Política de Segurança da Informação e Comunicações (PoSIC)

Publicada no Boletim de Serviço do Ministério da Saúde Nº 19, Brasília 07/05/2018

DIRETRIZES E NORMAS

A POSIC/INCA institui diretrizes, responsabilidades e competências que visam viabilizar a disponibilidade, integridade, confidencialidade e autenticidade das informações e comunicações, bem como a conformidade, padronização e normatização das atividades de gestão de segurança da informação e comunicações no INCA.

MUNDO
VIRTUAL,
SEGURANÇA
REAL.

ANA CRISTINA PINHO MENDES
Diretora Geral

GÉLCIO LUIZ QUINTELLA MENDES
Vice-Diretor Geral

Equipe de Elaboração da PoSIC

Portaria INCA nº 73 de 22/01/2018
Boletim de Serviço do MS Nº 11, Brasília 12/03/2018

AILSE RODRIGUES BITTENCOURT
Gabinete da Direção Geral - Membro Titular

LUIZ EDUARDO CHAUVET
Gabinete da Direção Geral - Membro Suplente

THIAGO AUGUSTO KNOP MOTTA
Coordenação de Administração Geral - Membro Titular

ANDRÉ FABIANO DE OLIVEIRA LEAL
Coordenação de Administração Geral - Membro Suplente

GÉLCIO LUIZ QUINTELLA MENDES
Coordenação de Assistência - Membro Titular

RAFAEL TAVARES JOMAR
Coordenação de Assistência - Membro Suplente

TELMA DE ALMEIDA SOUZA
Coordenação de Ensino - Membro Titular

CAMILA BELO TAVARES FERREIRA
Coordenação de Ensino - Membro Suplente

GIOVANI ALVES CATA PRETA
Coordenação de Gestão de Pessoas - Membro Titular

FERNANDO ANDRÉ SANTANA DE SOUZA
Coordenação de Gestão de Pessoas - Membro Suplente

MARIANA LIMA BORONI MARTINS
Coordenação de Pesquisa - Membro Titular

NICOLE SCHERER
Coordenação de Pesquisa - Membro Suplente

LUCIANO AZEVEDO DE SOUZA
Coordenação de Prevenção e Vigilância - Membro Titular

IVO DE JESUS OLIVEIRA
Coordenação de Prevenção e Vigilância - Membro Suplente

ROBERTO DE ARAÚJO LIMA
Unidade I do Hospital do Câncer - Membro Titular

ÉLCIO NOVAES
Unidade I do Hospital do Câncer - Membro Suplente

RODOLFO ESPINOZA
Unidade II do Hospital do Câncer - Membro Titular

PAULO ALEXANDRE RIBEIRO MORA
Unidade II do Hospital do Câncer - Membro Suplente

PATRÍCIA CHAVES DE FREITAS CAMPOS JUCÁ
Unidade III do Hospital do Câncer - Membro Titular

SÉRGIO RODRIGUES FRAZÃO
Unidade III do Hospital do Câncer - Membro Suplente

JOÃO LUIZ GASPARELLI BARBOSA
Unidade IV do Hospital do Câncer - Membro Titular

CELSO BREDA MARCELLO
Unidade IV do Hospital do Câncer - Membro Suplente

THIAGO PETRA DA SILVA
Divisão de Planejamento - Membro Titular

GUSTAVO GUEDES FURTADO
Divisão de Planejamento - Membro Suplente

ANTÔNIO AUGUSTO GONÇALVES
Chefe do Serviço de Tecnologia da Informação - Coordenador Titular

CARLOS HENRIQUE FERNANDES MARTINS
Governança e Inovação em TIC - Coordenador Suplente

CARLOS HENRIQUE FERNANDES MARTINS
Governança e Inovação em TIC – Membro Titular
Serviço de Tecnologia da Informação

JORGE MARCOS FERNANDES
Governança e Inovação em TIC – Membro Titular
Serviço de Tecnologia da Informação

CID AJAY LIMA PIRES
Governança e Inovação em TIC – Membro Titular
Serviço de Tecnologia da Informação

ROBERTO LUIZ SILVA DOS SANTOS
Recursos Tecnológicos – Membro Titular
Serviço de Tecnologia da Informação

CEZAR CHENG
Desenvolvimento de Sistemas – Membro Titular
Serviço de Tecnologia da Informação

LUIZ ALBERTO PEREIRA AFONSO RIBEIRO
Desenvolvimento de Sistemas – Membro Suplente
Serviço de Tecnologia da Informação

CONTROLE DE DISTRIBUIÇÃO

Quanto ao grau de confidencialidade, este documento é classificado como **PÚBLICO.**

CONTROLE DE REVISÕES

Data	Revisão	Natureza da Alteração	Autor
02/10/2009	Original	Elaboração	Área de Recursos Tecnológicos - STI
31/03/2015	1ª Revisão	Atualização	Área de Recursos Tecnológicos - STI
20/05/2016	2ª Revisão	Atualização	Área de Recursos Tecnológicos - STI
10/07/2017	3ª Revisão	Atualização	Área de Gov. e Inovação em TIC - STI

