PORTARIA Nº 14, DE 10 DE ABRIL DE 2018

O DIRETOR DO CENTRO DE TECNOLOGIA MINERAL - CETEM, no uso de suas atribuições que lhe foram delegadas pela Portaria n.º 407, de 29 de junho de 2006, publicada no Diário Oficial da União de 30 de junho de 2006, e considerando a Política de Segurança da Informação e Comunicações do MCTIC, aprovada pela Portaria MCTIC nº 4.711, de 18/08/2017, e o disposto no art. 5º, inciso VII, da Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, resolve:

Art. 1º Fica aprovada, na forma do Anexo, a Política de Segurança da Informação e Comunicações do Centro de Tecnologia Mineral (POSIC /CETEM).

Art. 2º Fica revogada a Ordem Interna nº 054, de 19 de dezembro de 2013.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

FERNANDO ANTONIO FREITAS LINS
Diretor

ANEXO
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES – POSIC

Art. 1º O presente documento institui a Política de Segurança da Informação e Comunicações - POSIC no âmbito do Centro de Tecnologia Mineral.

CAPÍTULO I
DO ESCOPO

Art. 2º A Política de Segurança da Informação e Comunicações do Centro de Tecnologia Mineral (POSIC/CETEM) alinha-se ao PDU do CETEM, às estratégias do Ministério da Ciência, Tecnologia, Inovações e Comunicações e objetiva garantir a disponibilidade, integridade, confidencialidade e autenticidade (DICA) das informações produzidas ou custodiadas pelo CETEM independentemente do meio onde estejam registradas.

Parágrafo único. Para os efeitos desta Portaria, considera-se os conceitos e definições dispostos no Capítulo II.

Art. 3º A POSIC/CETEM define as diretrizes, competências e responsabilidades relativas ao uso e compartilhamento de dados, informações e documentos em conformidade com a legislação vigente, as normas técnicas pertinentes, os valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 4º Integram também a POSIC/CETEM os documentos que a complementam, os quais destinam à proteção da informação e à disciplina de sua utilização.

Art. 5º A POSIC/CETEM também aplica-se ao seu Núcleo Regional do Espírito Santo, devendo ser observada em todos os ambientes informatizados e/ou convencionais que executem atividades vinculadas a este Centro.

Parágrafo único. Todos são responsáveis e devem estar comprometidos com a segurança da informação e comunicações do CETEM.

Art. 6º Esta Política também se aplica, no que couber, ao relacionamento do CETEM com outros órgãos e entidades públicos ou privados.

§ 1º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo CETEM devem atender, no que couber, a esta Política e demais normas relacionadas.

§ 2º Os contratos, convênios, acordos e instrumentos congêneres devem conter a previsão de termo específico de responsabilidade e sigilo, quando a natureza de seu objeto ou condições específicas assim o exigirem.

§ 3º Os contratos, convênios, acordos e instrumentos congêneres devem prever a obrigação de divulgação desta POSIC e suas normas complementares aos empregados envolvidos em atividades do contrato, por meio da assinatura de termo de ciência, quando a natureza de seu objeto ou condições específicas assim o exigirem.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 7º Para efeitos desta POSIC são estabelecidos os significados dos seguintes termos e expressões:

I. Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade. (Ref.: NC07/IN01/DSIC/GSIPR/2010);

II. Acesso remoto: funcionalidade que permite acesso ao conteúdo ou controle de um determinado computador através da internet;

III. Agente público: todo aquele que exerce cargo, emprego ou função no CETEM, ainda que transitoriamente com ou sem remuneração, por nomeação, designação, contratação ou qualquer outra forma de vínculo (servidores públicos, servidores temporários regidos pela Lei nº 8.745/1993 e empregados públicos regidos pela Lei nº 9.962/2000, e colaboradores);

IV. Algoritmo de Estado: função matemática utilizada na cifração e na decifração, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, não comercializável (Ref.: NC09/IN01/DSIC/GSIPR/2013);

V. Algoritmo registrado: função matemática utilizada na cifração e na decifração de informações não classificadas, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, cujo código fonte e método de processo sejam passíveis de controle e auditoria (Ref.: NC09/IN01/DSIC/GSIPR/2013);

VI. Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (Ref.: 04/IN01/DSIC/GSI/PR/2013);

VII. Assinatura eletrônica: geração, por computador, de qualquer símbolo ou série de símbolos executados, adotados ou autorizados por um indivíduo para ser um laço legalmente equivalente à assinatura manual do indivíduo;

