	SERVIÇO PÚBLICO FEDERAL **MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA E COMÉRCIO EXTERIOR** **INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL**

PR	**29/07/2013**

Instrução Normativa	**Nº 24/2013**

Assunto: Institui a Política de Segurança da Informação e Comunicações no âmbito do Instituto Nacional da Propriedade Industrial – INPI.

O PRESIDENTE e a COORDENADORA-GERAL DE TECNOLOGIA DA INFORMAÇÃO do INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL – INPI, no exercício das atribuições regimentais, conferidas na forma Decreto Nº 7.356, de 12 de novembro de 2010 e tendo em vista o 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; a Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008 e a Norma Complementar nº 03 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 30 de junho de 2009,

RESOLVEM:

Art. 1° Instituir a política de Segurança da Informação e Comunicações (PoSIC) no âmbito do Instituto Nacional da Propriedade Industrial – INPI.

CAPÍTULO I

DO ESCOPO

Art. 2º A Política de Segurança da Informação e Comunicações - PoSIC objetiva instituir diretrizes estratégicas, responsabilidades e competências, visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações e documentos do Instituto Nacional da Propriedade Industrial.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para fins desta Portaria, entende-se por:

I - **Segurança da Tecnologia da Informação e Comunicações**: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações em recursos de Tecnologia da Informação;

II - **Segurança da Informação Administrativa e Documental**: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações em recursos administrativos e documentais;

III - **Quebra de Segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

IV - **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

V - **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

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

VII - **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;

VIII - **Gestão de Segurança da Informação e Comunicações**: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança lógica aos processos institucionais estratégicos, operacionais e táticos, limitada à tecnologia da informação e comunicações;

IX - **Gestão de Segurança da Informação Administrativa e Documental**: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, , segurança física, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos limitada à área adminstrativa e documental;

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

XI - **Usuário Interno**: servidores efetivos ou à disposição do INPI, agentes públicos e prestadores de serviço, através de seus representantes e empregados, autorizados a obter acesso à informações e sistemas;

XII – **Usuário Externo**: qualquer pessoa física ou jurídica, que acesse as informações disponibilizadas pelo INPI;

XIII - **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;

XIV - **Gestor de Segurança da Informação e Comunicações**: responsável pelas ações de segurança da informação e comunicações em tecnologia da informação no âmbito deste órgão;

XV - **Gestor de Segurança da Informação Administrativa e Documental**: responsável pelas ações de segurança física, administrativa e documental no âmbito deste órgão;

XVI - **Comitê de Segurança da Informação e Comunicações**: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito deste órgão;

XVII - **Equipe de Tratamento e Resposta à Incidentes em Redes Computacionais (ETIR)**: grupo de pessoas com a responsabilidade de receber, analisar e responder à notificações e atividades relacionadas à incidentes de segurança em computadores;

XVIII - **Equipe de Tratamento e Resposta à Incidentes Administrativos e Documentais (ETRAD)**: grupo de pessoas com a responsabilidade de receber, analisar e responder à notificações e atividades relacionadas à incidentes de segurança administrativo e documental.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 4º A PoSIC deve obedecer aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal, notadamente, os seguintes princípios:

I – **Responsabilidade**: todos os servidores, consultores, estagiários e prestadores de serviço do INPI são responsáveis pelo cumprimento das normas de segurança da informação e comunicações e normas de segurança da informação administrativas e documentais;

II – **Conhecimento**: os servidores, os colaboradores, os consultores externos, os estagiários e os prestadores de serviço no INPI tomarão ciência de todas as normas de segurança da informação e comunicações e normas de segurança da informação administrativas e documentais para o pleno desempenho de suas atribuições;

III – **Legalidade**: as ações de segurança da informação e comunicações e segurança da informação administrativas e documentais levarão em consideração as leis, as normas e as políticas organizacionais, administrativas, técnicas e operacionais do INPI, formalmente estabelecidas; e

IV – **Proporcionalidade**: o nível, a complexidade e os custos das ações de segurança da informação e comunicações e segurança da informação administrativas e documentais no INPI serão adequados ao entendimento administrativo e ao valor do ativo à proteger.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 5º A Gestão da Segurança da Tecnologia da Informação e Comunicações se limita à tecnologia da informação, compreendendo ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança lógica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, tendo em vista as atribuições regimentais da área de Tecnologia da Informação do INPI.

