Sumário

Histórico de Revisão			
Versão	**Data**	**Responsável**	**Aprovação**
00	08/12/2014	STI	RD nº 09/324ª de 08/12/2014

Informações Adicionais

Este Instrumento Normativo revoga a CSIC 002 - Norma para Utilização de Ativos de Informação, aprovada pela RD 04/223ª de 16/09/2011, vigente até esta data.

1. Objetivo

Estabelecer as regras que norteiam as atividades de Segurança da Informação e Comunicações da Empresa de Pesquisa Energética (EPE).

2. Campo de Aplicação

Aplica-se a todas as áreas da EPE.

3. Definições e Siglas

3.1. Definições

Ameaça – Conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Ataque de Negação de Serviços – Prática maliciosa que consiste em submeter um grande volume de solicitações a um serviço computacional, exaurindo os recursos computacionais e resultando em negação do serviço a outros usuários.

Ativos de Informação – Os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

Autenticidade – Propriedade de que a informação foi produzida, modificada ou descartada por uma determinada pessoa física, órgão, entidade ou sistema.

Caixa Postal – Área de armazenamento de mensagens de correio eletrônico associada a um endereço eletrônico.

CSIC – Comitê composto por representantes de todas as Diretorias, Presidência e da STI para preparar e propor estratégias, planos e normas de SIC.

Código Malicioso – Programa computacional produzido com finalidades escusas, tais como induzir o outro usuário a fornecer informações sigilosas, danificar a integridade de um computador, etc.

Confidencialidade – Propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

Contêineres dos Ativos de Informação – O contêiner é o local onde "vive" o ativo de informação, onde está armazenado, como é transportado ou processado.

Criticidade – Define a importância da informação para a continuidade do negócio da instituição.

Custodiante do ativo de informação – É o responsável pelos contêineres dos ativos de informação e pela aplicação dos níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações comunicadas pelos proprietários dos ativos de informação.

Disponibilidade – Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

Gestor do ativo de informação – Indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

Incidente em segurança da informação e comunicações – Qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações do negócio ou ameaçar a SIC.

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.

Informação Privilegiada – A que diz respeito a assuntos sigilosos ou aquela relevante ao processo de decisão no âmbito do Poder Executivo Federal que tenha repercussão econômica ou financeira e que não seja de amplo conhecimento público.

Informação Sigilosa – Informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

Integridade – Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

Lista de Discussão – Grupo de usuários de correio eletrônico criado com objetivo de trocar informações relacionadas a uma determinada área ou assunto.

Mensagem de correio eletronico – Um ou mais registros eletrônicos de computador ou mensagens criadas, enviadas, encaminhadas, respondidas, transmitidas, arquivadas, mantidas, copiadas, mostradas, lidas ou impressas por um ou vários sistemas ou serviços de correio eletrônico.

Navegador – *Software* utilizado para visualização de páginas na web (por exemplo, o Internet Explorer).

Política de Segurança da Informação e Comunicações – Documento aprovado pela autoridade responsável do órgão ou entidade da Administração Pública Federal, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.

PDSIC – Documento que estabelece um plano de ação, tático e operacional, na área de SIC para atingir os objetivos estratégicos definidos no PETI, assegurando seu alinhamento com os objetivos de negócio da Empresa contidos no PEI.

Recurso de Tecnologia da Informação – Qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, ou quando aplicável, as instalações físicas que os abriguem.

Recurso de Trabalho Remoto – Categorias de ativos de informação (notebooks, telefones celulares, pagers, modems, pendrives), disponibilizados aos usuários para fins de execução de trabalho remoto (fora das instalações da empresa), ou para permitir a comunicação dos mesmos, visando a otimização e flexibilização do trabalho.

Risco de Segurança da Informação e Comunicações – 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 Empresa.

Segurança da Informação e Comunicações – Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Serviço de Correio Eletrônico – Sistema de mensageria utilizado para criar, enviar, encaminhar, responder, transmitir, arquivar, manter, copiar, mostrar, ler ou imprimir informações, com o propósito de comunicação entre redes de computadores ou entre pessoas ou grupos.

Serviço de Rede – É uma aplicação distribuída que executa em dois ou mais computadores, conectados por uma rede.

Site – Conjunto de páginas disponibilizadas no ambiente web (rede mundial de computadores).

