data centers de computador, por meio de arquivos de definição legíveis por máquina, em vez de configuração física de hardware ou ferramentas de configuração interativas.

Infraestrutura como Serviço (IaaS): tipo de serviço de computação em nuvem onde o provedor de serviço de nuvem oferece ao cliente a capacidade de criar redes virtuais em seu ambiente de computação. Uma solução IaaS permite que o cliente selecione quais sistemas operacionais instalar em máquinas virtuais, bem como a estrutura da rede, incluindo o uso de switches virtuais, roteadores e firewalls. O IaaS também fornece total liberdade quanto ao software ou código personalizado executado nas máquinas virtuais. Uma solução IaaS é a mais flexível de todos os serviços de computação em nuvem; permite uma redução significativa do hardware pelo cliente em sua própria instalação local. Geralmente, é a forma mais cara de serviço de computação em nuvem.

Infraestrutura Crítica: instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança.

Infraestrutura Crítica de Informação: sistemas de TIC que suportam ativos e serviços chaves da Infraestrutura Nacional Crítica.

Infraestrutura de Chave Pública (PKI): do inglês (Public Key Infrastructure). Sistema de recursos, políticas, e serviços que suportam a utilização de criptografia de tecla pública para autenticar as partes envolvidas na transação. Não há nem um único padrão que define os componentes de uma infraestrutura de chave pública, mas uma infraestrutura de chave pública geralmente inclui Autoridades Certificadoras (ACs) e Autoridades de Registro (ARs). O padrão ITU-T X.509 fornece a base para a infraestrutura de chave pública padrão de mercado.

Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil): cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual

do cidadão. Essa infraestrutura é um conjunto elaborado de práticas, técnicas e procedimentos que serve para suportar um sistema criptográfico baseado em certificados digitais. O modelo adotado no Brasil para a infraestrutura de chaves públicas é chamado de certificação com raiz única, em que existe uma Autoridade Certificadora Raiz (AC-Raiz). Além de desempenhar esse papel, a AC-Raiz credencia os demais participantes da cadeia, além de supervisionar e auditar os processos. Foi criada pela MP 2002-2/2001 e está regulamentada pelas resoluções do Comitê-Gestor da ICP-Brasil.

Infraestrutura de TIC: conjunto de bens utilizados para o processamento e as comunicações de informações, compreendendo equipamentos (hardware), programas (software), redes de dados e telecomunicações, estações de trabalho, bancos de dados, impressoras, entre outros elementos.

Infraestrutura Nacional Crítica: ativos, virtuais ou físicos, que são essenciais para o devido funcionamento da sociedade e da economia nacional (como energia, transporte, saúde, telecomunicações etc.).

Infrastructure of Technology Information Library (ITIL): é uma biblioteca do conjunto das melhores práticas desenvolvidas para o fornecimento de serviço de TI.

Inspeção para Credenciamento (Habilitação) de Segurança: averiguação da existência dos requisitos indispensáveis à habilitação de órgãos e entidades para o tratamento de informação classificada.

Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

Inteligência Artificial (IA): a inteligência artificial é um ramo de pesquisa da ciência da computação que busca, através de símbolos computacionais, construir mecanismos e/ou dispositivos que simulem a capacidade do ser humano de pensar, resolver problemas, ou seja, de ser inteligente.

Interface de Programação de Aplicações (API): Application Programming Interface, mais conhecida como API, tem por objetivo principal disponibilizar recursos de uma aplicação para serem usados por outra aplicação, abstraindo os detalhes da implementação e muitas vezes restringindo o acesso a esses recursos com regras específicas para tal.

Internet: associação mundial de redes de computadores interligadas, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação através de: transferência de arquivos, conexões à distância, serviços de correio eletrônico etc.

Internet das Coisas (IOT): Internet of Things. Sistema interrelacionado de dispositivos computacionais, equipamentos digitais e mecânicos, e objetos aos quais são vinculados UIDs e que possuem a habilidade de transferir dados pela rede sem a necessidade de interação do tipo pessoa-pessoa ou pessoa-computador.

Internet Protocol (IP): endereço IP, de forma genérica, é uma identificação de um dispositivo (computador, impressora, etc) em uma rede local ou pública. Cada computador na internet possui um IP (Internet Protocol ou Protocolo de internet) único, que é o meio em que as máquinas usam para se comunicarem na Internet.

Interoperabilidade: capacidade de um sistema se comunicar, realizar intercâmbio de dados e requerer a execução de funções e programas com outros sistemas, locais ou remotos, requerendo medida de padronização comum de protocolo de comunicação, transporte, armazenamento e representação de informações.

Interoperabilidade Semântica: a adoção, conforme contexto de uso, de técnicas de modelagem de informação, modelos de informação e uso de vocabulários padronizados, como terminologias, classificações, taxonomias e ontologias, que garantam o entendimento humano de uma estrutura integrada de informações.

Intranet: rede privada, acessível apenas aos membros da organização que atende. Utiliza os mesmos recursos e protocolos da Internet, mas é comumente separada desta através de firewalls.

Intrusion Protection System - IPS (Sistema de Proteção a intrusos): é um sistema, similar ao IDS (Intrusion Detection System), voltado para a prevenção de ataques a redes de computadores. A diferença básica entre um IPS e um IDS é que o primeiro, além de detectar um tráfego anômalo, é capaz de tratá-lo.

Invasão: incidente de segurança no qual o ataque foi bem sucedido, resultando no acesso, na manipulação ou na destruição de informações em um computador ou em um sistema da organização.

Investigação para Credenciamento de Segurança: averiguação da existência dos requisitos indispensáveis para a concessão da credencial de segurança a pessoas naturais, para o tratamento de informação classificada.

ISO 20000: International Organization for Standardization - A ISO/IEC 20000 versa sobre gestão de qualidade de serviços de TI (Tecnologia da Informação). Essa norma define requisitos para a correta gestão de uma empresa prestadora de serviços de TI, garantindo a entrega de serviços de qualidade aos clientes. São requisitos da norma a definição de políticas, objetivos, procedimentos e processos de gestão para assegurar a qualidade efetiva na prestação de serviços de TI.

