MINISTÉRIO DA CULTURA

DICIONÁRIO DE REFERÊNCIA

ORIGEM

Ministério da Cultura – MinC.

REFERÊNCIAS LEGAIS E NORMATIVAS

Portaria nº 327/2014/MinC - Aprova, no âmbito do Ministério da Cultura, norma de Segurança que estabelece as Diretrizes de Segurança da Informação e Comunicações.

Portaria nº 119/2011/MinC - Institui a Política de Segurança da Informação e Comunicações do Ministério da Cultura e o Sistema de Segurança da Informação e Comunicações e dá outras providências.

Portaria nº 40/2013/MinC – Aprova o Regimento Interno do Ministério da Cultura.

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

ABNT NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação.

ABNT NBR ISO/IEC 27002:2007 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação.

Decreto nº 7.724, de 16 de maio de 2012 – Regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

Decreto nº 7.845, de 14 de novembro de 2012 – Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Instrução Normativa IN 01/2008 GSI – Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal – APF direta e indireta, e dá outras providências.

Instrução Normativa IN 02/2013 GSI – Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.

Instrução Normativa IN 03/2013 GSI – Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.

Instrução Normativa MP/SLTI nº 04 – Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal.

Lei nº 12.527, de 18 de novembro de 2011 – Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990.

Norma Complementar nº 01/IN02/DSIC/GSIPR – Disciplina o credenciamento de segurança de pessoas naturais, órgãos e entidades públicas e privadas para o tratamento de informações classificadas.

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

Norma Complementar nº 04/IN01/DSIC/GSIPR – Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos e entidades da APF.

Norma Complementar nº 05/IN01/DSIC/GSIPR – Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da APF.

Norma Complementar nº 06/IN01/DSIC/GSIPR – Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da APF, direta e indireta.

Norma Complementar nº 07/IN01/DSIC/GSIPR – Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da APF, direta e indireta.

Norma Complementar nº 09/IN01/DSIC/GSIPR – Estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da APF, direta e indireta.

Norma Complementar nº 10/IN01/DSIC/GSIPR – Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da APF, direta e indireta.

Norma Complementar nº 11/IN01/DSIC/GSIPR – Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da APF, direta e indireta.

Norma Complementar nº 12/IN01/DSIC/GSIPR – Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da APF, direta e indireta.

Norma Complementar nº 13/IN01/DSIC/GSIPR – Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da APF, direta e indireta.

Norma Complementar nº 14/IN01/DSIC/GSIPR – Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da APF, direta e indireta.

Norma Complementar nº 15/IN01/DSIC/GSIPR – Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da APF, direta e indireta.

Norma Complementar nº 16/IN01/DSIC/GSIPR – Estabelece diretrizes para desenvolvimento e obtenção de software seguro nos órgãos e entidades da APF.

Norma Complementar nº 18/IN01/DSIC/GSIPR – Estabelece diretrizes para as atividades de ensino em segurança da informação e comunicações nos órgãos e entidades da APF.

CAMPO DE APLICAÇÃO

Este documento se aplica no âmbito do Ministério da Cultura – MinC.

SUMÁRIO

1. OBJETIVO

1.1 Definir, no âmbito do MinC, o conjunto dos termos técnicos utilizados na Política de Segurança da Informação e Comunicações, bem como em suas respectivas normas e documentos complementares.

2. ESCOPO

2.1 Documentar de maneira clara quaisquer termos, classificações ou expressões, cujos significados possam causar dúvidas ou permitir interpretação adversa do que se pretende. Este Dicionário de Referência corresponde ao significado dos termos utilizados pela Política de Segurança da Informação e Comunicações.

3. PÚBLICO-ALVO

3.1 Esta norma destina-se aos servidores e colaboradores do Ministério da Cultura, sendo responsabilidade de cada um o seu cumprimento.

4. PRINCÍPIOS

4.1 A Política de Segurança da Informação e Comunicações está fundamentada nos princípios da disponibilidade, integridade, confidencialidade e autenticidade, visando à proteção e à preservação das informações necessárias às atividades da instituição.

5. TERMOS E EXPRESSÕES

5.1 **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 (Ref. NC 07/IN01/DSIC/GSIPR).

5.2 **Administradores de recursos de tecnologia da informação** – servidores e colaboradores que exercem função de administração dos recursos de tecnologia da informação da rede corporativa do MinC.

5.3 **ADSL (*Asymmetrical Digital Subscriber Line*)** – tecnologia que utiliza linha telefônica digital para tráfego de dados.

5.4 **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 (Ref. NC 18/IN01/DSIC/GSIPR).

5.5 **Agente público com dispositivos móveis corporativos** – servidores ou empregados da Administração Pública Federal (APF) que utilizam dispositivos móveis de computação de propriedade dos órgãos ou entidade a que pertencem (Ref. NC 12/IN01/DSIC/GSIPR).

