BOLETIM DE SERVIÇO
Fundação Nacional do Índio
Desenho Kadiwéu - MS

SUMÁRIO

PRESIDÊNCIA

PORTARIA Nº 739/PRES, de 19 de junho de 2020

Institui a Política de Segurança da Informação e Comunicações (PoSIC) da Fundação Nacional do Índio - FUNAI.

O PRESIDENTE DA FUNDAÇÃO NACIONAL DO ÍNDIO, no uso das atribuições que lhe são conferidas pelo Estatuto, aprovado pelo Decreto nº 9.010, de 23 de março de 2017, e

CONSIDERANDO a Deliberação e aprovação da Política de Segurança da Informação e Comunicações, pelo Comitê de Governança Digital, instituído pela portaria nº 320/PRES, de 25 de março de 2019;

CONSIDERANDO o Decreto nº 9.637/2018 que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO a Norma Complementar nº 03/IN01/DSIC/GSIPR que estabelece diretrizes, critérios e procedimentos para a elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (PoSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

CONSIDERANDO a necessidade de assegurar a continuidade dos serviços, garantir a segurança dos sistemas, gerenciar a central de serviço e os incidentes, gerenciar a configuração, gerenciar mudanças, monitorar e avaliar o desempenho de TI e monitorar e avaliar os controles internos;

CONSIDERANDO a necessidade de viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação no âmbito da Fundação Nacional do Índio; e

CONSIDERANDO o constante dos autos do processo nº 08620.011370/2019-03,

RESOLVE:

Art. 1º Instituir no âmbito da Fundação Nacional do Índio - FUNAI, a Política de Segurança da Informação,e Comunicações (PoSIC).

Parágrafo único: A Política de que trata este artigo tem por finalidade estabelecer as diretrizes para a segurança do manuseio, tratamento e controle e para proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio pelos sistemas de informação a serem obrigatoriamente observados na definição de regras operacionais e procedimentos no âmbito desta Fundação.

Art. 2º As diretrizes de segurança da informação estabelecidas nesta Portaria são aplicáveis a todos servidores, colaboradores, estagiários e demais agentes públicos, que oficialmente executem atividade vinculada à atuação institucional da FUNAI.

Art. 3º Fica revogada a Portaria nº 054/DAGES de 19 de julho de 2016.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

MARCELO AUGUSTO XAVIER DA SILVA
Presidente da Fundação Nacional do Índio

ANEXO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

1. ESCOPO

1.1. Institui no âmbito da Fundação Nacional do Índio - Funai, a Política de Segurança da Informação e Comunicações - PoSIC.

1.2. As diretrizes, normas complementares e manuais de procedimentos desta PoSIC, aplica-se a todos, servidores, colaboradores, estagiários e demais agentes públicos, que oficialmente, executem atividade vinculada à atuação institucional da FUNAI.

1.3. Dos objetivos:

1.3.1. Tratar do uso e do compartilhamento de dados, informações e conhecimento em todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte), em observância à legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações;

1.3.2. Estabelecer diretrizes para garantir a confidencialidade, a integridade, a disponibilidade, a autenticidade, o não-repúdio, o tratamento, o controle, o manuseio, a proteção dos dados, das informações, e dos conhecimentos produzidos e armazenados ou transmitidos, pelos sistemas de informação, no âmbito da Fundação Nacional do Índio - FUNAI;

1.3.3. Estabelecer mecanismos de controle para garantir a efetiva proteção e a redução dos riscos de ocorrência de perdas de dados, das informações e dos conhecimentos gerados, evitando alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações e conhecimentos gerados;

1.3.4. Estabelecer o arcabouço normativo acerca da Segurança da Informação e Comunicações - SIC da FUNAI;

1.3.5. Estimular a adoção de práticas de Segurança da Informação e Comunicação - SIC, aplicando as normas e os procedimentos sobre o assunto;

1.3.6. Apoiar a estrutura de Gestão de Segurança da Informação e Comunicações – GSIC, nas tomadas de decisões institucionais em segurança que visem a eficiência, eficácia e efetividade das atividades de SIC;

1.3.7. Possibilitar a elaboração de Instruções Normativas destinadas à proteção da informação e à disciplina de sua utilização e que Integraram a PoSIC.

1.4. Esta política também se aplica, no que couber, ao relacionamento da FUNAI com outros órgãos e entidades públicas ou privadas;

2. CONCEITOS E DEFINIÇÕES

2.1. Os conceitos e definições dos termos técnicos presentes na elaboração da PoSIC, encontram-se postuladas no ANEXO I.

3. REFERÊNCIAS NORMATIVAS

3.1. As referências legais e normativas utilizadas para a elaboração da PoSIC, encontram-se postuladas no ANEXO II.

4. PRINCÍPIOS

4.1. **Princípios basilares da PoSIC:**

4.1.1. Confidencialidade: garante que a informação será acessada apenas por servidores, colaboradores, estagiários e demais agentes públicos, sistema, órgão ou entidade autorizada e credenciada;

4.1.2. Integridade: garante que a informação não será modificada, gravada ou excluída sem autorização ou acidentalmente;

4.1.3. Autenticidade: garante a identificação de servidores, colaboradores, estagiários e demais agentes públicos, sistema, órgão ou entidade que produziu, expediu, modificou ou excluiu a informação;

4.1.4. Irrefutabilidade ou não-repúdio: garante a rastreabilidade e incontestabilidade dos atos praticados pelos usuários; e

4.1.5. Disponibilidade: garante que a informação estará acessível e utilizável por servidores, colaboradores, estagiários e demais agentes públicos, sistema, órgão ou entidade quando requisitada.

