Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

JOSÉ CARLOS FERRER SIMÕES

ANÁLISE DA MATURIDADE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DOS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA FEDERAL DIRETA

Brasília
2014

JOSÉ CARLOS FERRER SIMÕES

ANÁLISE DA MATURIDADE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DOS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA FEDERAL DIRETA

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Governança em Tecnologia da Informação.

Orientador: Prof. Dr. Maurício Lyra.

Brasília
2014

JOSÉ CARLOS FERRER SIMÕES

ANÁLISE DA MATURIDADE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DOS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA FEDERAL DIRETA

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Governança em Tecnologia da Informação.

Orientador: Prof. Dr. Maurício Lyra.

Brasília, 01 de agosto de 2014.

Banca Examinadora

_____

Prof. Dr. Maurício Lyra

_____

Prof. Dr. Paulo Rogério Foina

_____

Prof. Dr. Gilson Ciarallo

Dedico este singelo trabalho:

Aos meus pais, meus maiores mestres e orientadores, Getúlio Garcia Simões e Lúcia Helena Ferrer Simões, que não se encontram mais presentes entre nós, mas que estão na presença do nosso Senhor, me dando o suporte espiritual e necessário para que nunca desista dos desafios a que somos postos diariamente; e

À minha querida esposa Kelli Cristina e a meus filhos Carlos Gustavo e Pedro Lucas, as razões da minha vida, pela compreensão e incentivo constante na minha caminhada acadêmica e profissional.

.

RESUMO

O avanço da tecnologia da informação nesta última década aliado com o crescimento vertiginoso dos sistemas informatizados integrados por meio de redes é um fato determinante para a evolução do conhecimento. No entanto, esta nova sociedade digital fica sujeita a várias ameaças que comprometem seriamente a segurança do simples usuário até mesmo as grandes organizações. A tecnologia da informação pode auxiliar e até mesmo mitigar grande parte destas ameaças, porém não é capaz de resolvê-la na sua íntegra. Os sistemas de tecnologia da informação necessitam de uma política de segurança da informação e comunicação aliada e que contemple, de forma equilibrada, não somente aspectos tecnológicos, mas aspectos humanos e principalmente comportamentais a fim de mitigar possíveis ameaças e vulnerabilidades às organizações. Com este enfoque, este trabalho teve por finalidade apresentar as melhores práticas para a construção de uma política de segurança da informação e comunicação adequada no âmbito das organizações da administração pública federal direta. Tal abordagem visa a verificar como estas organizações estão em conformidade com estas melhores práticas na elaboração de suas políticas de segurança da informação e comunicação, assim como realizar um estudo comparativo a fim de avaliar a maturidade destes documentos imprescindíveis para estes órgãos. Para tanto, procedeu-se a uma coleta de artigos e trabalhos na área de segurança da informação assim como das políticas de segurança da informação e comunicação de dez órgãos da administração púbica federal direta. Os resultados obtidos sugeriram de forma geral uma heterogeneidade no nível de maturidade das políticas de segurança da informação e comunicação destes órgãos analisados.

Palavras-chave: Segurança da Informação. Política de Segurança da Informação. Normas e Padrões de Segurança. Governança em Tecnologia da Informação.

ABSTRACT

The advancement of information technology in this last decade associate with the rapid growth of integrated computer systems through networks is a key factor in the evolution of knowledge. However, this new digital society is subject to various threats that seriously compromise the security of the simple user even large organizations. Information technology can assist and even largely mitigate these threats, but is not able to solve it in its entirety. The information technology systems require a security policy of information and communication together and including a balanced way, not only technological aspects but mainly human and behavioral aspects in order to mitigate potential threats and vulnerabilities for organizations. With this approach, this paper aims to present best practices for building a security policy of information and communication within the direct federal public administration organizations. This approach seeks to check how these organizations are in compliance with these best practices in developing their security policies of information and communication, as well as accomplish a comparative study in order to evaluate the maturity of these essential documents to these organs. So, we proceeded to a collection of articles and papers in the area of information security policies as well as security policy of information and communication of ten pubic direct federal administration organs. The results suggest a general heterogeneity in the level of maturity of security policies of information and communication of these organs analysed.

Keywords: Information Security. Information Security Policy. Standards and Security. Governance in Information Technology.

LISTA DE ABREVIATURAS E SIGLAS

PSIC	Política de Segurança da Informação e Comunicação
SGSI	Sistema de Gestão de Segurança da Informação

SUMÁRIO

INTRODUÇÃO

As transformações vividas pelas organizações a partir dos avanços tecnológicos fez com que a informação seja o ativo o mais valioso das grandes empresas e consequentemente passamos a ter um bem altamente sensível e vulnerável que deve ser cada vez mais protegido de possíveis ameaças. Com isso, as organizações passaram cada vez mais a ter os seus sistemas de informações e redes de computadores expostos a riscos suscetíveis a prejuízos financeiros.

A fim de mitigar este risco, começou-se a discutir a implementação de Governança Corporativa nas empresas onde seria baseada nos princípios da transparência, independência e prestação de contas (accountability) como meio para atrair investimentos para as organizações.

Contudo, pelo fato das informações financeiras das empresas estarem salvos em sistemas de informação, os gestores de negócio precisam ter garantias que as informações nestes sistemas são confiáveis e para isso inicia-se a discussão e criação da Governança de TI, onde podemos observar que se trata de um dos principais itens da Governança Corporativa.

A Governança de TI tem o papel de criar estes controles de forma que a TI trabalhe de uma maneira o mais transparente possível perante os stakeholders (sócios, funcionários da empresa, terceirizados, etc.)

Podemos destacar que a Governança de TI tem foco no direcionamento e monitoramento das práticas de gestão e uso da TI de uma organização, tendo como indutor e principal beneficiário a alta administração da organização.

A implementação da Governança de TI nas organizações são baseadas em guias de melhores práticas, frameworks e normas. Neste trabalho, abordaremos os aspectos de Segurança da Informação, mas precisamente faremos um estudo sobre a política de segurança da informação nas organizações públicas, item imprescindível para a boa Governança de TI destes órgãos.

Sabendo da importância das informações processadas nos órgãos e entidades da Administração Pública Federal, o Presidente da República editou o Decreto nº. 3.505, de 13 de junho de 2000, onde instituiu a Política Nacional de Segurança das Informações, que determina que todos os órgãos e entidades da Administração Pública Federal, direta e indireta tenham uma Política de Segurança da Informação.

Esse decreto apresenta a necessidade de proteção das informações consideradas sensíveis assim como contempla as orientações gerais que devem ser adotadas para prevenir e tratar vulnerabilidades, ameaças e riscos e que mereçam tratamento especial por todos os órgãos e entidades da Administração Pública Federal. Também, podemos destacar que uma Política de Segurança da Informação organizacional, além de implementada, deve ser formalmente divulgada a todos os servidores e intervenientes que tenham acesso a um tipo de informação, assim como o apoio e o comprometimento da alta direção, são os primeiros e principais passos de estratégia de segurança da informação nas organizações.

E, para que isto ocorra de forma plena, o governo federal vem direcionando os seus esforços para que a implementação da Segurança da Informação seja realizada nos órgãos da Administração Pública Federal de modo a atender suas necessidades de forma compatível com: as melhores práticas, tais como, NBR ISO/IEC 27002:2013 - Técnicas de segurança - Código de prática para gestão da segurança da informação; e legislações federais como o Decreto nº. 3505 de 2000, que Institui a Política de segurança da Informação nos Órgãos da Administração Pública Federal e a Instrução Normativa nº. 0001 de 2008 do Gabinete de Segurança da Institucional da Presidência da República (GSI/PR).

Sabendo que desde o ano 2000, temos a publicação do Decreto nº. 3505, que instituiu e ordenou a todos órgãos da Administração Pública Federal a formularem uma PSIC, temos a proposta de atingir o seguinte objetivo geral neste trabalho:

• Verificar o nível de maturidade da Política de Segurança da Informação dos órgãos da administração pública federal.

Deste objetivo, outros mais **específicos** se depreendem:

• Elencar as melhores práticas para criação de uma PSIC para as organizações;

• Obter as PSIC de dez órgãos da administração pública federal direta;

• Verificar quais itens da PSIC de cada organização são ou não atendidos quanto às melhores práticas levantadas neste trabalho;

• Realizar uma análise das PSIC dos órgãos públicos federais e apresentar uma matriz com o grau de maturidade destes documentos analisados.

Para alcançar esses objetivos, realizamos pesquisa bibliográfica em artigos científicos, monografias e dissertações de mestrado nos repositórios da Universidade de Brasília - UnB e do Centro Universitário de Brasília – Uniceub, assim como também fizemos uma pesquisa em livros técnicos especializados que tratam do assunto de Segurança da Informação. Mapeamos as melhores práticas para criação de uma PSIC para as organizações por meio das normas da família ISO/IEC 27000. Realizamos uma pesquisa na web da PSIC de dez órgãos da administração pública federal direta, onde escolhemos órgãos de diferentes áreas de atuação (estratégico, fundamental e especial), com intuito de realizarmos uma análise comparativa destas PSIC com as melhores práticas levantadas. E, por fim, realizamos uma análise crítica e comparativa de forma a apresentarmos uma matriz com o nível de maturidade das PSIC das organizações analisadas, assim como uma análise destas PSIC conforme suas áreas de atuação.

A justificativa para tal trabalho se deve a ser um tema atual e com grande relevância para as organizações, onde tal análise trará uma visão geral do nível de maturidade das PSIC dos órgãos da Administração Pública Federal.

O presente trabalho foi estruturado em cinco capítulos. Inicia-se o trabalho Introdução, onde faz referência ao tema, definição, objetivos gerais e específicos, a metodologia utilizada e por fim uma breve explicação da estrutura do trabalho.

No primeiro capítulo, inicia-se com conceitos relacionados à segurança da informação, tais como os princípios, atributos, ameaças, vulnerabilidades, assim como normas e padrões relacionados ao tema.

No capítulo seguinte, abordam-se aspectos de uma PSIC, apresentando informações sobre a estruturação de uma PSCI, as suas tipologias, assim como uma análise crítica deste documento e os requisitos e necessários que contemplam uma política adequada segundo as melhores práticas.

No terceiro capítulo, analisam-se as PSIC de dez órgãos da administração pública federal direta, onde se apresenta uma matriz com o grau de maturidade destas PSIC.

No final, apresenta-se a conclusão do trabalho.

1 SEGURANÇA DA INFORMAÇÃO

1.1 Definição da Segurança da Informação

Sêmola (2003) define segurança da informação como sendo “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

> Segundo Fontes (2006), Segurança da Informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada.

Para Beal (2005), segurança da informação pode ser entendida como o processo de proteger informações das ameaças para garantir a sua integridade, disponibilidade e confidencialidade. Porém, segurança da informação não pode ser encarada como “guardar em um cofre todas as informações disponíveis”, mas sim elaborar uma boa política de proteção evitando riscos e vulnerabilidade.

1.2 Princípios da Segurança da Informação

> Conforme Spanceski (2004), quando se pensa em segurança da informação, a primeira ideia que nos vem à mente é a proteção das informações, não importando onde estas informações estejam armazenadas. Um computador ou sistema computacional é considerado seguro se houver uma garantia de que é capaz de atuar exatamente como o esperado. Porém a segurança não é apenas isto. A expectativa de todo o usuário é que as informações armazenadas hoje em seu computador, lá permaneçam, mesmo depois de algumas semanas, sem que pessoas não autorizadas tenham tido qualquer acesso a seu conteúdo.

1.2.1 Autenticidade

O controle de autenticidade está associado com identificação de um utilizador ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo. Normalmente, isso é implementado a partir de um mecanismo de senhas ou de assinatura digital. A verificação de autenticidade é necessária após todo processo de identificação seja de um usuário para um

sistema ou de um sistema para outro sistema. A autenticidade é a medida de proteção de um serviço/informação contra a personificação por intrusos por Spanceski (2004).

1.2.2 Confidencialidade

Confidencialidade é proteger informações contra acesso por alguém não autorizado - interna ou externamente. Consiste em proteger a informação contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação. A informação deve ser protegida qualquer que seja a mídia que a contenha, como por exemplo, mídia impressa ou mídia digital. O objetivo da confidencialidade é proteger informação privada (cidadãos, indústrias, governo, militar) por Spanceski (2004).

1.2.3 Integridade

A integridade consiste em evitar que os dados sejam apagados ou de alguma forma alterada, sem a permissão do proprietário da informação. O conceito de dados nesse objetivo é mais amplo, englobando dados, programas, documentação, registros, fitas magnéticas, etc. Dias (2000 apud SIEWERT, s/d).

1.2.4 Disponibilidade

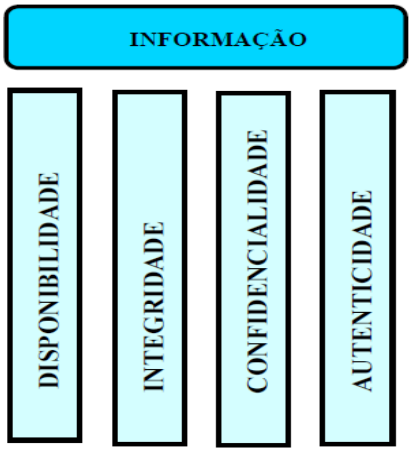
A disponibilidade consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao utilizador o acesso aos dados sempre que deles precisar (…) Spanceski (2004).

Segundo Dias (2000 apud SIEWERT, s/d) a disponibilidade protege os serviços de informática de tal forma que não sejam degradados ou fiquem indisponíveis sem a devida autorização. Para um utilizador autorizado, um sistema não disponível quando se necessita dele, pode ser tão ruim quanto um sistema inexistente ou destruído.

As medidas relacionadas a esse objetivo, podem ser a duplicação de equipamentos ou backup, disponibilidade pode ser definida como a garantia de que os serviços prestados por um sistema são acessíveis, sob demanda, aos utilizadores autorizados Dias (2000 apud SIEWERT, s/d).

A figura “1” abaixo nos apresenta como os princípios da segurança da informação se relacionam.