ITIL V4: Information Technology Infrastructure Library - A Biblioteca de infraestrutura de tecnologia da informação, é um guia de boas práticas, desenvolvido pela Agência Central de Computação e Telecomunicações (CCTA) do governo britânico, sobre gerenciamento de serviços de tecnologia da informação que se concentra no alinhamento dos serviços com as necessidades dos negócios.

ITSM / GSTI - IT Service Management: Gerenciamento de Serviços de TI, tem por objetivo prover um serviço de TI com qualidade e alinhado às necessidades do negócio, buscando redução de custos a longo prazo.

J

Jailbreak: processo que modifica o sistema operacional original de um dispositivo, permitindo que ele execute aplicativos não-autorizados pelo fabricante. Um aparelho com um software do tipo jailbreak é capaz de instalar aplicativos anteriormente indisponíveis nos sites oficiais do fabricante, por meio de instaladores não-oficiais, assim como aplicações adquiridas de forma ilegal. O uso de técnicas jailbreak não é recomendado pelos fabricantes, já que permitem a execução de aplicativos não certificados, que podem inclusive conter malware embutidos.

Janela de Backup: período de tempo durante o qual as cópias de segurança sob execução agendada ou manual poderão ser executadas.

K

Keylogger: tipo específico de spyware. Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Normalmente a ativação do keylogger é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.

Kit de Desenvolvimento de Software ou Software Development Kit (SDK): é um conjunto de ferramentas de desenvolvimento e de códigos pré-gravados que podem ser usados pelos desenvolvedores para criar aplicativos. Geralmente ajudam a reduzir a quantidade de esforço e de tempo que seria necessário para os profissionais escreverem seus próprios códigos.

L

LAI: acrônimo de Lei de Acesso à Informação.

LDAP (Lightweight Directory Access Protocol): é um protocolo de aplicação aberto, livre de fornecedor e padrão de indústria para acessar e manter serviços de informação de diretório distribuído sobre uma rede de Protocolo da Internet (IP).

LGPD: acrônimo de Lei Geral de Proteção de Dados Pessoais.

Lista de Controle de Acesso ou Access Control Lists (ACL): Mecanismo que implementa o controle de acesso para um recurso enumerando as entidades do sistema que possuem permissão para acessar o recurso e definindo, explicitamente ou implicitamente, os modos de acesso concedidos a cada entidade.

Livro Razão Distribuído ou Distributed Ledger Techonology (DLT): banco de dados distribuído por vários nós ou dispositivos de computação. Cada nó replica e salva uma cópia idêntica do livro-razão. Cada nó participante da rede atualiza-se de forma independente. O recurso inovador da tecnologia de contabilidade distribuída é que a planilha não é mantida por nenhuma autoridade central. Atualizações para o livro-razão são independentemente construídas e registradas por cada nó. Os nós então votam nessas atualizações para garantir que a maioria concorde com a conclusão alcançada. Um sistema blockchain é uma forma de tecnologia de contabilidade distribuída. No entanto, a estrutura do sistema blockchain é distinta de outros tipos de livro-razão distribuídos, pois os dados em um sistema blockchain são agrupados e organizados em blocos que são então ligados entre si e protegidos usando criptografia.

Log ou Registro de Auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional, para posterior análise, podendo ser gerado por sistemas operacionais, aplicações, entre outros.

M

Malwares: programas de computadores ou parte de código executável com capacidade de autorreplicação. Da mesma forma que os vírus biológicos, os códigos maliciosos de computador podem se disseminar com rapidez e a sua erradicação normalmente é difícil. Eles podem se anexar a praticamente qualquer tipo de arquivo e se disseminam como arquivos que são copiados e enviados de uma pessoa para outra. Esse tipo de software malicioso costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de malware estão os vírus, worms, trojans (ou cavalos de Troia), spyware, adware e rootkits.

Máquina Virtual (VM - Virtual Machine): as máquinas virtuais são computadores de software, com a mesma funcionalidade que os computadores físicos. Assim

como os computadores físicos, elas executam aplicativos e um sistema operacional. No entanto, as máquinas virtuais são arquivos de computador, executados em um computador físico, e se comportam como um computador físico. Geralmente, são criadas para tarefas específicas, cujas execuções são arriscadas em um ambiente host, como por exemplo, o acesso a dados infectados por vírus e a testes de sistemas operacionais. Como a máquina virtual é separada por sandbox do restante do sistema, o software dentro dela não pode adulterar o computador host. As máquinas virtuais também podem ser usadas para outras finalidades, como a virtualização de servidores.

Máquina Virtual Confiável (TVM): instância de uma máquina virtual (VM), que apresenta as seguintes características: a) máquinas virtuais devem ser lançadas em servidores com integridade de inicialização comprovável; b) imagens de máquinas virtuais devem ser criptografadas em trânsito, em repouso e durante a execução. Isso é essencial para preservar a confidencialidade e o sigilo. As chaves estão sob o controle do cliente e só são disponibilizadas (política de gerenciamento de chaves) para o provedor de serviços, quando ele atesta que as imagens da máquina virtual estão sendo lançadas em servidores confiáveis; c) apenas imagens de máquinas virtuais qualificadas e atestadas podem ser lançadas e provisionadas, sendo o provedor de serviço responsável por atestar a integridade de lançamento na infraestrutura.

Marcação: aposição de marca que indica o grau de sigilo da informação classificada.

Material de Acesso Restrito: qualquer matéria, produto, substância ou sistema que contenha, utilize ou veicule conhecimento ou informação classificada, em qualquer grau de sigilo, informação econômica ou informação científico-tecnológica, cuja divulgação implique risco ou danos aos interesses da sociedade e do Estado, tendo seu acesso restrito às pessoas autorizadas pelo órgão ou entidade.