4.2. **Princípios que orientam as ações de SIC:**

4.2.1. Criticidade: define a importância da informação para a continuidade do negócio da organização;

4.2.2. Celeridade: garante respostas rápidas a incidentes e falhas de segurança;

4.2.3. Clareza: as regras e a documentação sobre segurança da informação e comunicações devem ser elaboradas de forma clara, precisa, concisa e de fácil entendimento;

4.2.4. Ética: preserva o direito dos servidores, colaboradores, estagiários e demais agentes públicos, sem que ocorra o comprometimento da segurança da informação e comunicações;

4.2.5. Legalidade: devem ser levadas em consideração as leis, normas e políticas organizacionais administrativas, técnicas e operacionais vigentes; e

4.2.6. Responsabilidade: os usuários são responsáveis pelo cumprimento desta PoSIC e devem respeitar a legislação e normas pertinentes à Segurança da Informação e Comunicações vigentes.

4.3. A adoção dos princípios apresentados tem por fim a preservação do direito pessoal e coletivo, sigilo da correspondência e das comunicações individuais, proteção dos dados, informações e conhecimentos produzidos.

4.4. São observados, ainda, sem prejuízo dos demais, os princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal

5. DIRETRIZES

5.1. As diretrizes nortearão a elaboração, adoção de políticas e normas e as ações de Gestão de SIC, no âmbito da FUNAI.

5.2. **Diretrizes gerais:**

5.2.1. A PoSIC ficará disponível permanentemente nos canais de comunicação interno e externo da FUNAI a todos os servidores, colaboradores, estagiários e demais agentes públicos e privados, após sua publicação;

5.2.2. Todos os mecanismos de proteção utilizados para a segurança da informação deverão ser mantidos para preservar a continuidade do negócio a fim de regular exercício das funções institucionais;

5.2.3. Todas as regras corporativas sobre uso de internet e intranet visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, a proteção dos ativos de informação da FUNAI deverá sempre ser privilegiada.

5.3. A preservação da disponibilidade, integridade, confiabilidade e autenticidade dos dados, informações e conhecimentos que compõem o ativo da informação da FUNAI, pauta-se pela:

5.3.1. Continuidade das atividades;

5.3.2. Economicidade da proteção dos ativos de informação;

5.3.3. Pessoalidade e utilidade do acesso aos ativos de informação; e

5.3.4. Responsabilização do usuário pelos atos que comprometam a segurança do sistema da informação.

5.4. Estar consoante aos objetivos estratégicos, processos, requisitos legais e estrutura da FUNAI, bem como os princípios e diretrizes gerais da PoSIC do MJSP.

5.5. Estabelecer medidas e procedimentos para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

5.6. Elaborar e implementar mecanismos de auditoria e conformidade, com o objetivo de garantir a exatidão dos registros de acesso aos ativos de informação e avaliar sua conformidade com as normas de SIC em vigor.

5.7. Implementar controles de acesso lógico aos softwares e redes de computadores, e implantar controles de acesso físico às instalações, com o objetivo de preservar os ativos de informação;

5.8. Definir regras claras e precisas de uso dos ativos de informação institucionais, com o objetivo de evitar o uso pelos agentes públicos para fins particulares, como abuso de direito ou violação à imagem da entidade, em desrespeito às leis, aos costumes e à dignidade da pessoa humana; e

5.9. Observar as boas práticas e procedimentos de SIC recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

5.10. Os contratos, convênios, acordos, termos e outros instrumentos congêneres celebrados pela FUNAI devem atender ou estarem aderentes a esta PoSIC.

5.11. Esta política também se aplica, no que couber, ao relacionamento da FUNAI com outros órgãos e entidades públicas ou privadas.

5.12. **Diretrizes específicas:**

5.12.1. **Tratamento da Informação**

5.12.1.1. Toda informação produzida, adquirida ou custodiada pelo usuário, no exercício de suas atividades, é considerada bem e propriedade da FUNAI, deve ser protegida segundo as diretrizes descritas nesta PoSIC e demais regulamentações em vigor, com o objetivo de minimizar riscos às atividades e serviços do órgão e preservar sua imagem.

5.12.1.2. Tais diretrizes serão disciplinadas por normativo próprio a ser elaborado com completa observância e conformidade aos termos desta PoSIC, bem como a legislação vigente que trate de matéria análoga.

5.12.2. **Tratamento de Incidentes de Rede**

5.12.2.1. A FUNAI, com auxílio da área de Tecnologia da Informação e Comunicações - CGTIC, manterá equipe de tratamento e resposta a incidentes em redes computacionais, ficando delegada a esta a responsabilidade por receber, apreciar e responder notificações de atividades relacionadas a incidentes de rede.