Figura 1 – Princípios da Segurança da Informação



Fonte: Quadro constitutivo com base no livro “Sistema de Segurança da Informação”, Campos, 2007.

1.3 Ameaças e vulnerabilidades à Segurança da Informação

O conceito de ameaça é definido por possíveis danos aos ativos, intencionais ou não. Ameaças são subdivididas em: desastres naturais (enchentes, incêndio, terremoto), humanas (subdividida em intencional, onde ocorre diretamente por hackers e funcionários descontentes e não intencional, onde funcionários com pouco conhecimento sobre a tecnologia aplicada) e ambientais (engloba toda parte tecnológica, software, hardware, falhas de sistema operacional, falha elétrica. Resumidamente, ameaças são “os meios pelos quais a confidencialidade, integridade e disponibilidade da informação podem ser comprometidas.” (SÊMOLA, 2003).

Vulnerabilidade são as circunstâncias que aumentam a possibilidade de uma ameaça ser concretizada, aumentando sua frequência e seu impacto. Na análise do risco, vulnerabilidade é a falta de segurança para determinado ativo ou grupo de ativos (SÊMOLA, 2003).

Segundo a ISO 27002:2013, os ativos são objetos de ameaças, tanto acidentais como deliberadas, enquanto que os processos, sistemas, redes e pessoas têm vulnerabilidades

inerentes. Mudanças nos processos e sistemas do negócio ou outras mudanças externas (como novas leis e regulamentações), podem criar novos riscos de segurança da informação. Desta forma, em função das várias maneiras nas quais as ameaças podem se aproveitar das vulnerabilidades para causar dano à organização, os riscos de segurança da informação estão sempre presentes. Uma segurança da informação eficaz reduz estes riscos, protegendo a organização das ameaças e vulnerabilidades e, assim, reduzindo o impacto aos seus ativos.

Um sistema de informação de uma empresa pode ser considerado seguro se não contém vulnerabilidades. Ainda que existam ameaças, a ausência de vulnerabilidades torna tais ameaças sem efeito, já que não há nenhuma fragilidade a ser explorada. As vulnerabilidades podem ser de dois tipos: técnicas ou de gestão.

Vulnerabilidades técnicas são fraquezas associadas aos softwares e hardware dos ativos. A má configuração e conexão dos ativos de uma organização e a especificação precária de políticas podem dar origem a vulnerabilidades gerenciais.

Políticas inadequadas podem levar a problemas de segurança, da mesma forma usuários podem potencialmente fazer o mau uso de seus direitos e violar a segurança dos ativos da empresa (SENGUPTA; MAZUMDAR; BAGCHI, 2009)

1.4 Normas e Padrões de Segurança da Informação

A ISO/IEC 27001 é um padrão para sistema de gestão da segurança da informação (ISMS - Information Security Management System) publicado em outubro de 2005 pelo International Organization for Standardization e pelo International Electrotechnical Commision. Seu nome completo é ISO/IEC 27001:2005 - Tecnologia da informação - técnicas de segurança - sistemas de gerência da segurança da informação - requisitos mais conhecido como ISO 27001. Esta norma foi elaborada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

A adoção de um SGSI deve ser uma decisão estratégica para uma organização. A especificação e implementação do SGSI de uma organização são influenciadas pelas suas

necessidades e objetivos, exigências de segurança, os processos empregados e o tamanho e estrutura da organização.

A série 27000 agrupa a família de segurança da informação relacionado aos padrões ISO, conforme abaixo:

- ISO 27000 - Vocabulário de Gestão da Segurança da Informação.
- ISO 27001 - Esta norma foi publicada em Outubro de 2005 e substituiu a norma BS 7799-2 para certificação de sistema de gestão de segurança da informação.
- ISO 27002 - Esta norma trata do Código de prática para controles da segurança da informação e substituiu a ISO 17799:2005.
- ISO 27003 - Esta norma aborda as diretrizes para Implementação de Sistemas de Gestão de Segurança da Informação, contendo recomendações para a definição e implementação de um sistema de gestão de segurança da informação.
- ISO 27004 - Esta norma disciplina sobre as métricas e relatórios de um sistema de gestão de segurança da informação.
- ISO 27005 - Esta norma será constituída por indicações para implementação, monitoramento e melhoria contínua do sistema de controles. O seu conteúdo deverá ser idêntico ao da norma BS 7799-3:2005 – “Information Security Management Systems - Guidelines for Information Security Risk Management”, a publicar em finais de 2005. A publicação da norma ISO 27005 ocorreu em 2008.
- ISO 27006 - Esta norma especifica requisitos e fornece orientações para os organismos que prestem serviços de auditoria e certificação de um sistema de gestão da segurança da informação.

A partir de 2007, a nova edição da ISO/IEC 17799 foi incorporada ao novo esquema de numeração como NBR ISO/IEC 27002:2013 que é um código de práticas para a gestão segurança da informação. Atualmente, após uma revisão desta norma, foi publicada em dezembro de 2013 a NBR ISO/IEC 27002:2013 que nos apresenta mais três seções de controle que a primeira edição. Esta norma pode ser considerada como um ponto de partida para o desenvolvimento de diretrizes e princípios gerais sobre metas geralmente aceitas para a gestão da segurança da informação.

A NBR ISO/IEC 27002:2013 tem como principal característica descrever controles preventivos, em sua grande maioria, evitando a ocorrência de incidentes envolvendo as

informações corporativas, visando reduzir o tempo de exposição ao risco, que permitem detectar, de maneira mais rápida e efetiva, eventuais violações às regras do Sistema. Esta é uma norma que é utilizada nas empresas independentemente do seu porte ou setor no âmbito da segurança da informação, pois esta foi criada com a intenção de ser um padrão flexível, nunca guiando seus utilizadores a seguirem uma solução de segurança específica em prejuízo de outra.

Embora o conteúdo da PSIC possa variar de acordo com o tipo da instituição, o seu tamanho, área de atuação, cultura organizacional, missão, estágio de maturidade, grau de informatização, ativos informacionais críticos, entre outros aspectos, ela deverá abranger, sempre que cabível, o máximo de controles.

Na norma NBR ISO/IEC 27002:2013, a definição de controle compreende a forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

Segundo Campos (2007), um controle é todo e qualquer mecanismo utilizado para diminuir a fraqueza ou a vulnerabilidade de um ativo, seja esse ativo uma tecnologia, uma pessoa, em processo ou um ambiente.

Nesta norma há 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 da organização, fatores imprescindíveis para a construção de uma PSIC adequada à organização.

De acordo com a norma NBR ISO/IEC 27002:2013, temos 14(quatorze) seções de controle de segurança da informação com os seus respectivos objetivos, os quais são dispostos abaixo, onde também há as considerações de alguns autores referenciados sobre estes controles.

1.4.1 Documento da Política de segurança da Informação

Segundo a NBR ISO/IEC 27002:2013, o objetivo primordial de uma PSIC é prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

> Para Castro (2002), a Política de Segurança da Informação é basicamente um manual de procedimentos que descreve como os recursos de que manipulam as informações da empresa devem ser protegidos e utilizados, e é o pilar da eficácia da Segurança da Informação, estabelecendo investimentos em recursos humanos e tecnológicos.

A elaboração da Política de Segurança deve considerar os processos, os negócios, toda e qualquer legislação que os envolva, os aspectos humanos, culturais e tecnológicos da organização. Ela servirá de base para a criação de normas e procedimentos que especificaram as ações no nível micro do ambiente organizacional, além de ser facilitadora e simplificadora do gerenciamento dos demais recursos da organização (NAKAMURA; GEUS, 2003).

1.4.2 Organização da Segurança da Informação

Segundo a NBR ISO/IEC 27002:2013, a organização da segurança da informação deve estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização.

1.4.3 Segurança em Recursos Humanos

A NBR ISO/IEC 27002:2013 disciplina que a organização deve ter como objetivo reduzir os riscos de erro humano, roubo, fraude assim como o uso indevido das instalações. Para isto, deve-se observar que as responsabilidades de segurança sejam atribuídas na fase de recrutamento, incluídas em contratos e monitoradas durante a vigência de todo o contrato de trabalho do funcionário.

De acordo com Rezende e Abreu (2000), as organizações devem procurar dar mais atenção ao ser humano, pois é ele que faz com que as engrenagens empresariais funcionem perfeitas e harmonicamente, buscando um relacionamento cooperativo e satisfatório. Dessa forma, seria importante destacar que o elo mais fraco de um processo de segurança é a pessoa (ou grupos de pessoas), que por sua vez, é a responsável por garantir a fidelidade da informação.

Para mitigar riscos quanto aos recursos humanos a serem contratados numa organização, a NBR ISO/IEC 27002:2013 disciplina que antes da contratação deste profissional, seja verificado o histórico do candidato ao emprego de acordo com a ética, regulamentações e leis relevantes. Ainda, disciplina que durante a contratação, a direção deve solicitar a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização. Para que este requisito seja essencialmente cumprido por todos, é recomendado que a direção demonstre seu total apoio às políticas, procedimentos e controles, e aja como tal, de forma exemplar.

Segundo Spanceski (2004) dentre os controles considerados como melhores práticas para a segurança da informação temos: definição das responsabilidades na segurança da informação e educação e treinamento em segurança da informação;

Da mesma forma, a NBR ISO/IEC 27002:2013 ratifica que a conscientização, educação e treinamento em segurança da informação deve ser prevista para todos os funcionários da organização e, quando pertinente, para as partes externas intervenientes.

Quanto ao encerramento do contrato do funcionário, a NBR ISO/IEC 27002:2013 disciplina que as responsabilidades e obrigações pela segurança da informação devem estar previstas mesmo após o encerramento do contrato.

1.4.4 Gestão de ativos

A NBR ISO/IEC 27002:2013 disciplina que os ativos da organização devem ser devidamente identificados por meio de um inventário de ativos estruturado. Além do que, sempre deve haver um proprietário para este inventário de ativos.

Quanto a classificação da informação, esta norma, disciplina que tem como objetivo assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização. Esta classificação deve ser incluída nos processos da organização e ser consciente e coerente em toda a organização.

A classificação da informação é importante para que as organizações possam determinar o nível de proteção das informações, de modo que a segurança das informações nas organizações possa ser assegurada Dias (2000) apud Spanceski (2004).

De acordo com Sêmola (2003, p. 106, grifo nosso), os critérios normatizados para admissão e demissão de funcionários, criação e manutenção de senhas, **descarte de informação em mídia magnética ou em papel**, desenvolvimento e manutenção de sistemas, uso da internet, acesso remoto, uso de notebooks, contratação de serviços terceirizados e **classificação das informações,** são alguns exemplos de normas de uma típica Política de Segurança da Informação.

Para que a gestão de ativos seja efetiva, a NBR ISO/IEC 27002:2013 descreve que as mídias devem ser adequadamente tratadas a fim de prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias. Esta norma, também destaca que o descarte de mídias deve ser realizado de forma segura, quando não forem mais necessárias, por meio de procedimentos formais.

1.4.5 Controle de Acesso

> Segundo Monteiro e Boavida (2000), a capacidade de impedir o acesso não autorizado a um recurso é, genericamente, designada por controle de acesso. Por vezes são incluídas na categoria de controlo de acesso as funções que limitam a quantidade de recursos a utilizar, o que é correto de um ponto de vista de segurança.

Segundo a NBR ISO/IEC 27002:2013, a organização deve ter como objetivo limitar o acesso à informação e aos recursos de processamento da informação. Para que este controle seja atendido plenamente pela organização, esta deve adotar uma política de controle de acesso, gerenciamento de acesso do usuário, definir as responsabilidades dos usuários e um controle de acesso aos sistemas e aplicações.

O processo mais adequado quando se pensa em manter o controle efetivo sobre os acessos aos sistemas é propor processos com intervalos periódicos para a revisão das contas de usuários e seus respectivos privilégios no sistema da organização (FERREIRA; ARAUJO, 2006, p.71).

1.4.6 Criptografia

Conforme descrito na NBR ISO/IEC 27002:2013, os Controles Criptográficos devem assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

A criptografia é utilizada visando proteger as informações que são consideradas de risco e para as quais outros controles não fornecem proteção adequada. O controle criptográfico deve levar em conta se é apropriado e qual tipo deve ser aplicado (FERREIRA; ARAUJO, 2006, p.78).

Para Tadano (2002), a criptografia é a arte ou ciência de escrever em cifra ou em códigos, utilizando um conjunto de técnicas que torna uma mensagem ilegível, chamado de texto cifrado, de forma a permitir que apenas o destinatário desejado consiga decodificar e ler a mensagem com clareza (…).

Na perspectiva de Laureano (2005), a criptografia representa um conjunto de técnicas que são usadas para manter a informação segura. Estas técnicas consistem na utilização de chaves e algoritmos de criptografia. Tendo conhecimento da chave e do algoritmo usado é possível desembaralhar a mensagem recebida.

1.4.7 Segurança física e do ambiente

A Política de Segurança Física precisa considerar o planejamento das instalações, gerenciamento e procedimentos de recuperação de desastres. O objetivo é garantir a segurança da infraestrutura da empresa, deve contemplar a localização dos equipamentos, a construção e o controle de acesso às instalações e planos de contingência (MARTINS, 2003).

> Segundo Fontes (2006), a segurança não envolve somente o ambiente de tecnologia. Existe outra preocupação, que normalmente é tratada com uma certa indiferença, que é a segurança física. As ameaças internas podem ser consideradas como o risco número um à segurança da informação. Um bom programa de segurança física é passo inicial para a defesa da corporação no sentido de proteger as suas informações contra acessos indevidos.

Consoante com a NBR ISO/IEC 27002:2013, a organização deve prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e nas informações da organização. Quanto aos equipamentos, convém que estes sejam protegidos e colocados em locais seguros de forma a reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.

Qualquer acesso às dependências da organização, desde as áreas de trabalho até àquelas consideradas severas (onde ocorre o processamento das informações críticas e confidenciais) deve ser controlado sempre fazendo necessária sua formalização (FERREIRA; ARAÚJO, 2008).

1.4.8 Segurança nas operações

Segundo a NBR ISO/IEC 27002:2013, a organização deve garantir a operação segura e correta dos recursos de processamento da informação. Os procedimentos de operação devem ser documentados e disponibilizados para todos os usuários que necessitem deles.