FICHA TÉCNICA

Elaboração

ÁREA DE RECURSOS TECNOLÓGICOS - STI

Revisão

ÁREA DE GOVERNANÇA E INOVAÇÃO EM TIC

Aprovação

COMITÊ ESTRATÉGICO E GESTOR DE TECNOLOGIA DA INFORMAÇÃO (CEGTI)

LISTA DE SIGLAS

APF	Administração Pública Federal
CEGTI	Comitê Estratégico e Gestor de Tecnologia da Informação
ETIR	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais
CSIC	Comitê de Segurança da Informação e Comunicações
STI	Serviço de Tecnologia da Informação
DSIC	Departamento de Segurança da Informação e Comunicações do GSI – Gabinete de Segurança Institucional da Presidência da República
GCN	Gestão de Continuidade de Negócios
GRSIC	Gestão de Riscos em Segurança da Informação e Comunicações
GSIC	Gestor de Segurança da Informação e Comunicações
TIC	Tecnologia da Informação e Comunicações

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES

1.1 Apresentação

Esta POLÍTICA é uma declaração formal do INCA acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda;

Esta POLÍTICA norteará à implementação de medidas de proteção que deverão ser aplicadas a toda e qualquer informação, independentemente de onde ela se encontre, com vistas ao resguardo da imagem e dos objetivos institucionais do INCA; e

Suas orientações devem ser lidas, entendidas, seguidas e cumpridas em todos os níveis hierárquicos, para que seu maior patrimônio, a informação, tenha o grau de confidencialidade, integridade, disponibilidade e autenticidade exigidos.

1.2 Convenções

Para os fins do disposto nesta POLÍTICA a palavra INCA e a expressão *no âmbito do INCA, incluindo todas as Unidades Administrativas e Hospitalares* se equivalem.

Esta POLÍTICA, incluindo todos os DOCUMENTOS COMPLEMENTARES que a compõem serão doravante denominados simplesmente de POLÍTICA.

1.3 Comprometimento da Direção

O Serviço de Tecnologia da Informação (STI) declara que está comprometido em proteger os ATIVOS DE INFORMAÇÃO abrangidos nesta POLÍTICA, apoiando as metas e os princípios da Segurança da Informação, alinhada com os objetivos e estratégias do INCA.

1.4 Metas Globais

Esta POLÍTICA tem por meta as seguintes ações:

- A institucionalização e formalização clara dos princípios da Segurança da Informação através da divulgação desta POLÍTICA na Intranet e de ações de conscientização;
- Formalização das ações de prevenção, correção e de contingência contra INCIDENTES DE SEGURANÇA DA INFORMAÇÃO através das Normas ou Políticas de Segurança da Informação;

1.5 Público-alvo

Esta POLÍTICA aplica-se a todo AGENTE PÚBLICO 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 pública no INCA. Equipara-se a AGENTE PÚBLICO quem trabalha para empresa prestadora de serviços contratada ou conveniada para a execução de atividade, de qualquer natureza, desenvolvida no INCA.

1.6 Implantação

Esta POLÍTICA será implementada no INCA por meio de procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função desempenhada, bem como de vínculo empregatício ou prestação de serviço.

1.7 Publicação

Esta POLÍTICA encontra-se publicada e disponibilizada, pelo **SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO**, para acesso ou *download*, a qualquer tempo, a todos os usuários, de forma permanente nos canais de comunicação internos do INCA (inclusive na Intranet do INCA), disposta de maneira que seu conteúdo possa ser consultado a qualquer momento, sem prejuízo dos pertinentes meios oficiais de publicação aplicáveis, e no D.O.U.

1.8 Divulgação

A divulgação das regras e orientações desta POLÍTICA aplicadas aos usuários deve ser objeto de campanhas internas permanentes, disponibilização integral e contínua na Intranet, seminários de conscientização e quaisquer outros meios, como forma de ser criada uma cultura de Segurança da Informação dentro do INCA.

Em nenhuma hipótese será permitido o descumprimento desta POLÍTICA pela alegação de desconhecimento da mesma por parte do usuário.

2 ESCOPO

Esta POLÍTICA aplica-se, de forma mandatória e em sentido amplo, exclusivamente no âmbito do INCA, incluindo todas as suas Unidades Administrativas e Hospitalares, para todo o PÚBLICO-ALVO desta POLÍTICA.

2.1 Objetivos

Esta POLÍTICA objetiva, essencialmente:

- Fornecer diretrizes, critérios e suporte administrativos suficientes à implementação da Segurança da Informação e Comunicações.
- Estabelecer mecanismos e controles para assegurar o simultâneo acesso e a proteção dos dados, das informações e dos conhecimentos gerados, de propriedade do INCA ou sob a sua custódia.
- Nortear a definição, a elaboração e o detalhamento de normas e procedimentos específicos de Segurança da Informação, contemplando sua estrutura, suas diretrizes e suas

responsabilidades, bem como à implementação de controles e processos para seu atendimento.

- Servir como referência a questões de Segurança da Informação e, também, para auditoria, apuração e/ou avaliação de responsabilidades.
- Dar ciência a cada colaborador de que os ambientes, sistemas, computadores e redes internas do INCA poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

2.2 Vigência

Esta POLÍTICA tem prazo de validade indeterminado, portanto, sua vigência se estenderá desde sua publicação, gerando efeitos imediatos, até a edição de outro marco normativo que motive sua atualização ou a revogação.