5.12.2.2. Sua criação, estrutura e modelo de implementação serão definidas em Instrução Normativa que deverá estar em conformidade com as diretrizes desta PoSIC.

5.12.3. **Gestão de Risco**

5.12.3.1. A gestão de riscos se encarrega da avaliação, mapeamento, identificação, análise e monitoramento contínuo das vulnerabilidades e riscos associados a ativos de tecnologia da informação, com fins a subsidiar o planejamento de ações preventivas e mitigatórias.

5.12.3.2. Os riscos devem ser continuamente monitorados e tratados, de acordo com as vulnerabilidades associadas aos ativos de informação e aos níveis de risco, conforme procedimentos definidos em norma específica, a serem postuladas na Política de Gestão de Riscos de SIC da FUNAI, e serão tratadas pelo Comitê de Governança Digital desta Fundação.

5.12.4. **Gestão de Continuidade**

5.12.4.1. Os recursos necessários para garantir a integridade e a disponibilidade das informações da FUNAI têm que ser suportados por um plano de continuidade dos Recursos de Tecnologia da Informação e Comunicação para reduzir a um nível aceitável a possibilidade de interrupção causada por desastres ou falhas nos recursos que suportam os processos de negócio, devendo ser testado, revisado e documentado conforme a necessidade;

5.12.4.2. Tais diretrizes serão disciplinadas por normativo próprio a ser elaborado com completa observância e conformidade aos termos desta PoSIC, bem como a legislação vigente que trate de matéria análoga.

5.12.5. **Auditoria de Conformidade**

5.12.5.1. Devem ser definidos critérios de auditoria com o intuito de aferir o cumprimento desta PoSIC, suas Normas Complementares e Procedimentos;

5.12.5.2. Devem ser estabelecidos critérios de salvaguarda de logs dos ativos de tecnologia da informação e comunicações, a fim de possibilitar auditoria; e

5.12.5.3. Deve ser continuamente avaliada a conformidade desta PoSIC com a legislação vigente, no que diz respeito a Gestão de Segurança da Informação e Gestão de Tecnologia da Informação.

5.12.5.4. Os procedimentos e diretrizes adotados para realização de auditorias e acompanhamento de conformidade serão disciplinadas por ato normativo próprio a ser elaborado com completa observância e conformidade aos termos desta PoSIC, bem como a legislação vigente que trate de matéria análoga.

5.12.6. **Controles de Acesso**

5.12.6.1. O controle de acesso aos recursos computacionais (de forma presencial ou remota), o credenciamento de agentes e definição de perfis de acesso a ativos de informação da FUNAI, serão definidos em normativo próprio elaborado com completa observância e conformidade aos termos desta PoSIC, bem como a legislação vigente que trate de matéria análoga.

5.12.7. **Uso de E-mail**

5.12.7.1. A disponibilização do serviço de correio eletrônico corporativo aos servidores, colaboradores, estagiários e demais agentes públicos a serviço da FUNAI será disciplinada por normativo próprio elaborado com completa observância e conformidade aos termos desta PoSIC, bem como a legislação vigente que trate de matéria análoga.

5.12.8. **Uso da Internet e Intranet**

5.12.8.1. A definição dos critérios para administração, utilização e acesso à rede local (Intranet) e mundial (internet) de computadores será pautado por ato normativo próprio elaborado com completa observância e conformidade aos termos desta PoSIC, bem como a legislação vigente que trate de matéria análoga.

5.12.9. **Uso de Recursos Computacionais**

5.12.9.1. Os critérios e procedimentos para o uso dos recursos computacionais disponíveis aos usuários da rede da FUNAI, assim como o controle, administração e requisitos mínimos desses recursos serão estabelecidos por ato normativo próprio elaborado com completa observância e conformidade aos termos desta PoSIC.

5.12.10. **Organização da Segurança da Informação**

5.12.10.1. A definição das diretrizes de organizacionais que regem a segurança da informação serão regidos por ato normativo próprio elaborado com completa observância e conformidade aos termos desta PoSIC, bem como a legislação vigente que trate de matéria análoga.

5.12.11. **Segurança em Recursos Humanos**

5.12.11.1. A definição dos protocolos de segurança e controles de acesso aos ativos de informação críticos da FUNAI será realizada em conjunto com as diretrizes de segurança em recursos humanos a serem disciplinadas por ato normativo próprio elaborado com completa observância e conformidade aos termos desta PoSIC, bem como a legislação vigente que trate de matéria análoga; e

5.13. Para cada uma das diretrizes constantes das Seções deste Capítulo devem ser elaboradas normas específicas, manuais e procedimentos.

6. DEVER DOS USUÁRIOS

6.1. Conhecer e cumprir os princípios, diretrizes e responsabilidades desta PoSIC e demais normas e resoluções relacionados à SIC;

6.2. Obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação;

6.3. Comunicar os incidentes que afetam a segurança dos ativos de informação;

6.4. Os Usuários são responsáveis pela segurança dos ativos e processos que estejam sob sua custódia e por todos os atos executados com suas identificações, tais como: login, senha eletrônica, certificado digital e endereço de correio eletrônico. Sua identificação deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o seu reconhecimento;

6.5. Obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação; e

6.6. Comunicar os incidentes que afetam a segurança dos ativos de informação a área de Tecnologia da Informação.

6.7. É vedado comprometer a integridade, confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela FUNAI.

