MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PARÁ
CONSELHO SUPERIOR

Fls nº 64

RESOLUÇÃO Nº 023/2018-CONSUP DE 08 DE FEVEREIRO DE 2018

Aprova, *"ad referendum"*, a Política de Segurança da Informação e Comunicação do Instituto Federal de Educação, Ciência e Tecnologia do Pará - IFPA.

O PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PARÁ, nomeado através do Decreto Presidencial de 02 de abril de 2015, publicado no D.O.U. de 06 de abril de 2015, seção 2, página 1, empossado no dia 28.04.2015, no uso de suas atribuições legais, e considerando o disposto no processo administrativo nº 23051.025418/2017-86, o qual destaca:

I – a responsabilidade da Alta Administração do IFPA para a definição de uma política de segurança da informação e comunicação, cujo objetivo seja a redução de riscos, a conformidade com as leis e regulamentos existentes e a garantia da continuidade operacional, da integridade e da confidencialidade da informação;

II – que a informação no âmbito do IFPA é essencial para viabilizar o alcance dos objetivos e metas institucionais e a interconectividade, expondo a informação a um crescente número de usuários e a uma grande variedade de ameaças e vulnerabilidades;

III – que a Segurança da Informação, e todos os seus processos, não está somente vinculada à segurança relacionada à Tecnologia da Informação;

IV – que a NBR ISSO/IEC 27002:2005, norma que estabelece boas práticas em segurança da informação, recomenda revisões periódicas da política de segurança da informação das instituições;

RESOLVE:

Art. 1º Aprovar, *"ad referendum"*, a Política de Segurança da Informação e Comunicação (PSIC) do Instituto Federal de Educação, Ciência e Tecnologia do Pará – IFPA, que observará os princípios, objetivos e diretrizes estabelecidos nesta Resolução.

CAPÍTULO I
CONCEITOS E DEFINIÇÕES

Art. 2º No âmbito desta PSIC, considera-se:

I – agente responsável pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): servidor da área de Tecnologia da Informação do IFPA ocupante de cargo efetivo incumbido de chefiar e gerenciar a ETIR;

II – ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

III – ativos de informação: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV – autenticidade: propriedade de que a informação foi produzidas, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

V – capacitação em Segurança da Informação e Comunicação (SIC): proporciona aos servidores o conhecimento do que é segurança da informação e comunicação, aplicando em sua rotina pessoal e profissional, servindo como multiplicador do tema e aplicando os conceitos e procedimentos na organização como gestor de SIC;

VI – classificação da informação: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;

VII - Comitê Gestor de Segurança da Informação (CGSI): colegiado de caráter deliberativo responsável pela normatização e supervisão da segurança da informação e comunicação no âmbito do IFPA;

VIII – confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados ou credenciados;

IX – conscientização em SIC: conhecimento que o servidor precisa ter sobre segurança da informação e comunicação, aplicando-o em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema;

X – controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XI – CTIR.GOV: Centro de Treinamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República (DSIC/CSI/PR);

XII – custodiantes do ativo de informação: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

XIII – disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade;

XIV – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): colegiado com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores no âmbito do IFPA;

XV – especialização em SIC: conhecimento que o servidor precisa ter sobre segurança da informação e comunicação, aplicando-o em sua rotina pessoal e profissional, que lhe permita ser multiplicador sobre o tema, aplicando os conceitos e procedimentos na organização como gestor de SIC e tornando-se referência na pesquisa de novas soluções e modelos de SIC;

XVI – Estrutura de GSIC: grupo responsável pela gestão e execução da SIC;

XVII – gestão de ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

XVIII – gestão de continuidade dos negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem, fornecendo uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

XIX – gerenciamento de operações e comunicações: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suportam, satisfazendo os acordos de níveis de serviço;

XX – gestão de riscos de segurança da informação e comunicação (GRSIC): conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiras envolvidos;

XXI – gestão de segurança da informação e comunicação (GSIC): ações e métodos que viam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, ao âmbito da tecnologia da informação e comunicação;

