PREVIDÊNCIA SOCIAL
INSTITUTO NACIONAL DO SEGURO SOCIAL

RESOLUÇÃO Nº 323/PRES/INSS, DE 22 DE JULHO DE 2013

Institui a Política de Segurança da Informação e Comunicações do Instituto Nacional do Seguro Social.

FUNDAMENTAÇÃO LEGAL:
Decreto nº 3.505, de 13 de junho de 2000;
Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008; e
Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009.

O **PRESIDENTE DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS**, no uso das atribuições que lhe confere o Decreto nº 7.556, de 24 de agosto de 2011, considerando a necessidade de estabelecer diretrizes para proteção das informações geradas, processadas e armazenadas,

RESOLVE:

Art. 1º Fica instituída no âmbito do INSS e nos termos do Anexo a esta Resolução, a Política de Segurança da Informação e Comunicações - POSIC-INSS.

Art. 2º Esta Resolução entra em vigor na data de sua publicação e seu Anexo será publicado em Boletim de Serviço.

LINDOLFO NETO DE OLIVEIRA SALES
Presidente

Publicado no DOU nº 140, de 23/7/2013 seção 1 pag.38

ANEXO
RESOLUÇÃO Nº 323/PRES/INSS, DE 22 DE JULHO DE 2013

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS

1. INTRODUÇÃO

A Política de Segurança da Informação e Comunicações do Instituto Nacional do Seguro Social – POSIC-INSS, visa preservar a disponibilidade, integridade, confidencialidade, autenticidade e salvaguarda das informações geradas, processadas e armazenadas no âmbito do Instituto.

2. ESCOPO

2.1 Objetivo:

Esta POSIC-INSS tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação e Comunicações, especificamente para o INSS, para orientação quanto ao uso adequado da informação de sua propriedade, em complemento e em consonância com o estabelecido na Política de Segurança da Informação e Comunicações da Previdência Social, estabelecida pela Portaria Conjunta MPS/INSS/DATAPREV nº 1, de 5 de novembro de 2008.

2.2 Abrangência:

Os termos definidos nesta Política e em suas normas complementares aplicam-se a todos os agentes públicos e privados com vínculo direto ou indireto com o INSS.

3. CONCEITOS

Para os efeitos desta Política de Segurança da Informação e Comunicações ficam estabelecidos os seguintes conceitos e definições:

3.1 segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e autenticidades das informações;

3.2 salvaguarda de informações: medidas aplicadas na proteção das informações, quanto ao acesso, à divulgação e perda, utilizadas para prevenir ou remediar prejuízo aos objetivos institucionais;

3.3 acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade;

3.4 necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança, tenha acesso a dados ou informações sigilosos;

3.5 agente público: todas as pessoas físicas que manifestam, por algum tipo de vínculo, a vontade do Estado, abarcando servidores, ocupantes de cargo comissionado ou em comissão, prestadores de serviço e estagiários;

3.6 ativo: tudo que tenha ou gere valor para a organização;

3.7 ativos de informação: é o ativo composto por todos os dados, informações e conhecimentos gerados, armazenados e processados no INSS, bem como os locais onde se encontram e as pessoas que têm acesso;

3.8 vínculo direto: agentes públicos contratados diretamente pelo INSS;

3.9 vínculo indireto: agentes públicos pertencentes a órgãos ou unidades da Administração Pública Federal, Estadual ou Municipal que mantenham contrato, convênio ou acordo de cooperação técnica com o INSS ou agentes privados pertencentes às empresas que mantenham contrato com o Instituto, que obtenham acesso às informações do INSS;

3.10 ameaças: conjunto de fatores externos ou causa potencial de um incidente, que podem resultar em risco para um sistema ou organização;

3.11 vulnerabilidade: fatores internos ou causa potencial de um incidente indesejado, que podem ser evitados por uma ação interna de segurança da informação e comunicações;

3.12 riscos 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 organização;

3.13 gestão de riscos de segurança da informação e comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

3.14 gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e possíveis impactos nas operações de negociação, caso essas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes, reputação, marca da organização e suas atividades de valor agregado;