Usuário – Qualquer empregado ocupante de cargo efetivo, cargo em comissão, cedido, prestador de serviço terceirizado, estagiário ou qualquer outro indivíduo que tenha acesso, de forma autorizada, aos recursos computacionais da EPE.

Vulnerabilidade – Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou Empresa, os quais podem ser evitados por uma ação interna de segurança da informação.

3.2. Siglas

ABNT – Associação Brasileira de Normas Técnicas

CSIC – Comitê de Segurança da Informação e Comunicações

GSI – Gabinete de Segurança Institucional da Presidência da República

GSIC – Gestor de Segurança da Informação e Comunicações

PDSIC – Plano Diretor de Segurança da Informação e Comunicações

PEI – Plano Estratégico Institucional

SIC – Segurança da Informação e Comunicações

TIC – Tecnologia da Informação e Comunicações

4. Documentos de Referência

- Decreto nº 3.505, de 13 de Junho de 2000: Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- GSI IN 1/2008: Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
- INC nº 14/IN01/DSIC/GSIPR, de 30 de janeiro de 2012: Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC).
- INC nº 15/IN01/DSIC/GSIPR, de 11 de junho de 2012:: Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais.
- ABNT NBR ISO/IEC 27002:2013: Fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação e comunicações da Empresa.
- Política de Segurança da Informação e Comunicações: Estabelece orientações específicas sobre as práticas de Segurança da Informação a serem adotadas para o cumprimento da Missão e o alcance da Visão da Empresa.

5. Descrição

5.1. Segurança da Informação e Comunicações

Trata da SIC da EPE, visando a garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações e compreendendo os meios de armazenamento, transmissão e processamento e os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

5.1.1. Papéis e Responsabilidades

Custodiante do ativo de informação:

- Garantir que todos os requisitos de SIC definidos pelo gestor da informação sejam satisfeitos.
- Comunicar tempestivamente ao gestor sobre situações que comprometam a segurança das informações sob custódia.
- Comunicar ao GSIC eventuais limitações para cumprimento dos critérios de SIC, para que este decida quanto à cessão ou não da informação.

Gestor do ativo de informação

- Descrever o ativo de informação.
- Definir as exigências de segurança da informação e comunicações do ativo de informação.
- Definir procedimentos e critérios de acesso das informações, observados os dispositivos legais e regimentais relativos ao sigilo e a outros requisitos de classificação pertinentes.
- Propor regras específicas ao uso das informações.
- Indicar os riscos que podem afetar os ativos de informação.
- Comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários.
- Buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento.

Gestor de Segurança da Informação e Comunicações - GSIC

- Gerir o processo de SIC, orientando as demais áreas quanto sua aplicação.

- Elaborar um PDSIC, a partir das definições estratégicas estabelecidas pelo CSIC. Este plano deverá ser revisto a cada 2 (dois) anos.
- Coordenar as ações do PDSIC e dos projetos nele relacionados.
- Propor recursos necessários às ações de SIC.
- Subsidiar a Diretoria Executiva na tomada de decisão quanto à SIC.
- Designar responsáveis pelos contratos relacionados à SIC.
- Promover a cultura de SIC na empresa.
- Promover palestras e treinamentos para conscientização dos usuários e atualização das ações de segurança.
- Coordenar as ações necessárias na ocorrência de incidentes de SIC de acordo com o plano de contingenciamento de riscos de incidentes de SIC.
- Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança.
- Coordenar o CSIC e a equipe de tratamento e resposta a incidentes em redes computacionais.
- Realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na SIC.
- Propor ao CSIC normas relativas à SIC.
- Fornecer subsídios às atividades do CSIC.
- Realizar análises de risco periódicas no que tange à tecnologia, ambientes, processos e pessoas, de acordo com as normas internas e as normas da ABNT específicas referentes à matéria.
- Emitir relatórios sobre o uso dos recursos de tecnologia, apontando irregularidades e não conformidades na utilização.
- Atuar de forma coordenada com outras áreas nos assuntos de SIC.
- Manter o CSIC informado sobre o nível de segurança alcançado nos ambientes tecnológicos, por meio de relatórios gerenciais provenientes das análises de risco, e sobre a ocorrência e tratamento de incidentes relacionados à SIC.

