MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE DA INTEGRAÇÃO INTERNACIONAL DA LUSOFONIA AFRO-BRASILEIRA

RESOLUÇÃO CGD/UNILAB Nº 1, DE 26 DE OUTUBRO DE 2022

Aprova a Política de Segurança da Informação e Comunicações (PoSIC) da Universidade da Integração Internacional da Lusofonia Afro-Brasileira - Unilab.

O COMITÊ DE GOVERNANÇA DIGITAL, no uso de suas atribuições legais, em sua 1º sessão ordinária, realizada no dia 26 de outubro de 2022, considerando o processo nº 23282.015361/2022-51,

RESOLVE:

Art. 1º Aprovar a Política de Segurança da Informação e Comunicações (PoSIC) da Universidade da Integração Internacional da Lusofonia Afro-Brasileira - Unilab, nos termos do anexo, parte integrante desta Resolução.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

CLÁUDIA RAMOS CARIOCA
Presidente do Comitê de Governança Digital

Documento assinado eletronicamente por **CLAUDIA RAMOS CARIOCA**, **PRESIDENTE DA COMISSÃO**, em 27/10/2022, às 16:33, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.unilab.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0563040** e o código CRC **8655074F**.

ANEXO À CGD/UNILAB Nº 1, DE 26 DE OUTUBRO DE 2022

POLÍTICA DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA UNIVERSIDADE DA INTEGRAÇÃO INTERNACIONAL DA LUSOFONIA AFRO-BRASILEIRA

CAPÍTULO I

ESCOPO, OBJETIVOS E PRINCÍPIOS

Art. 1º Instituir a Política de Segurança da Informação e Comunicações (PoSIC) da Universidade da Integração Internacional da Lusofonia Afro-Brasileira (Unilab), observados os princípios, objetivos e diretrizes estabelecidos nesta Resolução, bem como as disposições constitucionais, legais, planejamento estratégico e regimentais vigentes.

§ 1º A PoSIC estabelece as orientações e diretrizes corporativas gerais de segurança e controle dos ativos de informação da Unilab ou sob sua guarda, objetivando sua proteção, estabelecendo regras e padrões para prevenção e responsabilidade legal para os usuários.

§ 2º Integram também a PoSIC normas gerais e específicas de segurança da informação e comunicações, bem como procedimentos complementares, destinados à proteção dos ativos de informação e à disciplina de sua utilização, originados na Unilab.

Art. 2º A Segurança da Informação e Comunicações da Unilab é integrada por três instrumentos normativos, de níveis hierárquicos distintos, relacionados a seguir:

I - a Política de Segurança da Informação e Comunicações (PoSIC) - que define a estrutura, as diretrizes e as obrigações referentes à segurança da informação e comunicações;

II - as Normas de Segurança da Informação e Comunicações - que identificam obrigações e procedimentos em conformidade com as diretrizes da PoSIC, a serem seguidas em todas as situações em que a informação é tratada; e

III - os Procedimentos de Segurança da Informação e Comunicações - que instrumentalizam os dispositivos, permitindo a direta aplicação nas atividades da Unilab.

Art. 3º A PoSIC se alinhará às estratégias da Unilab e terá por objetivo garantir os princípios de segurança da informação e comunicações, das informações produzidas ou custodiadas pela universidade, abrangendo aspectos físicos, tecnológicos e humanos da organização.

Art. 4º A Segurança da Informação e Comunicações (SIC) terá, dentre outros inerentes à Administração Pública Federal, os seguintes princípios:

I - confidencialidade: garante que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada;

II - disponibilidade: assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

III - integridade: atesta que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

IV - autenticidade: certifica que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

V - responsabilidade: preservação da integridade e tratamento de maneira adequada, de acordo com sua classificação, da informação, bem como preservar e zelar pelos ativos de informação;

VI - clareza: as regras que se fundam nesta PoSIC devem ser claras, objetivas e concisas, a fim de viabilizar sua fácil compreensão; e

VII - publicidade: transparência às informações, respeitando a privacidade do cidadão.

Art. 5º A PoSIC e as normas de segurança da informação e comunicações devem ser divulgadas a todos os usuários da Unilab, devendo ser dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Parágrafo único. Os procedimentos de segurança da informação e comunicações devem ser divulgados apenas às áreas relacionadas à sua execução.

CAPÍTULO II

CONCEITOS E DEFINIÇÕES

Art. 6º Para fins desta Resolução, serão considerados os conceitos constantes do Glossário de Segurança da Informação, anexo A.