3.15 gestão de segurança da informação e comunicações: ações e métodos que visam à integração das atividades de gestão de riscos e de continuidade de negociação, tratamento de incidentes e da informação, conformidade, credenciamento, segurança cibernética, física, lógica, orgânica e organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação e Comunicação;

3.16 gestor de segurança da informação e comunicações: servidor nomeado pelo Presidente como responsável pela gestão de segurança da informação e comunicações no âmbito do INSS;

3.17 Comitê de Segurança, Tecnologia da Informação e Comunicações do Instituto Nacional do Seguro Social – CSTIC-INSS: colegiado responsável em propor políticas, diretrizes, normas, padrões, metodologia, planos, programas e projetos de Segurança, Tecnologia da Informação e Comunicações no âmbito do INSS;

3.18 Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR-INSS: equipe com responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores no âmbito do INSS; e

3.19 tratamento de incidentes: 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.

4. REFERÊNCIAS LEGAIS E NORMATIVAS

Esta Política tem o objetivo de declarar o comprometimento da direção do INSS com vistas a promover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a Gestão de Segurança da Informação e Comunicações neste Instituto e foi elaborada com base nos seguintes documentos:

a. Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

b. Lei nº 9.279, de 14 de maio de 1996, que regula direitos e obrigações relativas à propriedade industrial;

c. Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe acerca da proteção da propriedade intelectual de programa de computador e sua comercialização no País;

d. Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), que dispõe sobre a tipificação de crimes digitais contra a Administração Pública;

e. Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

f. Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

g. 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;

h. Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

i. 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;

j. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008, que disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

k. Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que estabelece as diretrizes para elaboração de política de segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal; e

l. NBR ISO/IEC 27002-2005, que institui código de melhores práticas para a Gestão de Segurança da Informação.

5. PRINCÍPIOS

5.1 A segurança da informação e comunicações busca reduzir os riscos de vazamentos, fraudes, erros, uso indevido, sabotagens, paralisações e roubo de informações ou qualquer outra ameaça que possa prejudicar os sistemas de informação, os recursos de processamento da informação ou os equipamentos do INSS.

5.2 A confiabilidade: requer que os meios, nos quais a informação trafega e é armazenada, sejam preparados para promover e garantir eficientemente a recuperação dessa informação caso haja insucesso de mudança ou evento inesperado, com observância dos demais princípios de segurança.

5.3 A responsabilidade: propriedade de que todo ativo de informação possua um responsável que garanta sua correta utilização, além de monitorá-lo de maneira que o uso indevido seja reportado e as ações cabíveis tomadas.

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

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

5.6 Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada ou não credenciada.

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

5.8 Legalidade: as ações de segurança devem levar em consideração as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais do INSS.

5.9 Ética: os direitos e interesses legítimos dos usuários devem ser preservados sem comprometimento da Segurança da Informação e Comunicações.

6. DIRETRIZES GERAIS

6.1 O cumprimento desta POSIC e de suas normas complementares devem ser avaliados periodicamente por meio de verificações de conformidade.

6.2 A Gestão de Segurança da Informação e Comunicações – GSIC no INSS deve ser orientada pelas diretrizes estabelecidas nesta POSIC-INSS e também pelas melhores práticas e procedimentos de Segurança da Informação e Comunicações – SIC, recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento destes padrões.

6.3 Os servidores que compõem a estrutura de GSIC do INSS devem receber periodicamente capacitação especializada nas disciplinas relacionadas à SIC.

6.4 Todo acesso a informação será motivado pela necessidade de conhecer.

7. DIRETRIZES ESPECÍFICAS

7.1 Tratamento da Informação

7.1.1 Toda informação criada ou custodiada que for manuseada, armazenada, transportada ou descartada pelos agentes públicos ou privados vinculados ao INSS, no exercício de suas atividades, é de propriedade desta Entidade e será protegida. Para tanto, o Instituto deve criar, gerir, avaliar e divulgar os critérios de tratamento, de salvaguarda e de classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, segundo as diretrizes estabelecidas nesta POSIC e nas regulamentações em vigor.