Comitê de Segurança da Informação e Comunicações - CSIC

- Assessorar o GSIC na implementação das ações de SIC.
- Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC.
- Propor à Diretoria Executiva da EPE normas relativas à SIC.
- Rever periodicamente os instrumentos normativos referentes à SIC, sugerindo possíveis alterações.
- Garantir a conformidade das atividades de SIC com a política que trata do mesmo assunto.
- Recomendar ações para sanar as não conformidades.

- Aprovar as metodologias e processos relacionados à SIC.
- Identificar as ameaças significativas.
- Promover a educação, treinamento e conscientização da SIC, por toda a Empresa.
- Dirimir dúvidas e deliberar sobre questões não contempladas nos instrumentos normativos e em documentos relacionados.
- Receber e analisar as comunicações de descumprimento dos instrumentos normativos de SIC, apresentando parecer à autoridade/órgão competente à sua apreciação.
- Solicitar, sempre que necessário, a realização de auditorias pela STI, relacionadas ao uso dos recursos de tecnologia da informação no âmbito da EPE.
- Solicitar, sempre que necessário, a realização de auditorias externas de SIC, independentemente das auditorias internas realizadas.

Superintendência de Tecnologia da Informação – STI

- Instalação de programas e sistemas homologados.

Diretoria

- Designar o representante da diretoria para integrar o CSIC.

Diretoria Executiva

- Nomear o GSIC.
- Aprovar programa orçamentário específico para as ações de SIC.
- Promover as ações necessárias à implementação e manutenção da SIC.
- Promover a capacitação de recursos humanos para o desenvolvimento de competência tecnológica em SIC.
- Aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra de segurança.
- Remeter os resultados consolidados dos trabalhos de auditoria de Gestão de SIC para o GSI.

Usuários

- Observar e seguir as recomendações, normas e procedimentos de SIC.
- Solicitar orientações quando necessário.

5.2. Detalhamento

A Segurança da Informação e Comunicações na EPE é coordenada pelo GSIC, nomeado pela Diretoria Executiva, e assessorado pelo CSIC.

As medidas de SIC devem ser planejadas, aplicadas, implementadas e, periodicamente, avaliadas, de acordo com os objetivos institucionais e os riscos para as atividades da EPE.

O uso adequado dos recursos de tecnologia da informação visa garantir a continuidade da prestação de serviços da EPE.

As informações recebidas de pessoa física ou jurídica externa à EPE serão submetidas, adicionalmente, a medidas de SIC compatíveis com os requisitos pactuados com quem as forneceu.

Os Diretores podem indicar, orientar e autorizar, a qualquer tempo, procedimentos a serem seguidos pelos respectivos gestores da informação, que visem garantir a SIC nos processos e documentos de sua competência.

Os Diretores das áreas da EPE e seus Superintendentes devem:

- Conscientizar os usuários sob sua supervisão, em relação aos conceitos e às praticas de SIC.
- Incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC.
- Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC, por parte dos usuários sob sua supervisão.

5.2.1. Comitê de Segurança da Informação e Comunicações (CSIC)

O CSIC é um órgão colegiado de natureza consultiva e de caráter permanente composto por representantes de todas as diretorias, da Presidência e da Consultoria Jurídica e coordenado pelo GSIC. A nomeação dos representantes no CSIC é feita pelo Diretor de cada área e pelo Presidente.

5.2.2. Gestor de Segurança da Informação e Comunicações (GSIC)

O profissional designado como Gestor de Segurança da Informação e Comunicações deve ter um perfil multidisciplinar, com uma visão completa do que é SIC, dominar as técnicas de gerência de projeto, ter experiência em coordenação de equipes e liderança.

5.2.3. Usuários

Para ser habilitado para utilizar os recursos de TIC da EPE, o USUÁRIO deve tomar conhecimento desta Norma e formalizar a ciência da mesma.

Todo usuário é responsável pela utilização de seu computador e dos recursos de TIC disponibilizados pela Empresa para que execute suas atividades e funções. Contudo, a EPE não é responsável pelas atitudes e serviços de cunho pessoal, realizados pelo funcionário, ou prestador de serviço, tais como utilização de Internet *Banking* e utilização de *webmail* pessoal.

Uma vez decidido o desligamento de um empregado ou término dos serviços de terceiros, a unidade responsável pelo término do relacionamento do usuário com a EPE, deverá comunicar à STI a data do último dia de vinculação do usuário à Empresa para que o acesso aos recursos computacionais e ao correio eletrônico seja bloqueado ao final do expediente.