CAPÍTULO III

DIRETRIZES GERAIS

Art. 7º A Segurança da Informação e Comunicações (SIC) deve ser responsabilidade de todos, baseada em hábitos, posturas, responsabilidade e cuidados constantes no momento do uso dos ativos de informação.

Art. 8º A utilização dos ativos de informação deve ser sempre compatível com a ética, confidencialidade, legalidade e finalidade das atividades desempenhadas pelo usuário.

Art. 9º Os dirigentes das unidades e demais chefias da Unilab assumem o compromisso de atuar junto à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (EPTRIC), naquilo que porventura sejam solicitados, e a desenvolver suas atividades de forma colaborativa em estrita observância às orientações determinadas pela EPTRIC, naquilo que tange a SIC, objetivando minimizar as vulnerabilidades e ameaças que possam comprometer o negócio da instituição.

Seção I

Tratamento da Informação

Art. 10. Todo ativo de informação sob a responsabilidade da Unilab é considerado um bem e deve ser protegido pela instituição, de acordo com as diretrizes descritas nesta PoSIC e demais regulamentações em vigor, com o objetivo de minimizar os riscos aos serviços e atividades, bem como preservar a imagem institucional.

Art. 11. A classificação da informação obedecerá às diretrizes estabelecidas pela Lei de Acesso à Informação (LAI), regulamentada pelo Decreto nº 7.724, de 16 de maio de 2012, do Governo Federal, pela Lei Geral de Proteção dos Dados (LGPD), regulamentada pela Lei nº 13.709, de 14 de agosto 2018, do Governo Federal, e do Serviço de Informação ao Cidadão (SIC) no âmbito da Unilab.

Art. 12. Para assegurar que a informação recebe um nível adequado de proteção, ela deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade.

Seção II

Segurança Física e do Ambiente de TI

Art. 13. A segurança física e do ambiente de TI tem como objetivo manter as instalações físicas e as áreas de processamento de informações críticas ou sensíveis protegidas contra acesso indevido, danos e interferência, seguindo a NBR/ISO/IEC 27001 e legislação vigente.

Parágrafo único. A segurança física e do ambiente de TI será implementada da seguinte forma:

I - área segura: para a entrada física nas áreas seguras devem ser utilizados perímetros de segurança e protegidas por controles apropriados de entrada para assegurar que só tenham acesso às pessoas autorizadas;

II - acesso à sala de equipamentos ou data center: qualquer concessão de acesso será autorizada pelo gestor da área responsável. Caso tenha a entrada de prestadores de serviços e visitantes nos ambientes, deve ser sempre acompanhada por pessoal interno da área responsável, que se responsabilizará pelas ações do terceiro no ambiente;

III - proteção dos equipamentos críticos de TI: para proteção dos equipamentos classificados como críticos, os ambientes devem ser projetados com fornecimento adequado de sistema de energia elétrica com redundância, proteções físicas contra incêndios, calor, enchentes, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem;

IV - segurança de equipamentos: para impedir perdas, danos, furto ou comprometimento de ativos de TI e interrupção das atividades, os equipamentos devem estar em local apropriado ou protegido para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado. Devem ser tomadas medidas de segurança para equipamentos que operem fora das dependências da Unilab, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora dos domínios institucionais; e

V - manutenção dos equipamentos: os equipamentos devem receber manutenção, conforme indicação do fabricante ou da equipe responsável, para assegurar sua disponibilidade e

integridade permanente.

Seção III

Gestão de Incidentes em Segurança da Informação

Art. 14. Para evitar ou minimizar os impactos de situações de interrupção dos sistemas de informação e comunicações causados por incidentes de segurança, a EPTRIC deverá manter um Plano de Gerenciamento de Incidentes, elaborado e alinhado aos Processos de Gestão de Continuidade de Negócio em Segurança da Informação, conforme IN PR/GSI Nº 3, de 28 de maio de 2021, ou documento correspondente que venha a substituí-lo.,

Art. 15. Todo incidente de segurança, bem como suas providências, deverá ser comunicado ao Gestor de Segurança da Informação e Comunicações da Unilab.

Seção IV

Gestão dos Ativos

Art. 16. O gestor de segurança da informação designará um agente responsável pela gestão dos ativos de informação, que manterá informações atualizadas do inventário dos ativos de TI com objetivo de alcançar e manter a proteção adequada da instituição.

Art. 17. A Unilab deverá adotar processo contínuo de Gestão dos Ativos, conforme estabelecido na IN PR/GSI nº 3, de 28 de maio de 2021, ou documento correspondente que venha a substituí-lo.