Art. 6º A Gestão da Segurança da Informação Administrativa e Documental compreende ações e métodos que visam à garantia do funcionamento institucional envolvendo, dentre outros, as seguranças física, orgânica e organizacional relativas às questões institucionais estratégicas, operacionais e táticas, tendo em vista as atribuições regimentais da área Administrativa do INPI.

Art. 7º Cabe às Unidades do INPI, no âmbito de suas competências, a implementação e o acompanhamento de ações para a segurança da informação e comunicação.

Art. 8º Toda informação criada, adquirida ou custodiada pelo usuário interno, no exercício de suas atividades no INPI, é considerada um bem e propriedade do Instituto e deve ser protegida segundo as diretrizes descritas nesta Política e demais regulamentações em vigor.

Art. 9º Servidores, usuários, colaboradores, consultores externos, estagiários e prestadores de serviço no INPI devem observar que:

I – A informação deve ser tratada como um patrimônio da instituição devendo ser classificada e manipulada de acordo com normas específicas, mantendo a segurança durante todo o ciclo de vida da informação;

II – Os incidentes de redes serão tratados pela Equipe de Tratamento e Resposta à Incidentes em Redes Computacionais;

III – O processo de Gestão de Riscos deve ser estabelecido com a finalidade de subsidiar e suportar o Sistema de Segurança da Informação e Comunicações e à Gestão de Continuidade dos Negócios;

IV – Devem ser estabelecidas normas internas que tratem da Gestão de Continuidade dos Negócios;

V – A Coordenação Geral de Tecnologia da Informação deverá realizar periodicamente, mantendo registros e procedimentos, como trilhas de auditoria e outros que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos e rede interna do INPI.

VI - O Controle de Acesso físico e lógico será sistematizado, a fim de evitar a quebra de segurança da informação e comunicações, administrativo e documental. A identificação, a autorização, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para a concessão de acesso ao INPI e o processo de controle deve ser pautado no processo de Gestão de Riscos;

VII – Uso de email corporativo será restrito para uso funcional para trato de assuntos das atividades do órgão e regido por norma interna;

VIII – O acesso à internet será regido por norma interna.

Seção I

Da Sensibilização, Conscientização e Capacitação

Art. 10 O INPI desenvolverá processo permanente de divulgação, sensibilização, conscientização e capacitação dos usuários internos sobre as responsabilidades e obrigações relacionadas à Segurança da Informação e Comunicações, visando reduzir riscos de erro humano, furto, fraude e uso não apropriadoo da informação.

Seção II

Da Contratação de Terceiros

Art. 11 - Nos editais de licitação, nos convênios e nos contratos de empresas prestadoras de serviços com o INPI deverá constar cláusula específica sobre a obrigatoriedade de atendimento às normas desta PoSIC. Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo INPI devem atender a esta PoSIC.

Parágrafo Único: Os contratos deverão conter Termo de Responsabilidade e de Confidencialidade .

Seção III

Da Classificação da Informação

Art. 12 - As informações criadas, armazenadas, manuseadas, transportadas ou descartadas no INPI devem ser classificadas segundo a Lei nº 12.527, Lei de Acesso à Informação.

Art. 13 - Todo usuário interno deve ser capaz de identificar a classificação atribuída a uma informação tratada pelo INPI e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

CAPÍTULO V

DAS PENALIDADES

Art. 14 O descumprimento ou violação de um ou mais itens desta Política de Segurança da Informação e Comunicações poderá resultar na aplicação de sanções administrativas, penais ou civis.