7. COMPETÊNCIAS E RESPONSABILIDADES

7.1. A Política, as normas complementares e os procedimentos de SIC se aplicam a todos servidores, colaboradores, estagiários e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional da FUNAI, sendo dever do agente público conhecer e zelar pelo cumprimento da PoSIC

7.2. Os servidores, colaboradores, estagiários e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional da FUNAI são responsáveis pela segurança dos ativos e processos que estejam sob sua custódia e por todos os atos executados com suas identificações, tais como crachá, login, senha eletrônica, certificado digital e endereço de correio eletrônico.

7.3. A identificação do usuário deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o seu reconhecimento.

7.4. **Compete à Alta Gestão:**

7.4.1. Garantir a provisão dos recursos necessários para a implementação da PoSIC;

7.4.2. Comprometer-se em proteger todos os ativos de informação da instituição;

7.4.3. Assegurar que a implementação dos controles de SIC tenha atividades coordenadas e permeie toda a organização;

7.4.4. Assegurar os recursos necessários para a implementação e gestão da PoSIC e normas complementares na FUNAI;

7.4.5. Promover a cultura de segurança da informação e comunicações, por meio de atividades de sensibilização, conscientização, capacitação e especialização; e

7.4.6. Assegurar os investimentos e recursos financeiros, materiais e humanos necessários ao seu cumprimento, alinhados aos objetivos institucionais e ao arcabouço legal-normativo.

7.4.6.1. Os investimentos e recursos financeiros devem ser dimensionados segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos para o negócio, atividade fim e os objetivos institucionais;

7.5. **Compete ao Comitê de Governança Digital - CGD:**

7.5.1. Auxiliar a Alta Gestão a buscar meios de assegurar os recursos financeiros necessários para investimentos e custeios em medidas de SIC;

7.5.2. Aprovar a Política de Segurança da Informação e Comunicação;

7.5.3. Aprovar as normas específicas de Segurança da Informação e Comunicação;

7.5.4. Instituir o Comitê Gestor de Segurança da Informação – CGSI;

7.5.5. Desempenhar as atividades do CGSI enquanto este não for instituído;

7.5.6. Definir critérios para auditoria periódica destinada a aferir o cumprimento da PoSIC, suas Normas e Procedimentos;

7.5.7. Manifestar-se sobre a PoSIC, com posterior encaminhamento ao Presidente da FUNAI;

7.5.8. Assessorar na implementação das ações de SIC;

7.5.9. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

7.5.10. Propor alterações na PoSIC;

7.5.11. Propor normas relativas à segurança da informação e comunicações;

7.5.12. Promover cultura de SIC;

7.5.13. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

7.5.14. Propor recursos necessários às ações de SIC;

7.5.15. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC;

7.5.16. Propor normas relativas à SIC;

7.5.17. Definir estratégias para a implantação da PoSIC;

7.5.18. Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança;

7.5.19. Apurar os incidentes de segurança críticos e encaminhar os fatos apurados para aplicação das penalidades previstas;

7.5.20. Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de SIC;

7.5.21. Manter a análise de risco atualizada, refletindo o estado corrente da organização;

7.5.22. Identificar controles físicos, administrativos e tecnológicos para mitigação do risco;

7.5.23. Recepcionar, organizar, armazenar, tratar informações de eventos de segurança e tratar os incidentes de segurança, determinando aos gestores as ações corretivas ou de contingência em cada caso; e

7.5.24. Exercer outras atribuições que lhes forem atribuídas em regimento interno.

7.6. **Cabe ao Comitê Gestor de Segurança da Informação - CGSI:**

7.6.1. Assim como o CGD, o CGSI deve auxiliar a Alta Gestão a buscar meios de assegurar os recursos financeiros necessários para investimentos e custeios em medidas de SIC;

7.6.2. Assessorar na implementação das ações de segurança da informação e comunicações;

7.6.3. Desenvolver a cultura de segurança da informação e das comunicações na Instituição;

7.6.4. Coordenar as ações de segurança da informação e das comunicações;

7.6.5. Propor, aprovar e publicar normas e procedimentos complementares à PoSIC;

7.6.6. Dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PoSIC;

7.6.7. Avaliar criticamente a PoSIC, visando a sua aderência aos objetivos institucionais e à legislação vigente, e propor sua revisão, quando necessário;

7.6.8. Indicar o Gestor de Segurança da Informação e das Comunicações;

7.6.9. Instituir e implementar a Equipe de Tratamento de Incidentes de Redes de Computadores (ETIR), supervisionar suas ações e referendar o seu Regimento Interno;

7.6.10. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e das comunicações;

7.6.11. Constituir grupo de trabalho para realizar auditoria de segurança da informação e das comunicações;

7.6.12. Receber e consolidar os resultados dos trabalhos de auditoria de segurança da informação e das comunicações e remetê-los à Reitoria;

7.6.13. Responder às demandas dos órgãos de controle quando referentes à segurança da informação e das comunicações;

7.6.14. Realizar e/ou acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e das comunicações;

7.6.15. Elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos em segurança da informação e das comunicações;

7.6.16. Propor o Plano de Investimentos em Segurança da Informação e das Comunicações;

7.6.17. Desenvolver o Plano de Continuidade de Negócios, dentro de sua área de competência;

7.6.18. Desempenhar as atividades da ETIR enquanto esta não estiver instituída.

7.6.19. Propor normas e procedimentos internos relativos à segurança da informação e comunicações, em conformidade com a legislação existente sobre o tema.