Esta norma ainda informa que convém que os procedimentos de operação especifiquem:

a) a instalação e configuração de sistemas;

b) processamento e tratamento da informação, tanto automática como manual;

c) cópias de segurança (backup);

d) requisitos de agendamento, incluindo interdependências com outros sistemas, a primeira hora para início da tarefa e a última hora para o término da tarefa;

e) instruções para tratamento de erros ou outras condições excepcionais, que possam ocorrer durante a execução de uma tarefa, incluindo restrições de uso dos utilitários do sistema;

f) contatos para suporte e escalação, incluindo contatos de suporte externos, para o caso de eventos operacionais inesperados ou dificuldades técnicas;

g) instruções quanto ao manuseio de mídias e saídas especiais, como o uso de formulários especiais ou o gerenciamento de dados confidenciais, incluindo procedimentos para o descarte seguro de resultados provenientes de rotinas com falhas;

h) procedimento para o reinício e recuperação em caso de falha do sistema;

i) gerenciamento de trilhas de auditoria e informações de registros (logs) de sistemas;

j) procedimentos de monitoramento.

Ferreira e Araújo (2006, p.86) citam que o backup é um dos recursos mais efetivos para assegurar a continuidade das operações em caso de algum ataque ou dano as informações da empresa. Por isso, cabe a instituição levar em consideração a importância da informação que tem, classificando-a adequadamente, levando em conta sua periodicidade de atualização e sua volatilidade para saber o que deve realmente proteger.

A NBR ISO/IEC 27002:2013 também disciplina que a auditoria de sistemas de informação deve seguir atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais de forma que sejam cuidadosamente planejados e acordados para minimizar interrupção de processos do negócio.

1.4.9 Segurança nas comunicações

A NBR ISO/IEC 27002:2013 disciplina que a organização para atender este controle de segurança deve observar o gerenciamento da segurança em redes, segurança dos serviços de rede, segregação de redes, transferência de informação, políticas e procedimentos para transferência de informações, acordos para transferência de informações, proteção adequada às mensagens eletrônicas e acordos de confidencialidade e não divulgação.

A segurança lógica envolve aspectos de prevenção contra interceptação e modificação de informações, sigilo no tráfego dos dados na rede, alterações de softwares, invasões em sistema, acessos não a autorizados a informação e demais aspectos relacionados ao aceso e manipulação dos dados da empresa Sousa (2006).

1.4.10 Aquisição, desenvolvimento e manutenção de sistemas

Segundo a NBR ISO/IEC 27002:2013, a organização para atender este controle de segurança deve observar os requisitos de segurança de sistemas de informação, de segurança

em processos de desenvolvimento e de suporte e, por fim, assegurar a proteção dos dados usados para teste.

1.4.11 Relacionamento na cadeia de suprimento

A NBR ISO/IEC 27002:2013 diciplina que a organização para atender este controle de segurança deve observar:

a) a segurança da informação na cadeia de suprimento;

b) a política de segurança da informação no relacionamento com os fornecedores;

c) a segurança da informação nos acordos com fornecedores;

d) a cadeia de suprimento na tecnologia da informação e comunicação;

e) o gerenciamento da entrega do serviço do fornecedor;

f) o monitoramento e análise crítica de serviços com fornecedores; e

g) o gerenciamento de mudanças para serviços com fornecedores.

1.4.12 Gestão de incidentes de segurança da informação

De acordo com a NBR ISO/IEC 27002:2013 para assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação, deve-se atentar com a(s):

a) responsabilidades e procedimentos;

b) notificação de eventos de segurança da informação – os eventos de segurança da informação devem ser relatados por meio dos canais de gestão, o mais rapidamente possível;

c) notificação das fragilidades de segurança da informação;

d) avaliação e decisão dos eventos de segurança da informação;

e) resposta aos incidentes de segurança da informação;

f) aprendizado com os incidentes de segurança da informação; e

g) coleta das evidências.

1.4.13 Aspectos da segurança da informação na gestão de continuidade do negócio

De acordo com a NBR ISO/IEC 27002:2013, é prudente que a continuidade da segurança da informação seja contemplada nos sistemas de gestão da continuidade do negócio da organização. A organização deve determinar quais são seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, como por exemplo, durante uma crise ou desastre.

A organização deve estabelecer, documentar, implementar e manter processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação durante uma situação adversa.

Por fim, é prudente que os recursos de processamento da informação sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade.

De acordo com Sêmola (2003), a gestão de continuidade do negócio tem como objetivo permitir a continuidade de processos e informações essenciais à sobrevivência da organização, no menor intervalo de tempo possível, com vistas a evitar/minimizar os impactos de incidentes.

1.4.14 Conformidade

Conforme a NBR ISO/IEC 27002:2013, a organização para atender este controle de segurança deve observar: conformidade com requisitos legais e contratuais; identificação da legislação aplicável e de requisitos contratuais; direitos de propriedade intelectual; proteção de registros; proteção e privacidade de informações de identificação pessoal; regulamentação de controles de criptografia; análise crítica da segurança da informação; análise crítica independente da segurança da informação; conformidade com as políticas e procedimentos de segurança da informação; e análise crítica da conformidade técnica.

2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

2.1 Definição de Política de Segurança da Informação e Comunicação

Política de Segurança da Informação é basicamente um manual de procedimentos que descreve como os recursos de que manipulam as informações da empresa devem ser protegidos e utilizados e é o pilar da eficácia da Segurança da Informação, estabelecendo investimentos em recursos humanos e tecnológicos (CASTRO, 2002).

Segundo Sousa (2006) o desenvolvimento de uma política de segurança é a base de segurança de informação em uma empresa. Alguns padrões e normas internacionais de segurança foram desenvolvidos por organizações normalizadoras como ISO (Internacional Standards Organization) e a BS (British Standard), como ISO 17799 e a BS 7799.

Conforme descrito por Marciano (2006) uma política de segurança da informação é um conjunto de regras, normas e procedimentos que regulam como deve ser gerenciada e protegida a informação sensível, assim classificada pela organização ou pelo estado, além dos recursos e utilizadores que com ela interagem. Todo o ciclo de vida da informação deve ser objeto da política.

Conforme Campos (2006) uma política de segurança não é um grande livro informando tudo o pode existir de segurança da informação dentro de uma corporação ou instituição, nem mesmo são poucas regras gerais que se aplicam a qualquer aspecto da segurança da informação. Ainda que essas duas hipóteses não possam ser descartadas, nenhuma delas define exatamente o que é uma política de segurança da informação.

Mas afinal de contas o que significa a palavra política, que atualmente está sendo tão utilizada pelas corporações e instituições? Atualmente é comum ouvir frases do tipo “a política da nossa empresa é a qualidade total de nossos produtos”, ou então “a política de recursos humanos não tolera funcionários que tenham registro policial”. Esses são dois exemplos, mas que ajudam a entender o que significa a palavra política. A primeira frase é bastante abrangente e qualquer procedimento, ação ou decisão visando como objetivo a qualidade dos produtos fabricados, está de acordo com a política estabelecida pela empresa. Já a segunda frase é mais específica e deve ser considerada no processo de seleção e recrutamento de funcionários da empresa, conforme estabelecido na política de recursos humanos da empresa citado por Marciano (2006).

Com a política de segurança não é diferente, ou seja, ela deve indicar como as coisas devem acontecer na organização ao que se refere a segurança da informação, sendo assim, uma política nada mais é do que um conjunto de regras que determina como deve ser o comportamento de pessoas que tem qualquer tipo de relacionamento com a organização no que diz respeito as informações que são trocadas, enviadas ou recebidas citado por Campos (2006).

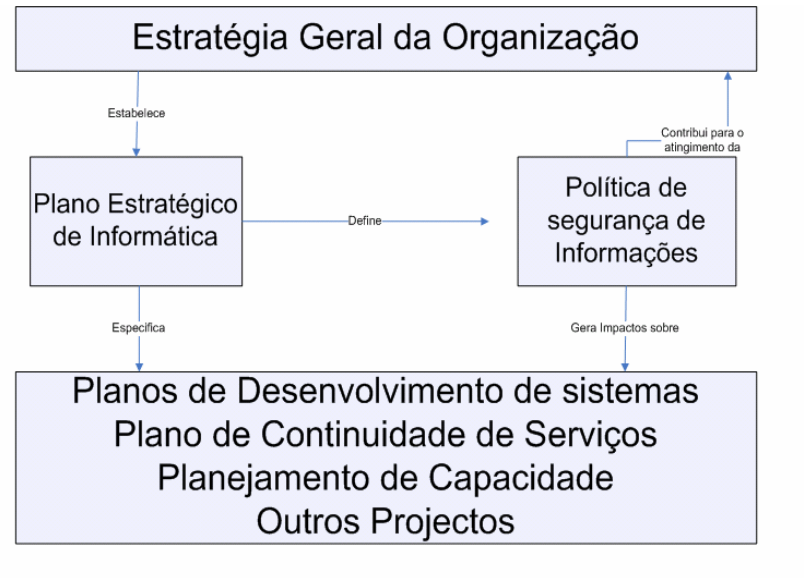
No que diz respeito às políticas de segurança da informação, existe ainda um requisito a mais a ser cumprido: prover o equilíbrio entre funcionalidade e segurança, motivo pelo qual torna-se essencial uma análise da situação operacional da organização em foco. Esta análise, que no contexto da segurança da informação é conhecida como análise de vulnerabilidades, deve se restringir, como é de hábito, a uma busca por eventuais brechas de segurança nos sistemas de informação sobre os quais se aplica. Antes, deve-se conhecer a fundo os fluxos de informação aplicados (formais e informais) a fim de mapear-se de modo consistente e dinâmico a realidade, em termos da informação e dos atores que com ela interagem citado por Marciano (2006).

A política de segurança de informações deve estabelecer princípios institucionais de como a organização irá proteger, controlar e monitorar seus recursos computacionais e, consequentemente, as informações por eles manipuladas. É importante que a política estabeleça ainda as responsabilidades das funções relacionadas com a segurança e discrimine as principais ameaças, riscos e impactos envolvidos citado por Laureano (2005).

Laureano (2005) também salienta que a política de segurança, deve ir além dos aspectos relacionados com sistemas de informação ou recursos computacionais, ela deve estar integrada as políticas institucionais da empresa, metas de negócio e ao planejamento estratégico da empresa.

A figura 2 mostra o relacionamento da política de segurança de informações com a estratégia da organização, o plano estratégico de informática e os diversos projetos citado por Laureano (2005).

Figura 2: Política de segurança e seus relacionamentos



Fonte: Laureano (2005)

2.2 Características de uma Política de Segurança da Informação e Comunicação

Conforme exposto por Ferreira (2006), uma política e segurança da informação não deve ser elaborada se não tiver as seguintes características:

a) Simples;
b) Compreensível, ou seja, escrita de maneira clara e objetiva;
c) Homologada e assinada pela Alta Administração;
d) Estruturada, estabelecendo padrões;
e) Alinhada com a estratégia da missão da organização;
f) Orientada aos riscos, ou seja, direcionar para os riscos da organização;
g) Flexível, ou seja, moldáveis aos novos requerimentos de tecnologia;
h) Protetora dos ativos de informação, priorizando os de maior valor e de maior importância;
i) Positiva e não apenas concentradas em ações proibitivas ou punitivas;
j) Deve conter atribuições de regras e responsabilidades;
k) Deve conter a forma de educar os usuários;

l) Deve ser dinâmica, ser atualizada sempre que necessário;
m) Deve ser acessível a todos; e
n) Deve ser exequível, ou seja, descreva regras de comportamentos que possam ser cumpridas, fáceis de executar, sejam na área tecnológica ou humana.

Por meio das afirmações de Ferreira (2006), podemos entender que uma política de segurança da informação e comunicação somente pode ser implementada com o apoio da alta administração da organização e para que esta política seja efetiva, todas as diretrizes, objetivos e metas devem estar de forma clara, transparente e sucinta, de forma que qualquer pessoa da organização possa compreender e aplicar nas suas atividades. Por oportuno, é interessante destacar que esta política de segurança da informação e comunicação deve ser revista periodicamente a fim de que este documento acompanhe as atualizações tecnológicas e mudanças procedimentais quando ocorrerem.

2.3 Tipos de Políticas de Segurança da Informação e Comunicação

Os tipos de políticas de segurança da informação e comunicação, conforme exposto por Ferreira (2003), são as políticas dos tipos regulatória, consultiva e informativa. Ele salienta que estes tipos de políticas poderão ser adotadas nas organizações conforme definições abaixo. No entanto, se a organização entender pertinente não adotar nenhuma destas políticas na sua íntegra conforme definições abaixo, esta poderá mesclar estes três tipos de políticas para atender a sua organização:

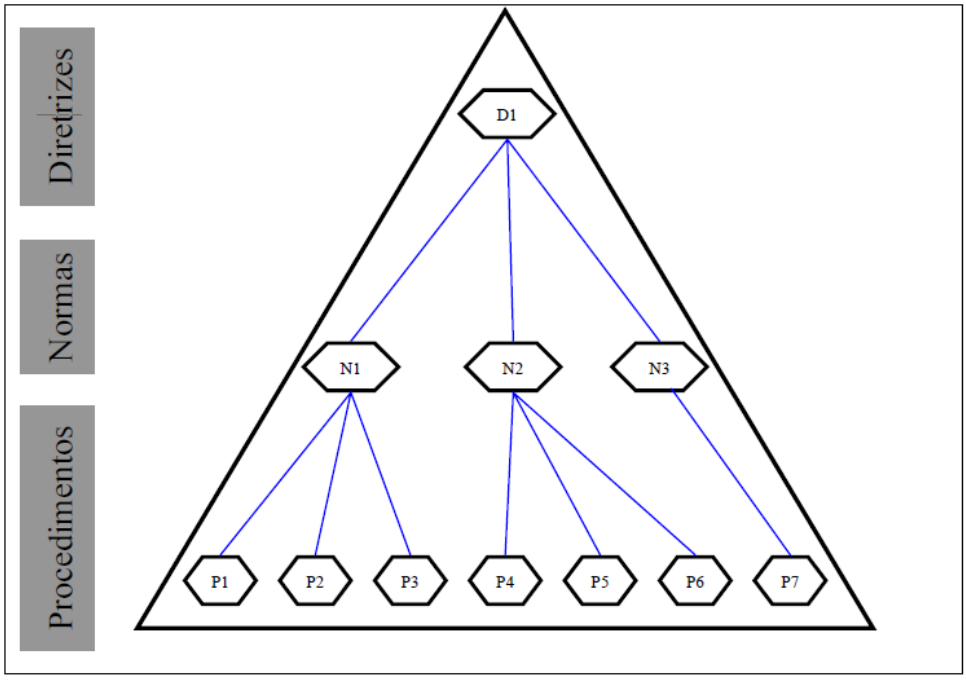
a) Política do Tipo Regulatória: O formato e o conteúdo de uma política regulatória são definidos como se fosse uma série de especificações legais. Ela descreve com riquezas detalhes do que deve ser feito quem deve fazer e fornecer algum tipo de parecer, relatando porque tal ação é importante. Portanto, políticas regulatória são implementadas devido às necessidades legais que são impostas à organização;
b) Política do Tipo Consultiva: Uma política consultiva sugere quais ações ou métodos devem ser utilizados para a realização de uma determinada tarefa ou atividade. A característica desta política é prover aos usuários conhecimentos básicos das atividades cotidiana da organização;

c) Política do Tipo Informativa: Uma política informativa possui caráter apenas informativo. Nenhuma ação é desejada e não existem riscos, caso não seja cumprida. Este tipo de política não é tão rigorosa quanto à regulatória ou consultiva.