VIII. Ativo classificado: ativo de informação com informação classificada;

IX. Ativo de informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio. Inclui meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

X. Ativo sob restrição de acesso: ativo de informação com informação institucional não pública ou com informação de acesso transitoriamente restrito;

XI. Auditabilidade: atributo que garante a rastreabilidade dos diversos passos de um processo informatizado, identificando os participantes, ações e horários de cada etapa;

XII. Auditoria: atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais, com o intuito de verificar sua conformidade com os objetivos e políticas institucionais, orçamentos, regras, normas e padrões;

XIII. Autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema (Ref.: Lei nº 12.527/2011);

XIV. 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;

XV. Colaborador: pessoa jurídica ou pessoa física que desempenhe serviço, em caráter permanente ou eventual;

XVI. Comissão de Tecnologia da Informação e Comunicação (CTIC): comissão instituída pela Portaria nº 26, de 29 de agosto de 2014, no âmbito do CETEM, com a responsabilidade de assessorar a Seção de Tecnologia da Informação e Comunicações – SeTIC, quanto as definições, elaborações, atualizações e implementações das ações de segurança da informação e comunicações, das políticas de aquisição dos recursos computacionais e do PDTIC do CETEM;

XVII. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

XVIII. Continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos de informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido. (Ref.: NC06/IN01/DSIC/GSIPR/2009);

XIX. CTIR.GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSI/PR;

XX. Custodiante do ativo de informação: 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;

XXI. Desastres: evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação (Ref.: NC06/IN01/DSIC/GSIPR/2009);

XXII. Disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados (Ref.: Lei nº 12.527/2011);

XXIII. Documento: unidade de registro de informações, qualquer que seja o suporte ou formato (Ref.: Lei nº 12.527/2011);

XXIV. Documento classificado: documento com informação classificada;

XXV. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores. (Ref.: NC03/IN01/DSIC/GSIPR/2009);

XXVI. Gestão da Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto à tecnologia da informação e comunicações. (Ref.: IN GSI/PR 01/2008);

XXVII. 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. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

XXVIII. Gestão de riscos: a gestão de riscos de segurança da informação e comunicações é um 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 financeiros envolvidos;

XXIX. Gestor de Segurança da Informação e Comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito do CETEM;

XXX. Proprietário do ativo de informação: autoridade legal responsável pela concessão de acesso ao ativo de informação a terceiros (pode ser a autoridade marcadora, a autoridade classificadora ou a autoridade instituidora do processo);

XXXI. Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato (Ref.: Lei nº 12.527/2011);

XXXII. Informações institucionais públicas: informações geradas ou custodiadas pelo CETEM ou por seus colaboradores, no exercício de suas funções, às quais o acesso será permitido, observando-se eventual restrição temporária. Dividem-se em de acesso:

a) ostensivo: aquelas que não estão sujeitas a nenhuma restrição de acesso;

b) transitoriamente restrito: aquelas referentes a documentos utilizados como fundamento de decisões e atos administrativos, às quais o acesso será franqueado após a edição do correspondente ato decisório, conforme previsto no parágrafo 3º do art. 7º da LAI, salvo se forem, posteriormente, objeto de classificação como sigilosas;

XXXIII. Informações institucionais não públicas: informações geradas ou custodiadas pelo CETEM ou por seus colaboradores, no exercício de suas funções, sujeitas a restrição de acesso. Dividem-se em:

a) informações pessoais: aquelas relacionadas à pessoa natural identificada ou identificável e que diga respeito à sua intimidade, vida privada, honra e imagem, cujo tratamento é regulado pelo art. 31 da LAI;

b) informações sujeitas a outros tipos de sigilo: aquelas sob segredo de justiça ou protegidas por sigilo comercial, bancário, fiscal, industrial ou outros, na forma da legislação vigente, conforme o disposto no art. 22 da LAI;

c) informação classificada: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada;

d) registros: informações contidas em anotações, levantamentos e análises preliminares, ou sejam aquelas de produção e guarda dos agentes públicos no exercício de suas funções, e que não integrem processo ou expediente que subsidie decisão administrativa editada.