7.7. **Cabe à Equipe de Tratamento de Incidentes de Redes de Computadores - ETIR:**

7.7.1. Promover cultura de segurança da informação e comunicações;

7.7.2. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

7.7.3. Propor recursos necessários às ações de segurança da informação e comunicações;

7.7.4. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

7.7.5. Propor normas relativas à segurança da informação e comunicações.

7.7.6. Facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

7.7.7. Promover a recuperação de sistemas;

7.7.8. Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;

7.7.9. Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;

7.7.10. Analisar ataques e intrusões na rede;

7.7.11. Executar as ações necessárias para tratar quebras de segurança;

7.7.12. Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

7.7.13. Cooperar com outras equipes de Tratamento e Resposta a Incidentes; e

7.7.14. Participar em fóruns, redes nacionais e internacionais relativas à SIC.

7.8. **Cabe ao Gestor do Ativo de Informação:**

7.8.1. Promover a segurança dos ativos de informação sob sua responsabilidade;

7.8.2. Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta PoSIC;

7.8.3. Conceder e revogar acessos aos ativos de informação;

7.8.4. Comunicar à ETIR a ocorrência de incidentes de SIC;

7.8.5. Designar custodiante dos ativos de informação, quando aplicável.

7.9. **Cabe ao Custodiante do Ativo de Informação:**

7.9.1. Proteger e manter as informações, bem como controlar o acesso de execução/alteração, de acordo com os requisitos definidos pelo gestor da informação e em conformidade com esta PoSIC.

7.9.2. O acesso às informações obedecerá ao disposto na Lei n° 12.527, de 18 de novembro de 2011, que regula o acesso a informações.

7.10. **Cabe ao titular da unidade administrativa:**

7.10.1. Corresponsabilizar-se pelas ações realizadas por aqueles que estão sob sua subordinação;

7.10.2. Conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SIC;

7.10.3. Incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;

7.10.4. Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;

7.10.5. Realizar o tratamento e a classificação da informação;

7.10.6. Autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa;

7.10.7. Comunicar à ETIR os casos de quebra de segurança; e

7.10.8. Manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores.

7.11. **Cabem aos Terceiros e Fornecedores:**

7.11.1. Tomar conhecimento da PoSIC conforme haja previsão em contrato;

7.11.2. Fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato;

7.11.3. Fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

7.12. **Compete ao Usuário:**

7.12.1. Cumprir fielmente as políticas, as normas, os procedimentos e as orientações de SIC;

7.12.2. Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

7.12.3. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados; e

7.12.4. Comunicar imediatamente ao Comitê de Segurança da Informação e Comunicações qualquer descumprimento ou violação desta Política e/ou de seus documentos complementares.

8. PENALIDADES

8.1. Nos casos de descumprimento ou violação de um ou mais itens da PoSIC ou de suas Normas, procedimentos ou atividades pertinentes à SIC, implicarão as sanções administrativas cabíveis nos termos da lei e normas complementares, sem prejuízo de outras previstas nas esferas cível e penal.

9. ATUALIZAÇÃO

9.1. A atualização desta PoSIC e instrumentos normativos adicionais obedecerão aos seguintes critérios:

9.1.1. **Atualização da Política**

- Nível de Aprovação: Presidente da Fundação Nacional do Índio.
- Periodicidade de atualização: sempre que se fizer necessário, não excedendo o período máximo de três anos;

9.1.2. **Atualização das Normas**

- Nível de Aprovação: Comitê de Governança Digital.
- Periodicidade de atualização: sempre que se fizer necessário, **ou quando ocorrer à atualização da PoSIC.**

10. DISPOSIÇÕES FINAIS

10.1. As dúvidas sobre a Política de Segurança da Informação e Comunicações e seus documentos devem ser submetidas ao Comitê de Segurança da Informação e Comunicações.

10.2. Os casos omissos e as dúvidas com relação a essa PoSIC serão submetidos ao Comitê de Governança Digital da FUNAI.

10.3. No âmbito da gestão dos recursos de tecnologia da informação da FUNAI, a PoSIC será regida por estrutura de Normas Complementares apresentadas sob forma de Instruções Normativas.

10.4. A PoSIC **será amplamente divulgada a fim de promover a cultura entre os** usuários dos recursos (servidores, colaboradores, estagiários e demais agentes públicos ou particulares) que, oficialmente executem atividade vinculada à atuação institucional da FUNAI por meio de:

- Correio eletrônico;
- Boletim Interno;
- Site Institucional; e
- Intranet.

10.4.1. Esta PoSIC será divulgada amplamente a fim de promover a cultura entre os servidores, colaboradores, estagiários e demais agentes públicos, que oficialmente, executem atividade vinculada à atuação institucional da FUNAI, no tocante a necessidade de segurança da informação e comunicações.