CAPÍTULO VI

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 15 Instituir, no âmbito INPI:

I – Gestor de Segurança da Tecnologia da Informação e Comunicações (GSIC);
II – Gestor de Segurança da Informação Administrativa e Documental (GSIAD)
III – Comitê de Segurança da Informação e Comunicações (CSIC).

Art. 16 As reuniões do Comitê poderão ser convocadas por qualquer um dos membros do mesmo.

Parágrafo Único: O quórum mínimo para a realização de uma reunião é de três membros.

Art. 17 O **Coordenador Geral de Tecnologia da Informação** atua como Gestor de Segurança da Tecnologia da Informação e Comunicações (GSIC), com as seguintes competências:

I – Promover cultura de segurança da informação e comunicações em tecnologia da informação;
II – Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança em tecnologia da informação;
III – Propor recursos necessários às ações de segurança da informação e comunicações em tecnologia da informação;
IV – Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta à Incidentes em Redes Computacionais;
V – Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
VI – 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 em tecnologia da informação;
VII – Propor Normas e procedimentos relativos à segurança da informação e comunicações em tecnologia da informação no âmbito do órgão ou entidade da APF.

Art. 18 O **Diretor de Administração** atua como Gestor de Segurança da Informação Administrativa e Documental (GSIAD), com as seguintes competências:

I – Promover cultura de segurança da informação administrativa e documental;
II – Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança administrativa e documental;
III – Propor recursos necessários às ações de segurança administrativa e documental;
IV – Integrar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta à Incidentes em Redes Computacionais;

V – Propor Normas e procedimentos relativos à segurança da informação administrativa e documetal no âmbito do órgão ou entidade da APF;

VI – Propor formas de disseminar as diretrizes de segurança corporativa;

VII – Propor a adoção de ações de conscientização e capacitação de pessoal visando difundir os conhecimentos e dar efetividade à Política de Segurança da informação e Comunicações.

Art. 19 O Comitê de Segurança da Informação e Comunicações (CSIC) será integrado pelos seguintes representantes da estrutura organizacional do INPI:

I – Presidente;

II – Vice-Presidente;

III – Chefe de Gabinete da Presidência;

IV – Diretor de Administração;

V – Diretor de Contratos, Indicações Geográficas e Registros;

VI – Diretor de Cooperação para o Desenvolvimento;

VII – Diretor de Marcas;

VIII – Diretor de Patentes;

IX – Coordenador-Geral de Tecnologia da Informação;

X – Coordenador-Geral de Planejamento e Orçamento;

XI – Coordenador-Geral de Comunicação Social; e

XII - Coordenador-Geral da Qualidade.

Art. 20 Ao Comitê de Segurança da Informação e Comunicações (CSIC) compete:

I – Assessorar na implementação das ações de segurança da informação e comunicações no órgão;

II – Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

III – Propor normas e procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.

IV – Instituir, no âmbito do INPI, a Equipe de Tratamento e Reposta à Incidentes em Redes Computacionais (ETIR), conforme norma específica.

V – Instituir, no âmbito do INPI, a Equipe de Tratamento e Reposta à Incidentes Administrativos e Documentais (ETRAD), conforme norma específica.

CAPÍTULO VII

DA ATUALIZAÇÃO

Art. 21 Todos os instrumentos normativos gerados a partir da PoSIC devem ser revisados sempre que se fizer necessário, não devendo exceder o período máximo de dois anos.

Art. 22. Os casos omissos e as dúvidas surgidas na aplicação desta Política serão dirimidas pelo Comitê de Segurança da Informação e Comunicações (CSIC).

Art. 23 Esta Instrução Normativa entra em vigor na data de sua publicação no Boletim de Pessoal, devendo ser revogada a Portaria nº Nº 503/11.

JORGE DE PAULA COSTA ÁVILA
PRESIDENTE

NEUSA MANSOUR
COORDENADORA GERAL DE TECNOLOGIA DA INFORMAÇÃO