O usuário a ser desligado pode solicitar a configuração de uma resposta automática padrão na sua caixa de correio eletrônico, que ficará ativa pelo prazo de um mês após a cessão de vínculo, denotando o seu novo endereço de e-mail (e-mail particular). Essa solicitação deverá ser encaminhada à STI com antecedência de 3 (três) dias. Ao final desse período, a caixa postal será definitivamente desativada.

Compete à chefia imediata de um usuário desligado da EPE a revisão dos seus arquivos armazenados em estação de trabalho ou em qualquer servidor de rede da EPE e, também, dos seus documentos em qualquer outro meio físico.

É responsabilidade da STI providenciar os recursos técnicos para que os dados e informações digitais pertencentes à Empresa, mas que estiveram em posse do usuário desvinculado, sejam repassados, cumpridos os requisitos da classificação da informação, à sua supervisão imediata.

O supervisor imediato do usuário que foi desvinculado passará a ser o gestor dessas informações.

5.2.4. Direito de Propriedade

As informações geradas no âmbito da EPE são de sua propriedade, independentemente da forma de sua apresentação ou armazenamento e devem ser adequadamente protegidas e utilizadas exclusivamente para fins relacionados às atividades desenvolvidas na Empresa.

O uso dos ativos de informação deve ser feito sem violar a legislação, regulamentação ou requisitos contratuais e, inclusive, sem violar os direitos de propriedade intelectual, como marcas e patentes, nome comercial, segredo empresarial, domínio na Internet, desenho industrial ou qualquer outro material que não tenha autorização expressa do autor ou proprietário dos direitos, relativos à obra artística, científica ou literária, nos moldes da legislação em vigor.

5.2.5. Utilização dos Ativos de Informação

A utilização dos ativos de informação da EPE está restrita aos usuários autorizados e credenciados a fazê-lo.

No entanto, a EPE poderá revogar os privilégios de acesso de usuário de ativos de informação, a qualquer momento, sempre que identificar condutas que interfiram na operação normal e adequada dos sistemas de informação e que adversamente afetem a capacidade de outras pessoas utilizarem esses sistemas de informação, bem como identificar condutas consideradas prejudiciais ou ofensivas, mediante anuência do GSIC.

É dever dos usuários dos ativos de informação da EPE observar as seguintes regras:

- Utilizar somente programas de computador licenciados e homologados para uso pela EPE.
- Utilizar os recursos computacionais da EPE para fins pessoais desde que com bom senso e em consonância com as práticas da Empresa, ficando o usuário ciente de que este ambiente está sujeito à monitoração.

É vedado aos usuários dos ativos de informação da EPE:

- Produzir arquivos compactados em formato executável (“.exe”) sem a autorização de autoridade competente, pois estes tipos são propícios à propagação de vírus.
- Armazenar arquivos executáveis, incluindo jogos, no computador ou nas áreas de armazenamento da rede.
- Criar, transmitir, distribuir, disponibilizar e armazenar documentos que infrinjam a ética, decência, probidade, honra e imagem de pessoas ou empresas, que exponham a vida privada e intimidade, ou que tenham conteúdo pornográfico ou de pedofilia.
- Introduzir códigos maliciosos nos sistemas de TIC.
- Tentar prejudicar qualquer serviço de rede, sobrecarregá-lo, desativá-lo ou, ainda, aderir ou cooperar com ataques internos ou externos de negação de serviços.
- Alterar registro de evento dos sistemas de TIC, com a finalidade de ocultar ações indevidas no sistema computacional.
- Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas de TIC.
- Monitorar ou interceptar o tráfego de dados nos sistemas de TIC, sem a autorização de autoridade competente.
- Violar medida de segurança ou de autenticação sem autorização de autoridade competente.

- Utilizar recurso informacional da EPE para fins comerciais, exceto postar anúncio na seção classificados da Intranet.

Para garantir a execução desta norma e de suas determinações, a EPE se reserva o direito de monitorar toda a utilização dos recursos de TIC por parte dos usuários, por meio da implantação de *softwares* e sistemas para monitoração do uso da Internet e demais recursos de rede, impressão e correio eletrônico e da inspeção de qualquer arquivo armazenado nas estações de trabalho locais ou armazenados na rede, visando o estrito cumprimento desta norma.