10.5. Em nenhuma hipótese será permitido o descumprimento da PoSIC e suas normas pela alegação de desconhecimento das mesmas por parte do usuário.

10.6. Esse documento entra em vigor na data de sua publicação.

ANEXO I

CONCEITOS E DEFINIÇÕES

Para os fins dessa Política, considera-se:

- Acesso Lógico: acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação;
- Acesso Remoto: ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da maquina do usuário;
- Agente público:aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira;
- Agente responsável: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal (APF), direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
- ADSL (Asymmetric Digital Subscriber Line): (Linha Digital Assime'trica para Assinante) tecnologia de transmissão que possibilita o transporte de voz e dados a alta velocidade através da rede telefônica convencional, analógica ou digital;
- Ameaça: conjunto de fatores externos, internos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- Análise/avaliação de riscos: processo completo de análise e avaliação para identificar fontes e estimar os riscos;
- Ativo de Tecnologia da Informação: composto por ativos de software e ativos físicos, permitindo o armazenamento, a transmissão e processamento das informações;
- Ativo da Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
- Ativo Sigiloso: qualquer bem tangível ou intangível que possa conter informações sigilosas que, se acessadas por pessoas não autorizadas, podem causar danos significativos à organização;
- Auditoria em Segurança da Informação: verificação e avaliação dos controles de segurança da informação, sistemas e procedimentos internos implementados, com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;
- Autenticação: é o ato de confirmar que algo ou alguém e' autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;
- 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;
- Banco de Dados (ou Base de Dados): é um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações;
- Biometria: uso de mecanismos de identificação para restringir o acesso a determinados lugares ou serviços. Exemplos de identificação biométrica: através da íris (parte colorida do olho), da retina (membrana interna do globo ocular), da impressão digital, da voz, do formato do rosto e da geometria da mão;
- Bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso;
- Bluetooth: tecnologia de transmissão de dados via sinais de rádio de alta frequência, entre dispositivos eletrônicos próximos;
- Classificação da informação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;
- Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
- Contingência: descrição de medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos a corporação;
- Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
- Cópia de Segurança (Backup): copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;
- Correio Eletrônico: é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;
- Credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha;
- Criptografia: é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta");
- Custodiante do ativo: unidade administrativa responsável pelo armazenamento, operação, administração e preservação de ativos;

- Custodiante da informação: colaborador responsável pela guarda adequada do dado;
- CGD: Comitê de Governança Digital da Fundação Nacional do Índio;
- Dado: representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;
- CGTIC: Coordenação de Geral de Tecnologia da Informação;
- Diretriz: descrição que orienta o que deve ser feito, e como, para se alcançar os objetivos estabelecidos nas políticas;
- Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
- Documento:toda a base de conhecimento, fixada materialmente, suscetível de ser utilizada para consulta, estudo ou prova
- Download: (Baixar) copiar arquivos de um servidor (site) na internet para um computador pessoal;
- Espelhamento: Sistema de proteção de dados onde o conteúdo é espelhado em tempo real. Todos os dados são duplicados entre as áreas de armazenamento disponíveis.
- Evento de segurança da informação: 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 desconhecida, que possa ser relevante para a segurança da informação
- FTP (File Transfer Protocol): (Protocolo de Transferência de Arquivo) e um protocolo da Internet para transferência de arquivos;
- Gestão de Continuidade de Negócios: Processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia-a-dia;
- Gestão de Risco: 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 equilibra-los com os custos operacionais e financeiros envolvidos;
- 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 equilibra-los com os custos operacionais e financeiros envolvidos;
- Hardware: é a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressora, teclado e outros;
- HTTP (Hyper Text Transfer Protocol): (Protocolo de Transferência de Hipertexto) e uma linguagem para troca de informação entre servidores e clientes da rede;
- HTTPS (HyperText Transfer Protocol Secure): (Protocolo de Transferência de Hipertexto Seguro) e uma linguagem para troca de informação entre servidores e clientes da rede, com recursos de criptografia, autenticação e integridade;
- Incidente de Segurança: é 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 transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- Informações Criticas: são as informações de extrema importância para a sobrevivência da instituição;
- Informação sigilosa: informação submetida temporariamente a 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;
- Instant Messenger (Mensageiro instantâneo): é uma aplicação que permite o envio e o recebimento de mensagens em tempo real;
- Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- Internet: rede mundial de computadores;
- Internet Protocol (Protocolo de Internet): é um protocolo de comunicação usado entre duas ou mais máquinas em rede para encaminhamento dos dados;
- Intranet: rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;
- Log: é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;

