INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PIAUÍ

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ

RESOLUÇÃO Nº 085/2018 - CONSELHO SUPERIOR

Aprova a Política de Segurança da Informação do IFPI.

O Presidente do Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, no uso de suas atribuições conferidas no Estatuto deste Instituto Federal, aprovado pela Resolução nº 001, de 31 de agosto de 2009, publicada no Diário Oficial da União, de 02 de setembro de 2009, considerando o Processo nº 23172.000662/2018-41, e, deliberação em reunião ordinária do dia 14 de novembro de 2018,

RESOLVE:

Art. 1º Aprovar a Política de Segurança da Informação no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Piauí – IFPI, conforme anexo.

Art. 2º Esta Resolução entrará em vigor na data de sua publicação

Teresina-PI, 14 de novembro de 2018.

Paulo Henrique Gomes de Lima
Presidente

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PIAUÍ

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO IFPI

APROVADO PELA RESOLUÇÃO Nº 085/2018 – CONSELHO SUPERIOR

CAPÍTULO I
DO ESCOPO

Art. 1º Nesta seção são apresentados o contexto, objetivos e a abrangência da Política de Segurança da Informação e Comunicações (POSIC), no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Piauí (IFPI).

SEÇÃO I
Da Contextualização

Parágrafo Único. De acordo com a Norma Complementar (NC) nº 03/IN01/DSIC/GSIPR, a POSIC é o documento formal que estabelece diretrizes, critérios e procedimentos, o qual busca proteger os ativos de informação e a gestão da Segurança da Informação (SI) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Segundo a ABNT NBR ISO/IEC 27002 (2005), SI é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. Dessa forma, a SI visa proteger a informação de ameaças relacionadas à sua integridade, disponibilidade e confidencialidade, a fim de evitar ou minimizar os riscos, relacionados ao negócio. Mediante o exposto, este documento trata da POSIC do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, o qual busca atender aos itens contemplados no capítulo III (Referências Legais e Normativas), além de garantir a proteção dos ativos da instituição.

SEÇÃO II
Dos Objetivos Gerais

Art. 2º Segundo o Decreto nº 3.505/2000, em seu artigo 3º, define-se os seguintes objetivos:

I. dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;

II. eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;

III. promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em Segurança da Informação;

IV. estabelecer normas jurídicas necessárias à efetiva implementação da Segurança da Informação;

V. promover as ações necessárias à implementação e manutenção da Segurança da Informação;

VI. promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de Segurança da Informação;

VII. promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a Segurança da Informação; e

VIII. assegurar a interoperabilidade entre os sistemas de Segurança da Informação.

SEÇÃO III
Dos Objetivos Específicos

Art. 3º A Diretoria de Tecnologia da Informação (DTI) do IFPI estipula, ainda, os seguintes objetivos para POSIC:

I. estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, *internet*, telecomunicações e correio eletrônico institucional no IFPI;

II. constituir, determinar ou reorganizar as funções e atribuições do grupo responsável pela Segurança da Informação no âmbito institucional; e

III. viabilizar a confecção de mecanismos de controle, além de promover a otimização dos recursos e investimentos em Tecnologia da Informação (TI).

SEÇÃO IV
Da Abrangência

Art. 4º O conjunto de regras e metas estabelecidas nesta POSIC será aplicada a todos os níveis da instituição, sendo eles: Estratégico, Tático e Operacional. É importante frisar que este documento dá ciência à comunidade interna do IFPI, bem como, à externa, sobre as diretrizes que irão balizar o uso dos ambientes, sistemas, recursos computacionais e redes informacionais em todos os seus campi e reitoria.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 5º Para efeitos da POSIC e das normas vinculadas a ela, define-se:

I. ação de evitar o risco: decisão de não se envolver ou agir de forma a se retirar de uma situação de risco (NBR ISO/IEC 27005, 2008);

II. aceitar/reter o risco: aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco (NBR ISO/IEC 27005, 2008);

III. ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ISO/IEC 27000, 2014);

IV. ativo: qualquer coisa que tenha valor para a organização. (NBR ISO/IEC 27002, 2005);

V. insumos críticos de Tecnologia da Informação: abrange todos os ativos de Tecnologia da Informação indispensáveis às atividades alvo do IFPI, conforme deve estabelecer as ações estratégicas da instituição;

VI. fonte de conhecimento: dados, informações e conhecimentos obtidos, gerados, tratados e/ou armazenados no âmbito do IFPI. Exemplos desses ativos: base de dados, arquivos, acervo bibliográfico, registros acadêmicos, contratos, acordos, documentação de sistema, informações sobre pesquisa e extensão, manuais de usuário, material de treinamento, projetos técnicos de infraestrutura elétrica e de construção civil procedimentos e planos institucionais, processos de trabalho e outros;