2.4 Elaborando uma Política de Segurança da Informação e Comunicação

Conforme Campos (2006), não existe uma regra para criar o documento físico da política de segurança. É possível ter um documento único com as diretrizes, normas e procedimentos, ou um documento com as diretrizes, diversos outros com as normas e vários outros com os demais procedimentos. O fato principal é que as diretrizes, normas e procedimentos têm que existir em um documento com controle de versão e com revisão para garantir que sejam confiáveis e relevantes. A visão conceitual de uma política de segurança da informação e comunicação é apresentada na figura 3 abaixo.

Figura 3 – Visão conceitual da política de segurança



Fonte: adaptado de Campos (2006).

Na figura 3, é destacada a relação entre diretrizes, normas e procedimentos, ou seja, um objeto depende do outro, se existir algum procedimento que não tem relacionamento com nenhuma norma, e alguma norma não tiver relacionamento com alguma diretriz, então a política de segurança está com algo errado, e deve ser revista.

De acordo com Silva (2004), a política de segurança deve ir além dos aspectos de sistemas de informação e recursos computacionais, integrando as políticas institucionais relativas à segurança em geral, às metas de negócios da organização e ao plano estratégico de informática. O objetivo da PSIC é atingido quando o relacionamento da estratégia da organização, o plano estratégico de informática e demais projetos estiverem sincronizados, conforme figura 1.

2.5 Princípios que norteiam uma Política de Segurança da Informação e Comunicação

A correta gestão da segurança da informação é atingida com o compromisso de todos os usuários quanto à aplicação das normas e procedimentos estabelecidos visando à padronização das ações de planeamento, implementação e avaliação das atividades voltadas à segurança Wiliams (2001) apud Marciano (2006).

Estas diferentes atividades podem ser agrupadas conforme a disposição da Information Systems Audit and Control Foundation - ISACF, (2001) apud Marciano (2006):

> "• Desenvolvimento de políticas, com os objetivos da segurança como fundamentos em torno dos quais elas são desenvolvidas;
>
> • Papéis e autoridades, assegurando que cada responsabilidade seja claramente entendida por todos;
>
> • Delineamento, desenvolvendo um modelo que consista em padrões, medidas, práticas e procedimentos;
>
> • Implementação, em um tempo hábil e com capacidade de manutenção;
>
> • Monitoramento, com o estabelecimento de medidas capazes de detectar e garantir correções às falhas de segurança, com a pronta identificação e atuação sobre falhas reais e suspeitas com plena aderência à política, aos padrões e às práticas aceitáveis;
>
> • Vigilância, treinamento e educação relativos à proteção, operação e prática das medidas voltadas à segurança." (MARCIANO, 2006, p. 129-130)

2.6 Aspectos que contemplam uma Política de Segurança da Informação e Comunicação

De acordo com Ferreira (2003), em seu livro Segurança da Informação, os aspectos que contemplam uma Política de Segurança da Informação e Comunicação são:

a) Especificação da política: A política deve ser breve, utilizar palavras simples e formalizar o que é esperado dos servidores da organização. Deve fornecer informações suficientes para saber se os procedimentos descritos na política são aplicáveis para eles ou não. Deve descrever sua finalidade específica, ou seja, se é orientada a pessoa, departamentos e/ou equipamentos;
b) Declaração da Alta administração: Uma declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação. Esta formalização demonstra aos servidores que a alta autoridade mostra seu comprometimento para que a política de segurança da informação seja adequadamente cumprida;
c) Autores/patrocinadores da política: Os nomes dos profissionais ou equipes, que desenvolveram a política devem estar especificados no documento;
d) Fazer referência a outras políticas, regulamentos ou regimentos: Em organizações é comum que as políticas de segurança em vigor façam referência a outros regulamentos internos já existentes;
e) Procedimentos para requisição de exceção à política: É importante preparar e divulgar a política, mas também é essencial ter um processo para requisição de exceção a ela;
f) Procedimentos para mudanças da política: Algumas organizações não atualizam suas políticas, sendo assim, é necessário ter um procedimento para atualização dela. Há situações que podem requerer somente revisões técnicas, mas outras necessitarão de justificativas detalhadas para solicitar mudanças nas políticas;
g) Punições para àqueles que violarem a política: A alta administração deve demonstrar que poderão ocorrer punições rígidas aos servidores da organização caso haja um desrespeito ou violarem as políticas internas;
h) Data de publicação, validade e revisão da política: A política e seus documentos complementares devem possuir assinatura do principal executivo, data da última atualização e do início de sua vigência.

2.7 Política de Segurança da Informação e Comunicação segundo a NBR ISO/IEC 27002:2013

2.7.1 Documento da Política de segurança da Informação e Comunicação

Segundo a NBR ISO/IEC 27002:2013, o documento de Política de Segurança da Informação e Comunicação deverá conter aspectos relevantes para que a sua elaboração seja alinhada com os objetivos e estratégia do negócio ou missão da organização. Também, segundo esta norma, o objetivo primordial de uma Política para segurança da informação e comunicação é prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

2.7.2 Políticas para a segurança da informação e comunicação

Segundo a NBR ISO/IEC 27002:2013, é prudente que um conjunto de políticas de segurança da informação e comunicação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes. É importante destacar que no mais alto nível, a organização defina uma política de segurança da informação, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança da informação.

É prudente que as PSIC contemplem requisitos oriundos de:

a) Estratégia do negócio;
b) Regulamentações, legislação e contratos;
c) Ambiente de ameaça da segurança da informação, atual e futuro.

Também é conveniente que a PSIC contenha declarações relativas a:

a) Definição de segurança da informação, objetivos e princípios para orientar todas as atividades relativas à segurança da informação;
b) Atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos;
c) Processos para o tratamento dos desvios e exceções.

No nível mais baixo, convém que a política da segurança da informação seja apoiada por políticas específicas do tema, que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos.

É muito importante que estas políticas sejam comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação.”

2.7.3 Análise crítica das políticas para segurança da informação e comunicação

Segundo a ISO/IEC 27002:2013, é conveniente que as políticas de segurança da informação e comunicação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequada e eficácia. Esta análise de maneira critica visa o aperfeiçoamento da política, de forma que possamos reavaliar o seu planejamento, os seus controles assim como analisar os incidentes de segurança da informação que ocorreram no período. E, por fim, verificar se a há novas ameaças e vulnerabilidades, de forma que política atenda plenamente aos objetivos da organização com a constante evolução tecnológica.

2.7.4 Requisitos consolidados e necessários para uma Política de Segurança da Informação e comunicação segundo ABNT NBR ISO/IEC 27002:2013

Após análise da norma da ABNT NBR ISO/IEC 27002:2013, verificamos que os requisitos abaixo são imprescindíveis e necessários para a construção de uma política de segurança da informação e comunicação adequada:

1) conter toda a regulamentação, legislação e contratos que a política dever estar amparada;
2) conter uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco;
3) contemplar o escopo da segurança da informação, conceitos, definições e a descrição da importância da Segurança da Informação;

4) deve estar declarado os Princípios da segurança da informação;
5) objetivos e princípios para orientar todas as atividades relativas à segurança da informação;
6) atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos;
7) processos para o tratamento dos desvios e exceções quando há violação na política de segurança da informação;
8) processo de gestão de continuidade do negócio;
9) políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos. (ex.: controle de acesso; classificação e tratamento da informação, etc.);
10) as políticas devem ser comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de um programa de conscientização, educação e treinamento em segurança da informação;
11) as políticas de segurança da informação devem ser analisadas criticamente em intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia;
12) deve haver a declaração do comprometimento da Direção apoiando as metas e princípios da organização.

2.7.5 Tabela om os requisitos necessários para uma Política de Segurança da Informação e comunicação segundo ABNT NBR ISO/IEC 27002:2013

A tabela 1 apresenta todos os requisitos necessários que devem estar contemplados numa Política de Segurança da Informação e Comunicação segundo a ABNT NBR ISO/IEC 27002:2013. Por meio da tabela 1, pode-se fazer uma análise do nível de maturidade das PSIC analisadas neste trabalho.

Tabela 1 – Verificar se a PSIC dos órgãos atende às melhores práticas segundo a ISO 27002:2013

Requisitos necessários para uma PSIC segundo a ISO 27002:2013	**Ministério da Defesa**	**Ministério da Justiça**	**Ministério da Saúde**	**Ministério da Ciência e Tecnologia**	**MPOG/ Secretaria do Orçamento Federal**	**Ministério da Cultura**	**Ministério do Turismo**	**Ministério do Trabalho e Emprego**	**Ministério da Educação**	**Ministério da Agricultura**
1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada?										
2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco?										
3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação?										
4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados?										
5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação?										
6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos?										
7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios)										
8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades)										
9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)?										
10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de "um programa de conscientização, educação e treinamento em segurança da informação?										
11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização)										
12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?										

Fonte: próprio autor.

3 ANÁLISE DAS PSIC DOS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Antes de realizarmos a análise das PSIC, é interessante destacar que foi realizado análise por amostragem de apenas 10 (dez) órgãos da administração pública federal direta, onde escolhemos órgãos de diferentes áreas de atuação (estratégico, essencial e especial), com intuito de realizarmos uma análise comparativa destas PSIC com as melhores práticas levantadas, dentre os quarenta órgãos atualmente existentes na administração pública federal direta (Presidência da República e 39 Ministérios).

Os dez órgãos - da administração pública federal direta - que faremos a análise dos requisitos necessários das PSIC, conforme as melhores práticas, são:

a) Ministério da Defesa;
b) Ministério da Justiça;
c) Ministério da Saúde;
d) Ministério da Ciência e Tecnologia e Inovação;
e) Ministério do Planejamento, Orçamento e Gestão;
f) Ministério da Cultura;
g) Ministério do Turismo;
h) Ministério do Trabalho e Emprego;
i) Ministério da Educação;
j) Ministério da Agricultura.

3.1 Análise da PSIC dos órgãos

3.1.1 PSIC do Ministério da Defesa

Por meio da Portaria nº 1530, publicada em 14 de maio de 2013, do Ministério da Defesa que instituiu a Política de Segurança da Informação e Comunicação deste órgão e verificou-se quais requisitos, segundo a ISO 27002:2013, estão previstos neste documento.

Tabela 2 – Análise da PSIC do Ministério da Defesa

	Ministério da Defesa	**Portaria nº 1530 do Ministério da Defesa**
Requisitos necessários para uma Política de Segurança da Informação e Comunicação segundo a ISO 27002:2013	1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada?	item 3
	2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco?	item 7
	3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação?	itens 1 e 2
	4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados?	item 4
	5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação?	item 4.2
	6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos?	item 7
	7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios)	item 5.6
	8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades)	item 6
	9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)?	item 5
	10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação?	item 7.7.3
	11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização)	item 9
	12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?	não

Fonte: próprio autor.

É de se observar que o requisito 12 – “Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?” apesar de não estar previsto na PSIC do Ministério da Defesa, temos uma ressalva no item 7.1 desta PSIC, onde há a descrição do comprometimento do gestor da segurança da informação que ficou imbuído pelas ações de segurança da informação no âmbito da Administração Central do Ministério da Defesa.

3.1.2 PSIC do Ministério da Justiça

Por meio da Portaria nº 3530, publicada em 03 de dezembro de 2013, do Ministério da Justiça que instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais requisitos, segundo a ISO 27002:2013, estão previstos neste documento.

Tabela 3 – Análise da PSIC do Ministério da Justiça

	Ministério da Justiça	**Portaria nº 3.530, de 3/12/2013/Ministério da Justiça**
Requisitos necessários para uma Política de Segurança da Informação e Comunicação segundo a ISO 27002:2013	1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada?	não
	2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco?	capítulo IV
	3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação?	artigo 3º
	4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados?	artigo 3º
	5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação?	Capítulo II
	6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos?	artigo 6º
	7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios)	artigo 4º, inciso IV
	8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades)	artigo 5º
	9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)?	artigo 4º, incisos V a VIII
	10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação?	não
	11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização)	artigo 14º
	12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?	não

Fonte: próprio autor.

É de se observar que o requisito 12 – “Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?” apesar de não estar previsto na PSIC do Ministério da Justiça, há o artigo 6º que descreve as várias responsabilidades do Gestor da Segurança da Informação.

3.1.3 PSIC do Ministério da Saúde

Por meio da Portaria nº 3207, publicada em 20 de outubro de 2010, do Ministério da Justiça que instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais requisitos, segundo a ISO 27002:2013, estão previstos neste documento.