5.6 **Agente público com dispositivos móveis particulares** – servidores ou empregados da Administração Pública Federal (APF) que utilizam dispositivos móveis de computação de sua propriedade. Para fins desta Norma Complementar, os dispositivos particulares que se submetem aos padrões corporativos de software e controles de segurança, e que são incorporados à rede de dados do órgão, são considerados como dispositivos corporativos (Ref. NC 12/IN01/DSIC/GSIPR).

5.7 **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: 1. Possuir credencial de segurança (Ref. IN03/DSIC/GSIPR); 2. Chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (Ref. NC 05/IN01/DSIC/GSIPR); 3. Chefiar e gerenciar o processo de Inventário e Mapeamento de Ativos de Informação (Ref. NC 10/IN01/DSIC/GSIPR); 4. Chefiar e gerenciar o uso de dispositivos móveis (Ref. NC 12/IN01/DSIC/GSIPR); 5. Implementar procedimentos relativos ao uso seguro de tecnologias de computação em nuvem (Ref. NC 14/IN01/DSIC/GSIPR); 6. Gestão do uso seguro das redes sociais (Ref. NC 15/IN01/DSIC/GSIPR); 7. Dentre outras atividades correlatas de gestão.

5.8 **Algoritmo de Estado** – função matemática utilizada na cifração e na decifração, desenvolvida pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, não comercializável (Ref. NC 09/IN01/DSIC/GSIPR).

5.9 **Ameaça** – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou instituição (Ref. NC 04/IN01/DSIC/GSIPR).

5.10 **Análise de Impacto nos Negócios (AIN)** – visa a 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 quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, suas prioridades de recuperação, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos (Ref. NC 06/IN01/DSIC/GSIPR).

5.11 **Análise de riscos** – uso sistemático de informações para identificar fontes e estimar o risco (Ref. NC 04/IN01/DSIC/GSIPR).

5.12 **Análise/avaliação de riscos** – processo completo de análise e avaliação de riscos (Ref. NC 04/IN01/DSIC/GSIPR).

5.13 **Antivírus** – são softwares projetados para detectar e eliminar tipos de Malware do computador, como vírus, *worms*, Cavalo de Tróia.

5.14 **APF** - Administração Pública Federal.

5.15 **Artefato malicioso** – qualquer arquivo no 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 (Ref. NC 05/IN01/DSIC/GSIPR).

5.16 **Atividade** – processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços (Ref. NC 06/IN01/DSIC/GSIPR).

5.17 **Atividades críticas** – 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 (Ref. NC 06/IN01/DSIC/GSIPR).

5.18 **Ativos de informação** – equipamentos, sistema de informação, meios de armazenamento, transmissão e processamento da informação. Enquadram-se como ativos os recursos humanos que possuem acesso a estes (Ref. NC 10/IN01/DSIC/GSIPR).

5.19 **Auditoria** – atividade com a finalidade de reconstruir um evento relacionado à segurança para auxiliar no exame de suas causas e seus efeitos.

5.20 **Autenticar** – processo que busca verificar a identidade de uma pessoa no momento em que é requisitado um acesso a determinado ambiente ou recurso computacional.

5.21 **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 (Ref. IN01/DSIC/GSIPR).

5.22 **Avaliação de Conformidade em Segurança da Informação e Comunicações** – exame sistemático do grau de atendimento dos requisitos relativos à SIC com as legislações específicas (Ref. NC 11/IN01/DSIC/GSIPR).

5.23 **Avaliação de riscos** – processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco (Ref. NC 04/IN01/DSIC/GSIPR).

5.24 **Bloqueio de acesso** – processo que tem por finalidade suspender temporariamente o acesso (Ref. 07/IN01/DSIC/GSIPR).

5.25 ***Bridge* ou ponte** – termo utilizado em informática para designar um equipamento que liga duas redes locais.

5.26 **Browser** – software utilizado para navegação na Internet, instalado nas estações de trabalho e notebooks do MinC. Exemplos – Internet Explorer, Mozila Firefox.

5.27 **Caixa postal** – local onde são armazenadas as mensagens do correio eletrônico institucional de cada usuário do MinC.

5.28 **Caixa postal institucional** – local onde são armazenadas as informações de cada correio eletrônico por seções ou segmentos administrativos sejam eles Serviço, Divisão, Coordenação, Diretoria, Secretaria, ou mesmo um Programa ou Projeto.

5.29 **Caixa postal funcional** – local onde são armazenadas as informações de cada correio eletrônico funcional do servidor, colaborador ou estagiário, utilizadas no exercício de suas atividades na instituição.