3 CONCEITOS E DEFINIÇÕES

Para os fins de uniformidade dos procedimentos contidos nesta POLÍTICA, considera-se os conceitos e definições que constam do **GLOSSÁRIO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.

Abaixo alguns dos principais conceitos e definições:

Autenticidade	Propriedade que garante ter sido a informação produzida, expedida, modificada ou destruída por determinada pessoa física ou por determinado sistema, órgão ou entidade.
Ciclo de vida da informação	Caracterizado pelo ciclo formado desde sua criação ou obtenção, passando por seu uso, manipulação, compartilhamento, armazenamento, transporte e descarte.
Classificação da informação	Ato de se atribuir grau de sigilo a informação que requeira

	medidas especiais de salvaguarda e, por consequência, ao documento, material ou área que a contenha, utilize ou veicule.
Confidencialidade	Propriedade de que a informação não esteja disponível ou revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizados e credenciados.
Conformidade	Cumprimento da legislação, das normas e dos procedimentos relacionados ao tema a que se referes a conformidade.
Criptografia	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").
Disponibilidade	Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.
Gestão de riscos	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.
Incidente de segurança da informação e comunicação	Qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação.
Informação	Dados contextualizados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio (digital ou físico), suporte, formato ou forma (escrita, verbal ou de imagem).
Integridade	Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.
Política de Segurança da Informação e Comunicações - PoSIC	Documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.
Sigilo	Propriedade da informação que indica o impedimento de acesso à mesma por pessoa não autorizada.
Tratamento da Informação	Recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

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

4 REFERÊNCIAS LEGAIS E NORMATIVAS

Esta POLÍTICA obedecerá aos princípios constitucionais, administrativos e ao arcabouço legislativo vigente que rege a Administração Pública Federal.

As referências legais e normativas utilizadas como base para a elaboração desta POLÍTICA são, principalmente, as seguintes:

- "**Boas Práticas em Segurança da Informação**" elaborado pelo TCU;
- "**Guia de Referencia para a Segurança da Informação - Usuário Final**" elaborado pela SLTI/MPOG;
- **NBR/ISO/IEC 27001:2006** - Gestão de Segurança da Informação (GSI), que dispõe sobre os requisitos para Sistemas de Gestão de Segurança da Informação;
- **NBR/ISO/IEC 27002:2005** - Código de Prática para a GSI, que dispõe sobre as Diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização; e
- **Guia de Orientações ao Gestor em Segurança da Informação e Comunicações**, de Fevereiro de 2014, Versão 01, que dispõe sobre orientações e dicas referentes à implementação das ações de segurança da informação na APF, elaborado pelo DSIC do Gabinete de Segurança Institucional da Presidência da República.

4.1 Normativas

4.1.1 Instruções Normativas (IN)

- **IN GSI/PR nº 01**, de 13 de junho de 2008, que dispõe sobre a Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal (APF), direta e indireta, e dá outras providências;
- **IN GSI/PR nº 02**, de 5 de fevereiro de 2013, que dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal; e
- **IN GSI/PR nº 03**, de 6 de março de 2013, que 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.

4.1.2 Normas Complementares (NC)

- **NC nº 02/IN01/DSIC/GSIPR**, de 15 de Julho de 2014, que dispõe sobre a Metodologia de Gestão de Segurança da Informação e Comunicações;
- **NC nº 03/IN01/DSIC/GSIPR**, de 3 de Junho de 2009, que dispõe sobre as Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações na APF;
- **NC nº 04/IN01/DSIC/GSIPR**, de 15 de Fevereiro de 2013, que dispõe sobre as Diretrizes para Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC);
- **NC nº 05/IN01/DSIC/GSIPR**, de 14 de Agosto de 2009, que dispõe sobre as Diretrizes para a Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR);
- **NC nº 06/IN01/DSIC/GSIPR**, de 11 de Novembro de 2009, que dispõe sobre as Diretrizes para Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações;

- **NC nº 07/IN01/DSIC/GSIPR**, de 15 de Julho de 2014, que dispõe sobre as Diretrizes para a Implementação de Controles de Acesso relativos à Segurança da Informação e Comunicações;
- **NC nº 08/IN01/DSIC/GSIPR**, de 15 de Julho de 2014, que dispõe sobre as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais na APF;
- **NC nº 09/IN01/DSIC/GSIPR**, de 15 de Julho de 2014, que dispõe sobre as Orientações Específicas para o Uso de Recursos Criptográficos em Segurança da Informação e Comunicações, na APF;
- **NC nº 10/IN01/DSIC/GSIPR**, de 15 de Julho de 2014, que dispõe sobre as Diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), na APF;
- **NC nº 11/IN01/DSIC/GSIPR**, de 30 de Janeiro de 2012, que dispõe sobre as Diretrizes para a Avaliação de Conformidade nos aspectos relativos à Segurança da Informação e Comunicações;
- **NC nº 12/IN01/DSIC/GSIPR**, de 15 de Julho de 2014, que dispõe sobre as Diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) na APF;
- **NC nº 13/IN01/DSIC/GSIPR**, de 15 de Julho de 2014, que dispõe sobre as Diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) na APF;
- **NC nº 14/IN01/DSIC/GSIPR**, de 15 de Julho de 2014, que dispõe sobre as Diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), na APF;
- **NC nº 15/IN01/DSIC/GSIPR**, de 15 de Julho de 2014, que dispõe sobre as Diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, na APF;