Seção V

Gestão de Riscos

Art. 18. A Unilab deverá adotar processo contínuo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC, conforme estabelecido na IN PR/GSI nº 3, de 28 de maio de 2021, ou documento correspondente que venha a substituí-lo.

Art. 19. O processo de GRSIC deverá ser revisto periodicamente pelo Serviço de Segurança da Informação e Comunicações - SSIC/DISIR/DTI, com a participação da EPTRIC, a fim de aperfeiçoar e agir proativamente contra riscos com origem às novas tecnologias e ameaças, objetivando a constante elaboração de planos de ação apropriados para a proteção dos seus ativos de informação.

Art. 20. Caberá ao Serviço de Segurança da Informação e Comunicações/DISIR/DTI (SSIC/DISIR/DTI) a criação e atualização do Plano de Tratamento de Riscos, com a participação da EPTRIC e de grupos de trabalho específicos.

Seção VI

Gestão de Continuidade

Art. 21. Com o objetivo de evitar situações de interrupção e manter em funcionamento os sistemas de informação e comunicações da Unilab, o SSIC/DISIR/DTI, com a participação da EPTRIC, deverá criar e manter um Programa de Gestão da Continuidade de Negócios, conforme IN PR/GSI Nº 3, de 28 de Maio de 2021, ou documento correspondente que venha a substituí-lo.

Seção VII

Auditoria e Conformidade

Art. 22. O SSIC/DISIR/DTI deverá propor normas complementares ao Comitê Gestor de Segurança da Informação (CGSI), com a participação da EPTRIC, a fim de manter registros, como mecanismo de auditoria que possibilite o rastreamento, acompanhamento, controle e verificação de acesso aos serviços, sistemas de informação e rede interna, em conformidade com a NC nº 21 PR/GSI/DSIC, de 8 de outubro de 2014, ou documento correspondente que venha a substituí-lo.

Seção VIII

Controles de Acesso

Art. 23. A concessão de acesso aos ativos de informação da Unilab tem por objetivo garantir aos usuários a realização de suas atividades.

Art. 24. O uso dos ativos de informação na Unilab, pelos seus usuários, deve ser direcionado prioritariamente para a realização das atividades de ensino, pesquisa, extensão e de administração desempenhadas nos limites da ética, razoabilidade e legalidade.

Art. 25. A conta de acesso e a senha de cada pessoa são únicas, individuais e intransferíveis, sendo reconhecidas como equivalentes à sua assinatura e representam nível de delegação concedida para o desempenho de suas funções.

Art. 26. O CGSI deverá normatizar o acesso físico e lógico aos ativos de tecnologia da informação da Unilab, como forma de garantir a sua proteção.

Seção IX

Uso de E-mail

Art. 27. O e-mail institucional da Unilab está regulamentado no Anexo I da Resolução Conad nº 01, de 25 de outubro de 2021, ou documento correspondente que venha a substituí-lo.

Seção X

Sites Institucionais

Art. 28. Os serviços e servidores da instituição, tais como os de páginas de Internet, correio eletrônico, sistemas administrativos e sistemas acadêmicos, deverão ser configurados para usar

tecnologias de autenticação e criptografia visando a garantir a integridade, o sigilo e a autenticidade das informações.

Art. 29. Caberá a DISIR/DTI definir e pôr em prática as medidas necessárias para preservar a segurança dos serviços e servidores institucionais que estiverem sob sua responsabilidade, com a participação da EPTRIC, de forma a não comprometer a segurança das redes internas e externas da instituição.

Parágrafo único. A unidade que adotar domínio próprio deverá pôr em prática as medidas necessárias para preservar a segurança dos seus serviços e servidores, definidas pela DISIR/DTI, de forma a não comprometer a segurança das redes internas e externas da instituição.

Seção XI

Gestão da Segurança da Informação e Comunicações

Art. 30. O processo de Gestão da Segurança da Informação e Comunicações deverá ser proposto pela SSIC, com a participação da DISIR/DTI e EPTRIC, e aprovado pelo CGSI em norma complementar.

Seção XII

Segurança Lógica do Ambiente de TI

Art. 31. A Unilab deverá manter soluções de proteção contra problemas de segurança lógica (vírus, acesso não autorizado, invasões, etc.), cabendo a DISIR/DTI, com a participação da EPTRIC, a definição de tais soluções de proteção, considerando a criticidade dos ativos de informação envolvidos e que estejam sob sua responsabilidade.