VII. insumos de Tecnologia da Informação: contempla os ativos físicos e de software, os quais permitem o armazenamento, a transmissão e processamento das informações. Dentre esses, pode-se destacar os aplicativos, sistemas, ferramentas de desenvolvimento e utilitários. Os

insumos físicos compreendem o pátio de equipamentos computacionais do IFPI, o qual é formado por servidores, computadores fixos e móveis, além dos dispositivos de intercomunicação (roteadores, *switchs*, pontos de acesso e outros);

VIII. responsável legal: reitor, pró-reitores, diretores ou coordenadores em geral responsáveis pela(s) informação(ões) que esteja(m) atrelada(s) ao exercício dos cargos e funções supracitadas, bem como aos seus subordinados;

IX. controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de garantir que os acessos aos ativos só ocorrerão após autorização e serão restritos, baseados nos requisitos de segurança e nas atividades do usuário. (ISO/IEC 27000, 2014);

X. contas de acesso: formadas por uma identificação única, concedida de forma pessoal e intransferível a uma pessoa, e por um método de autenticação. Esse par de informações habilita o seu dono a acessar equipamentos, sistemas e aplicações específicas, áreas restritas, de acordo com o perfil pré-definido;

XI. nível da Informação: identificação do nível de proteção requerido pela mesma, atribuído pelo responsável legal;

XII. mitigar/reduzir o risco: efetuar ações que reduzam a probabilidade, consequências negativas, ou ambas, associadas a um risco (NBR ISO/IEC 27005, 2008);

XIII. política: intenções e diretrizes da organização, formalmente expressas pela direção da Instituição (ISO/IEC 27000, 2014);

XIV. risco: efeito da incerteza sobre os objetivos de segurança da informação e é associado com o potencial de que as ameaças irão explorar vulnerabilidades

de um ativo de informação ou grupo de ativos de informação e, assim, causar danos a uma organização (ISO/IEC 27000, 2014);

XV. segurança da Informação: preservação da confidencialidade, da integridade e da disponibilidade das informações (ISO/IEC 27000, 2014);

XVI. vulnerabilidade: fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças (ISO/IEC 27000, 2014).

CAPÍTULO III
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 6º A DTI fundamenta a presente POSIC, através do conjunto de decretos, instruções normativas e normas complementares apresentados nesta seção, conforme descrito abaixo:

I. 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;

II. Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal (APF), direta e indireta, e dá outras providências;

