INSTITUTO DE PESQUISA ECONÔMICA APLICADA

PORTARIA nº 456 , DE 04 DE NOVEMBRO DE 2010.

Institui a Política de Segurança da Informação e Comunicações – POSIC, no âmbito do IPEA.

O PRESIDENTE DO INSTITUTO DE PESQUISA ECONÔMICA APLICADA, no uso de suas atribuições, tendo em vista o art. 17, do Decreto Nº 7.142, de 29 de março de 2010, publicado no DOU de 30 de março de 2010, e

Considerando a) o Decreto nº 3.505, de 13.06.2000, que institui a Política de Segurança da Informação e Comunicações da Administração Pública Federal;

Considerando b) a Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 13.06.2008, que disciplina a gestão de segurança da informação e comunicações no âmbito da Administração Pública Federal;

Considerando c) a Norma Complementar Nº 03 à Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 10.06.2009, que estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (POSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

Considerando d) a Portaria nº 310, de 02.07. 2009, que institui a Política de Segurança da Tecnologia da Informação da Presidência da República, da qual são parte integrante as normas e procedimentos complementares e afins editados pelos órgãos ou entidades integrantes da Presidência da República;

Considerando e) a Portaria nº 321, de 21 julho de 2010, Institui o Sistema de Gestão da Segurança da Informação - SGSI do IPEA;

Resolve:

Art. 1º Fica instituída a Política de Segurança da Informação e Comunicações – POSIC, no âmbito do IPEA, conforme definido a seguir.

CAPÍTULO I – DA ABRANGÊNCIA E CAMPO DE APLICAÇÃO

Art. 2º A Política de Segurança da Informação e Comunicações do IPEA é uma declaração formal do Instituto acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda.

Art. 3º Esta norma regulamenta as diretrizes institucionais relativas à Segurança da Informação e Comunicações no âmbito do IPEA.

§ 1º Essa política aplica-se às atividades de todos os servidores e colaboradores que exercem atividades no âmbito do IPEA e de suas unidades descentralizadas ou quem quer que venha a ter acesso a dados ou informações protegidos por esse regulamento.

§ 2º Essa política aplica-se também a órgãos, entidades e empresas, públicas ou privadas, que compartilhem as instalações físicas e lógicas do IPEA, inclusive em suas unidades descentralizadas.

Art. 4º A Política de Segurança da Informação faz parte do Sistema de Gestão da Segurança da Informação – SGSI do IPEA, instituído pela Portaria nº 321, de 21 de julho de 2010.

CAPÍTULO II – DOS TERMOS E DEFINIÇÕES

Art. 5º - Para efeitos da Política de Segurança da Informação, ficam estabelecidos os seguintes termos e definições:

I - Ameaças: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

II - Ataques: atos intencionais que podem produzir violações de segurança.

III - Ativos: qualquer coisa que tenha valor para a organização.

IV - Auditoria: o processo de auditoria colhe dados sobre atividades em um sistema, analisando-os para descobrir violações de segurança ou diagnosticar suas causas.

V - Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, por um determinado sistema, órgão ou entidade.

VI - Avaliação/Análise de Riscos: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

VII - Colaborador: todas as pessoas envolvidas com o desenvolvimento de atividades na organização, de caráter permanente, continuado ou eventual, incluindo prestadores de serviço, bolsistas, consultores e estagiários.

VIII - Comitê de Tecnologia da Informação - CTI: grupo de pessoas com a responsabilidade de assessorar o Presidente do Ipea na definição das diretrizes e das políticas de tecnologia da informação e de segurança da informação no âmbito do Ipea, em conformidade com as portarias nº 373, de 23 de dezembro de 2009 e nº 321, de 21 julho de 2010.

IX - Confiabilidade: é o grau de fidelidade da informação em relação ao original, bem como a capacidade de um elemento em desempenhar satisfatoriamente a função requerida, sob condições de operação estabelecidas, por um período de tempo predeterminado.

X - Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

XI - Conformidade: garantia formal de que um produto ou serviço, devidamente identificado, está de acordo com uma norma legal.

XII - Dado: qualquer elemento identificado em sua forma bruta, que em determinado contexto não conduz, por si só, à compreensão de determinado fato ou situação.

XIII - Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma entidade autorizada.

XIV - 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.

XV - Evento de Segurança da Informação: uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

XVI - Gestão de Riscos: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

XVII - Gestor de Segurança da Informação e Comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito do Ipea, conforme estabelecido na Portaria nº 321, de 21 julho de 2010.

XVIII - Incidente de Segurança da Informação: um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

XIX - Informação: dados organizados e inseridos em um contexto, de maneira a propiciar determinado retorno ao manipulador, permitindo a escolha entre os vários caminhos que possam levar a um resultado.