Tabela 4 – Análise da PSIC do Ministério da Saúde

	Ministério da Saúde	**Portaria nº 3.207, de 20/10/2010 / Ministério da Saúde**
Requisitos necessários para uma Política de Segurança da Informação e Comunicação segundo a ISO 27002:2013	1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada?	não
	2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco?	não
	3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação?	artigos 2º e 3º
	4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados?	não
	5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação?	artigo 3º
	6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos?	não
	7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios)	artigo 4º, inciso IV
	8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades)	artigo 18º
	9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)?	caput e art. 1º
	10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação?	não
	11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização)	artigo 5º
	12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?	não

Fonte: próprio autor.

3.1.4 PSIC do Ministério da Ciência e Tecnologia e Inovação

Por meio da Portaria nº 853, publicada em 05 de setembro de 2013, do Ministério da Ciência e Tecnologia e Inovação que instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais requisitos, segundo a ISO 27002:2013, estão previstos neste documento.

Tabela 5 – Análise da PSIC do Ministério da Ciência e Tecnologia e Inovação

	Ministério da Ciência e Tecnologia e Inovação	**Portaria nº 853, de 05/09/2013/MCTI-Ministério da Ciência e Tecnologia e Inovação**
Requisitos necessários para uma Política de Segurança da Informação e Comunicação segundo a ISO 27002:2013	1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada?	artigo 9º
	2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco?	capítulo VI, artigo 22º
	3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação?	capítulos I e II
	4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados?	capítulo IV
	5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação?	capítulo I
	6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos?	artigo 22º
	7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios)	artigo 49º
	8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades)	capítulo VII
	9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)?	capítulo VI
	10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação?	capítulo VIII, art. 71, inciso VI; art. 72, inciso I
	11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização)	capítulo IX, artigo 74º
	12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?	não

Fonte: próprio autor.

É de se observar que o requisito 12 – “Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?” apesar de não estar previsto na PSIC do Ministério da Ciência e Tecnologia e Inovação, há a figura do Gestor da Segurança da Informação destacada em vários artigos de sua PSIC.

3.1.5 PSIC do Ministério do Planejamento, Orçamento e Gestão - MPOG/SOF

Por meio da Portaria nº 142, publicada em 18 de novembro de 2011, do Ministério do Planejamento, Orçamento e Gestão/MPOG que instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais requisitos, segundo a ISO 27002:2013, estão previstos neste documento.

Tabela 6 – Análise da PSIC do Ministério do Planejamento, Orçamento e Gestão – MPOG/SOF

Ministério do Planejamento, Orçamento e Gestão/Secretaria de Orçamento Federal/SOF		**Portaria nº 142, de 18/11/2011/SOF – Secretaria do Orçamento Federal/ MPOG**
Requisitos necessários para uma Política de Segurança da Informação e Comunicação segundo a ISO 27002:2013	1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada?	art.68º
	2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco?	capítulo IV
	3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação?	capítulos I e II
	4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados?	capítulo III
	5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação?	capítulo I, seção I
	6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos?	artigo 57º
	7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios)	artigo 31º
	8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades)	art. 56º
	9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)?	capítulo V
	10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação?	art. 24º
	11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização)	art. 67º
	12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?	não

Fonte: próprio autor.

É de se observar que o requisito 12 – "Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?" apesar de não estar previsto na PSIC do Ministério do Planejamento, Orçamento e Gestão/Secretaria de Orçamento Federal/SOF, há a figura do Gestor da Segurança da Informação destacada no artigo 58º de sua PSIC.

3.1.6 PSIC do Ministério do Ministério da Cultura

Por meio da Portaria nº 119, publicada em 05 de dezembro de 2011, do Ministério da Cultura que instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais requisitos, segundo a ISO 27002:2013, estão previstos neste documento.

Tabela 7 – Análise da PSIC do Ministério da Cultura

	Ministério da Cultura	**Portaria nº 119, de 05/12/2011/MinC – Ministério da Cultura**
Requisitos necessários para uma Política de Segurança da Informação e Comunicação segundo a ISO 27002:2013	1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada?	não
	2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco?	artigo 10º
	3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação?	artigo 2º
	4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados?	capítulo I, artigo 3º
	5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação?	artigos 4º e 5º
	6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos?	capítulo II, seção I
	7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios)	artigo 6º, parágrafo 1º, inciso IV
	8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades)	não
	9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)?	artigo 6º
	10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de "um programa de conscientização, educação e treinamento em segurança da informação?	artigo 6º, parágrafo 1º, inciso VII
	11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização)	não
	12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?	não

Fonte: próprio autor.

3.1.7 PSIC do Ministério do Turismo

Por meio da Portaria nº 108, publicada em 22 de maio de 2013, do Ministério do Turismo que instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais requisitos, segundo a ISO 27002:2013, estão previstos neste documento.

Tabela 8 – Análise da PSIC do Ministério do Turismo

Ministério do Turismo		**Portaria nº 108, de 22/05/2013/Ministério do Turismo**
Requisitos necessários para uma Política de Segurança da Informação e Comunicação segundo a ISO 27002:2013	1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada?	Anexo
	2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco?	artigo 9º e capítulo VIII
	3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação?	Capítulos I, II e III
	4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados?	Capítulo IV
	5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação?	artigos 2º e 7º
	6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos?	Capítulo XXII
	7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios)	Capítulo XIV
	8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades)	Capítulo XX
	9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)?	Capítulos VII até o XVIII
	10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de "um programa de conscientização, educação e treinamento em segurança da informação?	artigo 47º
	11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização)	Capítulo XXII
	12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?	Artigo 65º

Fonte: próprio autor.

3.1.8 PSIC do Ministério do Trabalho e Emprego

Por meio da Portaria nº 1047, publicada em 16 de julho de 2013, do Ministério do Trabalho e Emprego que instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais requisitos, segundo a ISO 27002:2013, estão previstos neste documento.

Tabela 9 – Análise da PSIC do Ministério do Trabalho e Emprego

	Ministério do Trabalho e Emprego	**Portaria nº 1047 de 16/07/2013 / MTE - Ministério do Trabalho e Emprego**
Requisitos necessários para uma Política de Segurança da Informação e Comunicação segundo a ISO 27002:2013	1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada?	não
	2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco?	não
	3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação?	seções I e II
	4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados?	não
	5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação?	artigo 6º
	6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos?	não
	7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios)	artigos 16º até 19º
	8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades)	seção V
	9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)?	seção IV
	10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de "um programa de conscientização, educação e treinamento em segurança da informação?	artigo 13º
	11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização)	artigo 38º
	12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?	não

Fonte: próprio autor.

3.1.9 PSIC do Ministério da Educação

Por meio da Portaria nº 1054, publicada em 02 de agosto de 2011, do Ministério da Educação que instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais requisitos, segundo a ISO 27002:2013, estão previstos neste documento.

Tabela 10 – Análise da PSIC do Ministério da Educação

	Ministério da Educação	**Portaria n° 1054 , de 02/08/2011/Min. da Educação**
Requisitos necessários para uma Política de Segurança da Informação e Comunicação segundo a ISO 27002:2013	1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada?	capítulo III
	2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco?	não
	3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação?	capítulos I e II
	4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados?	não
	5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação?	artigo 7º
	6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos?	não
	7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios)	Capítulo V, seção VII
	8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades)	Capítulo VI
	9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)?	Capítulo V
	10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação?	não
	11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização)	artigo 40º
	12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?	não

Fonte: próprio autor.

É de se observar que o requisito 12 – "Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?" apesar de não estar previsto na PSIC do Ministério da Educação há a figura do Gestor da Segurança da Informação destacada em vários artigos de sua PSIC.

3.1.10 PSIC do Ministério da Agricultura

Por meio da Portaria nº 795, publicada em 05 de setembro de 2012, do Ministério da Agricultura instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais requisitos, segundo a ISO 27002:2013, estão previstos neste documento.

Tabela 11 – Análise da PSIC do Ministério da Agricultura

	Ministério da Agricultura	**Portaria nº 795, de 5/09/12/Min. da Agricultura**
Requisitos necessários para uma Política de Segurança da Informação e Comunicação segundo a ISO 27002:2013	1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada?	não
	2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco?	não
	3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação?	itens 2 e 3
	4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados?	Não estão declarados, mas estão descritos no item 1 - Objetivo.
	5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação?	item 4
	6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos?	item 6
	7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios)	item 5.13
	8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades)	item 7
	9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc)?	item 5
	10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de "um programa de conscientização, educação e treinamento em segurança da informação?	item 5.22
	11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização)	não
	12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?	não

Fonte: próprio autor.

É de se observar que o requisito 12 – “Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?” apesar de não estar previsto na PSIC do Ministério da Agricultura, há o item 5.23 desta PSIC que afirma que os diversos níveis gerenciais devem zelar pelo cumprimento das Diretrizes de Segurança da Informação e Comunicações no âmbito de sua competência.

3.2 Requisitos consolidados das PSIC atendidos por cada órgão

Tabela 12 – Requisitos consolidados das PSIC atendidos por cada órgão analisado

Requisitos necessários para uma PSIC segundo a ISO 27002:2013	**Ministério da Defesa**	**Ministério da Justiça**	**Ministério da Saúde**	**Ministério da Ciência e Tecnologia**	**MPOG/ Secretaria do Orçamento Federal**	**Ministério da Cultura**	**Ministério do Turismo**	**Ministério do Trabalho e Emprego**	**Ministério da Educação**	**Ministério da Agricultura**
1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada?	sim	não	não	sim	sim	não	sim	não	sim	não
2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco?	sim	sim	não	sim	sim	sim	sim	não	não	não
3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação?	sim	sim	sim	sim	sim	sim	sim	sim	sim	sim
4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados?	sim	sim	não	sim	sim	sim	sim	não	não	não
5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação?	sim	sim	sim	sim	sim	sim	sim	sim	sim	sim
6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos?	sim	sim	não	sim	sim	sim	sim	não	não	sim
7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios)	sim	sim	sim	sim	sim	sim	sim	sim	sim	sim
8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades)	sim	sim	sim	sim	sim	não	sim	sim	sim	sim
9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)?	sim	sim	sim	sim	sim	sim	sim	sim	sim	sim
10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de "um programa de conscientização, educação e treinamento em segurança da informação?	sim	não	não	sim	sim	sim	sim	sim	não	sim
11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização)	sim	sim	sim	sim	sim	não	sim	sim	sim	não
12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?	não	não	não	não	não	não	sim	não	não	não

Fonte: próprio autor.

Com as PSIC analisadas no item anterior, foi consolidado, por meio da tabela 12, quais requisitos, segundo a ISO 27002:2013, são atendidos ou não por cada Ministério analisado.

3.3 Análise das informações consolidadas

3.3.1 Quantidade de requisitos verificados por atributo

Para melhor entendermos os aspectos abordados ou não nas PSIC, classificamos os doze requisitos essenciais, segundo as melhores práticas, em três grandes grupos por apresentarem atributos semelhantes, na qual designamos por: regulação, prevenção e/ou controles e responsabilidades e/ou penalidades. Dentre os doze requisitos, foi identificado 4 (quatro) requisitos com atributos de regulação, 5 (cinco) requisitos com atributos de prevenção e/ou controles e 3 (três) requisitos com atributos de responsabilidade e/ou penalidades, conforme apresentado na tabela 13.

Nesta tabela 13, também, é apresentado o percentual dos requisitos, mapeados e necessários a uma PSIC conforme a ISO 27002:2013, atendidos pelos órgãos da administração pública federal direta dentre os órgãos analisados neste trabalho, assim como o percentual médio dos requisitos verificados por cada atributo devidamente classificado, sendo que para este percentual, calculamos por meio da média aritmética dos requisitos classificados em cada um dos atributos.

Por meio desta tabela, pode-se observar que há atributos com maior ou menor nível de maturidade, onde se identificou 82,0 % dos órgãos analisados com previsão do atributo “Prevenção e/ou controles”; 77,5 % dos órgãos analisados com previsão do atributo “Regulação”; e 56,7 % dos órgãos analisados com previsão do atributo “Responsabilidade e/ou penalidade”.

Embora nenhum dos três atributos classificados tenha plena previsão, é de destacar que o atributo “Prevenção e/ou Controle” apresentou uma maior previsibilidade nas PSIC, sendo que dos cinco requisitos que compuseram este atributo, dois destes requisitos (7 e o 9) estavam previsto em todas PSIC analisadas. O requisito 11 “As políticas de segurança da informação são analisadas criticamente em intervalos planejados?” apesar de estar ausente em somente duas PSIC, é de destacar que em todos os dez órgãos tiveram suas políticas atualizadas, o que nos mostrou que na prática o requisito vem sendo verificado, no entanto não há a previsão formal conforme defende as melhores práticas. Desta forma, para que este

atributo “Prevenção e/ou Controle” tenha previsão plena nos órgãos analisados da administração pública federal, é necessário que os requisitos 2 “Programa de conscientização, educação e treinamento em segurança da informação” e o requisito 10 “Conter uma estrutura para estabelecer objetivos de controle e os controles” sejam reavaliados de forma que este atributo seja prontamente atendido conforme estabelece as melhores práticas.

O atributo “Regulação”, o que teve a segunda melhor previsão nas PSIC, é composto por 4 (quatro) requisitos, sendo que 2(dois) destes requisitos (3 e 5) estão plenamente previstos em todas PSIC analisadas neste trabalho. Os requisitos 4 e o 5 estão previstos em somente cinco e seis, respectivamente, das dez PSIC analisadas, o que mostra uma necessidade dos órgãos da administração pública federal atuarem em parceria a fim de que haja maior interação quando da elaboração ou da revisão de suas PSIC. Pois, estes dois requisitos são requisitos simples e que de maneira geral indiretamente já estão previstos nas suas PSIC, pois os órgãos direta ou indiretamente já atuam respeitando os preceitos da segurança da informação e da legislação na qual estes requisitos estão amparados.

