DICIONÁRIO DOS TERMOS TÉCNICOS

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

ABNT ISO GUIA 73:2009 – Gestão de riscos – Vocabulário – Recomendações para uso em normas.

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.

ABNT NBR ISO/IEC 27005:2011 – Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.

Instrução Normativa IN 01/2008 GSI – Disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

Norma Complementar nº 03/IN01/DSIC/GSIPR – Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

SUMÁRIO

1. OBJETIVO

Apresentar termos, expressões, definições e siglas utilizadas na Política de Segurança da Informação e Comunicações - POSIC.

2. DESCRIÇÃO E ESCOPO

Documentar de maneira clara termos, classificações ou expressões, cujo significado possa causar dúvidas ou permitir interpretação adversa do que se pretende. Corresponde ao jargão utilizado pela Política de Segurança da Informação e Comunicações e deve ser observado por todos os usuários para que as regras sejam entendidas.

3. PÚBLICO-ALVO

Este documento destina-se aos servidores e colaboradores, sendo de responsabilidade de cada usuário o cumprimento desta norma.

4. CONCEITOS E DEFINIÇÕES

Para os efeitos da Política de Segurança da Informação e Comunicações, aplicam-se os termos e definições descritos nesse documento.

5. DICIONÁRIO DE TERMOS E VOCABULÁRIOS

5.1 **Aceitação de risco**: decisão de aceitar um risco.

5.2 **Acesso remoto**: ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário.

5.3 **Acesso**: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.

5.4 **Ação corretiva**: ação para eliminar a causa de uma falta de conformidade ou outras situações indesejáveis.

5.5 **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 Administração Pública Federal, direta e indireta.

5.6 **Agente Responsável**: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta, incumbido de chefiar e gerenciar o uso de dispositivos móveis.

5.7 **Ambiente de Desenvolvimento:** Ambiente em que os desenvolvedores utilizam para desenvolver.

5.8 **Ambiente de Homologação:** O ambiente de homologação é o ambiente de teste, o desenvolvedor irá produzir o software no ambiente de desenvolvimento e então irá publica-lo no ambiente de homologação.

5.9 **Ambiente de Produção e Sustentação:** O ambiente de produção é onde os usuários finais acessarão o software.

5.10 **Ameaça**: causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização.

5.11 **Análise de riscos**: uso sistemático de informações para identificar fontes e estimar o risco.

5.12 **Aplicações**: é um programa de computador que tem por objetivo ajudar o seu usuário a desempenhar uma tarefa específica, em geral ligada a processamento de dados.

5.13 **Artefato:** 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 e/ou redes de computadores.

5.14 **Ataque**: evento que pode comprometer a segurança de um sistema ou uma rede. Um ataque pode ter ou não sucesso. Um ataque com sucesso caracteriza uma intrusão. Um ataque também pode ser caracterizado por uma ação que tenha um efeito negativo (p.ex.: *Denial of Service)*.

5.15 **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.

5.16 **Autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

5.17 **Avaliação de Risco**: processo de análise de risco e avaliação de risco.

5.18 **Caixa Corporativa**: caixa postal Corporativa onde são armazenadas as mensagens do Correio Eletrônico do FNDE

5.19 **Caixa Pessoal:** caixa postal Pessoal onde são armazenadas as mensagens do Correio Eletrônico do FNDE

5.20 **Ciclo de vida da informação**: ciclo formado pelas fases da Produção e Recepção; Organização; Uso e Disseminação; e Destinação.

5.21 **Colaborador**: toda pessoa que se vincula ao FNDE, por meio de empresa prestadora de serviço ou por meio de contrato, convênio, acordo, ajuste ou outros instrumentos congêneres, tendo por finalidade a execução de atividades inerentes à Autarquia.

5.22 **Comitê Responsável pela Segurança da Informação e Comunicações**: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF.

5.23 **Comunicação Governamental:** meio de estruturar a comunicação externa e interna da Instituição através de planejamentos, implementações, gerenciamentos e uso de tecnologias.