XX - Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

XXI - Mecanismo de Segurança: um método, uma ferramenta ou um procedimento para implementar uma política de segurança. Os mecanismos de segurança têm por objetivo prevenir e detectar ataques a sistemas, além de recuperar o alvo de violações de segurança.

XXII - Não Repúdio: previne que a parte remetente ou destinatário de uma comunicação ou transação neguem sua participação.

XXIII - Política de Segurança da Informação e Comunicações (POSIC): 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;

XXIV - Procedimentos de Segurança da Informação: instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades do IPEA;

XXV - Rastro de Auditoria: evidências que demonstrem como uma transação específica foi iniciada, processada e encerrada. Os registros contidos nos rastros de auditoria devem ser suficientes para permitir a reconstrução, revisão e sequenciamento das ações no ambiente durante uma transação, desde o seu início até a saída dos resultados finais. São utilizados para detectar e dissuadir possíveis violações de segurança nos sistemas computacionais e identificar um mau uso.

XXVI - Responsabilidade: obrigações e deveres da pessoa que ocupa determinada função em relação aos ativos.

XXVII - Risco: 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.

XXVIII - Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. Outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

XXIX - Servidor: pessoa legalmente investida em cargo público.

XXX - Sistema de Gestão da Segurança da Informação – SGSI: a parte do sistema de gestão institucional, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

XXXI - Tratamento da Informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

XXXII - Usuário: indivíduo com acesso autorizado a dados e informações de acordo com as restrições e permissões definidas.

XXXIII - Violação de Segurança ou Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações em uma ou mais propriedades de segurança.

XXXIV - Vulnerabilidades: 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.

CAPÍTULO III – DOS PRINCÍPIOS

Art. 6º A Política de Segurança é regida pelos seguintes princípios:

I - Clareza: as normas e procedimentos de segurança devem ser claros o suficiente para que todos os envolvidos com a informação possam entender suas responsabilidades, direitos e limites;

II - Responsabilidade: as responsabilidades primárias e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas.

III - Conhecimento: para garantir a confiança no sistema, os administradores, os fornecedores e os usuários de um sistema de informação devem ter ciência de todas as normas e procedimentos de segurança necessários.

IV - Ética: todos os direitos e interesses legítimos devem ser respeitados sem comprometimento da segurança;

V - Legalidade: os processos de segurança devem levar em consideração os objetivos e a Missão do IPEA, bem como as leis, normas e políticas organizacionais, administrativas, comerciais, técnicas e operacionais.

VI - Proporcionalidade: o nível, a complexidade e os custos dos processos de segurança devem ser apropriados e proporcionais ao valor e à necessidade de confiança nos sistemas de informação considerando a severidade, a probabilidade e a extensão de um dano potencial ou atual.

VII - Integração: os processos de segurança devem ser coordenados e integrados entre si e com os demais processos e práticas da organização a fim de manter a coerência do Sistema de Gestão da Segurança da Informação.

VIII - Celeridade: as ações de resposta a incidentes e de correções de falhas de segurança devem ser tomadas o mais rápido possível.

IX - Atualização: as normas e os mecanismos de segurança devem ser reavaliados periodicamente, uma vez que os sistemas de informação e os requisitos de segurança variam com o tempo.

X - Liberdade: o Sistema de Gestão da Segurança da Informação deve ser compatível com o legítimo uso e fluxo de informações e de dados, devendo ser observadas as normas de privacidade e de direito de realização de auditorias.

XI - Interoperabilidade: os mecanismos de segurança devem seguir, sempre que viável, os Padrões de Interoperabilidade do Governo Eletrônico – e-PING.

XII - Intercâmbio: promover o intercâmbio científico e tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação.

XIII - Capacitação: promover a capacitação contínua de recursos humanos para o desenvolvimento de competência em segurança da informação.

CAPÍTULO IV – DAS DIRETRIZES GERAIS

Art. 7º A Política de Segurança da Informação e Comunicações do IPEA considera, prioritariamente, as seguintes diretrizes gerais:

I - Tratamento da Informação: todas as informações usadas e geradas no âmbito do IPEA devem ser tratadas para assegurar a aplicação dos princípios da integridade, confidencialidade, disponibilidade e autenticidade da informação, conforme procedimentos definidos em norma complementar editada por este órgão.

II - Tratamento de Incidentes de Rede: os incidentes de rede serão recebidos, analisados e tratados pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

III - Gestão de Riscos: os riscos devem ser continuamente monitorados e tratados, de acordo com as vulnerabilidades associadas aos ativos de informação e aos níveis de risco.

IV - Gestão de Continuidade: as ações relativas à garantia da continuidade dos processos críticos para o bom funcionamento do IPEA são previstas e tratadas pelo Plano de Continuidade do Negócio, definido em norma complementar; este plano deverá ser difundido, revisado e testado periodicamente.