5.30 **Caracteres especiais** – são caracteres não pertencentes ao conjunto de letras do alfabeto (de A a Z) e de números (de 0 a 9) que existem no teclado de um computador.

5.31 **Catálogo de Serviços** – documento que oferece uma descrição detalhada dos serviços operacionais, na linguagem do cliente, juntamente com os níveis de serviço associados que a área responsável pela administração dos recursos de tecnologia da informação pode fornecer para seus clientes.

5.32 **Cavalo de Tróia** – arquivo de computador normalmente recebido como um "presente" (por exemplo, vídeos, fotos, jogos, etc.), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário, podendo causar danos e comportamentos inesperados no sistema e comprometer a segurança do mesmo.

5.33 **Chave criptográfica** – valor que trabalha com um algoritmo criptográfico para cifração e/ou decifração (Ref. IN03/DSIC/GSIPR).

5.34 **Chefia imediato ou superior** – agente público que exerce função de chefia, coordenação, gerência ou direção dentro da instituição.

5.35 **Ciclo de vida da informação** – processo que envolve todas as fases da vida da informação, desde a criação, manuseio, armazenamento, transporte e descarte, considerando a sua confidencialidade, integridade, disponibilidade e autenticidade.

5.36 **Cifração** – ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais capazes de ser interpretados por outros ininteligíveis por pessoas não autorizadas a conhecê-la (Ref. IN03/DSIC/GSIPR).

5.37 **Classificação da informação** – atribuição de grau de segurança a dado, informação, documento ou matéria, pela Autoridade Classificadora ou por autoridade designada para este fim mediante provocação oficial. (Ref. Decreto 7.724, de 16 de maio de 2012).

5.38 **Código malicioso** – parte do código fonte do *Malware*. É a partir do código fonte que o usuário mal-intencionado irá designar as funções maliciosas, sejam elas, infectar outros arquivos, roubar dados, danificar o sistema ou qualquer que seja a intenção do *cyber* criminoso.

5.39 **Código móvel** – programa que tem sua fonte em um sistema remoto, possivelmente "não confiável", porém executado em um sistema local.

5.40 **Colaboradores** – prestadores de serviços, terceirizados, consultores e estagiários que executam alguma atividade profissional na instituição.

5.41 **Comitê de Segurança da Informação e Comunicações – CSIC** – 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 (Ref. NC 03/IN01/DSIC/GSIPR).

5.42 **Computação em nuvem** – modelo computacional que permite acesso por demanda, e independente 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 interação com o provedor de serviços (Ref. NC 14/IN01/DSIC/GSIPR).

5.43 **Comunicação do risco** – troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas (Ref. NC 04/IN01/DSIC/GSIPR).

5.44 **Comunidade ou Público Alvo** – conjunto de pessoas, setores, órgãos ou entidades atendidas por uma norma específica ou por Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (Ref. NC 05/IN01/DSIC/GSIPR).

5.45 **Conexão *stateful inspection*** – funcionalidade do firewall que possibilita o controle de suas conexões pré-estabelecidas sem a necessidade de criações de regras adicionais.

5.46 **Confidencialidade** – propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado (Ref. IN01/DISC/GSIPR).

5.47 **Conformidade em Segurança da Informação e Comunicações** – cumprimento das legislações, normas e procedimentos relacionados à Segurança da Informação e Comunicações da instituição (Ref. NC 11/IN01/DSIC/GSIPR).

5.48 **Console** – centro de controle que permite que um operador se comunique e gerencie um sistema de computador.

5.49 **Conta de acesso** – conjunto do "nome de usuário" e "senha".

5.50 **Contas de Serviço** – contas de acesso à rede corporativa de computadores necessárias a um procedimento automático (aplicação, script, etc.) sem qualquer intervenção humana no seu uso (Ref. NC 07/IN01/DSIC/GSIPR).

5.51 **Contêineres dos Ativos de Informação** – o contêiner é o local onde "vive" o ativo de informação, onde está armazenado, como é transportado ou processado (Ref. NC 10/IN01/DSIC/GSIPR).

5.52 **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 (Ref. NC 06/IN01/DSIC/GSIPR).

5.53 **Controle de acesso** – conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso (Ref. NC 07/IN01/DSIC/GSIPR).

5.54 **Controles de Segurança** – medidas adotadas para evitar ou diminuir o risco de um ataque. São exemplos de controles de segurança: a criptografia, a validação de entrada, o balanceamento de carga, as trilhas de auditoria, o controle de acesso, a expiração de sessão, os *backups*, etc. (Ref. NC 16/IN01/DSIC/GSIPR).

5.55 **Cópia de Segurança (*Backup*)** – uma cópia exata de um documento eletrônico, programa de computador ou disco, feito para fins de arquivamento ou para salvaguardar arquivos, na eventualidade de danificação ou destruição do original.