7.1.2 Todo usuário deve ser capaz de identificar a classificação atribuída a uma informação tratada pelo INSS e, a partir dela, conhecer e obedecer às restrições e divulgações associadas.

7.2 Tratamento de Incidentes de Rede

7.2.1 Os incidentes de segurança da informação serão relatados por meio dos canais apropriados da Instituição, o mais rápido possível.

7.2.2 Os agentes públicos usuários de sistemas e serviços de informação serão instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade de segurança em sistemas ou serviços.

7.2.3 Os procedimentos de gestão de incidentes de rede serão observados para assegurar respostas rápidas, efetivas e ordenadas quando necessário.

7.2.4 Soluções de contorno aplicadas para minimizar a ocorrência de incidentes de segurança serão temporárias e imediatamente submetidas ao gestor de segurança da informação e comunicações com definição do prazo para que a solução definitiva do problema seja implementada.

7.2.5 As evidências dos incidentes de segurança serão coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento, instituídas pelo órgão competente.

7.2.6 A gestão de incidentes de segurança da informação deverá ser regida por norma específica sobre a matéria.

7.3 Gestão de Risco

7.3.1 O INSS deve implementar e manter processo de gestão de riscos com vistas a minimizar possíveis impactos associados aos ativos de informação e comunicações.

7.3.2 O processo de gestão de riscos deve possibilitar a identificação, a seleção e a priorização dos ativos a serem protegidos, bem como a definição e implementação de controles e tratamento de possíveis riscos de segurança da informação.

7.3.3 O processo de gerenciamento de riscos será contínuo, com revisões periódicas a serem definidas pelo gestor de segurança da informação e comunicações.

7.4 Gestão de Continuidade

7.4.1 O INSS deve implementar, manter e testar periodicamente processo de gestão da continuidade de negócios visando reduzir, para um nível aceitável, a possibilidade de interrupção causada por desastres ou incidentes de segurança que afetem seus ativos de informação e comunicações.

7.4.2 O INSS deve incluir nos contratos de prestação de serviços de Tecnologia da Informação e Comunicações – TIC, cláusula estabelecendo que a prestadora de serviço deve apresentar semestralmente ao CSTIC-INSS os planos de continuidade de operações e serviços ou suas atualizações, acompanhadas da análise e avaliação de risco atualizada.

7.5 Auditoria e Conformidade

7.5.1 O uso dos recursos de TIC disponibilizados pelo INSS é passível de monitoramento e auditoria. Devem ser implementados e mantidos mecanismos e procedimentos, como trilhas de auditoria e outros que permitam o processo de auditoria e conformidade por meio da rastreabilidade dos acessos e operações.

7.5.2 As auditorias internas em segurança da informação serão reguladas e formalizadas e aprovadas pela Auditoria Interna do INSS.

7.6 Controles de Acesso

7.6.1 O INSS deve estabelecer e exigir das prestadoras de serviços de TIC contratadas, mecanismos de proteção que contemplem:

7.6.1.1 controle de Acesso Lógico: aplicáveis aos sistemas informatizados, permitindo a verificação da identidade dos usuários que utilizam seus serviços. Deve, ainda, utilizar a legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro; e

7.6.1.2 controle de Acesso Físico: aplicáveis a todas as instalações físicas do Instituto, por meio de mecanismos que garantam a identificação de todos os usuários que fazem uso das mesmas.

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

7.6.3 As proteções devem estar associadas aos riscos identificados.

7.7 Uso de *e-mail* e Acesso à internet

7.7.1 A ferramenta de correio eletrônico é um meio de comunicação corporativa do INSS e deve ser utilizada de acordo com os princípios estabelecidos nesta POSIC e demais normas que regulamentam seu uso.

7.7.2 Os recursos de internet, *e-mail* ou qualquer outro existente ou que venham a ser adotados, devem ser utilizados em consonância com os interesses do Instituto e de acordo com normativos específicos.

7.7.3 O uso de tais serviços devem ser disciplinados e serão fornecidos mediante o estabelecimento formal de Termo de Responsabilidade, que contemple a necessidade da disponibilização do recurso e o conhecimento por parte do usuário dos critérios, regras e responsabilidades estabelecidos nesta POSIC-INSS e demais normas e legislações que tratam desta matéria.