- Logon: Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível;
- Online (Estar disponível ao vivo): no contexto da Internet significa estar disponível para acesso imediato, em tempo real;
- Perfil de acesso: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;
- Plano de Contingência: Descrever as medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos críticos voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada;
- 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 num nível previamente definido, em casos de incidentes;
- Peer-to-peer (P2P) (Ponto a ponto): permite conectar o computador de um usuário a outro, para compartilhar ou transferir dados, como MP3, jogos, videos, imagens, entre outros;
- Politica 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;
- Protocolo: convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;
- Proxy: é um serviço intermediário entre as estações de trabalho de uma rede e a o Internet. O servidor de rede proxy serve para compartilhar a conexão com a Internet, melhorar o desempenho do acesso, bloquear acesso a determinadas páginas;
- Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
- Recursos Computacionais: 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;
- Rede Corporativa: conjunto de todas as redes locais sob a gestão da instituição;
- Rede Pública: rede de acesso a todos;
- Replicação: é a manutenção de cópias idênticas de dados em locais diferentes. O objetivo de um mecanismo de replicação de dados e permitir a manutenção de várias cópias idênticas de um mesmo dado em vários sistemas de armazenamento.
- Risco:combinação da probabilidade de ocorrência de um evento e de suas consequências;
- Roteador: equipamento responsável pela troca de informações entre redes;
- Sala Cofre: é uma sala fortificada que pode ser instalada em uma instituição, provendo um local seguro de invasões e outras ameaças. São ambientes projetados para resistir a vários tipos de catástrofes. Suportam, por exemplo, temperaturas de até 1.200 graus Celsius, inundações, cortes bruscos de energia, gases corrosivos, explosões e até ataques nucleares;
- Sala Segura: sala que proporciona um ambiente seguro no Datacenter, oferecendo maior garantia no armazenamento de informações eletrônicas. Uma Sala Segura possui gerador próprio, instalação elétrica independente, paredes especiais, piso elevado, ar-condicionado, detecção e combate a incêndios, iluminação, sinalização de emergência e monitoração do ambiente;
- Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
- Servidor de Rede: recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;
- Servidor: pessoa legalmente investida em cargo público;
- Sistemas de Informação: conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção;
- Sistema de Segurança da Informação: proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização, São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento;
- Software: são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;

- Site: Conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;
- Streaming: transferência de dados (normalmente áudio e vídeo) em fluxo contínuo por meio da Internet;
- Switches: é um equipamento eletrônico de comutação que funciona como um nó central numa rede no formato estrela, armazenando em memória o endereço físico de todos os computadores conectados a ele, relacionando cada endereço físico a uma de suas portas e permitindo assim a interligação entre os dispositivos conectados;
- Termo de Responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;
- Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;
- Tratamento de Incidentes de Segurança em Redes Computacionais: 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;
- Trilhas de Auditoria: são rotinas especificas 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;
- 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;
- VLAN (Virtual Local Area Network ou Virtual LAN - Rede Local Virtual): é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local;
- VPN (Virtual Private Network - Rede Privada Virtual): é uma rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública de uma maneira que emula uma conexão ponto a ponto privada, ' Vulnerabilidade - conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;
- Vulnerabilidade:fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.
- Wireless (rede sem fio): rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

ANEXO II

REFERENCIAS LEGAIS E NORMATIVAS

- Lei nº 13.853, de 08 de julho de 2019, Lei Geral de Proteção de Dados Pessoais (LGPD) Altera a Lei nº Lei nº 13.709/2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências
- Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014;
- Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
- Lei nº 12.527, de 18 de novembro de 2011 - Lei de acesso à informação;
- Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil, Art. 1.016, que institui que os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho e suas funções;
- Lei nº 9.983, de 14 de julho de 2000: Altera o Decreto Lei nº 2.848/1940, Código Penal, sobre tipificação de crimes por computador contra a Previdência Social e a Administração Pública;
- Lei nº 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais;
- Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;
- Decreto nº 10.278, de 18 de março de 2020, regulamenta o disposto no inciso X do caput do art. 3º da Lei nº 13.874/2019, e no art. 2º-A da Lei nº 12.682/2012, para estabelecer a técnica e os requisitos para a digitalização de

documentos públicos ou privados, a fim de que os documentos digitalizados produzam os mesmos efeitos legais dos documentos originais.

- Decreto nº 10.182, de 10 de dezembro de 2019, Altera o Decreto nº 9.668, que aprova a Estrutura Regimental do Gabinete de Segurança Institucional da Presidência da República e remaneja e transforma cargos em comissão e funções de confiança;
- Decreto Nº 9.832, de 12 de junho de 2019, Altera o Decreto nº 9.637, e o Decreto nº 7.845, para dispor sobre o Comitê Gestor da Segurança da Informação;
- Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, dispõe sobre a governança da segurança da informação, altera o Decreto nº 2.295/1997 e revoga os decretos nº 3.505/2000 e nº 8.135/2013;
- Decreto nº 7.845, de 14 de novembro de 2012, que 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;
- Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, que Dispõe sobre o acesso a informações;
- Decreto nº 9.668, de 02 de janeiro de 2019 - art. 11º do Anexo I - competência do Departamento de Segurança da Informação, alterado pelo Decreto nº 10.182;
- Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores –Internet;
- Decreto nº 1.171, de 24 de junho de 1994 que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências;
- Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;
- Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013, 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 GSI/PR nº 3, de 06 de março de 2013, 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.
- Norma Complementar nº 01/IN01/DSIC/GSIPR, Estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.
- Norma Complementar nº 02/IN01/DSIC/GSIPR, Defini a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta.
- Norma Complementar nº 03/IN01/DSIC/GSIPR, Estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (PoSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.
- Norma Complementar nº 04/IN01/DSIC/GSIPR, Estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal-APF, direta e indireta.
- Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo_nc_05_etir, Disciplinar a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
- Norma Complementar nº 06/IN01/DSIC/GSIPR, Estabelecer diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
- 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 Administração Pública Federal, direta e indireta - APF.
- Norma Complementar nº 08/IN01/DSIC/GSIPR, Disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal,direta e indireta - APF.
- Norma Complementar nº 09/IN01/DSIC/GSIPR, Normatizar o uso de recurso criptográfico para a segurança de informações produzidas nos órgãos e entidades da Administração Pública Federal -APF, direta e indireta.
- Norma Complementar nº 10/IN01/DSIC/GSIPR, 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 Administração Pública Federal, direta e indireta – APF.