Art. 32. Caberá a DISIR/DTI, com a participação da EPTRIC, a definição dos procedimentos de segurança para a implantação, manutenção, atualização, desinstalações e recuperação de softwares, sistemas operacionais, sistemas de gerenciamento de banco de dados (SGDBs), de forma a garantir que estes ambientes lógicos da Unilab não tragam vulnerabilidades que comprometam a segurança da informação, cabendo ao CGSI a normatização.

Art. 33. Cabe aos órgãos da Unilab providenciar para que os ambientes lógicos, sob sua responsabilidade, tenham o seu acesso restrito por senhas seguras, ou outros mecanismos de segurança apropriados, salvo em situações nas quais existam restrições técnicas impeditivas que serão analisadas pela DISIR/DTI.

Seção XIII

Segregação de Ambientes

Art. 34. A EPTRIC deverá assegurar que todos os sistemas de informação, sob a responsabilidade da DTI, sejam aderentes às diretrizes a seguir:

I - segregação de ambientes lógicos, de maneira que o ambiente de produção fique apartado dos demais;

II - os ambientes de produção somente poderão ser acessados por usuários internos responsáveis pela implantação dos sistemas de informação;

III - o acesso às bases de dados dos ambientes de produção será feito, sempre que possível, por meio dos sistemas de informação, ou, não sendo possível, o acesso deverá ser feito por um membro da equipe responsável pela base de dados com autorização de um usuário interno com nível gerencial da área solicitante. O acesso direto deverá ser registrado em meio que permita a identificação do que foi modificado e quem foi responsável pela modificação;

IV - os sistemas de informação que forem transferidos para o ambiente de produção deverão ter seu código-fonte original mantido por um sistema de gerenciamento de repositórios de código-fonte interno;

V - o código-fonte dos sistemas de informação sob domínio da EPTRIC deverão ser gerenciados por ferramenta específica de controle de versão. O acesso à ferramenta deverá ser restrito através de perfis de acesso específicos e registrados em trilhas de auditoria. O controle de versão deve permitir a identificação do responsável pela inclusão/exclusão/alteração do código-fonte, assim como a recuperação de versões recentes;

VI - o ambiente do sistema computacional destinado à execução dos sistemas e o ambiente de produção não deve ser utilizado para testes. Os testes devem ser feitos em ambiente apropriado e gerenciado; e

VII - a passagem de programas e dados para o ambiente de produção deve ser controlada de maneira a garantir a integridade e disponibilidade desse ambiente para sua execução.

Seção XIV

Computação em Nuvem

Art. 35. A Unilab deverá seguir os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem descritos na IN PR/GSI nº 5, de 30 de agosto de 2021, ou documento correspondente que venha a substituí-lo.

Seção XV

Mídias Sociais

Art. 36. A Unilab deverá seguir as diretrizes de segurança da informação para o uso seguro de mídias sociais tratada na IN PR/GSI nº 6, de 23 de dezembro de 2021, ou documento correspondente que venha a substituí-lo.

Seção XVI

Acesso à Internet

Art. 37. As normativas referentes ao acesso à internet deverão ser propostas pela SSIC/DISIR/DTI, com a participação da EPTRIC, e aprovado pelo CGSI em norma complementar.

CAPÍTULO IV

COMPETÊNCIAS E RESPONSABILIDADES

Art. 38. A estrutura para Gestão de Segurança da Informação e Comunicações na Unilab é composta pelo (a):

I - Comitê Gestor de Segurança da Informação (CGSI);

II - Gestor de Segurança da Informação e Comunicações; e

III - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (EPTRIC).

Seção I

Comitê Gestor de Segurança da Informação

Art. 39. Deverão ser seguidas as diretrizes do CGSI tratadas no Anexo I da Resolução CONAD nº 07, de 25 de outubro de 2021, ou documento correspondente que venha a substituí-lo.

Seção II

Gestor de Segurança da Informação e Comunicações

Art. 40. O Gestor de Segurança da Informação e Comunicações será indicado pelo Diretor de Tecnologia da Informação e será designado pelo Reitor.

Art. 41. Compete ao Gestor de Segurança da Informação:

I - promover a cultura de Segurança da Informação e Comunicações;

II - monitorar, em conjunto com o Agente Responsável, as operações da equipe de prevenção, tratamento e resposta a incidentes cibernéticos;

III - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de Segurança da Informação e Comunicações;

IV - propor recursos necessários às ações de Segurança da Informação e Comunicações;

V - propor e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na Segurança da Informação e Comunicações;

VI - manter, sistematicamente, contato direto com o diretor da Diretoria de Tecnologia da Informação (DTI), o gerente da Divisão de Infraestrutura Segurança da Informação e Redes (DISIR) e o chefe do Serviço de Segurança da Informação e Comunicações (SSIC) para o trato de assuntos relativos à Segurança da Informação e Comunicações;

VII - propor alterações a PoSIC; e

VIII - propor normas relativas à Segurança da Informação e Comunicações.