5.56 **Correio eletrônico** - serviço básico de troca de mensagens utilizando protocolos de rede Intranet e Internet.

5.57 **Correio eletrônico institucional** – serviço custeado pelo MinC e disponibilizado com nome de áreas, cargos, processos ou serviços, como ferramenta de trabalho, para o envio e recebimento de mensagens eletrônicas, que serão acessadas por um ou mais usuário(s) designado(s).

5.58 **Correio eletrônico funcional** – serviço custeado pelo MinC e disponibilizado ao usuário, com seu nome, como ferramenta de trabalho, para envio e recebimento de mensagens eletrônicas de interesse dos negócios do Ministério da Cultura.

5.59 **Correio eletrônico particular** – serviço contratado pelo usuário, em seu nome, sem interveniência do MinC, podendo ser pago ou gratuito, para envio e recebimento de mensagens eletrônicas.

5.60 **Credenciais ou contas de acesso** – permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou instituição ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha ou biométrica como impressão digital (Ref. NC 07/IN01/DSIC/GSIPR).

5.61 **Credenciamento** – processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso relacionado às suas atividades funcionais (Ref. NC 07/IN01/DSIC/GSIPR).

5.62 **Criptografia** – conjunto de princípios e técnicas empregadas para cifrar a informação, torná-la ininteligível para os que não tenham acesso às convenções combinadas. A criptografia tem o objetivo de proporcionar o sigilo da informação. Em conjunto com outras técnicas, proporcionam a integridade e autenticidade.

5.63 **Criticidade** – grau de importância da informação para a continuidade dos negócios do Ministério da Cultura (disponibilidade e integridade).

5.64 **CSIC** – Comitê de Segurança da Informação e Comunicações. Ver 5.41.

5.65 **CTIR GOV** – Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI (Ref. NC 05/IN01/DSIC/GSIPR).

5.66 **Custodiante** – colaborador ou área responsável pela guarda ou transporte de informações e pela manutenção das medidas de proteção estabelecidas na Política de Segurança da Informação e Comunicações, observada a legislação vigente.

5.67 **Custodiante do ativo de informação** – refere-se a qualquer indivíduo ou estrutura do órgão ou entidade da APF que tenha a responsabilidade formal de proteger um ou mais ativos de informação, como é armazenado, transportado e processado, ou seja, é o responsável pelos contêineres dos ativos de informação. Consequentemente, o custodiante do ativo de informação é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações comunicadas pelos proprietários dos ativos de informação (Ref. NC 10/IN01/DSIC/GSIPR).

5.68 **Decifração** – ato de decifrar, traduzir um texto cifrado, mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original (Ref. Decreto 7.845).

5.69 **Desastre** – evento repentino e não planejado que causa perda para toda ou parte da instituição gerando assim sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação (Ref. NC 06/IN01/DSIC/GSIPR).

5.70 **Diretriz** – descrição que estabelece orientação de como e o que deve ser feito para se alcançar os objetivos estabelecidos nas políticas.

5.71 **Disponibilidade** – propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade (Ref. IN01/DSIC/GSIPR).

5.72 **Dispositivos móveis** – consiste em equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: *notebooks*, *netbooks*, *smartphones*, *tablets*, *pendrives*, USB *drives*, HDs externos e cartões de memória (Ref. NC 12/IN01/DSIC/GSIPR).

5.73 **Documento Classificado** – documento que contenha informação classificada em qualquer grau de sigilo (Ref. IN02/DSIC/GSIPR).

5.74 ***Download*** – descarregamento, transferência de arquivos entre computadores por meio de uma rede.

5.75 ***Drive* Virtual** - Espécie de dispositivo que não está fisicamente presente no computador, mas que é interpretado pelo sistema operacional como um componente físico.

5.76 **DSIC** – Departamento de Segurança da Informação e Comunicações – subordinado ao GSI.

5.77 **E-mail$_1$** - Sistema de correio eletrônico para envio e recebimento de mensagens eletrônicas.

5.78 **E-mail$_2$ -** Mensagem enviada por meio de correio eletrônico.

5.79 **Endereço eletrônico –** Endereço ou codificação para o qual se destina o e-mail. Sinônimo de e-mail.

5.80 **Equipamentos de interconexão** – equipamentos que possibilitam a interligação de dois ou mais recursos computacionais, tais como servidores de rede e estações de trabalho.

5.81 **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 (Ref. NC 03/IN01/DSIC/GSIPR).

5.82 **Estimativa de riscos** – processo utilizado para atribuir valores à probabilidade e consequências de um risco (Ref. NC 04/IN01/DSIC/GSIPR).

5.83 **Estratégia de Continuidade de Negócios** – abordagem de um órgão ou entidade que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior (Ref. NC 06/IN01/DSIC/GSIPR).