XXII – gestor dos ativos de informação: unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;

XXIII – Gestor de SIC: servidor nomeado pelo Reitor para ser o responsável pela gestão de segurança da informação e comunicação no âmbito do IFPA;

XXIV – incidente de SIC: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XXV – informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XXVI – infraestrutura de TI: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, softwares, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica;

XXVII – integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXVIII – violação de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e da comunicação;

XXIX – recursos criptográficos: sistemas, programas, processos e equipamentos isolados ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

XXX – risco de SIC: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos por parte de uma ou mais ameaças com impacto negativo no negócio da organização;

XXXI – segurança física do ambiente: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;

XXXII – sensibilização em SIC: conhecimento que o servidor precisa ter sobre segurança da informação e comunicação, aplicando-o em sua rotina pessoal e profissional;

XXXIII – sistema estruturante: conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente;

XXXIV – terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao IFPA;

XXXV – tratamento de incidentes: 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;

XXXVI – tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XXXVII – vulnerabilidade da unidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças; e

XXXVIII – gestor de unidade: chefe de determinado setor, diretoria, departamento, pró-reitoria ou diretoria de Campus.

CAPÍTULO II
ESCOPO
Seção I
Objetivos da Política de Segurança da Informação e Comunicação

Art. 3º A PSIC é uma declaração formal que objetiva a preservação da confidencialidade, da integridade, da disponibilidade e autenticidade das informações produzidas ou custodiadas pelo IFPA.

Art. 4º O IFPA deve observar as diretrizes, normas, procedimentos, mecanismos, competências e responsabilidades estabelecidos nesta PSIC.

Art. 5º Integram também a PSIC as normas e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

Art. 6º As diretrizes de Segurança da Informação e Comunicação (SIC) devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e estrutura organizacional do IFPA.

Art. 7º A Gestão de Segurança da Informação e Comunicação (GSIC) deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de SIC.

Seção II
Abrangência

Art. 8º As diretrizes, normas complementares e manuais de procedimentos da PSIC do IFPA aplicam-se a servidores, prestadoras de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, execute atividades vinculadas a este Instituto.

Parágrafo único. Todos são responsáveis e devem estar comprometidos com a segurança da informação e comunicação.

Art. 9º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo IFPA devem atender a esta PSIC.

Art. 10. Esta política também se aplica, no que couber, ao relacionamento do IFPA com outros órgãos e entidades públicas e privadas.

CAPÍTULO III
PRINCÍPIOS

Art. 11. A PSIC deve obedecer aos princípios constitucionais, administrativos e ao arcabouço legislativo vigente que regem a Administração Pública Federal.

CAPÍTULO IV
DIRETRIZES GERAIS

Art. 12. O cumprimento desta política de segurança e de suas normas complementares deverá ser avaliado periodicamente por meio de verificações de conformidade realizadas por grupo de trabalho formalmente constituído pelo Comitê Gestor de Segurança da Informação (CGSI) do IFPA, buscando a certificação do cumprimento dos requisitos de segurança da informação e a garantia de cláusula de responsabilidade e sigilo.

Art. 13. Cabe ao CGSI instituir programas permanentes e regulares de conscientização, sensibilização e capacitação em SIC, buscando parcerias com outros órgãos e entidades.

Art. 14. Os órgãos e entidades do Sistema de Administração dos Recursos de Informação e Informática (SISP) podem adotar ou utilizar esta PSIC e suas normas complementares como modelos de referência para elaboração dos seus documentos.

Art. 15. Fica instituída a Estrutura de GSIC do IFPA, coposta pelo Comitê Gestor de Segurança da Informação (CGSI) e pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), os quais serão solidariamente responsáveis pelas seguintes atividades:

I – executar os processos de segurança da informação e comunicação;

II – desenvolver, implementar e monitorar estratégias de segurança que atendam aos objetivos estratégicos do IFPA;

III – avaliar, selecionar, administrar e monitorar controles apropriados de proteção dos ativos de informação;

IV – desenvolver ações de conscientização dos usuários a respeito da implementação desses controles;

V – fornecer subsídios visando à verificação de conformidade de segurança e comunicação; e

VI – promover a melhoria contínua dos processos e controles de GSIC.