Seção III

Equipe de Tratamento de Incidentes em Cibersegurança

Art. 42. A Unilab constituirá Equipe de Prevenção, Tratamento, Resposta de Incidentes em Cibersegurança (EPTRIC) e, no seu Documento de Constituição adotará as recomendações do Anexo A da NC PR/GSI/DSIC nº 5, de 14 de agosto de 2009, ou documento correspondente que venha a substituí-lo.

Parágrafo único. A EPTRIC será instituída por portaria normativa expedida pelo Reitor.

Seção IV

Gestores de Informação

Art. 43. São responsabilidades dos gestores da informação, no que concerne às informações sob sua gestão, produzidas ou custodiadas pela Universidade:

I - adotar as medidas e procedimentos necessários para garantir a segurança das informações;

II - definir procedimentos, critérios de acesso e classificar as informações, observados os dispositivos legais e regimentais relativos ao sigilo e a outros requisitos de classificação pertinentes, considerando a Portaria Normativa de que dispõe sobre os procedimentos da Lei de Acesso à informação, da Lei Geral de Proteção dos Dados e do Serviço de Informação ao Cidadão – SIC, no âmbito da Unilab;

III - propor regras específicas ao uso das informações; e

IV - manter o devido registro e controle ao autorizar e fornecer acesso aos ativos de TI sob sua responsabilidade aos usuários.

§ 1º As informações recebidas de pessoa física ou jurídica externa à Universidade serão submetidas, adicionalmente, às medidas de segurança da informação compatíveis com os requisitos pactuados com quem as forneceu.

§ 2º O Reitor, os Pró-Reitores, os Diretores Gerais, os Superintendentes, os Diretores de Instituto e os Coordenadores de Curso podem indicar, orientar e autorizar, a qualquer tempo, procedimentos que visem a garantir a segurança da informação, nos processos e documentos de sua competência, a serem seguidos pelos gestores da informação pertinentes.

Seção V

Custodiante da Informação

Art. 44. São responsabilidades do custodiante da informação:

I - garantir a segurança da informação sob sua custódia;

II - comunicar oportunamente ao CGSI sobre situações que comprometam a segurança das informações sob sua custódia;

III - comunicar ao CGSI eventuais limitações para cumprimento dos critérios definidos para segurança da informação; e

IV - observar procedimentos, critérios de acesso e classificação das informações definidos pelos Gestores da Informação.

Seção VI

Dirigentes das Unidades e Demais Chefias

Art. 45. São responsabilidades dos dirigentes e demais chefias das unidades da Unilab no que se refere à segurança da informação:

I - conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de segurança da informação;

II - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação;

III - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários sob sua supervisão;

IV - avaliar os danos, para sua área, decorrentes de quebra de segurança; e

V - tomar as providências cabíveis quando da comunicação conclusiva do incidente encaminhada pelo CGSI.

Seção VII

Usuários de Ativos de Informação

Art. 46. É dever de todos os usuários de ativos de informação:

I - conhecer e cumprir as diretrizes e normas desta PoSIC;

II - responsabilizar-se por todo e qualquer acesso aos ativos de informação da Unilab, bem como pelos efeitos desse acesso, realizado por meio de seu código de identificação;

III - comunicar o mais breve possível os incidentes de segurança da informação, por ele conhecido, ao setor responsável; e

IV - colaborar com as investigações de incidentes, envolvendo direta ou indiretamente sua área.

Seção VIII

Relacionamento com Terceiros

Art. 47. Nos editais de licitação, nos contratos ou acordos de cooperação técnica com entidades prestadoras de serviços para a Unilab, deverá constar cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta PoSIC.

CAPÍTULO V

SANÇÕES E PENALIDADES

Art. 48. Atos ou ações que violem o disposto nesta Resolução ou em quaisquer de suas normas e/ou procedimentos complementares, ou que prejudiquem os controles de segurança da informação, no âmbito da Unilab, serão apuradas mediante instauração de processo administrativo disciplinar.

Parágrafo único. Os responsáveis por prejuízos ou irregularidades mencionados no caput deste artigo responderão administrativa, civil e/ou penalmente pelos seus atos.

CAPÍTULO VI

POLÍTICA DE ATUALIZAÇÃO

Art. 49. Esta Resolução deverá ser revisada e atualizada a cada dois (2) anos, a contar da sua vigência ou quando identificada a necessidade pelo CGSI.