O atributo “Responsabilidade e/ou penalidade” identificado com menor previsibilidade nas PSIC analisadas se deve, além de ser um assunto relativamente novo, ao pouco apoio da alta administração, tendo em vista que é uma área que envolve assuntos ligados à tecnologia da informação e como tal muitas vezes uma área de pouco conhecimento pelos gestores públicos. E, isto se pode ratificar quando verificamos que somente um dos dez órgãos analisados apresenta a previsão do requisito 12 “Há a declaração do comprometimento da direção apoiando as metas e princípios da organização?” que teve a menor previsão nas PSIC analisadas. Para que haja um maior apoio destas atividades e responsabilidades ligadas à segurança da informação e consequentemente para aprimorar a governança de TI dos órgãos públicos pela alta administração, sugerimos que sejam utilizadas estruturas organizacionais, como por exemplo, criação de um comitê ligado diretamente à alta administração (Comitê Estratégico de TI) para apoiá-lo na elaboração da estratégia de TI e no acompanhamento do alcance dos objetivos estratégicos de TI, utilizando, entre outros instrumentos, relatórios periódicos sobre as ações relativas à TI, gerados pela área de TI de forma a dar maior amparo técnico para que a alta administração possa atuar com maior efetividade. Desta forma, acreditamos que a própria alta administração ficará imbuída de pautar a previsibilidade do requisito 12 na PSIC do órgão que é gestora quando da atualização periódica desta política.

Tabela 13 – Análise dos atributos dos requisitos

Atributo dos Requisitos	**Requisitos verificados por atributo**	**% dos requisitos atendidos pelos órgãos analisados**	**%Médio dos requisitos verificados por atributo**
Regulação	1 - Contém a regulamentação, legislação e contratos que a PSI deve estar amparada?	50 %	77,5 %
	3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação?	100 %	
	4 - Os Princípios da Política de Segurança da Informação estão declarados?	60 %	
	5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação?	100 %	
Prevenção e/ou Controles	2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco?	60 %	82,0 %
	7 - Há previsão para o processo de gestão de continuidade do negócio na PSI? (Gestão da Continuidade de Negócios)	100 %	
	9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)?	100 %	
	10 - As políticas de segurança da informação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação?	70 %	
	11 - As políticas de segurança da informação são analisadas criticamente em intervalos planejados? (Atualização)	80 %	
Responsabilidades e/ou Penalidades	6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos?	70 %	56,7 %
	8 - Caso haja violação da PSI, há declaração das consequências neste documento? (Penalidades)	90 %	
	12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?	10 %	

Fonte: próprio autor.

3.3.2 Quantidade de requisitos verificados por cada órgão público analisado

Na tabela 14 é apresentada a quantidade assim como o percentual de requisitos verificados, na política de segurança da informação e comunicação conforme a ISO 27002:2013, por cada órgão da administração pública federal direta analisado neste trabalho.

Tabela 14 – Quantidade de requisitos atendidos nos órgãos analisados

Órgão	Quantidade de requisitos verificados	% requisitos verificados no órgão
Ministério do Turismo	12	100,00%
Ministério da Ciência e Tecnologia e Inovação	11	91,67%
MPOG/ Secretaria do Orçamento Federal	11	91,67%
Ministério da Defesa	11	91,67%
Ministério da Justiça	9	75%
Ministério da Cultura	8	66,67%
Ministério do Trabalho e Emprego	7	58,33%
Ministério da Educação	7	58,33%
Ministério da Agricultura	7	58,33%
Ministério da Saúde	6	50%

Fonte: próprio autor.

Por meio desta tabela 14, pode-se observar que a média de requisitos verificados nas políticas de segurança da informação dos órgãos da administração pública federal, que foram objeto deste estudo, é de 8,9 ou 74,17 % de requisitos atendidos. Logo, dos dez órgãos que foram objeto de estudo, podemos verificar que somente cinco dos dez órgãos estão acima desta média de 8,9 de requisitos atendidos, enquanto os demais órgãos ficaram abaixo desta média.

3.4 Matriz com o nível de maturidade das políticas de segurança da informação e comunicação das organizações públicas federais analisadas

A média aritmética dos requisitos verificados nas políticas de segurança da informação e comunicação foi 8,9. Se calcularmos o desvio-padrão destes requisitos verificados teremos o valor de 2,07. Logo, se o número de requisitos estiver acima do valor da média + desvio padrão (8,90 + 2,07)= 10,97, teremos um nível de maturidade alto. Se o número de requisitos analisados estiverem no intervalo de 8,90 e 10,97, teremos um nível de maturidade bom com

relação a política de segurança da informação analisada. Agora, caso o valor obtido esteja no intervalo de 6,83 e 8,90, teremos uma política de segurança da informação com razoável grau de maturidade. No entanto, se o valor obtido for inferior a 6,83, teremos um grau de maturidade a desejar.

Com base nesta análise, é apresentada a tabela 15 com a matriz de maturidade das Políticas de Segurança da Informação e Comunicação dos órgãos da administração pública federal.

Tabela 15 – Matriz de maturidade das Políticas de Segurança da Informação e Comunicação

Média da quantidade de requisitos verificados nas PSIC analisadas	**Grau de Maturidade**	**Quantidade de órgãos analisados que atendem a esta faixa de requisitos**
Acima de 10,97	alto	4
Entre 8,9 e 10,97	bom	2
Entre 6,83 e 8,9	razoável	3
Menor que 6,83	a desejar	1

Fonte: próprio autor.

3.5 Análise por área de atuação dos órgãos analisados

Para melhor análise, classificamos os dez órgãos, conforme apresentado na tabela 16, em três segmentos (estratégicas, fundamentais e especiais) conforme sua área de atuação. Classificamos em área estratégica, os órgãos que determinam as diretrizes e planejamento do Estado, de tal forma que suas decisões impactam diretamente ou indiretamente os demais órgãos da administração pública federal. Classificamos em área fundamental, os órgãos que atuam com serviços indispensáveis à sobrevivência e ao bem estar social. Por fim, classificamos em área especial, os órgãos que não atuam com as áreas estratégicas e fundamentais.

Tabela 16 – Quantidade de requisitos atendidos por órgão conforme área de atuação

Área	Ministério	Quantidade de requisitos verificados em cada órgão
Estratégica	Planejamento, Orçamento e Gestão	11
	Ciência, Tecnologia e Inovação	11
	Defesa	11
	Justiça	9
Fundamental	Saúde	6
	Educação	7
	Trabalho e Emprego	7
	Agricultura, Pecuária e Abastecimento	7
Especial	Turismo	12
	Cultura	8

Fonte: próprio autor.

Dos quatro órgãos classificados neste trabalho como área estratégica, três destes - Ministério do Planejamento, Orçamento e Gestão, Ministério da Ciência, Tecnologia e Inovação e o Ministério da Defesa - apresentaram um alto nível de maturidade conforme matriz exposta na tabela 15, onde tiveram 11 dos 12 requisitos verificados em suas PSIC. O Ministério da Justiça apresentou um grau de maturidade "BOM", observando 9 dos 12 requisitos. O requisito 12 – "Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização?" foi o único não verificado nas PSIC destes quatro órgãos. No entanto, é de se destacar que apesar deste requisito não estar previsto nestas PSIC, se verifica a figura do Gestor da Segurança da Informação descrita nestas PSIC, que ficou imbuído pelas ações de segurança da informação no âmbito de cada um destes órgãos. Pode-se observar, por meio de nossa análise, que os Ministérios, que foram objeto deste estudo e classificados como áreas estratégicas, apresentaram uma PSIC com nível de maturidade acima da média dos outros órgãos analisados com relação à área de atuação. A nossa percepção por meio deste estudo, é que os órgãos classificados como "área estratégica", utilizaram um padrão com base nas melhores práticas para construção e atualização de suas PSIC. Por fim, pode-se dizer que as PSIC da área estratégica tem, no mínimo, uma boa homogeneidade e estão condizentes com o seu grau de atuação, apresentando documentação com praticamente todos os requisitos imprescindíveis para uma política.

Quanto as PSIC dos quatro órgãos classificados neste trabalho como áreas fundamentais - Ministério da Saúde, Ministério da Educação, Ministério do Trabalho e Emprego e o Ministério da Agricultura, Pecuária e Abastecimento - apresentaram um grau de maturidade de razoável a desejar, conforme matriz apresentada na tabela 15, sendo que 3 destes órgãos atenderam 7 dos 12 requisitos mapeados neste trabalho e o Ministério da Saúde atendeu a somente a 6 dos 12 destes requisitos, sendo este inclusive o órgão com o pior nível de maturidade, com relação a PSIC, observado neste estudo. A nosso entender, esta homogeneidade quanto ao nível de maturidade das PSIC destes órgãos analisados, por terem uma área de atuação similar, provavelmente, deve-se a não existência de um trabalho de benchmarking, onde elaboram estas PSIC sem maiores críticas ou análises, simplesmente utilizando como modelo a PSIC de um destes órgãos que já tinham criado este documento, gerando políticas com a ausência de vários requisitos importantes e imprescindíveis relacionadas aos aspectos de segurança da informação que deveriam estar abordados nestes documentos conforme as melhores práticas.

As PSIC dos dois órgãos classificados neste trabalho como áreas especiais (Ministério do Turismo e Ministério da Cultura) atenderam a 12 e 8 requisitos respectivamente. Logo, podemos observar que a PSIC do Ministério do Turismo apresentou o maior nível de maturidade dos órgãos que foram objeto de estudo deste trabalho, tendo sua PSIC classificada com nível de maturidade “ALTO”, conforme apresentado na tabela 15. O Ministério da Cultura obteve um nível de maturidade “RAZOÁVEL” conforme matriz de maturidade. Isto nos mostra que para estes órgãos, diferentemente dos órgãos classificados como de áreas estratégicas e fundamentais, apresentaram uma heterogeneidade muito grande, onde tivemos as suas PSIC variando de um nível de maturidade de “RAZOÁVEL” a “ALTO”. O que reforça nossa teoria quanto a áreas fundamentais, pois por atuarem com assuntos discretos e diferenciados, e talvez por não observarem similaridade dos assuntos tratados, não veem a necessidade ou não apresentam uma cultura de benchmarking entre estes órgãos, a fim de que haja uma maior homogeneidade nestas PSIC, criando uma discrepância quanto ao grau de maturidade destes órgãos analisados.

CONCLUSÃO

No estudo realizado, infere-se, por meio da análise de vários documentos - portarias, decretos e leis - que o governo federal está direcionando os seus esforços para que a implementação da segurança da informação seja realizada nestes órgãos de modo a atender suas necessidades de forma compatível com as melhores práticas e legislações específicas. No entanto, baseado nos dados levantados dos órgãos que foram objeto de estudo, pode-se verificar que as PSIC dos órgãos da administração pública federal direta estão num nível de maturidade bem diversificado, necessitando de uma melhor orientação a fim de que haja uma maior homogeneidade e maturidade com intuito de que estas políticas não sejam uma mera formalização, mas um documento que agregue valor e seja uma diretriz a ser seguida pela organização.

Com relação ao atendimento dos requisitos imprescindíveis numa PSIC, constatou-se que somente um dos órgãos analisados previu todos os doze requisitos, o que mostra uma deficiência e um risco aos órgãos públicos de forma geral, pois uma PSIC bem implementada pode mitigar ou mesmo responsabilizar ações indesejadas numa organização.

Outro aspecto abordado neste trabalho foi uma análise de todos os requisitos essenciais numa PSIC baseado em atributos, onde identificamos que os órgãos analisados tiveram maior previsibilidade quando o atributo se relaciona a “Prevenção e/ou Controle”, onde se infere que este fato se deve a cultura dos órgãos da Administração Pública Federal direta já terem regularmente uma fiscalização pelos órgãos de controle do Governo Federal, o que mostra, em nossa percepção, esse maior nível de maturidade dos requisitos com este atributo.

Quando realizamos a análise pela ótica da área de atuação dos órgãos da administração pública federal direta, constatou-se que os órgãos classificados como área estratégica assim como os órgãos classificados como área fundamental, apresentaram uma similaridade dos requisitos previstos em suas PSIC por sua área de atuação, o que se pode inferir que há uma tendência destes órgãos estarem imbuídos de atenderem às melhores práticas com relação à segurança da informação, porém não se verifica um estudo ou uma análise mais crítica dos requisitos imprescindíveis a serem abordados em suas politicas.

A fim de que as PSIC dos órgãos da administração pública federal direta atinjam um grau de maturidade “ALTO”, recomendamos que seja criado um comitê de segurança multidisciplinar, de caráter temporário, com a participação de várias áreas (estratégica, fundamental e especial), conforme apresentado neste trabalho, e que seja dirigido por um gestor com a responsabilidade de analisar, avaliar, criticar e revisar a PSIC de cada órgão da administração pública federal direta antes destas políticas serem publicadas. Com esta medida, espera-se que tenhamos PSIC coesas, precisas e condizentes com as melhores práticas da segurança da informação. É importante destacar que sempre a decisão de aceitar as recomendações deste comitê é do gestor de cada órgão, mas com certeza o órgão, ao receber um feedback de uma área especialista no assunto, ficará inclinado a no mínimo prever mesmo que seja de forma parcial tais recomendações nas suas PSIC. Acredita-se que a implementação deste comitê, mesmo que seja uma equipe de caráter transitório e que funcione periodicamente, poderá reduzir o risco existente sobre os ativos dos órgãos da administração pública federal, que é o principal objetivo quando tratamos de termos um documento formal como a política de segurança.

Por fim, apesar deste trabalho ter sido realizado com base em dez órgãos da administração pública federal direta, não podemos avaliar ou mesmo inferir como está o nível de maturidade dos outros 30 (trinta) órgãos não analisados. Outro fato que se deve destacar, é que neste estudo somente se considerou o valor quantitativo dos requisitos, onde não se abordou o mérito qualitativo destes requisitos. Baseado nestes fatos, entende-se que para uma avaliação precisa de como está as PSIC da administração pública federal direta, se faz necessário um estudo mais amplo abordando não somente todos os órgãos, mas uma análise minuciosa do valor qualitativo destes requisitos indispensáveis, o que poderá ser objeto de trabalhos futuros.