Parágrafo único. A Estrutura de GSIC deve definir um Plano de SIC para o IFPA.

Art. 16. As unidades administrativas que contam com corpo técnico e infraestrutura de tecnologia da informação próprios possuem autonomia para sua estrutura de GSIC, desde que submetidas e aderentes a esta PSIC.

Art. 17. A estrutura central de SIC do IFPA e as estruturas descentralizadas de gestão de SIC devem compartilhar o sistema de registro de incidentes de SIC.

Art. 18. Os membros da Estrutura da GSIC devem receber regularmente capacitação especializada nas disciplinas relacionadas à SIC.

Art. 19. A GSIC do IFPA deve auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias do Instituto e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

Art. 20. A Estrutura de GSIC deve planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança.

Art. 21. O IFPA, além das diretrizes estabelecidas nesta PSIC, deve também se orientar pelas melhores práticas e procedimentos de SIC recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 22. É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo IFPA.

Art. 23. O custodiante do ativo de informação deve ser formalmente designado pelo gestor do ativo de informação.

Parágrafo único. A não designação pressupõe que o gestor é o próprio custodiante.

Art. 24. Os contratos firmados pelo IFPA devem conter cláusulas que determinem a observância da PSIC e seus respectivos documentos.

Art. 25. A utilização da computação em nuvem deve ser regulamentada pelo CGSI por norma específica.

CAPÍTULO V
DIRETRIZES ESPECÍFICAS

Art. 26. Para cada uma das diretrizes constantes das seções deste capítulo devem ser elaboradas normas táticas específicas, manuais e procedimentos.

Seção I
Da Gestão de Ativos da Informação

Art. 27. Os ativos de informação devem:

I – ser inventariados e protegidos;

II – ter identificados os seus proprietários e custodiantes;

III – ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

IV – ter a sua entrada e saída nas dependências do IFPA autorizadas e registradas por autoridade competente;

V – ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de violação de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

VI – ser regulamentados por norma específica quanto à sua utilização; e

VII – ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 28. Os gestores da informação devem estabelecer regras e mecanismos que visem à manutenção de uma base de conhecimento sobre a Realização de atividades no IFPA, observadas as normas de SIC.

Art. 29. O IFPA deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 30. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 31. Os sistemas de informações e as aplicações do IFPA devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

Art. 32. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizado, deve ser condicionado ao aceite do termo de responsabilidade e sigilo.

Seção II
Da Gestão de Riscos

Art. 33. A Estrutura de GSIC deve estabelecer processo de Gestão de Riscos de Segurança da Informação e Comunicação (GRSIC) que possibilitem identificar ameaças e reduzir vulnerabilidades e impactos dos ativos de informação.
Art. 34. A GRSIC é um processo contínuo e deve ser aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicação, levando em consideração o planejamento, execução, análise crítica e melhorias da SIC no âmbito do IFPA.

Seção III
Da Segurança Física do Ambiente

Art. 35. A Estrutura de GSIC deve estabelecer mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências.
Art. 36. As proteções devem estar alinhadas aos riscos identificados.

Seção IV
Da Segurança em Recursos Humanos

Art. 37. Os usuários devem ter ciência:
I – das ameaças e preocupações relativas à SIC; e
II – de suas responsabilidades e obrigações no âmbito desta PSIC.

Art. 38. Todos os usuários devem difundir e exigir o cumprimento da PSIC, das normas de segurança e da legislação vigente acerca do tema.
Art. 39. Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os usuários do IFPA, de acordo com suas competências funcionais.
Art. 40. Os usuários devem ser sensibilizados e conscientizados para apoiar esta PSIC durante os seus trabalhos normais.
Art. 41. O controle de pessoal é de responsabilidade do titular da unidade administrativa juntamente com a Diretoria de Gestão de Pessoas, que devem estabelecer perfis, permissões e procedimentos para salvaguarda da SIC.