5.24 **Comunicação de Risco**: troca ou compartilhamento de informações sobre risco entre o tomador de decisão e outras partes interessadas.

5.25 **Comunicação Pública**: A comunicação pública trata dos processos de comunicação realizados pela sociedade civil organizada, Estado, governo e terceiro setor, com foco no interesse público, na formação de uma sociedade cidadã e democrática, em encurtar distâncias sociais reduzindo as diferenças e em ampliar a capacidade analítica individual em prol do coletivo.

5.26 **Confiabilidade**: propriedade de comportamento e resultados consistentes.

5.27 **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

5.28 **Controle**: meios de gestão de riscos, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, gerencial ou legal.

5.29 **Critérios de Risco**: termos de referência pelos quais a significância do risco é avaliada.

5.30 **Custodiante da informação**: refere-se a qualquer indivíduo ou estrutura do órgão ou entidade da APF que tenha a responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de SIC comunicadas pelo proprietário da informação.

5.31 **Declaração de aplicabilidade**: declaração documentada descrevendo os objetivos e controles que são relevantes e aplicáveis ao SGSI do FNDE.

5.32 **Diretriz**: recomendação do que se espera que seja feito para alcançar um objetivo.

5.33 **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

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

5.35 **Eficácia**: medida em que as atividades realizadas são planejadas.

5.36 **Eficiência**: relação entre os resultados obtidos e como os recursos foram utilizados.

5.37 **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR**: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores.

5.38 **Estimativa de Risco**: atividade para atribuir valores à probabilidade e consequências de um risco.

5.39 **Evento**: incidente ou ocorrência, a partir de fontes internas ou externas a uma entidade, capaz de afetar a realização dos seus objetivos.

5.40 **Fragilidades**: É uma coisa fraca ou sensível.

5.41 **Gerenciamento de Incidentes de Segurança da Informação**: processos para detectar, relatar, avaliar, respondendo a lidar e aprender com incidentes de segurança da informação.

5.42 **Gestão de Riscos de Segurança da Informação e Comunicações**: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

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

5.44 **Gestor de Segurança da Informação e Comunicações – GSIC**: é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF.

5.45 **Impacto**: alteração adversa do nível de objetivos de negócio alcançados.

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

5.47 **Informação**: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

5.48 **Informação classificada em grau de sigilo**: 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, a qual é classificada como ultrassecreta, secreta ou reservada.

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

5.50 **Informação sigilosa**: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade ou do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

5.51 **Informação Sensível**: é uma informação ou conhecimento que pode resultar em uma perda de vantagem ou do nível de segurança, caso revelado (divulgada) a outros, que podem ter baixa ou desconhecida confiabilidade ou intenções indetermináveis ou hostis.

5.52 **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

5.53 **Metadados:** conjunto de dados estruturados que descrevem informação primária.

5.54 **Não repúdio**: capacidade de comprovar a ocorrência de um evento ou ação reivindicada e suas titularidades, a fim de resolver disputas sobre a ocorrência ou não ocorrência do evento ou ação e envolvimento de entidades no evento.

5.55 **Parte envolvida** (*stakeholder*): um indivíduo, grupo ou organização que pode afetar, ser afetado, ou perceber-se afetado por um risco.

5.56 **Parte interessada**: pessoa ou grupo que tem um interesse no desempenho ou no sucesso de uma organização.

5.57 **Plano de Continuidade de Negócios – PCN**: 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 num nível previamente definido, em casos de incidentes.

5.58 **Política de Segurança da Informação e Comunicações – POSIC**: documento aprovado pela autoridade responsável do órgão ou entidade da APF, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.

5.59 **Prestador de serviço**: categoria composta por terceirizados contratados para execução de serviços específicos dentro das instalações do FNDE.

5.60 **Prestação de Contas**: responsabilidade de uma entidade por suas ações e decisões.

5.61 **Probe/Scan**: uma ação de varredura na rede em busca de vulnerabilidades que pode ser caracterizada como violação da segurança computacional.