REFERÊNCIAS

ABNT. Tecnologia da informação - Técnicas de segurança - **Código de prática para a gestão da segurança da informação: ABNT NBR ISO/IEC 27002:2013**. 2a. ed. Rio de Janeiro, 2013.

ABNT. Tecnologia da informação - Técnicas de segurança - **Sistemas de gestão de segurança da informação - Requisitos: ABNT NBR ISO/IEC 27001:2006**. 1a. ed. Rio de Janeiro, 2006.

BEAL, Adriana. **Segurança da Informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BRASIL. **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. Disponível em: *www.planalto.gov.br/ccivil_03/decreto/D3505.htm*. Acesso em: 19 mar 2014.

CAMPOS, André L. N. **Sistema de segurança da informação**: controlando os riscos. Florianópolis: Visual Books, 2006.

CAMPOS, André – **Sistema de Segurança da Informação**: Controlando os Riscos. 2. ed. / André Campos. – Florianópolis: Visual Books, 2007.

CASTRO, Mauro. **Política de Tecnologia da Informação no Brasil** (Um guia para o século XXI). 1.ed.: Politec, 2002.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação**. Rio de Janeiro: Editora Ciência Moderna LTDA., 2003.

FERREIRA, F.N.F.; ARAÚJO, M.T. **Política de Segurança da Informação** – Guia Prático para Elaboração e Implementação. Rio de Janeiro: Editora Ciência Moderna LTDA., 2006.

FONTES**,** Edson. **Segurança da Informação**: o usuário faz a diferença. Microsoft, São Paulo. Editora Saraiva, 2006.

Instrução Normativa GSI Nº 01, DE 13 DE JUNHO DE 2008 - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta. Disponível em: http://dsic.planalto.gov.br/documentos/nc_7_controle_acesso.pdf. Acesso em: 19 fev 2014.

LAUREANO, P. A. M, (2005), **Gestão de Segurança da Informação**, disponível em < www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf >. Acesso em: 19 fev 2014.

MARCIANO, P.L. João. **Segurança da Informação** - uma abordagem social, monografia de doutor em Ciências da Informação, 2006, publicada Universidade de Brasília. Disponível em <http://repositorio.unb.br/bitstream/10482/1943/1/Jo%C3%A3o%20Luiz%20Pereira%20Marciano.pdf >. Acesso em: 18 fev 2014.

MARTINS, José Carlos Cordeiro. **Gestão de Projetos de Segurança da Informação**. Rio de Janeiro, Brasport: 2003.

MONTEIRO, Edmundo; BOAVIDA, Fernando, **Engenharia de Redes Informáticas**, 4ª ed., FCA Editora de Informática Ltda, 2000.

NAKAMURA, E., GEUS, P. **Segurança de redes em ambientes cooperativos**: fundamentos, técnicas, tecnologias, estratégias. São Paulo: Novatec, 2003.

Portaria nº 142, de 18/11/2011/SOF – Secretaria do Orçamento Federal/MPOG**.** Institui a Política de Segurança da Informação e Comunicação – PoSIC da Secretaria de Orçamento Federal/MPOG. Disponível em: http://www.orcamentofederal.gov.br/orcamentos-anuais/orcamento-2011/programacao-orcamentaria-e-financeira/portaria-sof/Ptr_sof_142_de_181111.pdf . Acesso em: 04 abr 2014.

Portaria nº 1047 de 16/07/2013 / MTE - Ministério do Trabalho e Emprego. Institui a Política de Segurança da Informação e Comunicações – POSIC do Ministério do Trabalho e Emprego. Disponível em: http://www.diariodasleis.com.br/busca/exibelink.php?numlink=224048. Acesso em: 04 abr 2014.

Portaria nº 108, de 22/05/2013/Ministério do Turismo. Institui a Política de Segurança da Informação e Comunicação - POSIC, no âmbito do Ministério do Turismo. Disponível em: http://www.turismo.gov.br/turismo/legislacao/portarias/20130523.html. Acesso em: 04 abr 2014.

Portaria nº 1530, de 14/05/13/Ministério da Defesa. Institui a Política de Segurança da Informação e Comunicações da Administração Central do Ministério da Defesa. Disponível em: http://www.jusbrasil.com.br/diarios/54405781/dou-secao-1-16-05-2013-pg-33. Acesso em: 04 abr 2014.

Portaria nº 119, de 05/12/2011/MinC – Ministério da Cultura. Institui a Política de Segurança da Informação e Comunicações do Ministério da Cultura e o Sistema de Segurança da Informação e Comunicações. Disponível em: http://www2.cultura.gov.br/site/2011/12/07/portaria-n%C2%BA-1192011minc/. Acesso em: 04 abr 2014.

Portaria nº 3.530, de 3/12/2013/Ministério da Justiça. Institui a Política de Segurança da Informação e Comunicações do Ministério da Justiça. Disponível em: http://www.jusbrasil.com.br/diarios/62532816/dou-secao-1-04-12-2013-pg-22. Acesso em: 04 abr 2014.

Portaria nº 3.207, de 20/10/2010/Ministério da Saúde. Institui a Política de Segurança da Informação e Comunicações do Ministério da Saúde. Disponível em: http://bvsms.saude.gov.br/bvs/saudelegis/gm/2010/prt3207_20_10_2010.html. Acesso em: 04 abr 2014.

Portaria nº 853, de 05/09/2013/MCTI - Ministério da Ciência e Tecnologia e Inovação. Institui a Política de Segurança da Informação e Comunicações do Ministério da Ciência,

Tecnologia e Inovação (Posic/MCTI). Disponível em: http://www.jusbrasil.com.br/diarios/58795774/dou-secao-1-06-09-2013-pg-7. Acesso em: 07 abr 2014.

Portaria n° 1054, de 02/08/2011/Ministério da Educação e suas alterações na Portaria nº 996 de 06/08/2012. Aprova a Política de Segurança da Informação e Comunicações - POSIC do Ministério da Educação – MEC. Disponível em: http://www.educacao.gov.br/index.php?option=com_content&view=article&id=15451&Itemid=1078. Acesso em: 10 abr 2014.

Portaria nº 795, de 5/09/12/Ministério da Agricultura. Aprovar a atualização da Política de Segurança da Informação e Comunicações do Ministério da Agricultura, Pecuária e Abastecimento. Disponível em: http://www.agricultura.gov.br/arq_editor/file/acesso_informacao/pregao/Documentos-PREGAO-20-2013/10-Politica-Seguranca-Informacao-Comunicacoes.pdf. Acesso em: 10 abr 2014.

REZENDE, Denis Alcides. ABREU, Aline França. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. São Paulo: Atlas, 2000.

ROCHA, P.C.C. **Segurança da Informação** - Uma Questão Não Apenas Tecnológica. [S.l.], Brasília 2008. Monografia de Conclusão de Curso (Especialização) – Departamento de Ciência da Computação, Instituto de Ciências Exatas da Computação, Instituto de Ciências Exatas, Universidade de Brasília. Disponível em: http: //dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/paulo_cesar.pdf. Acesso em: 29 mai 2014.

SÊMOLA, M. **Gestão da Segurança da Informação** – Uma visão executiva. 3. Ed. Rio de Janeiro: Elsevier, 2003. 160p.

SENGUPTA, A.; MAZUMDAR C.; BAGCHI A. **A Formal Methodology for Detection of Vulnerabilities in an Enterprise Information System,** In Conference on Risks and Security of Internet and Systems (CRiSIS), p. 74-80, October 2009.

SIEWERT, C.Vanderson, (s/d), integração da politica de segurança da informação com o firewall, [em linha] disponível em http://artigocientifico.tebas.kinghost.net/uploads/artc_1202930234_72.pdf. Acesso em: 19 mar 2014.

SOUSA, B. Lindeberg, (2006), *TCP/IP Básico Conectividade em Redes*, Dados, 3ª Edição, Editora Érica Ltda.

SPANCESKI, R. Francini, (2004), Politica de segurança da informação – Desenvolvimento de um Modelo voltado para Instituições de ensino monografia de Bacharel, [em linha] disponível em <http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_francini_politicas.pdf> Acesso em: 19 mar 2014.

TADANO, K. Yumi. **Gestão Eletrônica de Documentos**: Assinatura Digital e Validação Jurídica de Documentos Electrónicos, Cuiabá MT – Brasil, 2002.

ANEXO A: PSIC DO MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO - MPOG/SOF

Capítulo I
ESCOPO

Art. 1º O presente documento tem por objetivo instituir a Política de Segurança da Informação e Comunicação – PoSIC, no âmbito da Secretaria de Orçamento Federal – SOF.

Seção I
Objetivo da PoSIC

Art. 2º A PoSIC objetiva garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações produzidas ou custodiadas pela SOF.

Art. 3º O órgão observará as diretrizes, as normas, os procedimentos, os mecanismos, as competências e as responsabilidades estabelecidos nesta PoSIC.

Art. 4º Integram também a PoSIC as normas e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

Art. 5º As diretrizes de Segurança da Informação e Comunicação – SIC consideram, prioritariamente, objetivos estratégicos, processos, requisitos legais e a estrutura da SOF.

Art. 6º A Gestão de Segurança da Informação e Comunicação – GSIC deverá apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de SIC.

Seção II
Abrangência

Art. 7º As diretrizes, normas complementares e manuais de procedimentos da PoSIC aplicam-se a servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e outros que executem atividades vinculadas à SOF.

Parágrafo único. Todos deverão ser responsáveis e estar comprometidos com a SIC.

Art. 8º Os acordos de cooperação, contratos, convênios e outros instrumentos do mesmo gênero, celebrados com a SOF, observarão o disposto nesta PoSIC.

Art. 9º Esta política também se aplica, no que couber, no relacionamento da SOF com outros órgãos e entidades públicos ou privados.

Capítulo II
CONCEITOS E DEFINIÇÕES

Art. 10. No âmbito da PoSIC, considera-se:

I - ameaça: evento que tem potencial para comprometer os objetivos da organização por meio de danos diretos aos ativos físicos ou de informação ou prejuízos decorrentes de situações inesperadas;

II - ativos de informação: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

III - 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;

IV - capacitação em SIC: saber o que é segurança da informação e comunicação, e sua aplicação para uso na rotina pessoal e profissional, servindo como multiplicador do tema e aplicando os conceitos e procedimentos na organização como gestor de SIC;

V - classificação da informação: identificação de quais são os níveis de proteção que as informações demandam e o estabelecimento de classes e formas de como identificá-las, além de determinar os controles de proteção necessários a cada uma delas;

VI - Comissão de Gestão da Informação – CGI: colegiado de caráter deliberativo responsável pela normatização e supervisão da gestão da informação, bem como pela gestão de SIC, no âmbito da SOF;
VII - Comitê de Segurança da Informação e Comunicação – CSIC: colegiado de caráter deliberativo responsável pela normatização e supervisão da segurança da informação e comunicação, no âmbito do Ministério do Planejamento, Orçamento e Gestão – MP;
VIII - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física ou jurídica, sistema, órgão ou entidade não autorizado e credenciado;
IX - conscientização em SIC: saber o que é segurança da informação e comunicação, e sua aplicação para uso pessoal e profissional, além de habilitar o usuário como multiplicador sobre o tema;
X - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de permitir ou bloquear o acesso;
XI - custodiante do ativo de informação: é aquele que, de alguma forma, zela pelo armazenamento, pela operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;
XII - disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade;
XIII - equipe de tratamento e resposta a incidentes em redes computacionais – ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;
XIV - estrutura de gestão de segurança da informação e comunicação: grupo responsável pela gestão e execução da SIC no âmbito da SOF;
XV - gestão de ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;
XVI - gestão de continuidade dos negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece a estrutura para que se desenvolva a resiliência organizacional que seja capaz de responder efetivamente a ameaças e a salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;
XVII - gerenciamento de operações e comunicações: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporta, satisfazendo os acordos de níveis de serviço;
XVIII - gestão de riscos de segurança da informação e comunicação – GRSIC: conjunto de processos contínuos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;
XIX - gestão de segurança da informação e comunicação – GSIC: 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, física, lógica, orgânica e organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, no âmbito da tecnologia da informação e comunicação;
XX - gestor dos ativos de informação: unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;
XXI - gestor de SIC: servidor titular da Coordenação Geral de Tecnologia e da Informação da Secretaria-Adjunta de Gestão Corporativa – CGTEC/SEAGE, responsável pela GSIC no âmbito da SOF;

XXII - incidente de SIC: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompida a execução de alguma atividade crítica por um período inferior ao tempo objetivo de recuperação;
XXIII - 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;
XXIV - infraestrutura de tecnologia da informação: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica;
XXV - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
XXVI - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da SIC;
XXVII - recursos criptográficos: sistemas, programas, processos e equipamento isolado ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;
XXVIII - risco de SIC: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por uma ou mais ameaças, com impacto negativo no negócio da organização;
XXIX - segurança física e do ambiente: processo que trata da proteção dos ativos físicos da instituição, englobando instalações físicas, internas e externas, nas localidades em que a organização está presente;
XXX - sensibilização em SIC: saber o que é segurança da informação e comunicação, de forma a aplicá-la nas rotinas pessoal e profissional;
XXXI - terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externas à SOF;
XXXII - tratamento de incidentes: 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;
XXXIII - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas; e
XXXIV - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Capítulo III
PRINCÍPIOS

Art. 11. A PoSIC obedecerá aos princípios constitucionais, administrativos e ao arcabouço legislativo vigente que regem a Administração Pública Federal.