5.2.5.1. Sistemas de Informação

Em relação aos Sistemas da Informação da EPE, é vedado aos usuários:

- Danificar, alterar e interromper a operação de qualquer sistema do ambiente de TIC.
- Obter indevidamente senhas de acesso, chaves criptográficas ou qualquer outro mecanismo de controle de acesso que possa possibilitar o acesso a recursos informacionais não autorizados.
- Acessar, modificar, remover ou copiar arquivos que pertençam a outro usuário sem a permissão expressa do mesmo.
- Executar testes ou tentativas de comprometimento de controles internos.
- Executar ou desenvolver qualquer tipo de programa ou processo externo ou incompatível com suas atividades.
- Desenvolver, gerar, compilar, copiar, coletar, propagar, executar ou tentar introduzir qualquer código projetado para se autorreplicar, danificar, expor conteúdos protegidos ou de outra maneira obstruir o acesso ou afetar o desempenho de qualquer computador, rede ou sistema de TIC da EPE.
- Utilizar qualquer *software* ou qualquer sistema externo à EPE que não esteja devidamente homologado e/ou licenciado e, conforme o caso, que não tenha sido adquirido pela Empresa.

5.2.5.2. Correio Eletrônico

O conteúdo do correio eletrônico dos usuários da EPE poderá ser acessado pela empresa caso ocorram situações de risco, a critério da empresa. Antes do acesso, a chefia imediata do USUÁRIO será comunicada, assim como também o Gestor de Segurança da Informação e Comunicações. Todas estas ações devem ser registradas formalmente a fim de se possibilitar que o procedimento seja auditado.

Cabe ao usuário notificar sua chefia imediata ou superior e ao GSIC, quando do recebimento de mensagens que comprometam a segurança da informação e comunicações da Empresa.

É vedado aos usuários do serviço de correio eletrônico da EPE:

- Acessar as caixas postais de terceiros, ficando os USUÁRIOS cientes de que as tentativas de acesso são registradas em *log*, cuja guarda e monitoração são de responsabilidade da STI.
- Enviar e/ou armazenar mensagens com conteúdo obsceno, ilegal ou não ético.
- Fazer propaganda não vinculada à Empresa através de mensagens do correio eletrônico.
- Enviar e/ou armazenar mensagens contendo vírus ou qualquer outro programa danoso.
- Enviar e/ou armazenar mensagens do tipo corrente.
- Enviar e/ou armazenar mensagens com conteúdo relacionado à nacionalidade, raça, cor, etnia, orientação sexual, religiosa, convicção política, ou qualquer outro assunto que possa vir a causar dano a qualquer pessoa física ou jurídica.
- Enviar mensagens simultâneas a grupos grandes de destinatários (como superintendências e diretorias inteiras), exceto quando relacionadas às suas atividades e necessidades de trabalho, ou quando expressamente autorizadas.
- Participar de listas de discussão, exceto quando relacionadas às suas atividades de trabalho.
- Abrir ou executar programas anexados a mensagens. e
- Enviar informações sigilosas ou privilegiadas, sem a devida autorização, para pessoas ou organizações.

As caixas postais corporativas de unidades administrativas ou grupos de trabalho deverão ser solicitadas à STI e ter um usuário responsável designado pela unidade administrativa ou grupo de trabalho.

5.2.5.3. Redes Sociais

Os perfis institucionais da empresa estabelecidos nas redes sociais públicas devem ser administrados e gerenciados por equipes integradas exclusivamente por servidores ou empregados públicos federais, ocupante de cargo efetivo, preferencialmente da EPE. Quando isso não for possível, a equipe poderá ser mista, desde que sob a coordenação e responsabilidade de um empregado efetivo da Empresa. Este empregado deverá estabelecer bons relacionamentos interpessoais, interagir e dialogar com as demais áreas presentes nestas redes e, principalmente, manter-se atualizado quanto ao negócio da EPE.

É vedada a terceirização completa da administração e da gestão de perfis da EPE nas redes sociais.

Para não comprometer a produtividade do trabalho e o tráfego de dados, os usuários da rede corporativa da EPE somente poderão acessar as redes sociais públicas a partir de suas estações de trabalho no seguinte período:

- antes das 9:00 horas;
- entre 12:00 e 14:00 horas; e
- a partir das 18:00 horas.