Matriz RACI: também conhecida como tabela RACI, trata-se de uma ferramenta visual que define com clareza as atribuições, papeis e responsabilidades de cada colaborador nas atividades de um processo. O acrônimo RACI representa: responsible (responsável), accountable (aprovador), consulted (consu ltado) e informed (informado).

Medidas de Segurança: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo.

Meio digital: informação disponível em um formato codificado digitalmente inteligível pelo homem e criado, processado, armazenado e disponibilizado por meios eletrônicos.

Metadados: representam "dados sobre dados" fornecendo os recursos necessários para entender os dados através do tempo, ou seja, são dados estruturados que fornecem uma descrição concisa a respeito dos dados armazenados e permitem encontrar, gerenciar, compreender ou preservar informações a respeito dos dados ao longo do tempo. Têm um papel importante na gestão de dados, pois a partir deles as informações são processadas, atualizadas e consultadas. As informações de como os dados foram criados/derivados, ambiente em que residem ou residiram, alterações realizadas, entre outras, são obtidas de metadados.

MFA: acrônimo de autenticação de multifatores (multifactor authentication).

Mídia: mecanismos em que dados podem ser armazenados, além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos, que são diferentes tipos de mídia.

Mineração de Dados: mineração de dados (em inglês, data mining) é o processo de encontrar anomalias, padrões e correlações em grandes conjuntos de dados para prever resultados. Através de uma variedade de técnicas, você pode usar essas informações para aumentar a renda, cortar custos, melhorar o relacionamento com os clientes, reduzir riscos e mais.

Modelo de Consenso: componente primário de sistemas distribuídos de blockchain e, definitivamente, um dos mais importantes para a sua funcionalidade. É a base sobre a qual os usuários podem interagir uns com os outros de maneira trustless. A maioria dos sistemas blockchain públicos utiliza o Consenso de Nakamoto, no qual os nós processadores, por convenção, tratam a mais longa história de blocos como a história oficial (ou certificada).

Modelo de Implementação de Nuvem Própria: solução compartilhada de recursos computacionais configuráveis cuja infraestrutura de nuvem pertence apenas a uma organização e suas subsidiárias.

Modelo de Implementação de Nuvem Comunitária: solução compartilhada de recursos computacionais configuráveis cuja infraestrutura de nuvem é compartilhada entre diversas organizações que possuem necessidades comuns, tais como missão, valores, requisitos de segurança, política e requisitos legais, entre outras.

Módulo de Segurança em Hardware (HSM): Hardware Security Module (HSM). Criptoprocessador dedicado, especificamente projetado para a proteção do ciclo de vida de uma chave criptográfica. Um HSM age como âncora segura que protege a infraestrutura criptográfica gerenciando, processando e armazenando chaves criptográficas em um ambiente seguro e resistente a adulterações.

Multinuvem: estratégia de utilização dos serviços de computação em nuvem por meio de dois ou mais provedores de serviços de nuvem.

N

Navegador de Internet (browser): software utilizado para navegação na Internet, instalado nos recursos computacionais. Exemplo: Google Chrome, Internet Explorer, Mozilla Firefox.

NBR ISO/IEC (International Organization for Standardization): é a sigla de Norma Brasileira aprovada pela ABNT, de caráter voluntário, e fundamentada no consenso da sociedade. Torna-se obrigatória quando essa condição é estabelecida pelo poder público.

Necessidade de Conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais.

Negação de Serviço (DoS): mais conhecido como DoS (Denial of Service) é o bloqueio de acesso devidamente autorizado a um recurso ou a geração de atraso nas operações e funções normais de um sistema, com a resultante perda da disponibilidade aos usuários autorizados. O objetivo do ataque DoS é interromper atividades legítimas de um computador ou de um sistema. Uma forma de provocar o ataque é aproveitando-se de falhas ou de vulnerabilidades presentes na máquina vítima, ou enviar um grande número de mensagens que esgotem algum dos recursos da vítima, como CPU, memória, banda, etc. Para isto, é necessário uma única máquina poderosa, com bom processamento e bastante banda disponível, capaz de gerar o número de mensagens suficiente para causar a interrupção do serviço.

Negação de Serviço Distribuída (DDoS): mais conhecido por DDoS (Distributed Denial of Service), é uma atividade maliciosa, coordenada e

distribuída pela qual um conjunto de computadores ou de dispositivos móveis é utilizado para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Embora os ataques do tipo DoS sejam em geral perigosos para os serviços de internet, a forma distribuída é ainda mais perigosa, justamente por se tratar de um ataque feito por várias máquinas, que podem estar espalhados geograficamente e não terem nenhuma relação entre si - exceto o fato de estarem parcial ou totalmente sob controle do atacante. Além disso, mensagens DDoS podem ser difíceis de identificar por conseguirem facilmente se passar por mensagens de tráfego legítimo pois enquanto é pouco natural que uma mesma máquina envie várias mensagens semelhantes a um servidor em períodos muito curtos de tempo (como no caso do ataque DoS), é perfeitamente natural que várias máquinas enviem mensagens semelhantes de requisição de serviço regularmente a um mesmo servidor, o que disfarça o ataque DDoS.

Network Operation Center - NOC (Centro de Operações de Rede): é uma estrutura de profissionais especializados que realiza o monitoramento e a gestão dos eventos de TI. Nessa estrutura, especialistas com conhecimentos focados principalmente em administração de redes realizam a monitoração dos alertas gerados pelos ativos de TI. Toda a equipe deve atuar em um modelo com processos bem definidos, com o objetivo de manter o ambiente o mais estável possível.

Níveis de Acesso: especificam quanto de cada recurso ou sistema o usuário pode utilizar.

Nível de risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação dos impactos e de suas probabilidades;

Notificação de Incidente: ato de informar eventos ou incidentes para uma ETIR ou grupo de segurança.

Núcleo de Segurança e Credenciamento (NSC): Órgão de Registro Central, instituído no Gabinete de Segurança Institucional da Presidência da República.