XXIV. Informação sob restrição de acesso: informação institucional não pública ou informação de acesso transitoriamente restrito;

XXXV. Integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino (Ref.: Lei nº 12.527/ 2011);

XXXVI. Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXXVII. Legalidade: atributo que garante a legalidade jurídica da informação, assegurando que todos os seus dados estão de acordo com as cláusulas contratuais pactuadas ou com a legislação nacional ou internacional vigente;

XXXVIII. Não repúdio: propriedade da informação que não possa ter seu envio ou conteúdo contestados, rejeitados ou repudiados por seu emissor ou por seu receptor;

XXIX. PDCA (do inglês: PLAN - DO - CHECK - ACT ou Adjust): é um método iterativo de gestão de quatro passos, utilizado para o controle e melhoria contínua de processos e produtos.

XL. Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações (Ref.: IN GSI/PR 01/2008);

XLI. princípios: são ideias centrais que estabelecem diretrizes a um dado sistema, conferindo-lhe um sentido lógico, harmonioso e racional;

XLII. privacidade: propriedade da informação privada que só possa ser acessada por terceiros com conhecimento e autorização prévios das pessoas de que ela trata;

XLIII. proprietário do ativo da informação: refere-se a parte interessada do órgão ou entidade da Administração Pública Federal, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

XLIV. quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações (Ref.: IN GSI/PR 01/2008);

XLV. recurso criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração (Ref.: IN GSI/PR 03/2013);

XLVI. recursos de tecnologia da informação: servidores de rede, estações de trabalho, equipamentos de conectividade, todo e qualquer hardware e software que compõem soluções e aplicações de Tecnologia da Informação;

XLVII. risco: risco, na área de SIC, é o 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;

XLVIII. segurança da informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (Ref.: IN GSI/PR 01/2008);

XLIX. segurança física e 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;

L. sensibilização em SIC: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional.

LI. terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao CETEM;

LII. tratamento de incidentes de segurança: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

LIII. tratamento da informação: conjunto de ações referentes à produção, classificação, utilização, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação (Ref.: Lei nº 12.527/ 2011);

LIV. usuário: agente público, auditores e quaisquer outros entes que podem acessar ativos de informação do CETEM mediante autorização de gestores de ativos;

LV. vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação (Ref.: NC04/IN01/DSIC/GSIPR/2013).

CAPÍTULO III
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 8º Esta Política de Segurança da Informação e Comunicações do Centro de Tecnologia Mineral (POSIC /CETEM) observa a legislação e as normas específicas, destacando-se:

I. Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e privados e dá outras providências;

II. Lei nº 8.745, de 9 de dezembro de 1993, que dispõe sobre a contratação por tempo determinado para atender a necessidade temporária de excepcional interesse público, nos termos do inciso IX do art. 37 da Constituição Federal, e dá outras providências;

III. Lei nº 9.962, de 22 de fevereiro de 2000, que disciplina o regime de emprego público do pessoal da Administração federal direta, autárquica e fundacional, e dá outras providências;

IV. Lei nº 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; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências;

V. 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;

VI. Decreto nº 4.073, de 3 de janeiro de 2002, que regulamenta a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados;

VII. Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, 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;

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

IX. Resolução nº 20, de 16 de julho de 2004, do Conselho Nacional de Arquivos, que dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos;

X. Resolução nº 32, de 17 de maio de 2010, do Conselho Nacional de Arquivos, que dispõe sobre a inserção dos metadados na Parte II do modelo de requisitos para sistemas informatizados de gestão arquivística de documentos - e-ARQ Brasil;

XI. Câmara Técnica de Documentos Eletrônicos. Conselho Nacional de Arquivos. e-ARQ Brasil: modelo de requisito para sistemas informatizados de gestão arquivística de documentos. Rio de Janeiro: Arquivo Nacional, 2011. v. 1.1;

XII. Câmara Técnica de Documentos Eletrônicos. Conselho Nacional de Arquivos. Glossário de termos técnicos (v5). 2010b;

XIII. Instrução Normativa nº 01, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá providências;

XIV. Instrução Normativa nº 02, de 5 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal;

XV. Instrução Normativa nº 03, de 6 de março de 2013, do Gabinete de Segurança Institucional da Presidência da República, 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;

XVI. Norma Complementar nº 03 da IN 01, de 30 de junho de 2009, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

XVII. Norma Complementar nº 04 da IN 01, de 15 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta;

XVIII. Norma Complementar nº 05 da IN 01, de 14 de agosto de 2009, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da Administração Pública Federal;

XIX. Norma Complementar nº 06 da IN 01, de 11 de novembro de 2009, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a gestão de continuidade de negócios em segurança da informação e comunicações;