- **NC nº 16/IN01/DSIC/GSIPR**, de 15 de Julho de 2014, que dispõe sobre as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta;
- **NC nº 17/IN01/DSIC/GSIPR**, de 15 de Julho de 2014, que dispõe sobre as Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) na APF;
- **NC nº 19/IN01/DSIC/GSIPR**, de 15 de Julho de 2014, que dispõe sobre os Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da APF;
- **NC nº 20/IN01/DSIC/GSIPR**, de 15 de Dezembro de 2014, que dispõe sobre as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da informação na APF; e
- **NC nº 21/IN01/DSIC/GSIPR**, de 15 de Julho de 2014, que dispõe sobre as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes na APF.

4.1.3 Decretos

- **Decreto nº 7.724**, de 16 de Maio de 2012, 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, que regulamenta os 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 3.505**, de 13 de Junho de 2000, que Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal; e

- **Decreto nº 3.587**, de 5 de Setembro de 2000, que estabelece normas para a Infraestrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov, e dá outras providências.

4.2 Leis

- **Art. 5º, incisos X e XIV, da Constituição Federal**, sobre a preservação dos direitos individuais;
- **Lei nº 10.180**, de 6 de fevereiro de 2001, parágrafo 3º do art. 26, nenhum processo, documento ou informação poderá ser sonegado aos servidores dos Sistemas de Contabilidade Federal e de Controle Interno do Poder Executivo Federal, no exercício das atribuições inerentes às atividades de registros contábeis, de auditoria, fiscalização e avaliação de gestão;
- **Incisos X e XXXIII do art. 5º, inciso II do § 3º do art. 37 da Constituição Federal**, sobre acesso à informação e direito à intimidade, à vida privada, à honra e à imagem;
- **Lei nº 12.527, de 18 de novembro de 2011**, que dispõe sobre o acesso à informação previsto na Constituição Federal;
- **Artigo 307 do Código Penal Brasileiro** (Decreto Lei 2.848/40) que pune a falsa identidade;
- **Lei n° 9.983, de 14 de julho de 2000**, que dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública; e
- **Lei n° 12.527, de 18 de novembro de 2011**, que 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.

4.3 Legislações Específicas

4.3.1 Acórdãos

- **Acórdão nº 1233/2012** – Plenário do TCU, que avalia se a gestão e o uso da tecnologia da informação estão de acordo com a legislação e aderentes às boas práticas de governança de TI.

5 PRINCÍPIOS

As ações de Segurança da Informação no INCA são norteadas pelos seguintes princípios:

- **Autenticidade**: Garantia de que a informação foi produzida, expedida, modificada ou destruída dentro de preceitos legais e normativos, por pessoa física, ou por sistema, órgão ou entidade vinculado ao INCA.
- **Celeridade**: As ações de Segurança da Informação e das Comunicações devem oferecer respostas rápidas a incidentes e falhas de segurança.
- **Confidencialidade**: Garantia de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada pelo INCA.
- **Conhecimento**: Os usuários devem conhecer e respeitar esta POLÍTICA, Normas Internas e demais regulamentações sobre Segurança da Informação do INCA.
- **Clareza**: As regras de Segurança da Informação e das Comunicações, documentação e comunicações devem ser precisas, concisas e de fácil entendimento.
- **Disponibilidade**: Garantia de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade vinculada ao INCA.

- **Ética**: Os direitos e interesses legítimos dos usuários devem ser preservados, sem comprometimento da Segurança da Informação e das Comunicações.
- **Integridade**: Garantia de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental, seja na sua origem, no trânsito e no seu destino.
- **Privacidade**: Garantia ao direito pessoal e coletivo, à intimidade e ao sigilo da correspondência e das comunicações individuais. Informação que fira o respeito à intimidade e à honra dos cidadãos não pode ser divulgada
- **Responsabilidade**: As responsabilidades primárias e finais pela segurança dos ativos do INCA e pelo cumprimento de processos de segurança devem ser claramente definidas.

Serão observados ainda, sem prejuízo das demais, os princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal, definidos no art. 37 da Constituição Federal.

6 DIRETRIZES GERAIS

Esta POLÍTICA é o instrumento que regula a proteção dos dados, das informações e dos conhecimentos do INCA, com vistas à garantia de integridade, disponibilidade, conformidade e confidencialidade;

Todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos para preservar a continuidade do negócio (regular exercício das funções institucionais);

O gerenciamento dos ATIVOS DE INFORMAÇÃO deverá observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua;

O cumprimento dessa POLÍTICA, bem como das normas complementares e procedimentos de Segurança da Informação no INCA será auditado periodicamente, de acordo com os critérios definidos pelo Comitê Estratégico e Gestor de Tecnologia da Informação (CEGTI) do INCA;

Devem ser criados e mantidos registros e procedimentos, como trilhas de auditoria que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas corporativos e REDE INTERNA DE COMUNICAÇÃO DE DADOS do INCA;