Art. 50. As diretrizes da PoSIC serão implementadas de forma incremental, conforme projeto de implantação aprovado pelo CGSI.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 51. O projeto de implantação da PoSIC será desenvolvido pelo Serviço de Segurança da Informação e Comunicações/DISIR/DTI.

Art. 52. Os casos omissos nesta Resolução serão decididos pelo Presidente do CSIC, ouvidos, quando for o caso, os membros do referido comitê.

ANEXO A - GLOSSÁRIO DE SEGURANÇA DA INFORMAÇÃO

2

2FA - acrônimo de Autenticação de Dois Fatores (2Factor Authentication).

A

AAA - acrônimo de Autenticação, Autorização e Auditoria;

AC - acrônimo de Autoridade Certificadora;

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;

ACL - acrônimo de Lista de Controle de Acesso (Access Control List);

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 DE REDE - pessoa física que administra o segmento de rede correspondente à área de abrangência da respectiva unidade;

ADWARE - do inglês Advertising Software, é um tipo específico despyware 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 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 - servidor público, empregado, ou militar de carreira de órgão ou entidade da APF, direta ou indireta, que

utilize dispositivo móvel de computação de propriedade dos órgãos ou entidades a que pertence;

AGENTE PÚBLICO COM DISPOSITIVO MÓVEL PARTICULAR - servidor público, empregado, ou militar de carreira de órgão ou entidade da APF, direta ou indireta, 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 - servidor público ou empregado ocupantes de cargo efetivo ou militar de carreira de órgão ou entidade da APF, direta e indireta, 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;

AGENTES DE TRATAMENTO - o controlador e o operador;

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;

ALTA ADMINISTRAÇÃO - Ministros de Estado, ocupantes de cargos de natureza especial, ocupantes de cargo de nível 5 (cinco) do Grupo Direção e Assessoramento Superiores - DAS e presidentes e diretores de autarquias, inclusive as especiais, e de fundações públicas ou autoridades de hierarquia equivalente;

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 - conjunto de fatores externos 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 fontes e estimar o risco;

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;

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);

APT - acrônimo de Ameaça Avançada Persistente (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 INFORMAÇÃO - esfera de atividade que envolve a criação, transformação e uso da informação, a infraestrutura de TIC envolvida e a informação propriamente dita;

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 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;

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 das documentações. Para assinar digitalmente um documento é necessário possuir um certificado digital. Entre as principais vantagens do uso de assinatura digital estão o não repúdio (não deixa dúvidas quanto ao seu remetente) e tempestividade (a AC pode verificar data e hora da assinatura de um documento);

ASSINATURA ELETRÔNICA - nome dados 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;

ATIVO - qualquer coisa que tenha valor para a organização;

ATIVO DE REDE - equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores;

ATIVOS DE INFORMAÇÃO - os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;

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) - 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 a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

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

BaaS - acrônimo de Backend as a Service;

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. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

BANCO DE DADOS - coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados 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;

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 entidades exceto àquelas incluídas na blacklist;

BLOCKCHAIN - base de dados que mantem um conjunto de registro 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 bando 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 deworms, 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 doworm, 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.

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 - programa que, além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário;

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;

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;

CÓDIGO DE INDEXAÇÃO - código alfanumérico que indexa documento com informação classificada em qualquer grau de sigilo;

CÓDIGO MALICIOSO - programa, ou parte de um programa de computador, projetado especificamente para atentar contra a segurança de um sistema computacional, normalmente através de exploração de alguma vulnerabilidade de sistema;

COLETA DE EVIDÊNCIAS DE SEGURANÇA EM REDES COMPUTACIONAIS - processo de obtenção de itens físicos que contém 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 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 GESTOR DE SEGURANÇA DA INFORMAÇÃO - Comissão instituída pelo Decreto nº 9.637/2018, com atribuição de assessorar o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) nas atividades relacionadas à segurança da informação;

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 independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou de 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 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 pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;

CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - cumprimento das legislações, normas e procedimentos relacionados à SI da organização;

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;

CONTA DE SERVIÇO - conta de acesso à rede corporativa de computadores necessária 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 APF, 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 uma 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;

CREDENCIAL (OU CONTA 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;

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 APF, subordinado ao Departamento de Segurança da Informação - DSI do Gabinete de Segurança Institucional da Presidência da República - GSI;

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;

CUSTODIANTE - aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante - ou dos ativos de informação que compõem o sistema de informação - que não lhe pertence, mas que está sob sua custódia;