XX. Norma Complementar nº 07 da IN 01, de 06 de maio de 2010, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações;

XXI. Norma Complementar nº 09 da IN 01, de 15 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República, que estabelece orientações específicas para o uso de recursos criptográficos em segurança da informação e comunicações;

XXII. NBR ISO/IEC 27001:2006: Sistemas de gestão de segurança da informação;

XXIII. NBR ISO/IEC 27002:2007: Código de prática para a gestão da segurança da informação.

CAPÍTULO IV
DOS PRINCÍPIOS

Art. 9º A Segurança da Informação e Comunicações (SIC) do CETEM deve obedecer aos princípios do acesso, da disponibilidade, da integridade, da confidencialidade, da autenticidade, da legalidade, da privacidade, da auditabilidade e do não repúdio.

CAPÍTULO V
DAS DIRETRIZES GERAIS

Art. 10. A segurança da informação e comunicações tem como principal diretriz a proteção da informação, garantindo a continuidade do negócio, minimizando seus riscos, maximizando o retorno sobre os investimentos e as oportunidades pertinentes. (Ref. ISO/IEC 27.002:2006).

Art. 11. As diretrizes de segurança da informação e comunicações devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e a estrutura do CETEM.

Art. 12. As diretrizes de segurança da informação e comunicações descritas nesta Política devem ser observadas por todos os usuários que executem atividades vinculadas a esta instituição durante todas as etapas do tratamento da informação, a saber: produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Art. 13. O cumprimento desta Política, bem como dos normativos que a complementam deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente instituído pela Comissão de Tecnologia da Informação e Comunicação (CTIC), buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

Art. 14. O CETEM deve observar as diretrizes estabelecidas nesta Política e deve se orientar pelas melhores práticas e procedimentos de segurança da informação e comunicações recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 15. O CETEM deve criar, gerir e avaliar critérios de tratamento da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 16. Os recursos tecnológicos, as instalações de infraestrutura, sistemas de informação e as aplicações devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 17. É vedado comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo CETEM.

Parágrafo único. Cópias de documentos classificados deverão sofrer o mesmo processo de classificação de seu original.

Art. 18. O custodiante do ativo de informação deve ser formalmente designado pelo proprietário do ativo de informação.

Parágrafo único. A não designação pressupõe que o proprietário do ativo de informação é o próprio custodiante.

Art. 19. Os contratos, convênios, acordos e instrumentos congêneres firmados pelo CETEM devem conter cláusulas que determinem a observância desta Política e seus documentos complementares.

CAPÍTULO VI
DAS DIRETRIZES ESPECÍFICAS

Art. 20. Para cada uma das diretrizes constantes das seções deste capítulo deve ser observada a pertinência de elaboração de políticas, procedimentos, normas, orientações e/ou manuais que disciplinem ou facilitem o seu entendimento.

Seção I
DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 21. A Comissão de Tecnologia da Informação e Comunicação (CTIC) deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de segurança da informação e comunicações.

Art. 22. A CTIC deve compreender ações e métodos que visem a estabelecer parâmetros adequados, relacionados à segurança da informação e comunicações, 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 CETEM.

Parágrafo único. De forma a promover a gestão e fomentar os aspectos de segurança da informação, a Diretoria do CETEM deve:

I - instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR).

Seção II
DA PROPRIEDADE DA INFORMAÇÃO

Art. 23. As informações geradas, adquiridas ou custodiadas sob a responsabilidade do CETEM são consideradas parte do seu patrimônio intelectual não cabendo a seus criadores qualquer forma de direito autoral, salvo aqueles direitos garantidos no âmbito da Lei de Inovação e outros dispositivos legais, e devem ser protegidas segundo as diretrizes descritas nesta Política, em seus documentos complementares e demais regulamentações em vigor.

Art. 24. É vedada a utilização de informações produzidas por terceiros para uso exclusivo do CETEM em quaisquer outros projetos ou atividades de uso diverso ao originalmente estabelecido, salvo autorização específica emitida pelo proprietário do ativo de informação, nos processos e documentos de sua competência, ou pelo Diretor do CETEM, nos demais casos, observando a legislação em vigor.

Parágrafo único. 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. 25. Nos termos da Lei de Acesso à Informação (Lei n° 12.527, de 18 de novembro de 2011), é vedada a divulgação e uso por terceiros de informações restritas ou classificadas por grau de sigilo, produzidas ou custodiadas pelo CETEM, salvo nos casos de autorização específica.

