Poder Judiciário

Conselho Nacional de Justiça

ANEXO VIII – Glossário

Glossário

Material com definições e conceitos dos termos técnicos utilizados em Segurança Cibernética neste ato

Definição e Conceitos dos Termos Utilizados

A lista de termos com suas respectivas definições constante neste Anexo é aplicável no âmbito dos documentos de Segurança Cibernética produzidos pelo Comitê Gestor de Segurança Cibernética do Poder Judiciário e de quaisquer discussões acerca deles.

1. **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;
2. **Agente responsável pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)**: servidor público do Poder Judiciário incumbido de chefiar e gerenciar a ETIR;
3. **Alta administração**: unidades organizacionais com poderes deliberativos ou normativos no âmbito da organização;
4. **Ameaças**: conjunto de fatores externos ou causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;
5. **Apetite a risco**: nível de risco que a organização está disposta a aceitar para atingir os objetivos identificados no contexto analisado;
6. **Aquisição de evidência**: processo de coleta e cópia das evidências de incidente de segurança em redes computacionais;
7. **Ativo**: qualquer coisa que represente valor para uma instituição, tal como a informação;
8. **Ativos de informação**: meios de armazenamento, transmissão e processamento de informação, sistemas de informação e locais onde se encontram esses meios e as pessoas que a eles têm acesso;
9. **Atividades críticas**: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão, de maneira que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;
10. **Auditoria**: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se 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;

11. **Autenticação**: processo de identificação das partes envolvidas em um processo;
12. **Autenticidade**: propriedade indicativa de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
13. **Autorização**: processo que visa a garantir que as informações são acessíveis exclusivamente àqueles com permissão de acesso;
14. **Classificação da informação**: atribuição, pela autoridade competente, de grau de sigilo dado à informação, ao documento, ao material, à área ou à instalação;
15. **Coleta de evidências de segurança em redes computacionais**: processo de obtenção de itens físicos que contém potencial evidência, mediante a utilização de metodologia e ferramentas adequadas. Esse processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou coleção de dados que contenham evidências do incidente;
16. **Competência**: habilidade para aplicar conhecimentos e habilidades para atingir resultados pretendidos;
17. **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizada;
18. **Conformidade**: preenchimento de um requisito;
19. **Continuidade de serviços**: capacidade estratégica e tática do órgão de se planejar e de 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 nível aceitável, previamente definido;
20. **Crise**: um evento ou série de eventos danosos que apresenta propriedades emergentes capazes de exceder as habilidades de uma organização em lidar com as demandas de tarefas que eles geram; e que apresenta implicações que afetam proporção considerável da organização e de seus constituintes;

21. **Crise cibernética**: crise que ocorre em decorrência de incidente em dispositivos, serviços e redes de computadores. É decorrente de incidentes que causam dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;
22. **Controle**: providência que modifica o risco, incluindo qualquer processo, política, dispositivo, prática ou ação;
23. **Dado pessoal**: informação relacionada à pessoa natural identificada ou identificável;
24. **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
25. **Escopo de auditoria**: extensão e fronteiras de uma auditoria;
26. **Endereço IP (*Internet Protocol*)**: refere-se ao conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores;
27. **ETIR**: Equipe de Tratamento e Resposta a Incidentes de Segurança de Cibernética. Denominação tradicionalmente atribuída a grupos de resposta a incidentes de segurança da informação, embora os incidentes não mais se limitem a tecnologia;
28. **Estratégia de continuidade de serviços**: abordagem do órgão que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou com outro incidente maior;
29. **Evento**: qualquer ocorrência observável em um sistema ou rede de uma organização;
30. **Evidência digital**: informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento;
31. **Evidência de auditoria**: registros, declarações de fato ou outras informações verificáveis e relevantes para os critérios de auditoria;
32. **Gerenciamento de crise**: decisões e atividades coordenadas que ocorrem em uma organização durante uma crise corporativa, incluindo crises cibernéticas;

33. **Gestão de continuidade de serviços**: processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, concretizando-se, poderiam causar, fornecendo e mantendo nível aceitável de serviço diante de rupturas e desafios à operação normal do dia a dia;
34. **Gestão de Riscos de Segurança da Informação**: 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 para equilibrá-los com os custos operacionais e financeiros envolvidos;
35. **Gestão 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;
36. **Gestor da informação**: pessoa responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades;
37. **Gestor de Segurança da Informação e das Comunicações**: responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da administração pública federal (APF);
38. **Impacto do risco**: efeito resultante da ocorrência do risco;
39. **Informação**: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
40. **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;

41. **Incidente de segurança**: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
42. **Incidente grave**: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período inferior ao tempo objetivo de recuperação;
43. **Incidente de Segurança da Informação**: evento que viola ou representa ameaça iminente de violação de política de segurança, de política de uso aceitável ou de prática de segurança padrão;
44. **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
45. ***Log* ou registro de auditoria**: registro de eventos relevantes em um dispositivo ou sistema computacional;
46. **Metadados**: conjunto de dados estruturados que descrevem informação primária;
47. **Nível de risco**: magnitude do risco, expressa pelo produto das variáveis impacto e probabilidade;
48. **Plano de Gerenciamento de Incidentes**: plano de ação claramente definido e documentado para ser usado quando ocorrer incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;
49. **Política de Segurança da Informação e das Comunicações (POSIC)**: documento aprovado pela autoridade responsável pelo órgão ou entidade da administração pública federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;
50. **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;
51. **Probabilidade do risco**: possibilidade de ocorrência do risco;

52. **Procedimento**: conjunto de ações sequenciadas e ordenadas para o atingimento de um determinado fim;
53. **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
54. **Requisito**: necessidade ou expectativa declarada, geralmente implícita ou obrigatória;
55. **Resiliência**: poder de recuperação ou capacidade de determinada organização resistir aos efeitos de um incidente;
56. **Recursos computacionais**: recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, computadores, *notebooks*, servidores de rede, equipamentos de conectividade e infraestrutura;
57. **Resumo criptográfico**: é um método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho desta, gera resultado único e de tamanho fixo, também chamado de *hash*;
58. **Risco de Tecnologia da Informação e Comunicação (TIC)**: evento capaz de afetar positiva ou negativamente os objetivos da organização nos níveis estratégico, tático e operacional;
59. **Segurança da Informação e Comunicações**: ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações;
60. **Sistema de gestão de segurança da informação (SGSI)**: políticas, procedimentos, manuais e recursos associados e atividades coletivamente gerenciadas por uma organização na busca de proteger seus ativos de informação;
61. **Tolerância a risco**: margem que a administração permite aos gestores de suportar o impacto de determinado risco em troca de benefícios específicos, ainda que esse seja superior ao "apetite ao risco" determinado pela organização;
62. **Tratamento da informação classificada**: conjunto de ações referentes à produção, à recepção, à classificação, à utilização, ao acesso, à reprodução, ao

transporte, à transmissão, à distribuição, ao arquivamento, ao armazenamento, à eliminação, à avaliação, à destinação ou ao controle de informação classificada em qualquer grau de sigilo; e

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