5.62 **Procedimento**: maneira especificada de realizar uma atividade ou um processo.

5.63 **Processo**: conjunto de atividades inter-relacionadas ou interativas que transforma entradas em saídas.

5.64 **Proprietário de Ativos**: os responsáveis pelos ativos mantidos no inventário dos ativos.

5.65 **Proprietário da informação**: refere-se a parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência da informação.

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

5.67 **Recursos de processamento da informação**: qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem.

5.68 **Recursos de TI**: o conjunto de todas as atividades e soluções providas por recursos de computação que visam a produção, o armazenamento, a transmissão, o acesso, a segurança e o uso das informações.

5.69 **Rede Visitante:** A rede visitante é a rede implementada de forma isolada das demais redes corporativas do FNDE.

5.70 **Rede Corporativa:** A rede corporativa é implementada de forma isolada das demais redes do FNDE. Deverão ser adotados mecanismos de autenticação centralizada, controles de acesso e periodicamente realizada análise de vulnerabilidade na infraestrutura que suporta este ambiente mitigando eventuais riscos.

5.71 **Registro**: documento declarando os resultados obtidos ou fornecendo evidências das atividades realizadas.

5.72 **Riscos**: combinação da probabilidade de um evento e sua consequência.

5.73 **Riscos de segurança da informação e comunicações**: 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 do FNDE.

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

5.75 **Segurança da Informação e Comunicações – SIC**: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

5.76 **Segregação de Função**: segregação de função é um método para reduzir o risco de mau uso, acidental ou deliberado dos ativos.

5.77 **Servidor Público** - toda pessoa que se vincula ao FNDE, quer seja por meio de cargo, emprego ou função pública.

5.78 **Sistema de Gerenciamento de Segurança da Informação SGSI**: sistema de gestão com base numa abordagem de risco do negócio, para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar a segurança da informação.

5.79 **Sistema de Gestão**: quadro de políticas, procedimentos, orientações e recursos associados para arquivar os objetivos do FNDE.

5.80 **Sistema da Informação**: é a expressão utilizada para descrever um Sistema seja ele automatizado (que pode ser denominado como Sistema Informacional Computadorizado), seja manual, que abrange pessoas, máquinas e/ou métodos organizados para coletar, processar, transmitir e disseminar dados que representam informação para o usuário e/ou cliente.

5.81 **Sistema Aplicações:** software aplicativo, ou simplesmente aplicativo (português brasileiro) ou aplicação (português europeu), é um programa de computador que tem por objetivo ajudar o seu usuário a desempenhar uma tarefa específica, em geral ligada a processamento de dados.

5.82 **Sistema Operacional:** é um programa ou um conjunto de programas cuja função é gerenciar os recursos do sistema (definir qual programa recebe atenção do processador, gerenciar memória, criar um sistema de arquivos, etc.), fornecendo uma interface entre o computador e o usuário.

5.83 ***Smart Cards:*** possui capacidade de processamento, pois embute um microprocessador e memória (que armazena vários tipos de informação na forma eletrônica), ambos com sofisticados mecanismos de segurança.

5.84 **Tabela de Temporalidade:** Instrumento de destinação, aprovado pela autoridade competente, que determina os prazos em que os documentos devem ser mantidos nos arquivos correntes e intermediários, ou recolhidos aos arquivos permanentes, estabelecendo critérios para microfilmagem e eliminação.

5.85 ***Token*****:** dispositivo físico para autenticação. Exemplos: *token* criptográfico, *token* de senha dinâmica, *token* de memória, entre outros.

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

5.87 **Tratamento da informação**: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

5.88 **Tratamento de Risco**: processo de seleção e implementação de medidas para modificar o risco.

5.89 **Vulnerabilidade**: qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

5.90 **VPN (Rede Privada Virtual)**: é uma rede de comunicações privada construída sobre uma rede de comunicações pública (como por exemplo, a Internet).