III. Norma Complementar (NC) nº 02/IN01/DSIC/GSIPR – Metodologia de Gestão de Segurança da Informação e Comunicações;

IV. NC nº 03/IN01/DSIC/GSIPR – Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações na APF;

V. NC nº 04/IN01/DSIC/GSIPR – Gestão de Riscos de Segurança da Informação e Comunicações na APF;

VI. NC nº 05/IN01/DSIC/GSIPR (revisada em 2013) – Criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais na APF;

VII. NC nº 06/IN01/DSIC/GSIPR – Gestão de Continuidade de Negócios na APF;

VIII. NC nº 07/IN01/DSIC/GSIPR (revisada em 2014) – Implementação de Controles de Acesso na APF;

IX. NC nº 08/IN01/DSIC/GSIPR – Gerenciamento de Incidentes em Redes Computacionais na APF;

X. NC nº 09/IN01/DSIC/GSIPR (revisada em 2014) – Uso de Recursos Criptográficos na APF;

XI. NC nº 10/IN01/DSIC/GSIPR – Inventário e Mapeamento de Ativos de Informação na APF;

XII. NC nº 11/IN01/DSIC/GSIPR – Avaliação de conformidade na APF;

XIII. NC nº 12/IN01/DSIC/GSIPR – Dispositivos Móveis na APF;

XIV. NC nº 13/IN01/DSIC/GSIPR – Gestão de Mudanças na APF;

XV. NC nº 14/IN01/DSIC/GSIPR – Tecnologias de Computação em Nuvem na APF;

XVI. NC nº 15/IN01/DSIC/GSIPR – Uso de Redes Sociais na APF;

XVII. NC nº 16/IN01/DSIC/GSIPR – Desenvolvimento e Obtenção de Software Seguro na APF;

XVIII. NC nº 17/IN01/DSIC/GSIPR – Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações na APF;

XIX. NC nº 18/IN01/DSIC/GSIPR – Atividades de Ensino em Segurança da Informação e Comunicações na APF;

XX. NC nº 19/IN01/DSIC/GSIPR – Padrões Mínimos de Segurança da Informação e Comunicações na APF;

XXI. NC nº 20/IN01/DSIC/GSIPR – Instituição do Processo de Tratamento da Informação na APF;

XXII. NC nº 21/IN01/DSIC/GSIPR – Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes na APF.

XXIII. Decreto nº 7.579/2011 – Dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal;

XXIV. Aplicação de boas práticas em Tecnologia da Informação recomendadas pela Corte de Contas da União (TCU) e assinaladas na edição dos Acórdãos 1603/2008 - Plenário, 71/2007 – Plenário, 1092/2007-Plenário e 2023/2005 – Plenário;

XXV. ABNT NBR ISO/IEC 27001:2006 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gerência da Segurança da Informação – Requisitos;

XXVI. ABNT NBR ISO/IEC 27002:2005 – Código de Prática para a Gestão de Segurança da Informação;

XXVII. 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;

XXVIII. Portaria Interministerial nº 140, de 16 de março de 2006, que disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores - internet e dá outras providências;

XXIX. Acórdão do Tribunal de Contas da União nº 461/2004, de 28 de abril de 2004, que dispõe sobre a análise regular de arquivos logs com utilização, sempre que possível, de softwares utilitários específicos, para monitoramento do uso dos sistemas; e

XXX. ABNT NBR ISO/IEC 27005:2011 – Tecnologia da informação - técnicas de segurança - código de prática para a gestão de segurança da informação.

CAPÍTULO IV
DOS PRINCÍPIOS

Art. 7º A DTI define como princípios da POSIC proposta, os seguintes itens abaixo:

I. confidencialidade: somente pessoas devidamente autorizadas pela organização devem ter acesso à informação;
II. integridade: somente operações de alteração, supressão e adição autorizadas pela organização devem ser realizadas nas informações;
III. disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado;
IV. autenticidade: princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação;
V. criticidade: princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição;
VI. não-repúdio: garantia que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação.

Parágrafo Único. Toda informação produzida ou recebida pelos membros da comunidade interna ou externa do IFPI, como docentes, técnicos administrativos, discentes, visitantes, colaboradores, fornecedores e prestadores de serviço, em resultado da função exercida e/ou atividade profissional contratada, pertence ao IFPI. As exceções devem ser explícitas e formalizadas entre as partes.

CAPÍTULO V
DAS DIRETRIZES GERAIS

Art. 8º São diretrizes gerais da Política de Segurança da Informação e Comunicações do IFPI:

I. estar alinhada aos objetivos estratégicos, processos, requisitos legais e estrutura do IFPI, bem como ao Plano Diretor de Tecnologia da Informação;
II. estabelecer medidas e procedimentos para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
III. observar as boas práticas e procedimentos de Segurança da Informação e Comunicação recomendados por órgãos e entidades responsáveis pelo estabelecimento de padrões.

Art. 9º É dever de todos os usuários da informação zelar pela Segurança da Informação e Comunicação.

CAPÍTULO VI
DAS DIRETRIZES ESPECÍFICAS

Art. 10 A DTI define como diretrizes específicas da POSIC, cada uma das seguintes disciplinas relacionadas abaixo:

I. tratamento da Informação;
II. tratamento de Incidentes de Rede;
III. gestão de riscos;
IV. gestão de continuidade;
V. auditoria e conformidade;
VI. controle de acesso;
VII. uso de *e-mail*;

VIII. acesso à Internet;

IX. gestão de ativos de Informação;

X. segurança Física e do Ambiente;

XI. segurança em Recursos Humanos;

XII. gestão de Operações e Comunicações;

XIII. criptografia;

XIV. desenvolvimento Seguro de *Software*.

SEÇÃO I
Do Tratamento da Informação

Art. 11 As informações existentes no âmbito do IFPI apresentam diferentes níveis de confidencialidade e devem ser classificadas de acordo com a legislação vigente.

Art.12 Normas complementares estabelecerão procedimentos que visem garantir a integridade, a confidencialidade e a disponibilidade das informações, incluindo procedimentos para a criação, manutenção e verificação dos ativos de informação e de suas cópias de segurança.

SEÇÃO II

Do Tratamento de Incidentes de Rede

Art.13 O IFPI deve manter equipe para tratamento e resposta a incidentes de segurança da informação, de modo que esta seja capaz de extrair informações e propor medidas que corrijam a falha que ocasionou o incidente.