Número De Identificação Pessoal (PIN): Personal Identification Number (PIN). Número exclusivo conhecido somente pelo usuário e pelo sistema para a autenticação do usuário no sistema. PINs comuns são usados em caixas automáticos para realização de transações bancárias e em chips telefônicos.

Nuvem: uma vasta rede de servidores remotos ao redor do globo que são conectados e operam como um único ecossistema. Estes servidores são responsáveis por armazenar e gerenciar dados, executar aplicativos ou fornecer serviços ou conteúdos, que podem ser acessados de qualquer dispositivo com acesso à Internet.

Nuvem Comunitária: infraestrutura de nuvem dedicada para uso exclusivo de uma comunidade, ou de um grupo de usuários de órgãos ou de entidades não vinculados, que compartilham a mesma natureza de trabalho e obrigações, e sua propriedade e seu gerenciamento podem ser de organizações da comunidade, de terceiros ou de ambos.

Nuvem Híbrida: infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações.

Nuvem Privada (ou interna): infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade e seu gerenciamento podem ser da própria organização, de terceiros ou de ambos.

Nuvem Pública (ou externa): infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de organizações públicas, privadas ou de ambas.

O

Obsolescência Tecnológica: ciclo de vida do software ou de equipamento definido pelo fabricante ou causado pelo desenvolvimento de novas tecnologias.

One-time Password: acrônimo de senha descartável.

Open Web Application Security Project (OWASP): trata-se de uma comunidade on-line que cria e disponibiliza, de forma gratuita, artigos, metodologias, documentação, ferramentas e tecnologias no campo da segurança de aplicações web, a todos os interessados em aperfeiçoar a segurança em aplicações.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Operador de Backup: pessoa responsável por procedimentos de atendimento de primeiro nível, acompanhamento de execução de rotinas de backup, realização de restaurações de arquivos de usuários, manutenção de troca de fitas no robô e gerenciamento de estoque de fitas locais.

Opt-In: processo pelo qual o usuário autoriza uma determinada ação por parte de uma empresa, geralmente a coleta de dados e o seu compartilhamento com empresas parceiras ou o recebimento de mensagens enviadas por empresas.

Opt-Out: processo pelo qual o usuário desautoriza uma empresa a continuar com uma determinada ação previamente permitida.

Órgão de Pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Órgão de Registro: órgão ou entidade pública da administração pública federal habilitada para o tratamento de informação classificada.

Órgãos de Registro Nível 1 (ORN1): os Ministérios e os órgãos e entidades públicos de nível equivalente, credenciados pelo Núcleo de Segurança e Credenciamento.

Órgãos de Registro Nível 2 (ORN2): os órgãos e entidades públicos vinculados ao Órgão de Registro nível 1 e credenciados pelos mesmos.

Órgão Gestor de Segurança da Informação: órgão ao qual foi atribuída a competência legal para atuar no planejamento das ações de segurança da informação a serem implementadas, considerando requisitos ou pressupostos estabelecidos pela APF, bem como o acompanhamento da evolução da maturidade de SI.

P

Padrões Corporativos de Sistemas e de Controle: conjunto de regras e de procedimentos que compõem os normativos internos das corporações.

Padrões e Procedimentos Gerais STI – (PPG / STI): Este documento define regras, padrões, procedimentos, nomenclaturas e orientações de uso quanto aos bancos de dados, arquitetura de software, segurança da informação, infraestrutura e inteligência artificial/ciência de dados do MAPA.

Patch: atualizações de sistemas.

Perfil de Acesso: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.

Perfil Institucional: cadastro do órgão ou entidade da APF como usuário em redes sociais, alinhado ao planejamento estratégico e à POSIC da instituição, com observância de sua correlata atribuição e competência.

Plano de Backup: documento formal onde são definidos os responsáveis pela cópia dos dados, o que será armazenado, periodicidade de execução da cópia e tempo de retenção, de acordo com as orientações da Política de Backup.

Plano de Contingência de Serviços de TI: documento que habilita a organização a recuperar um processo de negócio sustentado pela TI, após um incidente crítico que venha caracterizar uma crise, causando indisponibilidade ou degradação grave à operação padrão do processo de negócio.

Plano de Continuidade de Negócios: documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes.

Plano de Continuidade de Serviços de TIC: conjunto dos Planos de Backup e dos Planos de Contingência de Serviço de TIC, possibilitando respostas imediatas a incidentes graves, permitindo a continuidade de determinado Processo de Negócio.

Plano de Gerenciamento de Incidentes: plano de ação claramente definido e documentado, para ser usado em caso de incidente que basicamente englobe os principais recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.

Plano de Recuperação de Negócios: documentação dos procedimentos e de informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas a normalidade.

Política de Gestão de Riscos: declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de risco.

Política de Segurança: conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das entidades.

Política de Segurança da Informação (POSIC): documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da SI (Este termo substituiu o termo Política de Segurança da Informação e Comunicações).

Política de Provedores de Serviços - PGPS: adota uma abordagem abrangente no estabelecimento de diretrizes para auxiliar na avaliação, seleção, monitoramento e revisão contínua dos provedores de serviços contratados pelo órgão.

Portfólio de TIC: coleção de projetos, programas, serviços ou qualquer outros trabalhos de TIC, em andamento ou planejados, estando eles relacionados de alguma forma ou não, que estão agrupados com o propósito de facilitar o gerenciamento efetivo das ações para atender aos objetivos estratégicos organizacionais.

POSIN: acrônimo de Política de Segurança da Informação. Substitui o acrônimo POSIC.

Posto de Controle: unidade de órgão ou entidade pública ou privada, habilitada, responsável pelo armazenamento de informação classificada em qualquer grau de sigilo.

Prazo Máximo de Interrupção Tolerável (PMIT): prazo máximo que um serviço pode ficar fora de operação.

Preposto: representante da contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto à contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

Preservação de Evidência de Incidentes em Redes Computacionais: processo que compreende a salvaguarda das evidências e dos dispositivos, de modo a garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações.

Prestador de Serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderá receber credencial especial de acesso.