As medidas de proteção devem ser planejadas e os gastos na aplicação de controles devem ser compatíveis com valor do ativo protegido;

O acesso às informações, sistemas e instalações depende da apresentação de identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento;

Todo o PÚBLICO-ALVO desta POLÍTICA, e que sejam usuários dos ativos sigilosos, devem assinar Termo de Compromisso quanto ao sigilo dos dados, informações e conhecimentos do INCA;

As responsabilidades pela Segurança da Informação devem ser definidas nas descrições de cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos do INCA;

Todos os usuários devem ser conscientizados e treinados nos procedimentos de Segurança da Informação;

O controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa;

As informações custodiadas ou de propriedade do INCA devem ser classificadas quanto aos aspectos de sigilo, disponibilidade e integridade de forma implícita ou explícita e receber o nível de proteção condizente com sua classificação, conforme normas e legislação específica em vigor;

O gestor da informação é responsável por atribuir o nível de classificação das informações sob sua responsabilidade;

A classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte;

Todo agente público deve ser capaz de identificar a classificação atribuída a uma informação custodiada ou de propriedade do INCA e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas;

De forma a promover a gestão e fomentar os aspectos de Segurança da Informação, devem ser instituídas normas operacionais que estabeleçam procedimentos, processos e mecanismos que garantam o controle de acesso às informações, instalações e sistemas de informação;

O **COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** regulamentará, por meio de políticas, normas, processos, planos e/ou procedimentos específicos, os seguintes temas:

- Classificação e Tratamento da Informação;
- Tratamento de Incidentes de Segurança da Informação;
- Gestão de Riscos;
- Gestão de Continuidade de Negócio;
- Auditoria, Monitoramento e Controle de Recursos Tecnológicos.
- Controle de Acesso Físico e Lógico;
- Uso de Serviços de Internet;
- Uso de Serviços de e-mail Institucional;
- Uso de Serviços de Sistemas Legados;
- Uso Institucional de Redes Sociais;
- Uso Institucional de Computação na Nuvem;

Conforme necessidade e conveniência do INCA podem ser criados normativos sobre outros temas, que também farão parte desta POLÍTICA.

6.1 Propriedade das Informações

Todo informação gerada, adquirida, utilizada, armazenada ou que trafegue pela REDE INTERNA DE COMUNICAÇÃO DE DADOS é de propriedade do INCA, devendo ser protegida conforme estabelecido nesta POLÍTICA e nas regulamentações em vigor. Como também, todos os documentos e *softwares* produzidos por intermédio de seus colaboradores, durante o exercício de suas atividades profissionais, são de propriedade do INCA;

Toda e qualquer informação produzidas por USUÁRIOS INTERNOS e USUÁRIOS COLABORADORES, no exercício de suas funções, são patrimônio intelectual do INCA e não cabe a seus criadores qualquer forma de direito autoral;

Quando as informações forem produzidas por terceiros para uso exclusivo do INCA, um instrumento próprio obrigará os criadores ao sigilo permanente do conteúdo dos produtos;

É vedada a utilização das informações a que se refere o parágrafo anterior em quaisquer outros projetos ou atividades de uso diverso ao estabelecido pelo INCA, salvo com autorização formal específica emitida pelo PROPRIETÁRIO ou CUSTODIANTE DA INFORMAÇÃO;

As exceções devem ser explícitas e formalizadas em contrato entre as partes; e

Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo INCA devem observar, no que couber, o contido nos parágrafos anteriores e nos demais dispositivos integrantes desta POLÍTICA.

6.2 Tratamento da Informação

Toda informação é patrimônio do INCA, devendo ser protegida no acesso, tráfego, uso, armazenamento e descarte de acordo com sua classificação em graus de sigilo ao INCA, ao Estado e as pessoas;

Deve ser preservada a integridade, a confidencialidade, a disponibilidade, a autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo INCA;

O armazenamento e o processamento de informações baseado em computação em nuvem devem obedecer às diretrizes e normas complementares dessa POLÍTICA e a legislação brasileira, que deve prevalecer sobre qualquer outra, de modo a ter todas as garantias legais enquanto tomadora do serviço e proprietária das informações hospedadas na nuvem; e

A informação hospedada na estrutura do Datacenter do INCA deve fazer uso de solução de backup (cópia de segurança) com locais, frequência e demais diretrizes previstas em norma complementar.

6.3 Gestão de Incidentes em Redes Computacionais (GIRC)

Deverá ser instituídas políticas ou normas que estabeleçam os processos de gestão para tratamento e respostas a Incidentes de Segurança da Informação e Comunicações; e

Deve ser instituída e mantida a **EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS** (ETIR).

6.4 Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC)

Deverá ser instituídas políticas ou normas que estabeleçam os critérios à identificação, à avaliação e a implementação das medidas de proteção necessárias à mitigação ou à eliminação dos riscos à Segurança da Informação.

6.5 Gestão de Continuidade de Negócios (GCN)

Deverá ser instituídas políticas ou normas que estabeleçam os critérios para a redução dos impactos decorrentes de interrupção de serviço causada por desastre ou falha de segurança, por intermédio de ações de prevenção, resposta e recuperação.