5.2.5.4. Armazenamento em Nuvem

Para contratação ou implementação de um serviço em nuvem deve-se garantir que:

- O ambiente de computação em nuvem, sua infraestrutura e canal de comunicação estejam aderentes à legislação e regulamentos da Administração Pública Federal.
- O contrato de prestação de serviço, quando for o caso, contenha cláusulas que garantam a disponibilidade, integridade, confidencialidade e autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço.

E as informações a serem hospedadas devem ser avaliadas, considerando:

- Classificação da informação: somente as informações classificadas como ostensivas poderão ser hospedadas em ambiente de nuvem contratada a terceiros;
- O valor do ativo de informação: informações que possam impactar o mercado mobiliário e informações de terceiros sob custódia da EPE somente poderão ser armazenadas em ambiente de nuvem sob administração direta da EPE;
- Os controles de acesso, físicos e lógicos necessários: os serviços de nuvem a serem utilizados devem aderir às regras estabelecidas na Norma de Controle de Acesso e Segurança Física;
- O modelo de serviço e implementação de computação em nuvem a serem adotados: informações classificadas como sigilosas e pessoais somente poderão ser armazenadas em nuvem própria; e
- A localização geográfica onde as informações estarão fisicamente armazenadas: os serviços de nuvem terceirizados deverão estar hospedados em território nacional.

Cabe ao CTIC e ao GSIC estabelecer a ferramenta padrão de armazenamento em nuvem própria.

5.2.5.5. Recursos de Impressão, Copiadoras e Aparelhos de Fax

A utilização dos recursos de impressão deve ser feita de modo que as informações sigilosas e pessoais não sejam expostas a pessoas não autorizadas.

A autorização para uso das impressoras coloridas pelos usuários será dada pelo respectivo Superintendente (ou cargo correspondente).

Compete aos usuários dos serviços e recursos de impressão, copiadoras e aparelhos de fax da EPE:

- Utilizar o recurso de proteção por senha, ao imprimir informações sigilosas, de forma a evitar que pessoas não autorizadas tenham acesso às informações;
- Cuidar para que não sejam deixadas informações sigilosas à disposição de pessoas não autorizadas, ao utilizar as impressoras, copiadoras ou aparelhos de fax;
- Solicitar a reposição de insumo, ao *Service Desk*, ao perceber que a impressora em questão encontra-se sem papel; e
- Utilizar as impressoras com bom senso, evitando o desperdício de recursos da empresa, devendo-se dar preferência a correções de trabalhos na tela do computador, ao invés de papel impresso.
- Dar preferência, no caso de impressões para provas, à impressão em preto e branco ao invés da colorida.

É vedado aos usuários dos serviços e recursos de impressão da EPE:

- Abandonar folhas impressas nas bandejas de saída das impressoras e nas mesas ou armários próximos a ela.
- Reinserir nas impressoras folhas em branco ou já impressas, devendo tais folhas ser tratadas como rascunho, desde que observadas as questões legais referente a informações classificadas como sigilosas e pessoais.

5.2.5.6. Rede de Dados

Compete aos usuários dos recursos de rede armazenar informações digitais dos trabalhos executados na EPE, e pela EPE, em áreas de dados incluídas nos procedimentos de *backup*.

O armazenamento de informações sigilosas deve ser feito em locais com acesso restrito e adequado ao nível de sigilo do documento e que possuam os níveis adequados de disponibilidade, integridade, confidencialidade e autenticidade.

Na pasta “Meus Documentos” de cada usuário devem ser salvos os trabalhos em andamento, confidenciais, temporários e importantes, sendo vedado salvar nesta pasta arquivos particulares e arquivos que precisam ser compartilhados com outros usuários.

O usuário deverá realizar, periodicamente, a manutenção da pasta individual “Meus documentos”, bem como dos diretórios compartilhados na rede à sua disposição, a fim de que contenham somente arquivos efetivamente necessários.

Só é permitido conectar à rede de comunicação da EPE recursos pessoais de TIC e de terceiros, sejam estes recursos computadores, *laptops*, celulares, *smartphones*, *pendrives* etc.., se autorizados pela STI.