Prevenção de Perda de Dados: também conhecida como DLP (Data Loss Prevention), é a prática de detectar e prevenir vazamentos de dados, exfiltração de dados ou a destruição de dados sensíveis de uma organização. O termo DLP se refere tanto a ações contra a perda de dados (evento no qual os dados são definitivamente perdidos pela organização) como ações contra vazamentos de dados (transferência indevida de dados para fora da fronteira da organização).

Primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

Princípios de TIC: conjunto de declarações estratégicas sobre como a TIC deve ser utilizada, compreendendo os valores e premissas fundamentais que devem ser respeitados nas atividades de governança e gestão de TIC.

Problema: é a causa-raiz desconhecida de um ou mais incidentes.

Processo: sequência contínua de fatos ou operações que apresentam certa unidade ou que se reproduzem com certa regularidade: ação continuada, realização contínua e prolongada de alguma atividade.

Programa de Gestão da Continuidade de Negócios: processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para

garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção.

Proof of Stake ou Prova de Participação (PoS): algoritmo com os mesmos objetivos do PoW, entretanto, ao contrário do PoW, onde o algoritmo recompensa mineiros que resolvem problemas matemáticos com o objetivo de validar transações e criar novos blocos, no PoS o criador de um novo bloco é escolhido de forma determinística, baseado no seu grau de participação, definido como stake. Nesse sistema o potencial criador já deve contar com uma "participação" na rede (moedas em caso de criptomoedas). Quanto maior a participação de um usuário no sistema maior a chance de ele ser o criador escolhido. Além disso, o usuário selecionado deverá alocar uma quantidade de ativos para este processo e caso tente comprometer ou alterar o bloco perderá suas ativos. Isto em teoria garante a integridade dos participantes.

Proof of Work ou Prova de Trabalho (PoW): requisito da operação de mineração, que precisa ser realizada de forma a criar um novo bloco num blockchain. Sendo um mecanismo de resistência a ataques Sybil, é um protocolo que tem por principal objetivo deter ataques cibernéticos como um DDoS que tem por objetivo esgotar os recursos de um sistema computacional pelo envio de múltiplas requisições falsas. Uma das principais desvantagens do PoW, no modelo público, reside no controle da geração de tokens de recompensa. Todos os nós competem para ser o primeiro a solucionar o enigma matemático vinculado ao bloco de transações, um problema que não pode ser resolvido de outra maneira senão por força bruta. Logo, esse modelo implica um enorme emprego - e, de certa forma, um desperdício - de recursos computacionais e de energia. O primeiro usuário a resolver o problema ganha o direito de criar o próximo bloco - e recebe o token de recompensa;

Proprietário da informação: parte interessada do órgão ou entidade da APF, direta e indireta, ou indivíduo legalmente instituído por sua posição ou cargo, que é responsável primário pela viabilidade e sobrevivência da informação.

Proprietário de Ativos de Informação: unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos em meio físico ou digital relacionados.

Protocolo: conjunto de parâmetros que definem a forma e como a transferência de informação deve ser efetuada.

Provedor de Serviços de Nuvem: ente, público ou privado, prestador de serviço de computação em nuvem.

Pseudonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Público-alvo da ETIR: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais. Também chamado de Comunidade da ETIR.

Q

Quarentena: período em que arquivos ou programas de computadores são colocados em monitoramento quando não existe a certeza da procedência ou do tipo de atividades realizadas por eles.

Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

R

RCV: Release, Control and Validation ITIL V3 - Liberação, Controle e Validação é o módulo que se concentra na aplicação prática das práticas de RCV para permitir o planejamento, teste e implementação bem-sucedidos de novos serviços que atendam às necessidades da organização ou dos usuários.

Recovery Point Objective (RPO): ponto no tempo em que os dados devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;

Recovery Time Objective (RTO): tempo estimado para restaurar os dados e tornar os clientes de backup novamente operacionais, correspondendo ao prazo máximo em que se admite manter os clientes de backup inoperantes até a restauração de seus dados após um incidente;

Recuperação de Desastre: estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica.

Recursos Computacionais: equipamentos utilizados para armazenamento, processamento e transmissão de dados.

Recursos Computacionais e de Comunicação: equipamentos utilizados para armazenamento, processamento e transmissão de dados ou voz.

Recursos Criptográficos: sistemas, programas, processos e equipamentos, isolados ou em rede, que utilizam algoritmo simétrico ou assimétrico, para realizar a cifração ou decifração de informações.

Recursos de TIC: compreende os ativos organizacionais relacionados a TIC (informação, serviços, infraestrutura e aplicações), que permitem a organização alcançar suas metas.

Rede de Computadores: interligação de dois ou mais computadores e outros dispositivos conectados entre si de forma a permitir o compartilhamento de recursos físicos e lógicos.

Rede de Telecomunicações: conjunto operacional contínuo de enlaces e equipamentos, incluindo funções de transmissão, comutação ou quaisquer outras indispensáveis à operação de Serviço de Telecomunicações.

Rede Interna: conjunto de todas as redes locais.

Rede Nacional de Pesquisa (RNP): é uma organização social que provê a integração global e a colaboração apoiada em tecnologias de informação e comunicação para a geração do conhecimento e a excelência da educação e da pesquisa.

Rede Privada Virtual (VPN): mais conhecida por VPN (Virtual Private Network), refere-se a construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

Redes Sociais: estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.

Reduzir Risco: uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco.

Relatório de Impacto à Proteção de Dados Pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Repositório de Arquivo: conjunto de documentos ou lugar onde os documentos são guardados.