6.6 Auditoria e Conformidade

Deverá ser instituídas políticas ou normas que estabeleçam os critérios para a realização de auditorias de conformidade quanto ao cumprimento da **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.

6.7 Controle de Acesso

O USUÁRIO receberá permissão de acesso físico e lógico apenas aos recursos necessários e indispensáveis ao desempenho de suas funções, definidas pela chefia imediata;

Todo USUÁRIO deverá possuir identificação pessoal e intransferível, qualificando-o, inequivocamente, como responsável por qualquer atividade desenvolvida sob essa identificação;

6.8 Uso dos Recursos Computacionais

O uso de RECURSOS COMPUTACIONAIS, disponibilizados pelo INCA, será regulamentado em norma específica visando estabelecer os critérios de manuseio, de prevenção e de responsabilidades sobre o uso destes, devendo ser aplicadas a todos os colaboradores que os utilizem;

São considerados RECURSOS COMPUTACIONAIS, dentre outros, os equipamentos (*hardware*), as instalações físicas, os programas de computador (*softwares*), os serviços que direta ou indiretamente estão relacionados ao processamento, ao armazenamento e à transmissão digital de dados, bem como, qualquer dado acessível por meio desses equipamentos ou programas de computador;

Os RECURSOS COMPUTACIONAIS de propriedade do INCA são fornecidos para uso corporativo, para os fins a que se destinam e no interesse da administração, estando sujeito o seu uso a monitoramento e auditora, e que os registros assim obtidos poderão ser utilizados para detecção de violações desta POLÍTICA e demais regulamentações em vigor;

É considerada imprópria a utilização dos RECURSOS COMPUTACIONAIS para propósitos não profissionais ou não autorizados;

A utilização dos RECURSOS COMPUTACIONAIS poderá ser monitorada, registrada e auditada com a finalidade de detectar divergências entre as normas que integram esta POLÍTICA e os registros de eventos monitorados, fornecendo evidências nos casos de Incidentes de Segurança da Informação; e

Os sistemas, as informações e os serviços utilizados pelos USUÁRIOS, no exercício de suas atividades, são de exclusiva propriedade do INCA, não podendo ser interpretados como de uso pessoal e devendo ser protegidos, segundo as diretrizes descritas nesta POLÍTICA e demais regulamentações em vigor.

6.9 Gestão de Ativos de Informação

O uso dos ATIVOS DE INFORMAÇÃO, disponibilizados pelo INCA, será definido em política específica visando estabelecer os critérios de manuseio, de prevenção e de responsabilidades sobre o uso destes, devendo ser aplicadas a todos os colaboradores que os utilizem;

Todos os ATIVOS DE INFORMAÇÃO deverão ser inventariados, classificados, documentados e sua documentação mantida atualizada, devendo ser revista mensalmente ou sempre que ocorrerem fatos que justifiquem sua atualização;

A documentação dos ATIVOS DE INFORMAÇÃO deverá conter informações que permitam sua recuperação após um desastre, incluído o tipo de ativo, formato, localização, informações sobre cópias de segurança e informações sobre a importância do ativo para a instituição.

6.10 Gestão de Mudança de Segurança da Informação e Comunicações (GMSIC)

Devem ser instituídas políticas ou normas que estabeleçam os critérios para evitar a ocorrência de mudanças mal sucedidas.

6.11 Termo de Confidencialidade

Termos de Confidencialidade ou de não divulgação quanto ao sigilo dos dados, informações e conhecimentos do INCA devem ser assinados por todos os USUÁRIOS como parte dos termos e condições iniciais de contratação, sendo usados como um alerta de que a informação é confidencial ou secreta;

Para colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente (que contenha o Termo de Confidencialidade), convém que seja exigida a assinatura do Termo de Confidencialidade, antes de ter acesso às instalações de processamento da informação; e

O Termo de Confidencialidade valerá durante todo o período do vínculo da força de trabalho com o INCA e adicionalmente terá duração de 5 (cinco) anos após o término deste vínculo. Em casos específicos, o prazo de validade do Acordo de Confidencialidade obedecerá a regulamentação que orienta a atividade específica, como: saúde, educação, propriedade intelectual, dentre outras.

7 PENALIDADES

O desrespeito, descumprimento ou violação de um ou mais itens constantes nesta POLÍTICA caracteriza infração funcional e resultará na suspensão temporária ou permanente de privilégios de acesso aos recursos de TIC, em penas e sanções legais impostas por meio de medidas administrativas sem prejuízo das demais medidas administrativas, cíveis e penais cabíveis, assegurados aos envolvidos o contraditório e a ampla defesa;

Todo o PÚBLICO-ALVO deverá comunicar imediatamente à ÁREA DE RECURSOS TECNOLÓGICOS – STI, quaisquer descumprimento desta POLÍTICA, de normas ou de procedimentos de Segurança da Informação, que porventura venha a tomar conhecimento ou chegue a presenciar; e

Os casos omissos e as dúvidas surgidas na aplicação dessa POLÍTICA serão submetidos ao COMITÊ ESTRATÉGICO E GESTOR DE TECNOLOGIA DA INFORMAÇÃO (CEGTI).

8 PAPÉIS E RESPONSABILIDADES

Deverá ser instituídas normas que estabeleçam o detalhamento das atribuições de responsabilidades específicas para os papéis envolvidos na segurança da informação.