Seção III
DOS CONTROLES DE ACESSO

Art. 26. Eventos relevantes, previamente definidos, devem ser registrados para a segurança e o rastreamento de acesso às informações.

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

Art. 27. A autorização, o acesso e o uso da informação e dos recursos de tecnologia da informação e comunicações devem ser controlados e limitados ao necessário para o cumprimento das atividades de cada usuário, e qualquer outra forma de uso ou acesso além do necessário dependem de autorização do proprietário do ativo de informação, observando-se a legislação em vigor.

§ 1º A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo o reconhecimento do usuário de maneira clara e irrefutável.

§ 2º O usuário é responsável por todos os atos praticados com suas identificações, entre as quais se destacam: nome do usuário na rede, carimbo, crachá, endereço de correio eletrônico, assinatura digital e recursos criptográficos, ficando encarregado pela segurança dos ativos, dos processos que estejam sob sua responsabilidade e por todos os atos executados com suas identificações, salvo se comprovado que o fato ocorreu sem o conhecimento ou consentimento do usuário.

§ 3º 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 CETEM.

§ 4º Todos os sistemas de informação do CETEM, automatizados ou não, devem ter um custodiante do ativo da informação, formalmente designado pelo proprietário do ativo de informação, que deve definir os privilégios de acesso às informações, observando a legislação em vigor.

Parágrafo único. A autorização de que trata o caput poderá ser delegada ao custodiante do ativo de informação.

Art. 28. É vedada a utilização de acesso remoto, salvo utilização de recursos próprios do CETEM, homologados pela área de Tecnologia da Informação do CETEM.

Seção IV
DA GESTÃO DE ATIVOS DA INFORMAÇÃO

Art. 29. Os ativos de informação devem:

I - ser inventariados e protegidos;

II - ter identificados, formalmente, o proprietário do ativo de informação e o custodiante do ativo de informação;

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

IV - ter a sua entrada e saída nas dependências dos órgãos e unidades citados no art. 5º autorizadas e registradas pelo proprietário do ativo de informação;

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

VI - 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. 30. Os gestores dos ativos de informação devem estabelecer regras e mecanismos que visem à manutenção de uma base de conhecimento sobre a realização de atividades no CETEM, observadas as normas de segurança da informação e comunicações.

Art. 31. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite a Termo de Responsabilidade, observando a legislação em vigor.

Art. 32. A gestão de ativos da informação será regulamentada por norma específica.

Seção V
DA CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 33. Informações geradas, adquiridas ou custodiadas pelo CETEM podem possuir classificação para indicar a necessidade, a prioridade e o nível esperado de proteção quanto ao seu tratamento.

Parágrafo único. Quando classificadas, serão observadas as exigências das atividades da instituição, considerando as implicações que um determinado grau de classificação trará para os seus objetivos institucionais, observando a legislação em vigor.

Seção VI
DA SEGURANÇA FÍSICA E DO AMBIENTE

Art. 34. A Comissão de Tecnologia da Informação e Comunicação (CTIC) em conjunto com a Seção de Tecnologia da Informação (SeTIC), deve promover mecanismos de proteção às instalações

físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências, em resposta aos riscos identificados.

Parágrafo único. Os mecanismos de proteção estabelecidos devem estar alinhados aos riscos identificados.

Seção VII
DA SEGURANÇA EM RECURSOS HUMANOS

Art. 35. Os usuários devem ter ciência:

I - das ameaças e preocupações relativas à segurança da informação e comunicações;

II - de suas responsabilidades e obrigações conforme estabelecidos nesta Política.

Art. 36. Todos os usuários devem difundir e exigir o cumprimento desta Política, de seus documentos complementares, das normas de segurança e da legislação vigente acerca do tema.

Art. 37. Serão estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os usuários do CETEM, de acordo com suas competências funcionais.

Seção VIII
DA GESTÃO DE RISCOS

Art. 38. As áreas responsáveis por ativos de informação devem implantar processos contínuos de gestão de riscos, os quais serão aplicados na implementação e operação da gestão da segurança da informação e comunicações.

Parágrafo único. A Comissão de Tecnologia da Informação e Comunicação (CTIC) em conjunto com a Seção de Tecnologia da Informação (SeTIC), deve avaliar os riscos relativos à segurança dos ativos de informação e a conformidade com exigências regulatórias ou legais.

Art. 39. A gestão de riscos de segurança da informação e comunicações será regulamentada por norma específica.