5.84 **ETIR** – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais. Ver 5.81.

5.85 **Evento** – ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente conhecida que possa ser relevante para a segurança da informação.

5.86 **Evitar 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 (Ref. NC 04/IN01/DSIC/GSIPR).

5.87 **Exclusão de acesso** – processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e do perfil de acesso (Ref. NC 07/IN01/DSIC/GSIPR).

5.88 **Formato digital** – qualquer informação disponível em um formato codificado digitalmente inteligível pelo homem e criado, processado, armazenado e disponibilizado por meios eletrônicos.

5.89 **GCN** – Gestão de Continuidade de Negócios.

5.90 **Gestão de Continuidade** – processo abrangente de gestão que identifica ameaças potenciais para uma instituição e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este 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 e a marca da instituição, e suas atividades de valor agregado (Ref. NC 06/IN01/DSIC/GSIPR).

5.91 **Gestão de mudanças nos aspectos relativos à SIC** – é o processo de gerenciamento de mudanças, de modo que ela transcorra com mínimos impactos no âmbito do órgão ou entidade da APF, visando viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação (Ref. NC 13/IN01/DSIC/GSIPR).

5.92 **Gestão de Riscos de Segurança da Informação e Comunicações** – **GRSIC** – 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 (Ref. NC 04/IN01/DSIC/GSIPR).

5.93 **Gestão de Segurança da Informação e Comunicações** – **GSIC -** 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 (Ref. IN01/DSIC/GSIPR).

5.94 **Gestor de Mudanças** – responsável pelo processo de mudanças no âmbito do órgão ou entidade da APF (Ref. NC 13/IN01/DSIC/GSIPR).

5.95 **Gestor de Segurança da Informação e Comunicações** – responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF (Ref. NC 03/IN01/DSIC/GSIPR).

5.96 **Grau de sigilo** – gradação de segurança atribuída a dados e informações em decorrência de sua natureza ou conteúdo.

5.97 **GRSIC** – Gestão de Riscos de Segurança da Informação e Comunicações. Ver 5.92.

5.98 **GSIC –** Gestão de Segurança da Informação e Comunicações. Ver 5.93.

5.99 **GSIPR** – Gabinete de Segurança Institucional da Presidência da República.

5.100 ***Hardware*** – parte física do computador, ou seja, conjunto de componentes eletrônicos, circuitos integrados e placas que formam o computador.

5.101 **Identificação de riscos** – processo para localizar, listar e caracterizar elementos do risco (Ref. NC 04/IN01/DSIC/GSIPR).

5.102 **Identificação e Classificação de Ativos de Informação** – processo composto por 6 (seis) etapas: (a) coletar informações gerais; (b) definir as informações dos ativos; (c) identificar o(s) responsável(is); (d) identificar os contêineres dos ativos; (e) definir os requisitos de segurança; e (f) estabelecer o valor do ativo de informação (Ref. NC 10/IN01/DSIC/GSIPR).

5.103 **Incidente** – 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 de tempo inferior ao tempo objetivo de recuperação (Ref. NC 06/IN01/DSIC/GSIPR).

5.104 **Incidente de segurança** – é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos ativos de informação, por exemplo, em sistemas de computação e em redes de computadores (Ref. NC 05/IN01/DSIC/GSIPR).

5.105 **Informação** – dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato (Ref. Lei 12.527).

5.106 **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, a qual é classificada como ultrassecreta, secreta ou reservada (Ref. IN02/DSIC/GSIPR).

5.107 **Informação Pessoal** – informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem (Ref. Decreto 7.724).

5.108 **Informação Sigilosa** – informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo (Ref. Decreto 7.724).

5.109 **Infraestrutura** – áreas que suportam as atividades relacionadas com banco de dados, redes, telecomunicações e desenvolvimento de sistemas do MinC.

5.110 **Infraestrutura Crítica da Informação** – são os meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso, que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (Ref. NC 10/IN01/DSIC/GSIPR).

5.111 **Integridade** – propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental (Ref. IN01/DSCI/GSIPR).

5.112 **Internet** – sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes. (Ref. Lei nº 12.965, de 23 de Abril de 2014).

5.113 **Intranet** – Rede de computadores privada que utiliza a mesma tecnologia da Internet, porém, de uso interno do Ministério da Cultura, que só pode ser acessada por seus usuários ou colaboradores internos.

5.114 **Inventário e Mapeamento de Ativos de Informação** – é um processo interativo e evolutivo, composto por 3 (três) etapas: (a) identificação e classificação de ativos de informação, (b) identificação de potenciais ameaças e vulnerabilidades e (c) avaliação de riscos (Ref. NC 10/IN01/DSIC/GSIPR).