V - Auditoria e Conformidade: a conformidade da aplicação da Política de Segurança da Informação e Comunicações deve ser auditada, no mínimo, a cada 12 meses.

VI - Controles de Acesso: o controle de acesso à informação deve ser implantado nos níveis físico e lógico, em conformidade com o tratamento da informação; o acesso à informação deve ser registrado e monitorado, possibilitando a geração de rastros de auditoria.

VII - Uso de recursos e serviços de tecnologia da informação: os equipamentos, softwares e serviços de tecnologia da informação providos pelo IPEA são ferramentas de produtividade para o uso exclusivamente corporativo; são exemplos de serviços de TI, entre outros, o e-mail corporativo, o acesso à internet, as bases de dados e os sistemas corporativos; a disponibilização e o uso destes recursos devem obedecer às regras definidas em normas complementares editadas por este órgão; todo uso aos recursos corporativos deve ser registrado e monitorado, possibilitando a geração de rastros de auditoria.

VIII - Sistemas de Informação e softwares: os produtos decorrentes e as atividades de contratação, manutenção e desenvolvimento de software devem considerar os princípios de segurança da informação definidos na POSIC, as metodologias e as normas complementares;

CAPÍTULO V – DAS PENALIDADES

Art. 8º As violações da Política da Segurança da Informação serão penalizadas de acordo com as normas institucionais, não excluindo as penalidades previstas na legislação vigente.

CAPÍTULO VI – DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 9º Compete exclusivamente ao Presidente do IPEA:

I - A aprovação de revisões do POSIC e das normas complementares para implantação das diretrizes estabelecidas nessa política de segurança;

II - Nomear o Gestor de Segurança da Informação e Comunicações dentre servidores públicos civis ou militares; e

III - Instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

Art. 10º O Comitê de Tecnologia da Informação deverá atuar em conformidade com as competências e responsabilidades definidas no Art. 3º da Portaria nº 321, de 21 julho de 2010.

Art. 11º Compete ao Gestor de Segurança da Informação e Comunicações:

I - Atuar em conformidade com as competências e responsabilidades definidas no Art 4º da Portaria nº 321, de 21 de julho de 2010; e

II - Propor ao Comitê de Tecnologia da Informação os planos de metas e ações para implantação e manutenção da POSIC.

Art. 12º Compete à Coordenação Geral de Tecnologia da Informação e Comunicações – CGTIC:

I – Prestar suporte técnico e administrativo ao Gestor de Segurança da Informação e Comunicações para o cumprimento de suas competências;

II - Implantar e gerenciar os mecanismos de segurança e controles definidos na POSIC e normas complementares; e

III - Executar, quando pertinente, avaliação de riscos sobre procedimentos não documentados e a adoção de novas tecnologias.

Art. 13º É de responsabilidade das chefias de unidades e diretorias do IPEA fomentar o bom uso dos recursos de Tecnologia da Informação e Comunicação, bem como garantir que essa norma seja respeitada pelos seus subordinados;

Art. 14º Compete a todos os servidores e colaboradores do IPEA:

I - Cumprir e fazer cumprir as normas e procedimentos relativos à segurança da informação e comunicações do IPEA;

II - Contribuir, quando necessário, com propostas para a melhoria da segurança da Informação e Comunicações do IPEA; e

III - Zelar pelo bom funcionamento dos mecanismos e procedimentos de segurança do IPEA.

Art. 15º. Deverão assinar o termo de responsabilidade sobre a observância da Política de Segurança da Informação do IPEA, todos os servidores, colaboradores, órgãos, entidades e empresas, públicas ou privadas, que exercem atividades no âmbito do IPEA ou que compartilhem as instalações físicas e lógicas do Instituto, inclusive em suas unidades descentralizadas.

CAPÍTULO VII – DA FREQUÊNCIA DE REVISÃO

Art 16º. A Política de Segurança da Informação e Comunicações será atualizada obrigatoriamente a cada 2 anos e revisada conforme auditorias ou quando se fizer necessário;

Parágrafo único. Os instrumentos normativos gerados a partir desta política devem ser revisados sempre que se fizer necessário.

CAPÍTULO VIII – DAS DISPOSIÇÕES FINAIS

Art. 17º. A Política e as Normas de Segurança da Informação devem ser divulgadas aos servidores, colaboradores, órgãos, entidades e empresas, públicas ou privadas, que exercem atividades no âmbito do IPEA ou que compartilhem as instalações físicas e lógicas do Instituto e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Parágrafo único. Os Procedimentos de Segurança da Informação devem ser divulgados às áreas diretamente relacionadas à sua aplicação.

Art. 18º. Casos omissos serão resolvidos pelo Comitê de Tecnologia da Informação do IPEA, observando-se a legislação em vigor.

Art. 19º. Esta Portaria entra em vigor na data de sua publicação.

MARCIO POCHMANN