A utilização de recursos pessoais de TIC para a realização de trabalho da EPE só poderá ser efetuada mediante prévia e expressa autorização do Superintendente do usuário. Nesse caso, fica o usuário ciente de que seu recurso poderá ser inspecionado e monitorado a qualquer momento e sujeito às demais considerações dessa norma e das demais normas de segurança da informação e comunicações vigentes na EPE.

5.2.5.7. Recursos de Trabalho Remoto

Para utilização de recursos de trabalho remoto (computação móvel, telefonia) em locais públicos, é necessário tomar cuidados relativos ao risco de captação da informação por pessoas não autorizadas assim como proteger fisicamente contra furto os equipamentos móveis, especialmente em viagens e atividades fora da Empresa, e executar qualquer trabalho remoto somente após ser devidamente autorizado.

O trabalho remoto por parte do usuário deve ser previamente autorizado pelo seu superior imediato.

5.2.5.8. Navegação na Web

Compete aos usuários quando da utilização do navegador da web:

- Digitar no navegador o endereço desejado dos *sites*, evitando utilizar links preparados por terceiros, que podem levar a *sites* mal intencionados que possuam endereços semelhantes.
- Observar, quando for o caso, as orientações para o tratamento de informações classificadas como sigilosas e pessoais.
- Verificar se o certificado de segurança do *site* acessado está íntegro e se corresponde realmente ao site desejado, observando ainda se o mesmo está dentro do prazo de validade.

- Utilizar somente as ferramentas seguras de compartilhamento e transmissão de dados disponibilizadas pela Empresa.
- Utilizar os recursos de Internet para acessar *sites*, tais como bancários, mercantis, de jornais, revistas e de pesquisa e busca em volume razoável, necessário ao atendimento de necessidades pessoais mínimas, com o objetivo de lhe proporcionar maior comodidade e agilidade, e desde que não haja risco para os sistemas e serviços de informática da EPE, nem fiquem comprometidas a eficiência, a produtividade e o andamento das atividades profissionais do usuário.

5.2.6. Informações Sigilosas

As informações geradas no âmbito da EPE são de sua propriedade, independentemente da forma de sua apresentação ou armazenamento. Assim, essas informações devem ser adequadamente protegidas e utilizadas exclusivamente para fins relacionados às atividades desenvolvidas na EPE.

Toda informação gerada pela EPE deverá ser classificada em função do seu grau de confidencialidade, criticidade, disponibilidade, integridade e prazo de retenção, e a autorização, o acesso e o uso dessas informações devem ser controlados de acordo com seu grau de sigilo.

O acesso às informações produzidas ou custodiadas pela EPE, que não sejam de domínio público, deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos usuários devidamente credenciados. Qualquer outra forma de uso que extrapole as atribuições necessárias ao desempenho das atividades dos usuários necessitará de prévia autorização formal.

O acesso, quando autorizado, dos usuários externos a informações produzidas ou custodiadas pela EPE que não sejam de domínio público, é condicionado ao aceite de termo de sigilo e responsabilidade.

Quando essas informações forem produzidas por terceiros para uso exclusivo da EPE, os criadores serão obrigados a manter sigilo permanente do seu conteúdo por meio de instrumento próprio devidamente validado pelo GSIC e CSIC e deverão eliminar tais informações, após autorização da EPE.

Não é permitido fornecer informações a terceiros sobre usuários ou serviços disponibilizados nos sistemas de TIC, exceto os de natureza pública ou mediante autorização de autoridade competente.

No tratamento em meios eletrônicos de informações classificadas como sigilosas ou pessoais, deverá ser observado o seguinte:

- Somente fornecer informações sigilosas em *sites* que ofereçam conexões seguras; e
- Utilizar criptografia sempre que enviar ou receber dados com informações sigilosas.

Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pela EPE devem observar o contido nesta norma e nos demais dispositivos integrantes da Política de Segurança da Informação e Comunicações da EPE.

6. Disposições Gerais

Esta norma e todas as normas relacionadas à SIC deverão ser revisadas no máximo a cada três anos ou sempre que se fizer necessário.

A não observância dessa norma pode implicar em ações administrativas, civis e penais nos termos da legislação aplicável.

Casos omissos ou excepcionais serão submetidos à decisão da Diretoria Executiva.

Este Instrumento Normativo entra em vigor em 19/01/2015, conforme decisão da Diretoria Executiva da EPE.

7. Anexos

Não se aplica.