9 REVISÃO E ATUALIZAÇÃO

Esta POLÍTICA e todos os seus DOCUMENTOS COMPLEMENTARES acessórios, serão tema de permanente acompanhamento e aperfeiçoamento, devendo ser revisados e atualizados periodicamente, no máximo, a cada 1 (um) ano, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata, incluindo o surgimento de novos requisitos corporativos, a edição de outro marco normativo, alterações na legislação pertinente ou de diretrizes políticas do Governo Federal que motivem sua atualização; e

Essas alterações podem decorrer de atualizações, migrações, implantação de novos produtos, novas demandas, aprendizado organizacional ou por necessidade de adaptação ao cenário imediato, entre outras modificações informadas pelas unidades de negócios para que o impacto apurado para cada processo esteja condizente com a realidade dos negócios.

10 DISPOSIÇÕES GERAIS

10.1 Denuncia de Vulnerabilidades ou de Ameaças

Vulnerabilidades e ameaças, identificadas por qualquer usuário, devem ser notificadas por e-mail à **ÁREA DE RECURSOS TECNOLÓGICOS;**

Por questões de segurança, o usuário denunciante deve manter a privacidade dos detalhes da vulnerabilidade ou das ameaças, até que uma solução seja divulgada;

A resposta à denuncia será fornecida em tempo hábil da seguinte forma:

- Reconhecimento da denúncia de vulnerabilidade ou de ameaça;
- Prazo para solucionar a questão; e
- Notificação de que a questão foi solucionada.

Somente a equipe de Segurança da Informação do INCA pode realizar pesquisas e testes de segurança.

11 DISPOSIÇÕES FINAIS

Assim como a ética, a Segurança da Informação deve ser entendida como parte fundamental da cultura interna do INCA. Ou seja, qualquer INCIDENTE DE SEGURANÇA DA INFORMAÇÃO subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição; e

Os casos omissos e as dúvidas com relação a esta POLÍTICA ou aos seus DOCUMENTOS COMPLEMENTARES devem ser submetidos ao **COMITÊ ESTRATÉGICO E GESTOR DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.

12 DOCUMENTOS COMPLEMENTARES (APÊNDICES)

Esta POLÍTICA é complementada por outros DOCUMENTOS COMPLEMENTARES, considerados partes integrantes e inseparáveis da mesma, que se fazem necessários para enfatizar outros aspectos, estabelecendo, na forma dos Anexos, as diretrizes complementares, as orientações, as regras, as metodologias, os procedimentos e as melhores práticas para as diversas disciplinas abordadas por esta POLÍTICA, sempre respeitando os limites impostos por ela e passando por aprovação junto aos participantes afetados; e

O INCA deve estruturar-se para a gestão de toda a documentação normativa relacionada à Segurança da Informação a ser elaborada ou revisada em seu âmbito. Estas documentações devem estar em consonância com esta POLÍTICA e os demais requisitos legais afetos ao tema.

12.1 Políticas

12.1.1 Política de Combate às Ameaças à Segurança da Informação e Comunicações (PoCASIC)

Dispõe sobre a implantação da Política de Combate às Ameaças à Segurança da Informação e Comunicações do INCA, definindo os objetivos e as diretrizes, nos aspectos relacionados à Segurança da Informação, consoante e complementar à POSIC do INCA.

12.1.2 Política de Controle de Acesso Físico e Lógico (PoCAFL)

Dispõe sobre a implantação da Política de Segurança de Acesso Físico às instalações envolvidas na guarda das informações do INCA e a Política de Segurança de Acesso Lógico, definindo os objetivos e as diretrizes, nos aspectos relacionados à Segurança da Informação, consoante e complementar à PoSIC do INCA.

12.1.3 Política de Gestão de Ativos de TI (PoGA)

Dispõe sobre a implantação da Política Corporativa de Gestão de Ativos de TI do INCA, definindo os objetivos e as diretrizes, nos aspectos relacionados à Segurança da Informação, consoante e complementar à PoSIC do INCA.

12.1.4 Política de Gestão de Continuidade de Negócios (PoGCN)

Define as diretrizes para a Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação.

12.1.5 Política de Gestão de Riscos de Segurança da Informação e Comunicações (PoGRSIC)

Dispõe sobre a implantação do Processo de Gestão de Riscos do INCA, definindo os objetivos e as diretrizes, nos aspectos relacionados à Segurança da Informação, consoante e complementar à PoSIC do INCA.

12.1.6 Política de Gestão de Incidentes de Redes Computacionais (PoGIRC)

Dispõe sobre a implantação da Política de Gestão de Incidentes em Rede Computacionais do INCA, definindo os objetivos e as diretrizes, nos aspectos relacionados à Segurança da Informação, consoante e complementar à PoSIC do INCA.

12.1.7 Política de Gestão de Mudanças de Segurança da Informação e Comunicações (PoGMSIC)

Dispõe sobre a implantação do Processo de Gestão de Mudanças do INCA, definindo os objetivos e as diretrizes, nos aspectos relacionados à Segurança da Informação, consoante e complementar à PoSIC do INCA.