Requisitos da contratação de TIC: conjunto de características e especificações necessárias para definir a solução de TIC a ser contratada;

Requisitos de Segurança de Software: conjunto de necessidades de segurança que o software deve atender, sendo tais necessidades influenciadas fortemente pela política de segurança da organização, compreendendo aspectos funcionais e não funcionais. Os aspectos funcionais descrevem comportamentos que viabilizam a criação ou a manutenção da segurança e, geralmente, podem ser testados diretamente. Na maioria dos casos, remetem a mecanismos de segurança como, por exemplo, controle de acesso baseado em papéis de usuários (administradores, usuários comuns, etc.), autenticação com o uso de credenciais (usuário e senha, certificados digitais, etc.), dentre outros. Os aspectos não funcionais descrevem procedimentos necessários para que o software permaneça executando suas funções adequadamente mesmo quando sob uso indevido. São exemplos de requisitos não funcionais, dentre outros, a validação das entradas de dados e o registro de logs de auditoria com informações suficientes para análise forense.

Resiliência: capacidade de uma organização ou de uma infraestrutura de resistir aos efeitos de um incidente, ataque ou desastre e retornar à normalidade de operações.

Responsabilidade: dever dos agentes públicos em conhecer e respeitar todas as normas de segurança da informação e comunicações da respectiva instituição.

Restauração (Recovery): processo de recuperação de dados e disponibilização de dados salvaguardados em determinada imagem de backup.

Resumo Criptográfico: resultado da ação de algoritmos que fazem o mapeamento de bits de tamanho arbitrário para uma sequência de bits de tamanho fixo menor - conhecida como resultado hash - de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash (resistência à colisão) e que o processo reverso também não seja realizável (utilizando-se apenas o hash não é possível recuperar a mensagem que o gerou).

Retenção: período de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração.

Reter Risco: forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado.

Risco (Conceito Geral): possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo mensurado em termos de impacto e de probabilidade.

Risco de Segurança da Informação: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

Risco de TIC: fonte de ameaças que potencializa uma vulnerabilidade, expondo a organização a impactos em seu funcionamento, como mal funcionamento de sistemas, roubo ou vazamento de informações, deficiências de desempenho em recursos tecnológicos.

Riscos Gerenciais: fatores organizacionais que devem ser controlados, mitigados e prevenidos e que podem afetar e até inviabilizar o desempenho de processos, projetos e programas.

Rollback: No contexto da Tecnologia da Informação, o termo rollback refere-se à ação de desfazer uma atualização, correção ou implementação. Isso geralmente ocorre quando algo causa problemas ou impactos indesejados no ambiente de produção. Esta ação deve envolver procedimentos e estratégias que permitam reverter alterações em um sistema de forma segura e eficiente.

Root of Trust ou Raiz de Confiança (ROT): fonte que pode ser considerada sempre confiável em um sistema criptográfico. Como a segurança criptográfica é dependente de chaves para a encriptação e decriptação de dados e para a execução de funções como a geração de assinaturas digitais, esquemas RoT geralmente incluem módulos de hardware reforçados (sendo o principal exemplo o HSM) que geram e protegem chaves e executam funções criptográficas em um ambiente seguro. O RoT é um componente crítico de PKIs para a geração e proteção de chaves de autoridade certificadora e de raiz; para a assinatura de código de forma a garantir que o software permaneça seguro, inalterado e autêntico; e para a criação de certificados digitais para o credenciamento e autenticação de dispositivos proprietários para aplicações IoT e para outros componentes de rede.

Rootkit: conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. É importante ressaltar que o nome rootkit não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (root ou Administrator) em um computador, mas, sim, para manter o acesso privilegiado em um computador previamente comprometido.

Roteador e Switch: recursos computacionais que possibilitam a interligação de dois ou mais ativos de informação físicos ou virtuais.

Rotina de Backup: procedimentos de realização de cópias de segurança.

S

Sabotagem Cibernética: ataques cibernéticos contra a integridade e disponibilidade de sistemas e de serviços de TIC.

Sanitização de Dados: eliminação efetiva de informação armazenada em qualquer meio eletrônico, garantindo que os dados não possam ser reconstruídos ou recuperados.

Saúde Digital: Saúde Digital compreende o uso de recursos de TIC para produzir e disponibilizar informações confiáveis, sobre o estado de saúde para quem precisa, no momento que precisa.

Screenlogger: tipo específico de spyware. Programa similar ao keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de Internet Banking.

Segurança Cibernética: ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

Segurança da Informação (SI): preservação da confidencialidade, da integridade e da disponibilidade da informação. Adicionalmente há outras propriedades, como autenticidade, responsabilidade, não repúdio e confiabilidade, que podem também estar envolvidas.

Segurança Física e do Ambiente: processo referente à proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização estiver presente.

Segurança Orgânica ou Corporativa: conjunto de medidas passivas com o objetivo de prevenir e até mesmo obstruir as ações que visem ao comprometimento ou à quebra de segurança de uma organização. Inclui os processos relacionados às áreas: de pessoal, de documentação, das comunicações, da tecnologia da informação, dos materiais e das instalações de uma organização, dentre outros.

SEI: acrônimo de Sistema Eletrônico de Informações (SEI). O SEI foi desenvolvido pelo Tribunal Regional Federal da 4ª Região (TRF4), é uma ferramenta de gestão de documentos e processos eletrônicos, e tem como objetivo promover a eficiência administrativa.

Sensibilização: atividade que tem por objetivo atingir uma predisposição dos participantes para uma mudança de atitude sobre a SI, de tal forma que eles possam perceber em sua rotina pessoal e profissional ações que devem ser corrigidas. É uma etapa inicial da educação em SI.

Service Desk: área responsável por atender às requisições, registrar, escalonar e solucionar as ocorrências reportadas pelos usuários, desde que estejam contempladas no Catálogo de Serviços do Service Desk da organização.

Serviço de TI: qualquer provimento de serviços de desenvolvimento, implantação, manutenção, armazenamento e recuperação de dados e operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico necessários à gestão da informação, que sustentem um processo de negócio essencial.

Serviço de TIC: atividades de fornecimento de infraestrutura e aplicações de TIC, bem como suporte técnico para seu uso, atendendo aos requisitos de qualidades definidos no acordo de nível de serviço.

Serviços (Conceito Geral): um meio de fornecer valor a clientes, facilitando a obtenção de resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos.