Seção V
Da Gestão de Operações e Comunicações

Art. 42. A Estrutura de GSIC deve estabelecer parâmetros adequados, relacionados à SIC, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais do IFPA.

Seção VI
Dos Controles de Acessos

Art. 43. Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.

Art. 44. Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 45. Os usuários do IFPA são responsáveis por todos os atos praticados com suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico e assinatura digital.

Art. 46. A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

Art. 47. A autorização, o acesso e o uso das informações e recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso, além do necessário, depende de prévia autorização do gestor da área responsável pela informação.

Art. 48. Todos os sistemas de informação do IFPA, automatizados ou não, devem ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações.

Parágrafo único. No caso de determinado sistema de que trata o Caput for constituído de vários módulos, e estes servirem a unidades diferentes, cada unidade terá um gestor para os respectivos módulos que estiverem sob sua responsabilidade.

Art. 49. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento do usuário do IFPA.

Parágrafo único. A chefia imediata deverá comunicar à Diretoria de Gestão de Pessoas (DGP) sobre as mudanças de atribuições ou de lotação ocorridas em sua unidade, devendo a DGP imediatamente comunicar à Diretoria de Tecnologia da Informação (DTI) do IFPA, para que esta proceda ao cancelamento dos privilégios de que trata o Caput deste artigo.

Art. 50. Os sistemas estruturantes devem possuir normas específicas, no âmbito de sua atuação, que regulem o controle de acesso quanto:

I – ao acesso às suas bases de dados;

II – à extração, carga e transformação de dados; e

III – aos serviços acessíveis via linguagem de programação.

Art. 51. Os sistemas estruturantes devem possuir mecanismos automáticos para:

I – revogar as concessões e desativar as contas de acesso do servidor nos casos de exoneração, demissão, aposentaria e falecimento do servidor;

II – bloquear as contas de acesso do servidor nos casos de licença, afastamento, cessão e disponibilidade do servidor; e

III - tratar os casos de remoção e redistribuição do servidor, segundo as definições constantes da norma de controle de acesso ao sistema.

Art. 52. É responsabilidade do gestor do Sistema Integrado de Administração de Recursos Humanos (SIAPE) disponibilizar, com periodicidade mensal, os registros de todas as movimentações de pessoal referenciadas no Art. 51 ocorridas no período, na forma definida por norma complementar.

Seção VII
Da Criptografia

Art. 53. O uso de recursos criptográficos interfere na confidencialidade, integridade, disponibilidade e autenticidade das informações, sendo, portanto, responsabilidade do Gestor de SIC a implementação dos procedimentos relativos ao seu uso, no âmbito das informações produzidas e custodiadas no IFPA, em conformidade com as orientações contidas em norma específica.
Art. 54. O usuário é responsável pelo recurso criptografado que receber, devendo assinar Termo de Responsabilidade pelo uso.

Seção VIII
Da Aquisição, do Desenvolvimento e da Manutenção de Sistemas

Art. 55. A Estrutura de GSIC deve estabelecer critérios e metodologias de segurança para desenvolvimento de sistema de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção.
Art. 56. O processo de aquisição de sistemas e aplicações corporativas deve atender requisitos de segurança previstos em norma específica.

Seção IX
Do Tratamento de Incidentes

Art. 57. A Estrutura de GSIC deve instituir metodologias ou normas que estabeleçam processos de gestão para tratamento e respostas a incidentes de segurança, de forma a observar o disposto no arcabouço técnico normativo do CTIR.GOV.
Art. 58. Deve ser constituída a Equipe de Tratamento e Resposta a Incidentes de Segurança.

Seção X
Da Gestão de Continuidade

Art. 59. A Estrutura de GSIC deve instituir metodologias ou normas que estabeleçam a Gestão de Continuidade do Negócio.