CUSTODIANTE DA INFORMAÇÃO - qualquer indivíduo ou estrutura de órgão ou entidade da APF, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de SI comunicadas pelo proprietário da informação;

D

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 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;

DDoS - acrônimo de Negação de Serviço Distribuída (Distributed Denial of Service);

DECIFRAÇÃO - ato de decifrar, mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

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 de informações, documentos, mídias e acervos digitais;

DIREITO DE ACESSO - privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

DISPONIBILIDADE - propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

DISPOSITIVOS MÓVEIS - equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não limitando a estes: notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HD externo, e cartões de memória;

DLT - acrônimo de Livro-Razão Distribuído (Distributed Ledger Techonology);

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 CIBERNÉTICO - domínio de processamento de informações (dados) eletrônicas composto de uma ou mais infraestruturas de TIC;

DoS - acrônimo de Negação de Serviço (Denial of Service).

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;

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. Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255. No caso de IPv6, o endereço IP é dividido em até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF;

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 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;

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 às consequências de um 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;

ETIR - acrônimo de Equipe de Tratamento de Incidentes de Rede;

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 - 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

FIREWALL - recurso destinado a evitar acesso não autorizado a uma determinada rede, ou a um 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.

G

GASTOS-DUPLOS - ato de usar o mesmo dado mais de uma vez em diferentes transações em uma rede blockchain;

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 - 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 MUDANÇAS NOS ASPECTOS RELATIVOS À SI - aplicação de um processo estruturado e de um conjunto de ferramentas de gerenciamento de mudanças, de

modo a aumentar a probabilidade de sucesso e fazer com que as mudanças transcorram com mínimos impactos no âmbito de órgão da APF, visando viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação;

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 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;

GESTOR DE MUDANÇAS - responsável pelo planejamento e implementação do processo de mudanças no âmbito do órgão ou entidade da APF;

GESTOR DE SEGURANÇA DA INFORMAÇÃO - responsável pelas ações de SI no âmbito do órgão ou entidade da APF;

GESTOR DE SEGURANÇA E CREDENCIAMENTO - responsável pela segurança da informação classificada em qualquer grau de sigilo nos Órgãos de Registro e Postos de Controle, devidamente credenciado;

GSI/PR - acrônimo de Gabinete de Segurança Institucional da Presidência da República; GSC - acrônimo de Gestor de Segurança e Credenciamento;

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;

HSM - acrônimo de Módulo de Segurança em Hardware (Hardware Security Module); HSTS - acrônimo de HTTP Strict Transport Security;

HTTP - acrônimo de Hypertext Transfer Protocol;

HTTPS - acrônimo de Hypertext Transfer Protocol Secure;

HYPERTEXT TRANSFER PROTOCOL SECURE (HTTPS) - extensão do HTTP utilizado 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;

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.

I

ICP-Brasil - acrônimo de Infraestrutura de Chaves Públicas Brasileira;

IDENTIDADE DIGITAL - representação unívoca de um indivíduo dentro do espaço cibernético; IDENTIFICAÇÃO DE RISCOS - processo de localizar, listar e caracterizar elementos de risco;

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 DE SEGURANÇA - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

INFORMAÇÃO - dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

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 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;

INFRAESTRUTURA CIBERNÉTICA - sistemas e serviços de informação e comunicações compostos por todo 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 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) - 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 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);

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;

INTERFACE DE PROGRAMAÇÃO DE APLICAÇÕES - 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 - rede global composta pela interligação de inúmeras redes. Conecta mais de 500 milhões de usuários, provendo comunicação e informações das mais variadas áreas de conhecimento;

INTERNET DAS COISAS (IoT) - 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;

INTEROPERABILIDADE - característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente;

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;

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 à pessoas naturais, para o tratamento de informação classificada;

IoT - acrônimo de Internet das Coisas (Internet of Things).

K

KEYLOGGER - tipo específico despyware. 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 (SDK) - 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

LISTA DE CONTROLE DE ACESSO (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 à cada entidade;

LIVRO RAZÃO DISTRIBUÍDO (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.

M

MALWARE - software malicioso projetado para infiltrar um sistema computacional com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software 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;

MARCAÇÃO - aposição de marca que indica o grau de sigilo da informação classificada;

MEDIDAS DE SEGURANÇA - medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

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;

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) - 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.

N

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 - 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 - mais conhecido por DDoS, 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;

NÍVEIS DE ACESSO - especificam quanto de cada recurso ou sistema o usuário pode utilizar;

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) - 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;

NSC - acrônimo de Núcleo de Segurança e Credenciamento.