Serviço da ETIR: conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

Serviços de Tecnologia da Informação: provimento de serviços de desenvolvimento, de implantação, de manutenção, de armazenamento e de recuperação de dados e de operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico necessários à gestão da informação.

Servidores de Rede: recursos computacionais que armazenam e disponibilizam informações em uma rede de dados.

Sistema de Acesso: conjunto de ferramentas que se destina a controlar e a dar permissão de acesso a uma pessoa a um recurso.

Sistema Biométrico: conjunto de ferramentas que se utiliza das características de uma pessoa, levando em consideração fatores comportamentais e fisiológicos, a fim de identificá-la de forma unívoca.

Sistema de Informação: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que

possibilitam a agregação dos recursos de tecnologia, informação e comunicações em forma integrada.

Sistema de Proteção Física: sistema composto por pessoas, equipamentos e procedimentos para a proteção de ativos contra danos, roubo, sabotagem e outros prejuízos causados por ações humanas não autorizadas, conforme gestão da segurança física e ambiental.

Sistema Estruturante: sistema com suporte de TIC fundamental e imprescindível para o planejamento, coordenação, execução, descentralização, delegação de competência, controle ou auditoria das ações de Estado, além de outras atividades auxiliares, desde que comum a dois ou mais órgãos ou entidades da APF, direta ou indireta, e que necessitem de coordenação central.

Sistemas Operacionais: softwares que têm como função servir de interface entre os recursos computacionais e o usuário.

Site: páginas contendo informações, imagens, fotos, vídeos, sons etc., que ficam armazenadas em provedores de acesso (computadores denominados servidores) à Internet, para serem acessadas por qualquer pessoa que se conecte à rede.

Software: programa de computador desenvolvido para executar um conjunto de ações previamente definidas.

Solução de TIC: conjunto de bens e/ou serviços que apoiam processos de negócio, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações.

SPAM: é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

Spoofing: é a prática de disfarçar uma comunicação de uma fonte desconhecida como se fosse de uma fonte conhecida e confiável ao destinatário. Pode ser aplicado a e-mails, ligações telefônicas (fixas ou móveis), sites, endereços IP, servidores DNS, e o Protocolo de Resolução de Endereços (ARP) entre outros. Geralmente é usado para obter acesso a informação pessoal, disseminar malware através de links e anexos, contornar os controles de acesso de uma rede ou redistribuir o tráfego de rede para conduzir ataques DoS.

Spyware: tipo específico de código malicioso. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Keylogger, screenlogger e adware são alguns tipos específicos de spyware;

SSL: acrônimo de Secure Sockets Layer.

Sustentação: compreende as atividades realizadas para a manutenção da disponibilidade, estabilidade e desempenho das aplicações de software, tais como manutenções corretivas, investigação de incidentes, resolução de problemas e apoio aos usuários, bem como atividades de suporte à manipulação de dados, monitoramento e operação das aplicações e seus componentes, compreendendo todos os ambientes em que a solução esteja instalada.

T

Tecnologia da Informação e Comunicação (TIC): ativo estratégico que suporta processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações.

Telecomunicações: é a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza.

Tempo Objetivo de Recuperação: tempo pré-definido no qual uma atividade deverá estar disponível após uma interrupção ou incidente.

Terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos à organização.

Termo de Responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

Termo de Confidencialidade: documento formal, a ser assinado por prestadores da organização, por meio do qual se comprometem a manter sigilo em relação às informações consideradas confidenciais e respeitar as normas de segurança vigentes.

Terrorismo Cibernético: crime cibernético perpetrado por razões políticas, religiosas ou ideológicas contra qualquer elemento da infraestrutura cibernética com os objetivos de: provocar perturbação severa ou de longa duração na vida pública; causar danos severos à atividade econômica com a intenção de intimidar a população; forçar as autoridades públicas ou uma organização a executar, a tolerar, a revogar ou a omitir um ato; ou abalar ou destruir as bases políticas, constitucionais, econômicas ou sociais de um Estado, organização ou empresa. É principalmente realizado por atos de sabotagem cibernética organizados e

gerenciados por indivíduos, grupos político-fundamentalistas, ou serviços de inteligência estrangeiros.

TIC: acrônimo de Tecnologia da Informação e Comunicações.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Token: algo que o usuário possui e controla (tipicamente uma chave, senha e/ou módulo criptográfico) que é utilizado para autenticar a identidade do requerente e/ou a requisição em si.

TLP (Traffic Light Protocol): O Traffic Light Protocol é um sistema de classificação de informações confidenciais criado no início dos anos 2000 pelo Centro de Coordenação de Segurança de Infraestrutura Nacional do Governo do Reino Unido, a fim de incentivar um maior compartilhamento de informações confidenciais.

TLS: acrônimo de Transport Layer Security.

Trabalho remoto: atividade de interesse da empresa realizada externamente pelos agentes públicos utilizando os recursos computacionais alocados internamente na infraestrutura do órgão.

Transferir risco: forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco.

Transferência Internacional de Dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Tratamento da Informação: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação.

Tratamento da Informação Classificada: conjunto de ações referentes a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo.

Tratamento de Artefatos Maliciosos: serviço que prevê o recebimento de informações ou cópia do artefato malicioso que foi utilizado no ataque, ou de

qualquer outra atividade desautorizada ou maliciosa. Uma vez recebido o artefato o mesmo deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou sugerida, uma estratégia de detecção, remoção e defesa contra esses artefatos.

Tratamento de Incidentes de Segurança em Redes Computacionais: serviço que consiste em receber, filtrar, classificar e responder às solicitações e aos alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

Tratamento de Problemas: processo que tem por objetivo encontrar a causa raiz de um ou mais incidentes de forma a eliminá-los da infraestrutura, evitando a recorrência dos incidentes e possibilitando o cumprimento dos Níveis de Serviço.

Tratamento de Riscos: processo de implementação de ações de SI para evitar, reduzir, reter ou transferir um risco.

Tratamento de Vulnerabilidades: serviço que prevê o recebimento de informações sobre vulnerabilidades, em hardware ou software, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção dessas vulnerabilidades.