SEÇÃO III

Da Gestão de Risco

Art.14 O IFPI deve adotar processo de Gestão de Risco contínuo, de modo a ser atualizado periodicamente, tratando novos riscos e estabelecendo estratégias para proteção dos seus ativos de informação.

SEÇÃO IV

Da Gestão da Continuidade

Art. 15 A DTI irá implementar plano de continuidade de negócios, a fim de evitar interrupções nos principais sistemas de informação do IFPI.

SEÇÃO V
Da Auditoria

Art. 16 Todos os ativos de informação no âmbito do IFPI são passíveis de auditoria, segundo estabelecido por norma específica.

SEÇÃO VI
Do Controle de Acesso

Art. 17 A DTI é responsável por determinar mecanismos de controle de acesso físico ao Data Center, bem como mecanismos de controle lógico aos serviços e sistemas do IFPI.

Art.18 As credenciais de acesso aos ativos de informação do IFPI são individuais e intransferíveis.

SEÇÃO VII
Do Uso de E-mail

Art. 19 Todo servidor do IFPI deverá ter conta de e-mail institucional.

Art. 20 O e-mail Institucional será utilizado como forma de comunicação oficial entre os(as) servidores(as) da Instituição, sendo considerado como documento comprobatório, podendo ser utilizado para fins de recebimento de ofícios, memorandos, notificações, solicitações, informativos, convocações, intimações, convites, dentre outros documentos oficiais ou similares.

Art. 21 É dever do(a) servidor(a) verificar diariamente sua caixa de entrada do correio eletrônico institucional.

SEÇÃO VIII
Do Acesso à Internet

Art. 22 Toda a comunidade do IFPI tem o direito de acesso à internet, conforme as normas específicas, com utilização para fins acadêmicos, científicos ou administrativos, portanto, o mesmo é passível de auditoria.

Art. 23 O acesso à Internet no âmbito do IFPI será concedido por meio de autenticação do usuário.

Art. 24 A DTI é responsável por implementar mecanismo de autenticação que determine a titularidade de todos os acessos à Internet dentro da rede do IFPI.

SEÇÃO IX
Da Gestão de Ativos da Informação

Art. 25 Os ativos da informação devem ser inventariados, classificados e documentados e revisados sempre que necessário.

Art. 26 Os ativos de cada setor ficarão sob responsabilidade de seu respectivo gestor, este ficará responsável por sua documentação e manutenção.

SEÇÃO X
Da Segurança Física e Do Ambiente

Art. 27 De acordo com a legislação vigente, a DTI, mediante norma específica, irá regulamentar o controle de acesso ao Data Center do IFPI, bem como especificar os requisitos mínimos para instalações físicas do mesmo.

SEÇÃO XI
Da Segurança em Recursos Humanos

Art. 28 O processo de gestão de segurança em recursos humanos será regulamentado por norma específica de acordo com a legislação vigente.

SEÇÃO XII
Da Gestão de Operações e Comunicações

Art. 29 A DTI deverá propor, com a participação do CSIC, processo de Gestão de Operações e Comunicações por meio de norma complementar.

SEÇÃO XIII
Da Criptografia

Art. 30 Caso julgue necessário, as informações pertencentes ao IFPI consideradas como sigilosas poderão ser criptografadas.

Art. 31 A DTI irá, mediante regulamentação específica, estabelecer procedimento para criptografia de informações no âmbito do IFPI.

SEÇÃO XIV
Do Desenvolvimento Seguro de Software

Art. 32 A equipe de desenvolvimento de sistemas do IFPI (DSI) deverá passar por contínuo processo de capacitação, especialmente em boas práticas de desenvolvimento seguro.

Art. 33 Deve constar no PDTI do IFPI calendário de capacitações para a equipe de TI.

CAPÍTULO VII
DAS PENALIDADES

Art. 34 Reserva-se o direito à DTI de monitorar o tráfego efetuado através das suas redes de comunicação, incluindo o acesso à Internet. Qualquer descumprimento desta Política será tratado como incidente de segurança e poderá implicar na aplicação de sanções administrativas, cíveis e penais de acordo com a legislação vigente ou em qualquer outra legislação que regule ou venha regular a matéria.

Art. 35 Uma vez detectada violação da política, determina-se a sua causa: negligência, acidente, erro ou por ação previamente determinada, ignorando a política estabelecida, técnicos da DTI identificarão os usuários - doravante chamados de infratores.

Art. 36 Se for provado que o usuário violou os preceitos existentes nesta Política e nos documentos elaborados a partir dela, a Controladoria/Corregedoria ficará responsável por sugerir a abertura de Processo Administrativo Disciplinar, com o objetivo de apurar o desvio de conduta do(a) servidor(a), garantindo o contraditório e a ampla defesa.