5.115 **ITIL (*Information Technology Infrastructure Library*)** – biblioteca do conjunto das melhores práticas desenvolvidas para o fornecimento de serviço de TI (Tecnologia da Informação).

5.116 ***Link*** – ligação que serve como referência em um documento em hipertexto a outro documento ou a outro recurso. O seu significado é "atalho", "caminho" ou "ligação".

5.117 ***Login (logon)*** – procedimento de identificação e autenticação do usuário no recurso computacional. É pessoal e intransferível.

5.118 ***Malware*** - termo criado para definir qualquer tipo de software que tenha intenção de realizar alguma atividade no computador sem o consentimento do proprietário. Vírus, *Worm*, *Trojan horse* (Cavalo de Tróia), *Backdoor* são exemplos de malware.

5.119 **Meio de comunicação** – nome dado à infraestrutura física e/ou lógica ao qual permite a troca de informações eletrônicas ou utilização de algum serviço.

5.120 **Mitigar risco** – forma de tratamento de risco na qual se decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco (Ref. NC 04/IN01/DSIC/GSIPR).

5.121 **Modelo de Implementação (computação em Nuvem)** – modelos de implementação da computação em nuvem em geral: Nuvem Própria, Nuvem Comunitária, Nuvem Pública e Nuvem Híbrida (Ref. NC 14/IN01/DSIC/GSIPR).

5.122 **Modelo de Serviço (computação em Nuvem)** – modelos de serviço da computação em nuvem, em geral: Software em Nuvem como um Serviço (Software as a Service - SaaS); Plataforma em Nuvem como um Serviço (Plataform as a Service - PaaS); e Infraestrutura em Nuvem como um Serviço (Infrastructure as a Service - IaaS) (Ref. NC 14/IN01/DSIC/GSIPR).

5.123 **Modem** – dispositivo eletrônico utilizado para conexão à Internet ou a outro computador.

5.124 **Mudança** – transição ou alteração de uma situação atual (Ref. NC 13/IN01/DSIC/GSIPR).

5.125 **Necessidade de conhecer** – condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade (Ref. IN02/DSIC/GSIPR).

5.126 **Nome de usuário** – identidade do usuário utilizada na Rede Local ou nos recursos computacionais.

5.127 **OLA (*Operational Level Agreement*)** – acordo de nível operacional entre as áreas internas a Infraestrutura de TI, que detalhe o serviço ou os serviços a serem fornecidos entre elas.

5.128 **Padrões Corporativos de sistemas e de controle** – conjunto de regras e procedimentos que compõem os normativos internos das corporações (Ref. NC 12/IN01/DSIC/GSIPR).

5.129 **Parte interessada** – pessoa ou instituição que pode afetar, ser afetada, ou perceber–se afetada por uma decisão ou atividade.

5.130 **PCN** – Plano de Continuidade de Negócios.

5.131 **PDCA** - método iterativo de gestão de quatro passos (do inglês *Plan*, *Do*, *Check*, *Act* – Planejar, Executar, Verificar e Ajustar), utilizado para o controle e melhoria contínua de processos e produtos. Também conhecido como ciclo de *Deming* ou ciclo de *Shewhart*.

5.132 **PDSIC** – Plano Diretor de Segurança da Informação e Comunicações.

5.133 **Perfil de acesso** – conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso (Ref. NC 07/IN01/DSIC/GSIPR).

5.134 **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 (Ref. NC 06/IN01/DSIC/GSIPR).

5.135 **Plano de Gerenciamento de Incidentes** – plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes (Ref. NC 06/IN01/DSIC/GSIPR).

5.136 **Política de Prevenção de Perda de Dados** – oriundo do termo em inglês DLP (*Data Loss Prevention)*, estabelece o processo de monitorar e evitar que dados sensíveis deixem os servidores ou a rede do MinC.

5.137 **Plano de Recuperação de Negócios** – documentação dos procedimentos e informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas a normalidade (Ref. NC 06/IN01/DSIC/GSIPR).

5.138 **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 (Ref. IN01/DSIC/GSIPR).

5.139 **POSIC** – Política de Segurança da Informação e Comunicações.

5.140 **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 (Ref. NC 07/IN01/DSIC/GSIPR).

5.141 **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 análises críticas, testes, treinamentos e manutenção (Ref. NC 06/IN01/DSIC/GSIPR).

5.142 **Proprietário do ativo de informação** – refere-se à 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 dos ativos de informação (Ref. NC 10/IN01/DSIC/GSIPR).

5.143 **Proxy** – serviço que possibilita o compartilhamento do acesso à Internet entre vários usuários na rede local.