7.8 Gestão de Mudanças

O INSS deverá adotar a gestão de mudança para toda e qualquer mudança estrutural em seus sistemas, que deverá incluir basicamente a:

7.8.1 manutenção de um registro dos níveis acordados de autorização;

7.8.2 análise crítica dos procedimentos de controle e integridade para assegurar que as mudanças não os comprometam;

7.8.3 identificação de todo *software*, informação, entidades em bancos de dados e *hardware* que precisam de emendas;

7.8.4 obtenção de aprovação formal para propostas detalhadas antes da implementação;

7.8.5 manutenção de um controle de versão de todas as atualizações de *softwares*; e

7.8.6 manutenção de uma trilha para auditoria de todas as mudanças executadas.

8. PENALIDADES

A não observância dos preceitos desta POSIC implicará na aplicação de sanções administrativas, cíveis e penais previstas no Estatuto do Servidor Público Federal - Lei n° 8.112, de 11 de dezembro de 1990; no Código Penal - Decreto-Lei n° 2.848, de 7 de dezembro de 1940; no Código Civil - Lei nº 10.406, de 10 de janeiro de 2002, e, ainda, em legislação que regule ou venha regular a matéria.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1 Estrutura de Gestão de SIC

A estrutura de Gestão de Segurança da Informação e Comunicações – GSIC, será composta:

9.1.1 pelo Gestor de Segurança da Informação e Comunicações do INSS;

9.1.2 pelo Comitê de Segurança da Informação e Comunicações do Instituto Nacional do Seguro Social – CSIC-INSS; e

9.1.3 pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR-INSS.

9.2 A composição e as atribuições do CSIC-INSS serão estabelecidas por portaria do Presidente do INSS.

9.3 O Gestor de Segurança da Informação e Comunicações deverá ser designado pelo Presidente do INSS e será responsável por:

9.3.1 promover cultura de segurança da informação e comunicações;

9.3.2 promover a melhoria contínua dos processos de gestão de segurança da informação e comunicação;

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

9.3.4 propor recursos necessários às ações de segurança da informação e comunicações;

9.3.5 coordenar o CSIC-INSS e a ETIR-INSS;

9.3.6 realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na segurança da informação e comunicações;

9.3.7 manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, para o trato de assuntos relativos à segurança da informação e comunicações;

9.3.8 propor normas e procedimentos relativos à segurança da informação e comunicações no âmbito do INSS;

9.3.9 promover e acompanhar a implementação desta POSIC-INSS, bem como propor e receber propostas de ajustes corretivos e de melhoria a serem incluídos nas suas revisões; e

9.3.10 Até que o CSIC-INSS seja instituído, o Gestor de Segurança da Informação e Comunicações atuará como membro do Comitê de Segurança e Tecnologia da Informação do INSS – CSTIC-INSS.

9.4 Cabe à ETIR-INSS:

9.4.1 facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

9.4.2 monitorar e atuar junto às empresas prestadoras de serviços de TIC na recuperação de sistemas corporativos;

9.4.3 agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;

9.4.4 realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, identificando causas, danos e responsáveis para fins de aplicação das devidas penalidades, se for o caso;

9.4.5 receber das empresas prestadoras de serviços de TIC, para fins de análise, relatórios relativos a ataques e intrusões na rede do INSS;

9.4.6 executar as ações necessárias para tratar quebras de segurança;

9.4.7 obter, junto às empresas prestadoras de serviços de TIC, informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, soluções praticadas, frequência e custos resultantes;

9.4.8 cooperar com outras Equipes de Tratamento e Resposta a Incidentes; e

9.4.9 participar em *fóruns*, redes nacionais e internacionais relativos à SIC.