Seção XI
Da Conformidade

Art. 60. Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de SIC do IFPA e de suas unidades administrativas com esta PSIC e suas normas e procedimentos complementares, bem como com a legislação específica de SIC.
Art. 61. A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o IFPA.
Art. 62. A verificação da conformidade será realizada de forma planejada, mediante calendário de ações proposto pela Estrutura de GSIC e aprovado pelo CGSI.
Art. 63. O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos identificados ou percebidos.
Art. 64. Nenhuma unidade administrativa poderá permanecer sem verificação de conformidade de suas práticas de SIC por período superior a 2 (dois) anos.

Art. 65. A execução da verificação de conformidade será realizada pela Estrutura de GSIC, podendo, com a prévia aprovação do CGSI, ser subcontratada no todo ou em parte.

Art. 66. É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

Art. 67. A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

Art. 68. Os resultados de cada ação de verificação de conformidade serão documentados em Relatório de Avaliação de Conformidade (RAC), o qual será encaminhado pelo Gestor de SIC ao Gestor da unidade administrativa verificada, para ciência e providências cabíveis.

Seção XII
Do Plano de Investimentos em SIC do IFPA

Art. 69. Os investimentos em SIC serão realizados de forma planejada e consolidados em um Plano de Investimentos.

Art. 70. O Plano de Investimentos será elaborado com base na priorização dos riscos s serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco.

Art. 71. Os investimentos em SIC constituirão ação orçamentária específica e permanente na Lei Orçamentária Anual (LOA), distinta das ações orçamentárias relativas a investimentos em segurança da informação destinados à Administração Pública Federal como um todo.

Art. 72. O Plano de Investimentos, assim como a correspondente proposta orçamentária, será aprovado pelo CGSI, mediante recomendação elaborada pela Estrutura de GSIC.

Art. 73. Caso a dotação concedida na LOA seja inferior à solicitada na proposta orçamentária, ou haja limitação na execução orçamentária, caberá ao CGSI realizar a correspondente revisão do Plano de Investimentos.

Seção XIII
Da Propriedade Intelectual

Art. 74. As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual do IFPA e não cabe a seus criadores qualquer forma de direito autoral.

§ 1º Quando as informações forem produzidas por terceiros, para uso exclusivo do IFPA, instrumento próprio obrigará os criadores ao sigilo permanente do conteúdo dos produtos.

§ 2º Fica vedada a utilização das informações, a que se refere o parágrafo anterior, em quaisquer outros projetos ou atividades de uso diverso ao estabelecido pelo IFPA, salvo autorização específica pelos titulares das unidades administrativas, nos processos e documentos de sua competência, ou pelo Reitor, nos demais casos.

Seção XIV
Dos Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 75. Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Art. 76. Os acordos com terceiros podem também envolver outras partes.
Parágrafo único. Os acordos que concedam o acesso a terceiros podem incluir, quando necessário e justificado, permissão para designação de outras partes interessadas e condições para seus acessos desde que expressamente autorizadas pelo IFPA.

Art. 77. Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta PSIC.
Art. 78. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar a PSIC e suas normas complementares aos seus empregados e prepostos envolvidos em atividades no IFPA.
Art. 79. Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.
Art. 80. Deve ser definido um processo adequado/objetivo de gestão de mudanças que será detalhado em norma específica.

CAPÍTULO VI
PENALIDADES

Art. 81. A não observância aos dispositivos da PSIC ou a quaisquer de suas diretrizes, normas e procedimentos ou que violem os controles de SIC do IFPA poderá acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

CAPÍTULO VII
COMPETÊNCIAS E RESPONSABILIDADES

Art. 82. Cabe ao Gestor de SIC:
I – promover a cultura de segurança da informação e comunicação;
II – acompanhar as investigações e as avaliações dos danos decorrentes de violação da segurança;
III – propor recursos necessários às ações de SIC;
IV – coordenar o CGSI e a ETIR;
V – realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC;
VI – manter contato direto com o DSIC/GSI/PR para o trato de assuntos relativos à segurança da informação e comunicação; e
VII – propor normas relativas à SIC.