Trilha de Auditoria: registro ou conjunto de registros gravados em arquivos de log ou outro tipo de documento ou mídia, que possam indicar, de forma cronológica e inequívoca, o autor e a ação realizada em determinada operação, procedimento ou evento.

Trustless: termo por vezes utilizado de forma ambígua na descrição de sistemas blockchain. Blockchains não eliminam realmente a confiança (trust). O que se entende por trustless, na verdade, é a minimização da quantidade de confiança que é necessária de cada ator individual no sistema. Isso é feito pela distribuição da confiança entre os diferentes atores envolvidos no sistema através de um jogo econômico que incentiva os atores a cooperarem com as regras definidas pelo protocolo. Na prática, o que se quer dizer com trustless em sistemas blockchain é que o poder e a confiança é distribuída entre os membros componentes do sistema ao invés de estar concentrado em um único indivíduo ou entidade.

U

UID: acrônimo de Identificador Único (Unique IDentifier) em sistemas de computadores. Baseados nessa definição, também temos o GUID (Identificador Global Único - Global Unique IDentifier) e UUID (Identificador Universal Único - Universal Unique IDentifier). Ressalta-se que, no sistema UNIX, UID significa Identificador do Usuário (User IDentifier).

Unidade de Armazenamento: dispositivo para armazenamento de dados em suporte digital.

Unidade de Armazenamento de Backup: unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais.

Unidades Portáteis de Armazenamento: dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, HD externo, Pen Drive, cartão de memória entre outros.

Uso Compartilhado de Dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Usuário: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitado pelo órgão para acessar os seus ativos de informação.

Usuário de informação: pessoa física, empregado, servidor ou prestador de serviços terceirizado, habilitado pela administração para acessar os ativos de informação de um órgão ou entidade da Administração Pública Federal, formalizada por meio da assinatura de Termo de Responsabilidade.

Usuários Visitantes: usuários que não pertençam ao quadro funcional da organização, que estejam visitando as dependências do órgão.

Usuário Visitante com Dispositivo Móvel: agentes públicos ou não que utilizem dispositivos móveis, de sua propriedade ou do órgão ou entidade a que pertencem, dentro dos ambientes físicos de órgãos ou entidades da APF dos quais não fazem parte.

URL: acrônimo de Uniform Resource Locator.

V

Vazamento de Dados: transmissão não-autorizada de dados de dentro de uma organização para um destino ou recipiente externo. O termo pode ser usado para

descrever dados que são transferidos eletronicamente ou fisicamente. Pode ocorrer de forma acidental ou intencional (pela ação de agentes internos, pela ação de agentes externos ou pelo uso de software malicioso). É conhecido também como roubo de dados low-and-slow (rasteiro-e-lento) pois a exfiltração de dados para fora da organização é feita usando técnicas do tipo low-and-slow a fim de evitar detecção.

Vendor Lock-In: também conhecido como lock-in proprietário ou lock-in do cliente, usado para designar a situação em que há um alto custo de troca para o consumidor em um ou mais serviços. Isso faz com que um cliente fique dependente de um fornecedor de produtos e serviços, pois a mudança de fornecedor implica em substanciais custos de mudança.

Verificação de Conformidade em Segurança da Informação: procedimentos que fazem parte da avaliação de conformidade que visam identificar o cumprimento das legislações, normas e procedimentos relacionados à SI da organização.

Vírus: seção oculta e autorreplicante de um software de computador, geralmente utilizando lógica maliciosa, que se propaga pela infecção (isto é, inserindo uma cópia sua e se tornando parte) de outro programa. Não pode se auto executar, ou seja, necessita que o seu programa hospedeiro seja executado para se tornar ativo.

Vishing: uma forma de ataque de phishing que ocorre em VoIP, sendo que as vítimas não precisam estar utilizando VoIP. O atacante usa sistemas VoIP para efetuar ligações para qualquer número de telefone, sem cobrança de taxas, e, geralmente, falsifica (spoofing) sua identificação de chamada, a fim de levar a vítima a acreditar que está recebendo um telefonema de uma fonte legítima ou confiável (como um banco, uma loja de varejo, entre outros).

VPN: acrônimo de rede privada virtual (Virtual Private Network).

Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

Vulnerabilidade de Dia Zero ou Zero-Day Vulnerability: falha na segurança de um software que ainda não é conhecida por seus desenvolvedores, pelos fabricantes de soluções de segurança e pelo público em geral. Também é considerada uma Vulnerabilidade de Dia Zero a falha de segurança que já é conhecida pelo fornecedor do produto mas para a qual ainda não existe um pacote de segurança para corrigi-la. Por não ser conhecida ou por não haver ainda um patch de segurança para essa falha, ela pode ser explorada por hackers em Explorações de Dia Zero. A correção de uma vulnerabilidade de dia zero geralmente é tarefa do fabricante do software, que precisará lançar um pacote de segurança para consertar a falha.

W

Whitelist: lista de itens aos quais é garantido o acesso a certos recursos, sistemas ou protocolos. Utilizar uma whitelist para controle de acesso significa negar o acesso a todas as entidades exceto àquelas incluídas na whitelist.

Worm: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou de falhas na configuração de programas instalados em computadores.

X

XSS: acrônimo de Cross-site Scripting.

Z

Zona de Nuvem: locais isolados dentro de cada região, dos quais os serviços de computação em nuvem pública se originam e operam.

Zona Desmilitarizada (DMZ): também conhecida como rede de perímetro, trata-se de uma sub-rede (física ou lógica) que se situa entre uma rede privada confiável e uma rede não confiável, e onde recursos computacionais são hospedados para serem acessados a partir da rede não confiável (em geral, a Internet), evitando o acesso à rede interna da organização. A DMZ garante o isolamento entre a rede confiável e não confiável por uma série de regras de conectividade mantidas em um firewall;

Zumbi: nome dado a um computador infectado por bot, pois pode ser controlado remotamente, sem o conhecimento do seu proprietário.