O

OBSOLESCÊNCIA TECNOLÓGICA - ciclo de vida do software ou de equipamento definido pelo fabricante ou causado pelo desenvolvimento de novas tecnologias;

OPERADOR - pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

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;

ÓRGÃOS DE REGISTRO NÍVEL 1 - os Ministérios e os órgãos e entidades públicos de nível equivalente, credenciados pelo Núcleo de Segurança e Credenciamento;

ÓRGÃOS DE REGISTRO NÍVEL 2 - 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;

ORN1 - acrônimo de Órgão de Registro Nível 1;

ORN2 - acrônimo de Órgão de Registro Nível 2.

P

PADRÕES CORPORATIVOS DE SISTEMAS E DE CONTROLE - conjunto de regras e de procedimentos que compõem os normativos internos das corporações;

PC - acrônimo de Posto de Controle;

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;

PIN - acrônimo de Número de Identificação Pessoal (Personal Identification Number);

PKI - acrônimo de Infraestrutura de Chave Pública (Public Key Infrastructure);

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 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 - 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);

POSIC - acrônimo de Política de Segurança da Informação e Comunicações. Foi substituído pelo acrônimo POSIN;

POSIN - acrônimo de Política de Segurança da Informação. Substituiu o acrônimo POSIC;
PoS - acrônimo de Prova de Participação (Proof of Stake);

PoW - acrônimo de Prova de Trabalho (Proof of Work);

POSTO DE CONTROLE - unidade de órgão ou entidade pública ou privada, habilitada, responsável pelo armazenamento de informação classificada em qualquer grau de sigilo;

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 poderão 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;

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 (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 dele 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 (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;

PROTOCOLO - conjunto de parâmetros que definem a forma e como a transferência de informação deve ser efetuada;

PROVA DE PARTICIPAÇÃO – veja Proof of Stake;

PROVA DE TRABALHO – veja Proof of Work;

PROVEDOR DE SERVIÇOS DE NUVEM - ente, público ou privado, prestador de serviço de computação em nuvem;

PSEUDONIMIZÇÃO - 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

QUEBRA DE SEGURANÇA - ação ou omissão, intencional ou acidental, que resulta no comprometimento da SI.

R

RAIZ DE CONFIANÇA – veja Root of Trust;

RECURSO CRIPTOGRÁFICO - sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

REDE DE COMPUTADORES - conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação;

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 PRIVADA VIRTUAL - mais conhecida por VPN, 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;

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;

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);

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 SI) - 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;

ROOT OF TRUST (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 autentico; 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 rootkits não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (rootou Administrator) em um computador, mas, sim, para manter o acesso privilegiado em um computador previamente comprometido;

RoT - acrônimo de Raiz de Confiança (Root of Trust).

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;

SCREENLOGGER - tipo específico despyware. 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;

SDK - acrônimo de Kit de Desenvolvimento de Software (Software Development Kit);

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 CORPORATIVA - veja Segurança Orgânica;

SEGURANÇA DA INFORMAÇÃO - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

SEGURANÇA ORGÂNICA - 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;

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;

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;

SI - Acrônimo de Segurança da Informação;

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;

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 despyware;

SSL - acrônimo de Secure Sockets Layer.

T

TECNOLOGIA DA INFORMAÇÃO - ativo estratégico que apoia 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;

TERMO DE RESPONSABILIDADE - termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

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;

TLS - acrônimo de Transport Layer Security;

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;

TRANFERÊNCIA INTERNACIONAL DE DADOS - transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

TRATADOS INTERNACIONAIS - instrumento internacional concluído por escrito entre Estados e regido pelo Direito Internacional, quer conste de um instrumento único, quer de dois ou mais instrumentos conexos, qualquer que seja sua denominação específica, conforme o art. 2º, da Convenção de Viena do Direito dos Tratados, de 23 de maio de 1969, promulgada pelo Decreto nº 7.030, de 14 de dezembro de 2009;

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 produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou 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 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;

TROJAN - veja Cavalo de Tróia;

TRUSTLESS - o 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);

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, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da APF, formalizada por meio da assinatura de Termo de Responsabilidade;

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.

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-slowa fim de evitar detecção;

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 auto-replicante 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 que se tornar ativo;

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 por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação;

VULNERABILIDADE DE DIA ZERO - 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 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.

Z

ZERO-DAY EXPLOIT - veja Exploração de Dia Zero;

ZERO-DAY VULNERABITLY - veja Vulnerabilidade de Dia Zero;

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