5.144 **Quebra de segurança** – ação ou omissão, intencional ou acidental, que resulte no comprometimento ou no risco de comprometimento de informação classificada (Ref. IN02/DSIC/GSIPR).

5.145 **RAID (*Redundant Array of Independent Disks*)** – conjunto redundante de discos Independentes é um meio de se criar uma unidade virtual composta por vários discos físicos individuais, com a finalidade de ganhar segurança e desempenho.

5.146 **Rastreabilidade** – capacidade de traçar o histórico ou a localização de um item em aplicações, processos, sistemas ou serviços, por meio de informações previamente registradas.

5.147 **Recurso Criptográfico** – sistemas, programas, processos e equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar a cifração ou decifração (Ref. Decreto 7.845).

5.148 **Recurso de processamento da informação** – qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem.

5.149 **Recurso de tecnologia da informação** – recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura.

5.150 **Rede Local** – conjunto de equipamentos interligados localmente com o objetivo de disponibilizar serviços aos usuários do MinC.

5.151 **Regimento Interno** – documento que estabelece a indicação da categoria e finalidade dos órgãos do Ministério Cultura, bem como detalha sua estrutura em unidades organizacionais, especificando as respectivas competências, e definindo as atribuições de seus dirigentes.

5.152 **Registro de Auditoria (*log*)** – arquivo eletrônico com a finalidade de registrar eventos, podendo ser gerado por sistemas operacionais, aplicações, entre outros, e armazenado durante um período pré-determinado.

5.153 **Resiliência** – poder de recuperação ou capacidade de uma instituição resistir aos efeitos de um desastre (Ref. NC 06/IN01/DSIC/GSIPR).

5.154 **Reter risco** – forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado (Ref. NC 04/IN01/DSIC/GSIPR).

5.155 **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 da instituição (Ref. NC 04/IN01/DSIC/GSIPR).

5.156 **Roteador** – equipamento responsável pela troca de informações entre redes.

5.157 **Segregação de função** – método no qual são estabelecidas precauções para impedir que um único usuário possa acessar, modificar, usar informações ou recursos de processamento de informação sem a devida autorização ou detecção.

5.158 **Segurança da Informação e Comunicações – SIC** – ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (Ref. IN01/DSIC/GSIPR).

5.159 **Senha ou palavra-chave** – palavra ou uma ação secreta previamente convencionada entre duas partes como forma de reconhecimento. Em sistemas de computação, senhas são amplamente utilizadas para autenticar usuários e permitir-lhes o acesso a informações personalizadas armazenadas no sistema.

5.160 **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 (Ref. NC 05/IN01/DSIC/GSIPR).

5.161 **Servidor** – pessoa legalmente investida em cargo público (Ref. Lei Nº 8.112/PR). Pode ser de caráter efetivo ou temporário.

5.162 **Servidor de conectividade** – recurso computacional que possibilita a interligação de redes, interligação de recursos computais e o controle entre eles.

5.163 **Servidores de rede** – recurso computacional com a finalidade de disponibilizar ou gerenciar serviços disponibilizados aos usuários do MinC.

5.164 **SIC** – Segurança da Informação e Comunicações.

5.165 ***Site* ou sítios** – conjunto de páginas na Internet. Também é chamado de website.

5.166 **SLA (*Service Level Agreement*)** – acordo de Nível de Serviço entre a instituição e o terceiro contratado com o intuito de definir as características e especificidades de um determinado serviço corporativo a ser disponibilizado.

5.167 ***Software*** – programa de computador composto por uma sequência de instruções, que é interpretada e executada por um processador ou por uma máquina virtual.

5.168 ***Software* autorizado** – programa de computador avaliado pela área responsável pela administração dos recursos de tecnologia da informação ao usuário, sem direito de suporte técnico.

5.169 ***Software* homologado** – programa de computador avaliado e aprovado pela área responsável pela administração dos recursos de tecnologia da informação ao usuário, com direito a suporte técnico.

5.170 **SPAM** – termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

5.171 **Streaming (fluxo de mídia)** - serviço que permite a distribuição de dados em multimídia através da internet, seja ele áudio ou vídeo, ao vivo ou sob demanda.

5.172 **Switch** – equipamento inteligente que interliga os recursos computacionais em uma mesma rede.

5.173 **Tempo Objetivo de Recuperação** – tempo pré-definido no qual uma atividade deverá estar disponível após uma interrupção ou incidente (Ref. NC 06/IN01/DSIC/GSIPR).

5.174 **Termo de ciência** - declaração de ciência quanto à manutenção de sigilo e das normas de segurança vigentes no órgão ou entidade, a ser assinado por todos os empregados da contratada diretamente envolvidos na contratação (Ref. IN 04 SLTI/MP).