9.5 Cabe aos terceiros e fornecedores, conforme previsto em contrato:

9.5.1 tomar conhecimento desta POSIC-INSS;

9.5.2 fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e

9.5.3 fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

9.6 São responsabilidades atribuídas aos usuários que utilizam os recursos de processamento pertencentes ou controlados pelo INSS:

9.6.1 conhecer e cumprir a POSIC-INSS;

9.6.2 zelar pelas informações e equipamentos disponibilizados para a execução do seu serviço; e

9.6.3 participar de eventos promovidos pelo CSIC-INSS relacionados à segurança de informação.

10. REVISÃO

A POSIC-INSS e todos os atos normativos dela decorrentes devem ser revisados, sempre que necessário, não excedendo o período máximo de três anos.

PREVIDÊNCIA SOCIAL
INSTITUTO NACIONAL DO SEGURO SOCIA

ANEXO
RESOLUÇÃO Nº 323/PRES/INSS, DE 22 DE JULHO DE 2013

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS

1. INTRODUÇÃO

A Política de Segurança da Informação e Comunicações do Instituto Nacional do Seguro Social – POSIC-INSS, visa preservar a disponibilidade, integridade, confidencialidade, autenticidade e salvaguarda das informações geradas, processadas e armazenadas no âmbito do Instituto.

2. ESCOPO

2.1 Objetivo:

Esta POSIC-INSS tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação e Comunicações, especificamente para o INSS, para orientação quanto ao uso adequado da informação de sua propriedade, em complemento e em consonância com o estabelecido na Política de Segurança da Informação e Comunicações da Previdência Social, estabelecida pela Portaria Conjunta MPS/INSS/DATAPREV nº 1, de 5 de novembro de 2008.

2.2 Abrangência:

Os termos definidos nesta Política e em suas normas complementares aplicam-se a todos os agentes públicos e privados com vínculo direto ou indireto com o INSS.

3. CONCEITOS

Para os efeitos desta Política de Segurança da Informação e Comunicações ficam estabelecidos os seguintes conceitos e definições:

3.1 segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e autenticidades das informações;

3.2 salvaguarda de informações: medidas aplicadas na proteção das informações, quanto ao acesso, à divulgação e perda, utilizadas para prevenir ou remediar prejuízo aos objetivos institucionais;

3.3 acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade;

3.4 necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança, tenha acesso a dados ou informações sigilosos;

3.5 agente público: todas as pessoas físicas que manifestam, por algum tipo de vínculo, a vontade do Estado, abarcando servidores, ocupantes de cargo comissionado ou em comissão, prestadores de serviço e estagiários;

3.6 ativo: tudo que tenha ou gere valor para a organização;

3.7 ativos de informação: é o ativo composto por todos os dados, informações e conhecimentos gerados, armazenados e processados no INSS, bem como os locais onde se encontram e as pessoas que têm acesso;

3.8 vínculo direto: agentes públicos contratados diretamente pelo INSS;

3.9 vínculo indireto: agentes públicos pertencentes a órgãos ou unidades da Administração Pública Federal, Estadual ou Municipal que mantenham contrato, convênio ou acordo de cooperação técnica com o INSS ou agentes privados pertencentes às empresas que mantenham contrato com o Instituto, que obtenham acesso às informações do INSS;

3.10 ameaças: conjunto de fatores externos ou causa potencial de um incidente, que podem resultar em risco para um sistema ou organização;

3.11 vulnerabilidade: fatores internos ou causa potencial de um incidente indesejado, que podem ser evitados por uma ação interna de segurança da informação e comunicações;

3.12 riscos 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 organização;

3.13 gestão de riscos de segurança da informação e comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

3.14 gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e possíveis impactos nas operações de negociação, caso essas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes, reputação, marca da organização e suas atividades de valor agregado;

3.15 gestão de segurança da informação e comunicações: ações e métodos que visam à integração das atividades de gestão de riscos e de continuidade de negociação, tratamento de incidentes e da informação, conformidade, credenciamento, segurança cibernética,

física, lógica, orgânica e organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação e Comunicação;

3.16 gestor de segurança da informação e comunicações: servidor nomeado pelo Presidente como responsável pela gestão de segurança da informação e comunicações no âmbito do INSS;

3.17 Comitê de Segurança, Tecnologia da Informação e Comunicações do Instituto Nacional do Seguro Social – CSTIC-INSS: colegiado responsável em propor políticas, diretrizes, normas, padrões, metodologia, planos, programas e projetos de Segurança, Tecnologia da Informação e Comunicações no âmbito do INSS;

3.18 Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR-INSS: equipe com responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores no âmbito do INSS; e

3.19 tratamento de incidentes: 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.