Seção IX
DA CONTINUIDADE DE NEGÓCIO

Art. 40. A Comissão de Tecnologia da Informação e Comunicação (CTIC) poderá solicitar a Diretoria do CETEM, instituir, formalmente, grupo de trabalho com objetivo de propor, manter e periodicamente testar medidas de gestão da continuidade e recuperação da informação, visando reduzir para um nível aceitável ou previamente definido a possibilidade de interrupção ou o impacto causado por desastres nos recursos de tecnologia da informação e comunicações que suportam os processos vitais do CETEM, até que se retorne à normalidade.

Art. 41. A gestão de continuidade de negócio será regulamentada por norma específica.

Seção X
DO TRATAMENTO DE INCIDENTES DE REDE

Art. 42. A Diretoria do CETEM deverá instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), em conformidade com a Instrução Normativa GSI/PR nº 1 e a Norma Complementar nº 05/IN01/DSIC/GSIPR, podendo para isso, solicitar o apoio das demais Unidades de Pesquisa do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC).

Art. 43. A gestão de incidentes de segurança da informação será regulamentada por norma específica.

Seção XI
DA CRIPTOGRAFIA

Art. 44. O uso de recursos criptográficos no CETEM seguirá as orientações previstas na Norma Complementar Nº 09/IN01/DSIC/GSIPR.

Art. 45. O usuário é responsável pelo recurso criptográfico que receber, devendo assinar Termo de Responsabilidade por seu uso.

Seção XII
DA AUDITORIA E CONFORMIDADE

Art. 46. A verificação de conformidade das práticas de segurança da informação e comunicações do CETEM deverá ser realizada sempre que necessária, não excedendo o período máximo de 3 (três) anos.

§ 1º A verificação da conformidade será realizada de forma planejada, mediante calendário de ações aprovado pela CTIC.

§ 2º A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o CETEM.

Art. 47. A execução da verificação de conformidade será realizada por grupo de trabalho formalmente instituído pela Diretoria do CETEM, com apoio da Comissão de Tecnologia da Informação e Comunicação (CTIC), podendo tal serviço ser subcontratado no todo ou em parte.

§ 1º É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

Art. 48. Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade e, com base neste, a Diretoria do CETEM tomará medidas cabíveis.

Seção XIII
DO PLANO DE INVESTIMENTOS EM SIC DO CETEM

Art. 49. Os investimentos em SIC serão realizados de forma planejada e consolidados em um plano de investimentos, de modo a garantir a provisão dos recursos necessários para a implementação das ações de segurança da informação do CETEM.

Art. 50. O plano de investimentos, sob a responsabilidade da Comissão de Tecnologia da Informação e Comunicação (CTIC), será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto dos riscos.

Art. 51. O plano de investimentos, assim como a correspondente proposta orçamentária, serão aprovados no âmbito da Diretoria do CETEM.

Parágrafo único. Caso a dotação concedida seja inferior à solicitada na proposta orçamentária, ou haja limitação na execução orçamentária, caberá a CTIC realizar a correspondente revisão do plano de investimentos, que deverá ser aprovada pela Diretoria do CETEM.

Seção XIV
DA GESTÃO DE OPERAÇÕES E COMUNICAÇÕES

Art. 52. A Seção de Tecnologia da Informação e Comunicações (SeTIC) do CETEM deve estabelecer modelos e arquiteturas de referência, que descrevam requisitos mínimos para a disponibilização de serviços, sistemas e infraestrutura, atendendo às necessidades operacionais e de segurança desta política.

Seção XV
DA RELAÇÃO COM TERCEIROS

Art. 53. Nos editais de licitação, nos contratos, contratos de gestão, convênios, acordos e instrumentos congêneres de cooperação técnica com entidades prestadoras de serviços para o CETEM deverá constar cláusula específica sobre a obrigatoriedade de observância a esta Política.

Art. 54. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta Política, bem como suas normas e procedimentos complementares aos seus empregados e prepostos envolvidos em atividades no CETEM.

Seção XVI
DA AQUISIÇÃO, DO DESENVOLVIMENTO E DA MANUTENÇÃO DE SISTEMAS

Art. 55. A Comissão de Tecnologia da Informação e Comunicação (CTIC) em conjunto com a Seção de Tecnologia da Informação (SeTIC) do CETEM deve estabelecer critérios de segurança para o desenvolvimento, manutenção e aquisição de sistemas e aplicações.