5.175 **Termo de Posse em Cargo Público –** termo assinado pelo servidor no ato de posse no qual constam as atribuições, os deveres, as responsabilidades e os direitos inerentes ao cargo ocupado. (Ref. Lei nº 8.112/PR)

5.176 **Termo de Responsabilidade do Usuário da Rede MinC** - termo assinado pelo servidor ou colaborador no qual declara ter ciência e estar de acordo com os procedimentos de acesso à rede corporativa, ao e-mail institucional ou ao funcional e aos demais serviços de tecnologia da informação, comprometendo-se a respeitá-los e cumpri-los plena e integralmente.

5.177 **Termo de Sigilo e Confidencialidade** - acordo de segurança com declaração de manutenção de sigilo e respeito às normas de segurança vigentes no órgão ou entidade, a ser assinado pelo representante legal do fornecedor e/ou por todos os empregados da contratada diretamente envolvidos na contratação (Ref. Termo de Compromisso e Termo de Ciência da IN 04 SLTI/MP).

5.178 **Teste de caixa branca** – técnica de teste que usa a perspectiva interna do sistema para modelar os casos de teste. No teste de software, a perspectiva interna significa basicamente o código fonte.

5.179 **Teste de caixa preta** – teste de software para verificar a saída dos dados usando entradas de vários tipos. Tais entradas não são escolhidas conforme a estrutura do programa, quanto mais entradas são fornecidas, mais rico será o teste. No teste de software do tipo caixa-preta, não existe acesso à perspectiva interna do sistema, ou seja, não existe acesso ao código fonte.

5.180 **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 (Ref. NC 04/IN01/DSIC/GSIPR).

5.181 **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 (Ref. Lei 12.527).

5.182 **Tratamento de Incidentes de Segurança em Redes Computacionais** – é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e 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 (Ref. NC 05/IN01/DSIC/GSIPR).

5.183 **Tratamento dos riscos** – processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco (Ref. NC 04/IN01/DSIC/GSIPR).

5.184 **Trilhas de Auditoria** – rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (logs) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários não autorizados.

5.185 **UC (*Underpinning Contract*)** – Contrato de Apoio para a prestação de serviço com um provedor externo ao MinC.

5.186 **Usuário** – servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade (Ref. NC 07/IN01/DSIC/GSIPR).

5.187 **Usuários visitantes com dispositivos móveis** – agentes públicos ou não que utilizam dispositivos móveis de sua propriedade, ou do órgão ou entidade a que pertencem, dentro dos ambientes físicos e virtuais de órgãos ou entidades da APF, dos quais não fazem parte (Ref. NC 12/IN01/DSIC/GSIPR).

5.188 **Valor do Ativo de Informação** – valor, tangível e intangível, que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos de um órgão ou entidade da APF, quanto o quão cada ativo de informação é imprescindível aos interesses da sociedade e do Estado (Ref. NC 10/IN01/DSIC/GSIPR).

5.189 **Verificação de Conformidade em Segurança da Informação e Comunicações** – procedimentos que fazem parte da avaliação de conformidade que visam identificar o cumprimento das legislações, normas e procedimentos relacionados à Segurança da Informação e Comunicações da instituição (Ref. NC 11/IN01/DSIC/GSIPR).

5.190 **Vírus** - softwares maliciosos que fazem cópias de si mesmo infectando outros arquivos legítimos do computador, ou seja, se tornam parte de outros programas. Os vírus geralmente dependem da ação do usuário para se tornarem ativos ou infectar outros computadores.

5.191 **Vulnerabilidade** – conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou instituição, os quais podem ser evitados por uma ação interna de segurança da informação (Ref. NC 04/IN01/DSIC/GSIPR).

5.192 **Wireless (sem fio)** – sistema de comunicação que não requer fios para transportar sinais.

6. PENALIDADES

6.1 Todos os servidores e colaboradores estão sujeitos às regras da Política de Segurança da Informação e Comunicações e devem observar integralmente o que dispõe este documento. A inobservância dessas regras acarretará em apuração das responsabilidades funcionais na forma da legislação em vigor, podendo haver responsabilização administrativa, civil e penal.

7. COMPETÊNCIAS E RESPONSABILIDADES

7.1 Os servidores e os colaboradores devem ter conhecimento da Política de Segurança da Informação e Comunicações, tendo a obrigação de seguir rigorosamente o disposto nas normas de segurança.

8. DISPOSIÇÕES GERAIS

8.1 Qualquer dúvida ou sugestões sobre a Política de Segurança da Informação e Comunicações e suas orientações devem ser imediatamente encaminhadas à área responsável por Segurança da Informação para análise e/ou esclarecimento.

9. ATUALIZAÇÃO

9.1 Todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 03 (três) anos.

10. VIGÊNCIA

10.1 Esta norma entra em vigor na data de sua publicação.