4. REFERÊNCIAS LEGAIS E NORMATIVAS

Esta Política tem o objetivo de declarar o comprometimento da direção do INSS com vistas a promover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a Gestão de Segurança da Informação e Comunicações neste Instituto e foi elaborada com base nos seguintes documentos:

a. Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

b. Lei nº 9.279, de 14 de maio de 1996, que regula direitos e obrigações relativas à propriedade industrial;

c. Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe acerca da proteção da propriedade intelectual de programa de computador e sua comercialização no País;

d. Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), que dispõe sobre a tipificação de crimes digitais contra a Administração Pública;

e. Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

f. Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

g. 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;

h. Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

i. 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;

j. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008, que disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

k. Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que estabelece as diretrizes para elaboração de política de segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal; e

l. NBR ISO/IEC 27002-2005, que institui código de melhores práticas para a Gestão de Segurança da Informação.

5. PRINCÍPIOS

5.1 A segurança da informação e comunicações busca reduzir os riscos de vazamentos, fraudes, erros, uso indevido, sabotagens, paralisações e roubo de informações ou qualquer outra ameaça que possa prejudicar os sistemas de informação, os recursos de processamento da informação ou os equipamentos do INSS.

5.2 A confiabilidade: requer que os meios, nos quais a informação trafega e é armazenada, sejam preparados para promover e garantir eficientemente a recuperação dessa informação caso haja insucesso de mudança ou evento inesperado, com observância dos demais princípios de segurança.

5.3 A responsabilidade: propriedade de que todo ativo de informação possua um responsável que garanta sua correta utilização, além de monitorá-lo de maneira que o uso indevido seja reportado e as ações cabíveis tomadas.

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

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

5.6 Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada ou não credenciada.

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

5.8 Legalidade: as ações de segurança devem levar em consideração as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais do INSS.

5.9 Ética: os direitos e interesses legítimos dos usuários devem ser preservados sem comprometimento da Segurança da Informação e Comunicações.

6. DIRETRIZES GERAIS

6.1 O cumprimento desta POSIC e de suas normas complementares devem ser avaliados periodicamente por meio de verificações de conformidade.

6.2 A Gestão de Segurança da Informação e Comunicações – GSIC no INSS deve ser orientada pelas diretrizes estabelecidas nesta POSIC-INSS e também pelas melhores práticas e procedimentos de Segurança da Informação e Comunicações – SIC, recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento destes padrões.

6.3 Os servidores que compõem a estrutura de GSIC do INSS devem receber periodicamente capacitação especializada nas disciplinas relacionadas à SIC.

6.4 Todo acesso a informação será motivado pela necessidade de conhecer.

7. DIRETRIZES ESPECÍFICAS

7.1 Tratamento da Informação

7.1.1 Toda informação criada ou custodiada que for manuseada, armazenada, transportada ou descartada pelos agentes públicos ou privados vinculados ao INSS, no exercício de suas atividades, é de propriedade desta Entidade e será protegida. Para tanto, o Instituto deve criar, gerir, avaliar e divulgar os critérios de tratamento, de salvaguarda e de classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, segundo as diretrizes estabelecidas nesta POSIC e nas regulamentações em vigor.

7.1.2 Todo usuário deve ser capaz de identificar a classificação atribuída a uma informação tratada pelo INSS e, a partir dela, conhecer e obedecer às restrições e divulgações associadas.

7.2 Tratamento de Incidentes de Rede

7.2.1 Os incidentes de segurança da informação serão relatados por meio dos canais apropriados da Instituição, o mais rápido possível.

7.2.2 Os agentes públicos usuários de sistemas e serviços de informação serão instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade de segurança em sistemas ou serviços.