12.1.8 Política para Desenvolvimento, Aquisição e Manutenção de Sistemas

Dispõe sobre a implantação da Política Corporativa de Desenvolvimento, Aquisição e Manutenção de Sistemas do INCA, definindo os objetivos e as diretrizes, nos aspectos relacionados à Segurança da Informação, consoante e complementar à PoSIC do INCA.

12.1.9 Política Permanente de Conscientização e Treinamento (PoPCT)

Dispõe sobre a implantação da Política Permanente de Conscientização e Treinamento do INCA, definindo os objetivos e as diretrizes, nos aspectos relacionados à Segurança da Informação, consoante e complementar à PoSIC do INCA.

12.1.10 Política de Auditoria de Segurança da Informação

Dispõe sobre a implantação da Política de Auditoria Segurança da Informação do INCA, definindo os objetivos e as diretrizes, nos aspectos relacionados à Segurança da Informação, consoante e complementar à PoSIC do INCA.

12.1.11 Política de Responsabilidades em Segurança da Informação e Comunicações (PoRSIC)

Dispõe sobre o detalhamento das atribuições de responsabilidades específicas relacionadas aos papeis envolvidos na Política Corporativa de Segurança da Informação do INCA, de modo que fiquem claramente explicitadas, consoante e complementar à PoSIC do INCA.

12.1.12 Política de Uso Institucional Seguro de Mídias Sociais (PoUISMS)

Dispõe sobre as orientações, as regras, as proibições e as responsabilidades mandatórias, direcionadas aos administradores dos perfis institucionais do INCA e aos demais colaboradores nas Mídias Sociais, associadas à conduta considerada adequada, assertiva e ética na geração de conteúdo, no relacionamento com o cidadão, no monitoramento das Mídias Sociais e na atuação em casos de gerenciamento de crise.

12.2 Normas

Contemplam as obrigações a serem seguidas de acordo com as diretrizes estabelecidas nesta POLÍTICA. Especificam, no plano tático, os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes desta POLÍTICA.

12.2.1 NSIC 01 – Concessão de Conta de Acesso Pessoal

Dispõe sobre as orientações, as regras, as responsabilidades e as proibições mandatórias associadas à disciplina de solicitação, de concessão e de revogação de contas de acesso pessoal para usuários, destinadas a utilização dos recursos computacionais, disponibilizados e mantidos pelo INCA para uso corporativo.

12.2.2 NSIC 02 – Uso dos Recursos Computacionais

Dispõe sobre as orientações, as regras, as responsabilidades e as proibições mandatórias associadas à disciplina e a utilização dos recursos computacionais, disponibilizados e mantidos pelo INCA para uso corporativo.

12.2.3 NSIC 03 – Classificação e Tratamento da Informação

Dispõe sobre as orientações, as regras e as responsabilidades mandatórias associadas à disciplina e a utilização da classificação, da reclassificação, da desclassificação, do tratamento e do descarte das informações produzidas ou custodiadas pelo INCA no exercício de suas competências, incluindo as autoridades classificadoras, os graus de confidencialidade, os prazos máximos de restrição de acesso e o procedimento para classificação das informações.

12.2.4 NSIC 04 – Datacenter

Dispõe sobre as orientações, as regras e as responsabilidades mandatórias associadas à disciplina e a utilização do *Datacenter* do INCA.

12.2.5 NSIC 05 – Gestão de Software Proprietário

Dispõe sobre as orientações, as regras e as responsabilidades mandatórias associadas à disciplina e a utilização do *software* proprietário dentro do INCA.

12.2.6 NSIC 06 – Gestão de Dados Corporativos

Dispõe sobre as orientações, as regras e as responsabilidades mandatórias associadas à disciplina, a utilização, a proteção e o acesso os dados corporativos do INCA.

12.2.7 NSIC 07 – Gestão de Cópias de Segurança

Dispõe sobre as orientações, as regras e as responsabilidades mandatórias associadas à disciplina para a salva guarda dos dados corporativos do INCA, visando manter a integridade e a disponibilidade da informação e dos recursos de processamento de informação.

12.2.8 NSIC 08 – Uso de Recursos Criptográficos

Dispõe sobre as orientações, as regras e as responsabilidades mandatórias associadas à disciplina e a utilização efetiva e adequada de criptografia na proteção da informação.

12.3 CSIC – Cartilha de Segurança da Informação e Comunicações

Dispõe sobre os conceitos básicos, as dicas, os cuidados e as boas práticas de Segurança da Informação a serem adotadas por todos no âmbito do INCA, com ênfase no esclarecimento dos usuários quanto aos perigos e as armadilhas existentes na *Internet* e como devem ser comportar para se protegerem de possíveis ameaças, principalmente para aqueles que desconhecem ou não tomam todas as precauções necessárias na hora de acessar a *Internet*.

12.4 GSIC – Glossário de Segurança da Informação e Comunicações

Dispõe sobre os termos, as palavras, os vocábulos e as expressões usadas no contexto técnico de Segurança da Informação, com ênfase no emprego combinado, a fim de contribuir para o entendimento comum do disposto na **POLÍTICA DE SEGURANAÇA DA INFORMAÇÃO** do INCA e nos seus DOCUMENTOS COMPLEMENTARES, bem como qualquer outra publicação referente à Segurança da Informação no âmbito do INCA.