- Norma Complementar nº 11/IN01/DSIC/GSIPR, Estabelece diretrizes para avaliação de conformidade nos aspectos relativos a Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta - APF.
- Norma Complementar nº 12/IN01/DSIC/GSIPR, Estabelecer 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 Administração Pública Federal (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 Administração Pública Federal, direta e indireta (APF).
- Norma Complementar nº 14/IN01/DSIC/GSIPR, Estabelece princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem, nos órgãos e entidades da Administração Pública Federal, direta e indireta.
- Norma Complementar nº 15/INOl/DSIC/GSIPR, Estabelecer diretrizes de Segurança da Informação e Comunicações para o uso das redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
- Norma Complementar nº 16/IN01/DSIC/GSIPR, Estabelece diretrizes de Segurança da Informação e Comunicações para a obtenção de software seguro nos órgãos e entidades da Administração Pública Federal, direta e indireta.
- Norma Complementar nº 17/IN01/DSIC/GSIPR, Estabelece diretrizes nos contextos de atuação e adequações para profissionais da área de Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF).
- Norma Complementar nº 18/IN01/DSIC/GSIPR, Estabelece diretrizes para as atividades de ensino em Segurança da Informação e Comunicações(SIC)nos órgãos e entidades da Administração Pública Federal, direta e indireta –APF.
- Norma Complementar nº 19/IN01/DSIC/GSIPR, Estabelece padrões mínimos para a segurança da informação e comunicações dos sistemas estruturantes nos órgãos e entidades da Administração Pública Federal, direta e indireta.
- Norma Complementar nº 20/IN01/DSIC/GSIPR, Estabelece diretrizes de Segurança da Informação e Comunicações (SIC) para instituição do processo de tratamento da informação, envolvendo todas as etapas do ciclo de vida da informação, nos órgãos e entidades da Administração Pública Federal(APF), direta e indireta.
- Norma Complementar nº 21/IN01/DSIC/GSIPR Estabelecer diretrizes para o registro, coleta e preservação de evidências de incidentes de segurança em redes computacionais dos órgãos e entidades da Administração Pública Federal, direta e indireta –APF e a comunicação às autoridades competentes.
- Norma Complementar nº 01/IN02/NSC/GSIPR, Estabelece e disciplina o credenciamento de segurança de pessoas naturais, órgãos e entidades públicas e privadas para o tratamento de informações classificadas, no âmbito do Poder Executivo Federal.
- Associação Brasileira de Normas Técnicas (ABNT), é responsável pela elaboração das Normas Brasileiras (ABNT NBR), elaboradas por seus Comitês Brasileiros (ABNT/CB), Organismos de Normalização Setorial (ABNT/ONS) e Comissões de Estudo Especiais (ABNT/CEE).
- Norma ABNT NBR ISO/IEC 27701:2019, Versão Corrigida:2020 Técnicas de segurança — diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para a gestão da privacidade dentro do contexto da organização.
- Norma ABNT NBR ISO/IEC 27005:2019, Diretrizes para o gerenciamento dos riscos de Segurança da Informação (SI);
- Norma ABNT NBR ISO/IEC 27035-1:2016 - Técnicas de segurança - Gerenciamento de incidentes de segurança da informação
- Norma ABNT NBR ISO/IEC 27002:2013 –Técnicas de segurança -Código de práticas para a segurança da informação;
- Norma ABNT NBR ISO/IEC 27001:2013 –Técnicas de segurança –Sistemas de gestão de segurança da informação – Requisitos;
- Norma ABNT ISO GUIA 73:2009 - Gestão de Riscos / Vocabulário - Recomendações para uso em normas;
- Portaria nº 320/PRES, de 25 de março de 2019, Institui o Comitê de Governança Digital no âmbito da Fundação Nacional do Índio, o qual compete também deliberar sobre as áreas de Governança de Tecnologia da Informação e Comunicações e de Segurança da Informação e Comunicações -SIC
- Cartilha de Segurança para Internet, desenvolvida pelo CERT.br e mantido pelo NIC.br. - https://cartilha.cert.br/
- Publicações - Segurança da Informação - http://dsic.planalto.gov.br/assuntos/publicacoes
- Legislação Relacionada à Lei de Acesso à Informação - http://dsic.planalto.gov.br/legislacao/legislacao_relacionada_a_lai.pdf
- Departamento de Segurança da Informação - http://dsic.planalto.gov.br/