7.2.3 Os procedimentos de gestão de incidentes de rede serão observados para assegurar respostas rápidas, efetivas e ordenadas quando necessário.

7.2.4 Soluções de contorno aplicadas para minimizar a ocorrência de incidentes de segurança serão temporárias e imediatamente submetidas ao gestor de segurança da informação e comunicações com definição do prazo para que a solução definitiva do problema seja implementada.

7.2.5 As evidências dos incidentes de segurança serão coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento, instituídas pelo órgão competente.

7.2.6 A gestão de incidentes de segurança da informação deverá ser regida por norma específica sobre a matéria.

7.3 Gestão de Risco

7.3.1 O INSS deve implementar e manter processo de gestão de riscos com vistas a minimizar possíveis impactos associados aos ativos de informação e comunicações.

7.3.2 O processo de gestão de riscos deve possibilitar a identificação, a seleção e a priorização dos ativos a serem protegidos, bem como a definição e implementação de controles e tratamento de possíveis riscos de segurança da informação.

7.3.3 O processo de gerenciamento de riscos será contínuo, com revisões periódicas a serem definidas pelo gestor de segurança da informação e comunicações.

7.4 Gestão de Continuidade

7.4.1 O INSS deve implementar, manter e testar periodicamente processo de gestão da continuidade de negócios visando reduzir, para um nível aceitável, a possibilidade de interrupção causada por desastres ou incidentes de segurança que afetem seus ativos de informação e comunicações.

7.4.2 O INSS deve incluir nos contratos de prestação de serviços de Tecnologia da Informação e Comunicações – TIC, cláusula estabelecendo que a prestadora de serviço deve apresentar semestralmente ao CSTIC-INSS os planos de continuidade de operações e serviços ou suas atualizações, acompanhadas da análise e avaliação de risco atualizada.

7.5 Auditoria e Conformidade

7.5.1 O uso dos recursos de TIC disponibilizados pelo INSS é passível de monitoramento e auditoria. Devem ser implementados e mantidos mecanismos e procedimentos, como trilhas de auditoria e outros que permitam o processo de auditoria e conformidade por meio da rastreabilidade dos acessos e operações.

7.5.2 As auditorias internas em segurança da informação serão reguladas e formalizadas e aprovadas pela Auditoria Interna do INSS.

7.6 Controles de Acesso

7.6.1 O INSS deve estabelecer e exigir das prestadoras de serviços de TIC contratadas, mecanismos de proteção que contemplem:

7.6.1.1 controle de Acesso Lógico: aplicáveis aos sistemas informatizados, permitindo a verificação da identidade dos usuários que utilizam seus serviços. Deve, ainda, utilizar a legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro; e

7.6.1.2 controle de Acesso Físico: aplicáveis a todas as instalações físicas do Instituto, por meio de mecanismos que garantam a identificação de todos os usuários que fazem uso das mesmas.

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

7.6.3 As proteções devem estar associadas aos riscos identificados.

7.7 Uso de *e-mail* e Acesso à internet

7.7.1 A ferramenta de correio eletrônico é um meio de comunicação corporativa do INSS e deve ser utilizada de acordo com os princípios estabelecidos nesta POSIC e demais normas que regulamentam seu uso.

7.7.2 Os recursos de internet, *e-mail* ou qualquer outro existente ou que venham a ser adotados, devem ser utilizados em consonância com os interesses do Instituto e de acordo com normativos específicos.

7.7.3 O uso de tais serviços devem ser disciplinados e serão fornecidos mediante o estabelecimento formal de Termo de Responsabilidade, que contemple a necessidade da disponibilização do recurso e o conhecimento por parte do usuário dos critérios, regras e responsabilidades estabelecidos nesta POSIC-INSS e demais normas e legislações que tratam desta matéria.

7.8 Gestão de Mudanças

O INSS deverá adotar a gestão de mudança para toda e qualquer mudança estrutural em seus sistemas, que deverá incluir basicamente a:

7.8.1 manutenção de um registro dos níveis acordados de autorização;

7.8.2 análise crítica dos procedimentos de controle e integridade para assegurar que as mudanças não os comprometam;

7.8.3 identificação de todo *software*, informação, entidades em bancos de dados e *hardware* que precisam de emendas;

7.8.4 obtenção de aprovação formal para propostas detalhadas antes da implementação;

7.8.5 manutenção de um controle de versão de todas as atualizações de *softwares*; e

7.8.6 manutenção de uma trilha para auditoria de todas as mudanças executadas.