Seção XVII
DA GESTÃO DE MUDANÇAS

Art. 56. No âmbito da segurança da informação e comunicações, a gestão de mudanças consiste em procedimentos e controles necessários para garantir que mudanças sejam formalmente

requisitadas, aprovadas, planejadas e adequadamente testadas, com objetivo de minimizar a ocorrência de erros quando da mudança.

CAPÍTULO VII
DAS PENALIDADES

Art. 57. A não observância desta Política e/ou de seus documentos complementares, bem como a quebra de controles de segurança da informação e comunicações, 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 VIII
DAS COMPETÊNCIAS E RESPONSABILIDADES

Seção I
Da Comissão de Tecnologia da Informação e Comunicação (CTIC)

Art. 58. A Comissão de Tecnologia da Informação e Comunicação (CTIC), de natureza consultiva, vinculada à Diretoria do CETEM, tem a finalidade de tratar sobre políticas, diretrizes, planejamento e demais ações relativas à Segurança da Informação e Comunicações (SIC)

Art. 59. São competências da CTIC:

I - assessorar na implementação das ações de segurança da informação e comunicações;

II – definir, elaborar e atualizar políticas de aquisição dos recursos computacionais do CETEM;

III – promover e estimular o desenvolvimento da informática no âmbito do CETEM;

IV - propor a Política de Segurança da Informação e Comunicações composta por políticas, diretrizes, normas e procedimentos relativos à segurança da informação e comunicações para o CETEM, em conformidade com as legislações existentes sobre o tema, bem como suas alterações, e submetê-la a Diretoria do CETEM para apreciação e pronunciamento.

V - propor normas relativas à segurança da informação e comunicações; e

VI - exercer outros atos de assessoramento e de proposição afetos à matéria de segurança da informação e comunicações.

Seção II
Da Seção de Tecnologia da Informação (SeTIC)

Art. 60. Compete a Seção de Tecnologia da Informação (SeTIC), do CETEM:

I - prestar apoio às atividades fins do CETEM, no que concerne as necessidades em tecnologia da informação;

II - implementar, manter e administrar as atividades relativas às áreas de informática e redes de comunicação de dados interna, bem como sua respectiva conectividade às redes acadêmicas e

comerciais, sempre em consonância com as demais unidades organizacionais e organismos gestores oficiais;

III - operar, manter e administrar a rede de comunicação de dados interna, com suas conexões às redes externas acadêmicas e comerciais, bem como prover o suporte operacional da infraestrutura computacional da instituição;

IV - implementar e gerenciar tecnologias que assegurem a disponibilidade, integridade e sigilo das informações digitais;

V - planejar, definir e homologar estruturas, arquiteturas, hardwares, softwares e materiais de informática que sejam adequados às necessidades do CETEM, com o apoio da Comissão de Tecnologia da Informação e Comunicação - CTIC;

VI - prestar apoio a Comissão de Tecnologia da Informação e Comunicação - CTIC, na elaboração de projetos que viabilizem a implantação e operação da rede de comunicação de dados interna institucional, bem como propor e orientar as demais áreas de atuação, quanto aos procedimentos de manutenção e atualização;

VII - assistir e facilitar aos usuários, através dos recursos computacionais da instituição, a localização e acesso de dados, informações e conhecimento nas áreas de informática, sistemas computacionais e redes de comunicação de dados, pertinentes ao exercício de suas atividades;

VIII - pesquisar, coordenar e propor o uso de produtos e serviços e tecnologias emergentes em informática, objetivando sua ampla disseminação e utilização como alternativas àquelas em uso, com a devida orientação aos usuários do sistema;

IX - disseminar informações relevantes sobre as facilidades da rede corporativa, credenciando usuários e estabelecendo condições de acesso à rede de comunicação de dados;

X - instalar, adaptar e atualizar os atuais sistemas operacionais em uso, bem como propor a implantação com a subsequente instalação e migração para sistemas operacionais, aplicativos e utilitários emergentes, baseados no conceito de software não proprietário;

XI - propor, desenvolver, realizar e supervisionar processos de treinamento sobre sistemas operacionais, programas e aplicativos de uso já consolidado, bem como as possíveis alternativas de novos sistemas operacionais, utilitários e aplicativos visando a universalização da informática, agilizar e melhorar o desempenho do usuário final;