Art. 83. Cabe ao CGSI:
I – normatizar e supervisionar a SIC no âmbito do IFPA;
II – constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;
III – propor alterações na PSIC;
IV – solicitar apurações quando da suspeita de ocorrências de violações da SIC;
V - avaliar, revisar e analisar criticamente a PSIC e suas normas complementares, visando à sua aderência aos objetivos institucionais do IFPA e às legislações vigentes;
VI – dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PSIC do IFPA;
VII – constituir grupos de trabalho para realizar verificações de conformidade;
VIII – aprovar o Plano de Investimentos em SIC do IFPA;

IX – monitorar e avaliar periodicamente o Plano de SIC de que trata o parágrafo único do Art. 15, assim como determinar os ajustes cabíveis; e
X – definir e atualizar seu Regimento Interno.

Art. 84. Cabe à ETIR:
I – facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;
II – promover a recuperação de sistemas;
III – 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;
IV – realizar ações reativas que incluam recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;
V – analisar ataques e intrusões na rede do IFPA;
VI – executar as ações necessárias para tratar violações de segurança;
VII – obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;
VIII – cooperar com outras equipes de Tratamento e Respostas a Incidentes;
IX – participar de fóruns, redes nacionais e internacionais relativos à SIC.

Art. 85. Cabe ao Gestor do Ativo de Informação:
I – garantir a segurança dos ativos de informação sob sua responsabilidade;
II – definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em consonância com esta PSIC;
III – conceder e revogar acessos aos ativos de informação;
IV – comunicar à ETIR a ocorrência de incidentes de SIC; e
V – designar custodiantes dos ativos de informação, quando aplicável.

Art. 86. Cabe ao custodiantes do ativo de informação proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta PSIC.
Art. 87. Cabe ao titular da unidade administrativa:
I – conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SIC;
II – incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;
III – tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;
IV – informar à DGP a movimentação de pessoal de sua unidade;
V – realizar o tratamento e a classe das informações de sua unidade;
VI – autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa;
VII – comunicar à ETIR os casos de violação de segurança; e
VIII – manter lista atualizada dos ativos da informação sob sua responsabilidade com seus respectivos gestores.

Art. 88. Cabe aos terceiros e fornecedores, conforme previsto em contrato:
I – tomar conhecimento desta PSIC;

II – fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e
III – fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

Art. 89. Cabe aos usuários:
I – conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta PSIC, bem como os demais normativos e resoluções relacionados à SIC;
II – obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação; e
III – comunicar os incidentes que afetam a segurança dos ativos de informação e comunicação à ETIR.

CAPÍTULO VIII
ATUALIZAÇÃO

Art. 90. Esta PSIC, bem como os documentos gerados a partir dela, deverão ser revisados no mínimo a cada cinco anos ou por deliberação do CGSI, de modo a atualizar a política frente a novos requisitos institucionais.
Parágrafo único. O CSI formalizará a proposta de revisão da PSIC por meio de Resolução, que deve ser apreciada e aprovada pelo Conselho Superior.

Art. 91. Esta Resolução entrará em vigor na data de sua publicação no D.O.U.

Claudio Alex Jorge da Rocha
Presidente do CONSUP

MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PARÁ
CONSELHO SUPERIOR

Fls nº 77

RESOLUÇÃO Nº 060/2018-CONSUP DE 09 DE MARÇO DE 2018.

O PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PARÁ, nomeado através do Decreto Presidencial de 02 de abril de 2015, publicado no D.O.U. de 06 de abril de 2015, seção 2, página 1, empossado no dia 28.04.2015, no uso de suas atribuições legais, e considerando o disposto no processo administrativo nº 23051.025418/2017-86.

Resolve:

Art.1º Convalidar a Resolução nº 023/2018-CONSUP/IFPA, de 08 de fevereiro de 2018, publicada no DOU nº 30, de 14/02/2018, seção 1, página 08, que aprovou, *ad referendum*, a Política de Segurança da Informação e Comunicação (PSIC) deste Instituto, conforme deliberação na 52ª Reunião Ordinária do Conselho Superior, realizada no dia 28 de fevereiro de 2018.

Art. 2º Esta Resolução entra em vigor na data da sua assinatura.

Claudio Alex Jorge da Rocha
Presidente do CONSUP