8. PENALIDADES

A não observância dos preceitos desta POSIC implicará na aplicação de sanções administrativas, cíveis e penais previstas no Estatuto do Servidor Público Federal - Lei n° 8.112, de 11 de dezembro de 1990; no Código Penal - Decreto-Lei n° 2.848, de 7 de dezembro de 1940; no Código Civil - Lei nº 10.406, de 10 de janeiro de 2002, e, ainda, em legislação que regule ou venha regular a matéria.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1 Estrutura de Gestão de SIC

A estrutura de Gestão de Segurança da Informação e Comunicações – GSIC, será composta:

9.1.1 pelo Gestor de Segurança da Informação e Comunicações do INSS;

9.1.2 pelo Comitê de Segurança da Informação e Comunicações do Instituto Nacional do Seguro Social – CSIC-INSS; e

9.1.3 pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR-INSS.

9.2 A composição e as atribuições do CSIC-INSS serão estabelecidas por portaria do Presidente do INSS.

9.3 O Gestor de Segurança da Informação e Comunicações deverá ser designado pelo Presidente do INSS e será responsável por:

9.3.1 promover cultura de segurança da informação e comunicações;

9.3.2 promover a melhoria contínua dos processos de gestão de segurança da informação e comunicação;

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

9.3.4 propor recursos necessários às ações de segurança da informação e comunicações;

9.3.5 coordenar o CSIC-INSS e a ETIR-INSS;

9.3.6 realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na segurança da informação e comunicações;

9.3.7 manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, para o trato de assuntos relativos à segurança da informação e comunicações;

9.3.8 propor normas e procedimentos relativos à segurança da informação e comunicações no âmbito do INSS;

9.3.9 promover e acompanhar a implementação desta POSIC-INSS, bem como propor e receber propostas de ajustes corretivos e de melhoria a serem incluídos nas suas revisões; e

9.3.10 Até que o CSIC-INSS seja instituído, o Gestor de Segurança da Informação e Comunicações atuará como membro do Comitê de Segurança e Tecnologia da Informação do INSS – CSTIC-INSS.

9.4 Cabe à ETIR-INSS:

9.4.1 facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

9.4.2 monitorar e atuar junto às empresas prestadoras de serviços de TIC na recuperação de sistemas corporativos;

9.4.3 agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;

9.4.4 realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, identificando causas, danos e responsáveis para fins de aplicação das devidas penalidades, se for o caso;

9.4.5 receber das empresas prestadoras de serviços de TIC, para fins de análise, relatórios relativos a ataques e intrusões na rede do INSS;

9.4.6 executar as ações necessárias para tratar quebras de segurança;

9.4.7 obter, junto às empresas prestadoras de serviços de TIC, informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, soluções praticadas, frequência e custos resultantes;

9.4.8 cooperar com outras Equipes de Tratamento e Resposta a Incidentes; e

9.4.9 participar em *fóruns*, redes nacionais e internacionais relativos à SIC.

9.5 Cabe aos terceiros e fornecedores, conforme previsto em contrato:

9.5.1 tomar conhecimento desta POSIC-INSS;

9.5.2 fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e

9.5.3 fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

9.6 São responsabilidades atribuídas aos usuários que utilizam os recursos de processamento pertencentes ou controlados pelo INSS:

9.6.1 conhecer e cumprir a POSIC-INSS;

9.6.2 zelar pelas informações e equipamentos disponibilizados para a execução do seu serviço; e

9.6.3 participar de eventos promovidos pelo CSIC-INSS relacionados à segurança de informação.

10. REVISÃO

A POSIC-INSS e todos os atos normativos dela decorrentes devem ser revisados, sempre que necessário, não excedendo o período máximo de três anos.

Publicado no BS nº 140, de 23 de julho de 2013