XII - apoiar a Comissão de Tecnologia da Informação e Comunicação - CTIC quanto ao estudo, elaboração e implantação de soluções corporativas de políticas de segurança da informação, em conformidade com os interesses da unidade organizacional, envolvendo todos os aspectos relevantes da instituição para a proteção, controle e monitoramento dos dados e dos recursos computacionais, trabalhando de forma coordenada com as demais unidades organizacionais e os organismos oficiais gestores da área de segurança de sistemas computacionais, objetivando a detecção, identificação, resolução e prevenção de incidentes de segurança;

XIII - gerenciar os dados e informações gerados durante a concretização de ações estruturadas recuperável e promover a disseminação de informações organizacionais;

XIV - gerenciar e controlar o acesso ao ambiente de rede, à internet e aos equipamentos de informática, visando maximizar a utilização dos mesmos;

XV - gerenciar, inventariar e controlar as licenças de software no CETEM;

XVI - especificar, gerenciar, acompanhar e implementar a operação física e lógica de redes locais;

XVII - auditar a utilização dos recursos computacionais, de acordo com as normas vigentes;

XVIII - orientar a execução de operações e manutenção da rede de comunicação de dados, bem como prover o suporte operacional da infraestrutura computacional;

XIX - dar suporte técnico aos usuários da rede, no que diz respeito à utilização dos equipamentos, hardware, softwares e serviços disponíveis;

XX - realizar diagnóstico para apuração de eventuais problemas em equipamentos ou na rede e gerenciar os serviços de manutenção contratados a terceiros;

XXI - realizar manutenção corretiva, adaptações e melhorias nos sistemas desenvolvidos, e atendimento das necessidades dos usuários; e

XXII - exercer outras competências que lhe forem cometidas no seu campo de atuação;

XXIII - apoiar na promoção da cultura de segurança da informação e comunicações;

XXIV - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

XXV - apoiar a CTIC e a equipe de tratamento e resposta a incidentes em redes computacionais; e

XXVI - manter contato direto com o Departamento de Segurança da Informação e Comunicações (DSIC/GSIPR) para o trato de assuntos relativos à segurança da informação e comunicações.

Seção III

Da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)

Art. 61. A ETIR tem a finalidade de facilitar, coordenar e executar as atividades de tratamento e resposta a incidentes em redes computacionais no ambiente do CETEM.

Art. 62. A ETIR do CETEM deverá ter como objetivos básicos:

I. monitorar as redes computacionais;

II. detectar e analisar ataques e intrusões;

III. tratar incidentes de segurança da informação;

IV. identificar vulnerabilidades e artefatos maliciosos;

V. recuperar sistemas de informação; e

VI. promover a cooperação com outras equipes, bem como participar de fóruns e redes nacionais e internacionais relativos à Segurança da Informação e Comunicações;

Art. 63. A ETIR será composta por servidores públicos, preferencialmente ocupantes de cargo efetivo, designados em portaria específica pelo Diretor do CETEM, podendo ter o apoio técnico de profissionais contratados para este fim.

Seção IV
Do Agente Responsável pela ETIR

Art. 64. Compete ao Agente Responsável pela ETIR do CETEM:

I - Estabelecer os procedimentos operacionais, gerenciar as atividades e distribuir tarefas para a ETIR;

II - Assistir o CTIR GOV com informações necessárias à atualização e manutenção das bases de dados de incidentes do Governo Federal.

Seção V
Dos Usuários

Art. 65. Compete aos usuários do CETEM:

I - cumprir fielmente as políticas, as normas, os procedimentos e as orientações de segurança da informação e comunicações do CETEM;

II - buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

III - assinar Termo de Responsabilidade, formalizando a ciência e o aceite da POSIC /CETEM, bem como assumindo responsabilidade por seu cumprimento;

IV - proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela Diretoria do CETEM;

V - assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo CETEM;

VI - comunicar imediatamente a Comissão de Tecnologia da Informação e Comunicação (CTIC) qualquer descumprimento ou violação desta Política e/ou de seus documentos complementares.

CAPÍTULO IX
METODOLOGIA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 66. A metodologia de gestão da segurança da informação do CETEM seguirá as orientações previstas na Norma Complementar 02/IN01/DSIC/GSIPR/2008, que se baseia em processo de melhoria contínua, considerando o "PDCA" (Plan-Do-Check-Act), referenciado pela norma ABNT NBR ISO/IEC 27001.

CAPÍTULO X
DA REVISÃO E ATUALIZAÇÃO

Art. 67. Esta Política bem como o conjunto de instrumentos normativos gerados a partir dela, será revisada de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 03 (três) anos.