CAPÍTULO VIII
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 37 A estrutura para a Gestão de Segurança da Informação e Comunicações no IFPI é composto pelo (a):

I. gestor de Segurança da Informação e Comunicações;
II. comitê de Segurança da Informação e Comunicações (CSIC);
III. equipe de Tratamento de Incidentes em Segurança da Informação (ETISI).

Art. 38 Compete ao Gestor de Segurança da Informação e Comunicações:

I. promover cultura de segurança da informação e comunicações;
II. acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
III. propor recursos necessários às ações de segurança da informação e comunicações;
IV. coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
V. realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
VI. manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações;
VII. propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do órgão ou entidade da APF.

Art. 39 Compete ao Comitê de Segurança da Informação e Comunicações:

I. assessorar na implementação das ações de segurança da informação e comunicações no órgão ou entidade da APF;
II. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações; e
III. propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.

Art. 40 Compete ao Reitor, Pró-Reitores, Diretores, Chefes de Departamento e Coordenadores do IFPI:

I. viabilizar o acesso ao conjunto de documentos atualizados que compõem a POSIC aos seus subordinados;
II. adotar as diretrizes da POSIC aos processos de trabalho referentes a sua gestão; e
III. exigir o cumprimento da POSIC pelos servidores sob sua gestão.

Art. 41 Compete ao usuário:

I. conhecer e cumprir as diretrizes e normas desta POSIC;
II. responsabilizar-se por todo e qualquer acesso aos ativos de informação do IFPI, bem como pelos efeitos desse acesso, realizado por meio de seu código de identificação;
III. comunicar o mais breve possível os incidentes de segurança da informação, por ele conhecido, ao setor responsável;
IV. colaborar com as investigações de incidentes, envolvendo direta ou indiretamente sua área.

Art. 42 O IFPI constituirá Equipe de Tratamento de Incidentes em Segurança da Informação (ETISI), seu documento de constituição adotará as recomendações da Norma Complementar nº 05 /IN01/DSIC/GSI/PR, de 14 de agosto de 2009.

CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS

Art. 43 Todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 03 (três) anos.

Art. 44 Os casos omissos serão julgados pelo Comitê de Segurança da Informação e Comunicações.

Art. 45 Esta norma entra em vigor na data de sua publicação.

Teresina (PI), 14 de novembro de 2018.

Paulo Henrique Gomes de Lima
Presidente

Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICA. NBR ISO/IEC 27001. Tecnologia da informação - técnicas de segurança - código de prática para gestão da informação. Rio de Janeiro, ABNT, 2005. Disponível em: <http://www.abnt.org.br/normalizacao/lista-de-publicacoes/abnt>. Acesso em: 12 jul. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002. Tecnologia da informação - técnicas de segurança - código de prática para a gestão de segurança da informação. Rio de Janeiro, ABNT, 2005. Disponível em: <http://www.abnt.org.br/normalizacao/lista-de-publicacoes/abnt>. Acesso em: 12 jul. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002. Tecnologia da informação - técnicas de segurança - código de prática para a gestão de segurança da informação. Rio de Janeiro, ABNT, 2013. Disponível em: <http://www.abnt.org.br/normalizacao/lista-de-publicacoes/abnt>. Acesso em: 12 jul. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27005. Tecnologia da informação - técnicas de segurança - código de prática para a gestão de segurança da informação. Rio de Janeiro, ABNT, 2008. Disponível em: <http://www.abnt.org.br/normalizacao/lista-de-publicacoes/abnt>. Acesso em: 12 jul. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27005. Tecnologia da informação - técnicas de segurança - código de prática para a gestão de segurança da informação. Rio de Janeiro, ABNT, 2011. Disponível em: <http://www.abnt.org.br/normalizacao/lista-de-publicacoes/abnt>. Acesso em: 12 jul. 2018.

Lei nº 8.112, de 11 de dezembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. Diário Oficial da República Federativa do Brasil, Brasília, DF, 12 de dez. 1990. Disponível em: <http://www.presidencia.gov.br/legislacao>. Acesso em: 12 jul. 2018.

Lei nº 9.983, de 14 de julho de 2000. Altera o Decreto-lei nº 2.848, de 7 de dezembro de 1940. Código Penal e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 17 jul. de 2000. Disponível em: <http://www.presidencia.gov.br/legislacao>. Acesso em: 12 jul. 2018.

Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: <http://www.presidencia.gov.br/legislacao>. Acesso em: 12 jul. 2018.