Capítulo IV
DIRETRIZES GERAIS

Art. 12. Fica instituída a estrutura organizacional de GSIC da SOF, composta pela CGI e pela área de SIC vinculada à CGTEC/SEAGE, as quais serão solidariamente responsáveis pelas seguintes atividades:
I - executar os processos de SIC;
II - desenvolver, implementar e monitorar estratégias de segurança que atendam aos objetivos estratégicos da SOF;
III - avaliar, selecionar, administrar e monitorar controles apropriados de proteção dos ativos de informação;

IV - desenvolver ações de conscientização dos usuários a respeito da implementação desses controles;
V - fornecer subsídios visando à verificação de conformidade de SIC; e
VI - promover a melhoria contínua nos processos e controles de GSIC.
Parágrafo único. A estrutura de GSIC deverá definir um Plano de SIC para a SOF.
Art. 13. A estrutura de GSIC da SOF compartilhará o sistema de registro de incidentes com a ETIR do MP.
Art. 14. Os membros da estrutura de GSIC da SOF serão regularmente capacitados nas disciplinas relacionadas à SIC.
Art. 15. A GSIC auxiliará a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias da SOF e as implicações que os níveis de segurança estipulados poderão trazer ao cumprimento dessas exigências.
Art. 16. A estrutura de GSIC da SOF planejará medidas de proteção e balanceará os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança.
Art. 17. A SOF, além das diretrizes estabelecidas nesta PoSIC, orientar-se-á pelas melhores práticas e procedimentos de SIC recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões no tema.
Art. 18. É vedado comprometer a autenticidade, a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela SOF.
Art. 19. Todos os sistemas de informação da SOF, automatizados ou não, terão um gestor formalmente designado pela CGI ou pelo titular da SOF.
Parágrafo único. A não designação pressupõe que o gestor é o titular da CGTEC/SEAGE.
Art. 20. O custodiante do ativo de informação será formalmente designado pelo gestor do ativo de informação.
Parágrafo único. A não designação pressupõe que o custodiante é o próprio gestor.
Art. 21. Os contratos firmados pela SOF conterão cláusulas que determinem a observância da PoSIC e seus respectivos documentos.

Capítulo V
DIRETRIZES ESPECÍFICAS
Seção I
Do Tratamento da Informação

Art. 22. Os ativos de informação devem:
I - ser inventariados e protegidos;
II - ter identificados os seus gestores e custodiantes;
III - ter mapeadas as suas ameaças, vulnerabilidades e interdependências;
IV - ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos; e
V - ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.
Art. 23. Os gestores da informação devem estabelecer regras e mecanismos que visem à manutenção de uma base de conhecimento sobre a realização de atividades na SOF, observadas as normas de SIC.
Art. 24. Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os usuários da SOF, de acordo com suas competências funcionais.

Parágrafo único. Os usuários da SOF devem ser sensibilizados e conscientizados para respeitar e apoiar esta PoSIC durante os seus trabalhos normais.

Art. 25. A SOF deverá criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 26. As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual da SOF e não cabe a seus criadores qualquer forma de direito autoral.

Art. 27. É vedada a utilização de informações produzidas por terceiros, para uso exclusivo da SOF, em quaisquer outros projetos ou atividades de uso diverso do estabelecido pela Secretaria, salvo se houver autorização específica do titular da SOF, nos processos e documentos de sua competência, ou do titular do MP, nos demais casos.

Seção II

Do Tratamento de Incidentes de Rede

Art. 28. Todos os eventos com potencial impacto à SIC deverão ser comunicados à estrutura de GSIC da SOF, por meio da área responsável da CGTEC/SEAGE.

Seção III

Da Gestão de Risco

Art. 29. A estrutura de GSIC estabelecerá processos de GRSIC que possibilitem identificar ameaças e reduzir vulnerabilidades e impactos dos ativos de informação.

Art. 30. A GRSIC deverá ser aplicada na implementação e operação da GSIC, tanto em planejamento, execução e análise crítica quanto em melhoria da SIC na SOF.

Seção IV

Da Gestão de Continuidade

Art. 31. Os sistemas de informação, as aplicações, os recursos tecnológicos e as instalações de infraestrutura da SOF deverão ser protegidos contra indisponibilidade, alterações, acessos indevidos, falhas e interrupções não programadas.

Art. 32. A estrutura de GSIC estabelecerá:

I - mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências; e

II - parâmetros adequados, relacionados à SIC, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiam.

Seção V

Da Auditoria e Conformidade

Art. 33. Deverão ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 34. Deverá ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de SIC da SOF com esta PoSIC e suas normas e procedimentos complementares, bem como com a legislação específica de SIC.

Parágrafo único. Nenhuma unidade administrativa da Secretaria poderá permanecer sem verificação de conformidade de suas práticas de SIC por um período superior a 2 (dois) anos.

Art. 35. A verificação de conformidade deverá ser realizada:

I - também, nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com a SOF; e

II - de forma planejada, mediante calendário de ações proposto pela estrutura de GSIC da SOF.

Art. 36. A execução da verificação de conformidade será realizada pela estrutura de GSIC e poderá ser subcontratada no todo ou em parte.

Art. 37. É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

Seção VI
Dos Controles de Acesso

Art. 38. A identificação do usuário, qualquer que seja o meio e a forma, é pessoal e intransferível e deve permitir, de maneira clara e inequívoca, o seu reconhecimento.

Art. 39. O usuário é responsável por todos os atos praticados com suas identificações, tais como nome de usuário/senha, crachá, carimbo, correio eletrônico e assinatura digital.

Art. 40. A autorização, o acesso e o uso das informações e dos recursos computacionais:

I - serão controlados e limitados ao necessário, considerando as atribuições de cada usuário;

II - estarão condicionados ao aceite a termo de sigilo e responsabilidade; e

III - dependerão de prévia autorização do gestor da área responsável pela informação.

Art. 41. A definição dos privilégios de acesso às informações será estabelecida pelo gestor do ativo.

Art. 42. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais deverão ser adequados imediatamente ou cancelados em caso de desligamento da SOF.

Art. 43. Os equipamentos de informática, notebooks, netbooks e tablets deverão ter a sua entrada e saída nas dependências da SOF autorizadas e registradas por autoridade competente.

Art. 44. O acesso à rede sem fio da SOF será regulamentado por meio de norma operacional específica.

Seção VII
Do Uso de Correio Eletrônico Corporativo

Art. 45. O uso de Correio Eletrônico Corporativo observará o disposto na Norma Operacional SPOA/MP/Nº 002, de 8 de maio de 2007.

Seção VIII
Do Acesso à Internet

Art. 46. Deverão ser adotados controles de SIC no acesso à internet, e seu uso está sujeito a monitoramento.

Parágrafo único. A Política de Uso Aceitável da internet será regulamentada por norma operacional específica, a ser editada em até 6 (seis) meses a partir da publicação desta Portaria.

Seção IX
Da Criptografia

Art. 47. O usuário é responsável pelo recurso criptográfico que receber e assinará Termo de Responsabilidade pelo seu uso.

Seção X
Da Aquisição, do Desenvolvimento e da Manutenção de Sistemas

Art. 48. A estrutura de GSIC estabelecerá critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção.

Art. 49. O processo de aquisição de sistemas e aplicações corporativas atenderá os requisitos de segurança previstos em norma específica.

Seção XI
Dos Contratos, Convênios, Acordos e Instrumentos do mesmo Gênero

Art. 50. Os acordos de nível de serviço serão compatíveis com padrões de mercado e requisitos de segurança.

Art. 51. Nos casos de obtenção de informações de terceiros, o gestor da área, na qual a informação será utilizada, providenciará junto ao cedente, se necessário, a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Art. 52. Os acordos com terceiros poderão incluir, quando necessário e justificado, permissão para acesso de outras partes, desde que expressamente autorizado pela SOF.

Art. 53. Todos os contratos, convênios, acordos e outros instrumentos do mesmo gênero conterão cláusulas que estabeleçam a obrigatoriedade de observância desta PoSIC.
Parágrafo único. O contrato, convênio, acordo ou instrumento do mesmo gênero deverá prever a obrigação da outra parte de divulgar esta PoSIC e suas normas complementares aos seus empregados e prepostos envolvidos em atividades na SOF.

Seção XII
Do Plano de Investimentos em SIC

Art. 54. Os investimentos em SIC serão realizados de forma planejada e consolidados em um plano de investimentos.
Art. 55. O plano de investimentos em SIC será:
I - elaborado com base na priorização dos riscos a serem tratados, com base em método que considere, no mínimo, a probabilidade e o impacto do risco; e
II - aprovado pela CGI/SOF, mediante recomendação proposta pela estrutura de GSIC.

Capítulo VI
PENALIDADES

Art. 56. Ações que violem a PoSIC ou quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SIC serão devidamente apuradas e aplicadas aos responsáveis as sanções penais, administrativas e civis em vigor.

Capítulo VII
COMPETÊNCIAS E RESPONSABILIDADES

Art. 57. Compete ao titular da SOF, ou a seu substituto, aprovar as atualizações da PoSIC.
Art. 58. Compete ao Gestor de SIC:
I - promover cultura de segurança da informação e Comunicação;
II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
III - propor recursos necessários às ações de SIC;
IV - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC;
V - propor normas relativas à SIC;
VI - manter lista atualizada dos gestores dos ativos de informação com seus respectivos ativos; e
VII - prover à CGI, quando necessário, as informações pertinentes à Gestão de SIC no âmbito da SOF.
Art. 59. Compete à CGI:
I - normatizar e supervisionar a SIC no âmbito da SOF;
II - constituir grupos de trabalho multidisciplinares para tratar de temas e propor soluções específicas sobre SIC;
III - propor alterações na PoSIC;
IV - solicitar apurações quando houver suspeita de ocorrências de quebras de SIC;
V - avaliar, revisar e analisar criticamente a PoSIC e suas normas complementares;
VI - dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PoSIC da SOF; e
VII - aprovar o plano de investimentos em SIC da SOF.
Art. 60. Compete à área de segurança da CGTEC/SEAGE:
I - manter contato direto com o Comitê de Segurança de Informação e Comunicação do MP (CSIC–MP) para o trato de assuntos relativos à SIC;
II - prover ao Gestor de SIC da SOF, qua ndo necessário, todas as informações pertinentes à GSIC;
III - propor normas relativas à SIC;
IV - facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;
V - atuar na recuperação de sistemas, quando da ocorrência de quebra de segurança;
VI - agir proativamente com o intuito 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;
VII - realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;
VIII - analisar ataques e intrusões na rede da SOF;
IX - executar ações necessárias para tratar quebras de segurança;
X - obter informações quantitativas acerca dos incidentes ocorridos e descrever sua natureza, causas, data de ocorrência, frequência e custos resultantes;
XI - cooperar com a ETIR do MP e, eventualmente, com outras equipes de Tratamento e Resposta a Incidentes; e
XII - participar em fóruns, redes e seminários nacionais e internacionais relativos à SIC.
Art. 61. Compete ao Gestor do Ativo de Informação:
I - garantir a segurança dos ativos de informação sob sua responsabilidade;
II - definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta PoSIC e suas normas relacionadas;
III - conceder e revogar acessos aos ativos de informação;
IV - comunicar à área de segurança da CGTEC/SEAGE a ocorrência de incidentes de SIC, bem como participar de sua investigação, quando necessário; e
V - designar custodiante dos ativos de informação sob sua responsabilidade, quando aplicável.
Art. 62. Compete ao Custodiante do Ativo de Informação proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta PoSIC.
Art. 63. Compete aos titulares das unidades organizacionais da SOF:
I - cumprir e fazer cumprir esta PoSIC e suas normas relacionadas;
II - assegurar que suas equipes possuam acesso à PoSIC, bem como às normas e aos procedimentos relacionados;
III - tomar medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;
IV - informar à área de Recursos Humanos da SOF a movimentação de pessoal de sua unidade;
V - autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade organizacional; e
VI - comunicar à área de segurança da CGTEC/SEAGE os casos de quebra de segurança.
Art. 64. Compete a terceiros e fornecedores, conforme previsto em contrato:
I - cumprir e fazer cumprir, no que lhes couber, o disposto nesta PoSIC e suas normas relacionadas;
II - fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e
III - fornecer a documentação dos sistemas, produtos, serviços relacionados às suas atividades.
Art. 65. Compete aos usuários:
I - difundir e exigir o cumprimento da PoSIC, das normas de segurança e da legislação vigente acerca do tema;
II - conhecer e cumprir os princípios, diretrizes e responsabilidades desta PoSIC, bem como os demais normativos e as resoluções relacionados à SIC;
III - obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação; e
IV - comunicar os incidentes que afetam a segurança dos ativos de informação e comunicação à sua chefia imediata ou à área de segurança da CGTEC/SEAGE.

Art. 66. Compete à área de Recursos Humanos da SOF informar prontamente à CGTEC/SEAGE os desligamentos, os afastamentos e as modificações no quadro funcional.

Capítulo VIII
ATUALIZAÇÃO

Art. 67. Esta PoSIC, bem como os documentos gerados a partir dela, deverão ser atualizados anualmente, ou por deliberação da CGI.

Capítulo IX
REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 68. Esta PoSIC foi elaborada com base os dispositivos legais e nas normas técnicas relacionados:

I - no Quadro I – Quadro de dispositivos legais de caráter federal aplicáveis à SIC;

II - no Quadro II – Quadro de legislação específica de caráter federal relacionada à SIC; e

III - no Quadro III – Quadro de normas técnicas relacionadas à SIC.

Quadro I – Quadro de dispositivos legais de caráter federal aplicáveis à SIC.

Dispositivo	**Aspecto da SI**
Constituição Federal, art. 5º, inciso X.	Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
Constituição Federal, art. 5º, inciso XII.	Sigilo dos dados telemáticos e das comunicações privadas.
Constituição Federal, art. 5º, inciso XIV.	Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
Constituição Federal, art. 5º, inciso XXXIII e art. 37, § 3º, inciso II.	Disponibilidade das informações constantes nos órgãos públicos.
Constituição Federal, art. 5º, inciso XXXIV.	Disponibilidade das informações constantes nos órgãos públicos.
Constituição Federal, art. 23, incisos III e IV.	Proteção da integridade, da autenticidade e da disponibilidade das informações pelo Estado.
Constituição Federal, art. 216, § 2º.	Proteção da integridade, da autenticidade, da disponibilidade e do sigilo das informações constantes nos órgãos e entidades integrantes da Administração Pública.
Constituição Federal, art. 37, caput.	Quanto melhor a gestão das informações, mais eficiente será o órgão ou entidade, daí a necessidade de implantação de uma Política de Segurança da Informação.
Constituição Federal, art. 37, § 6º, e Código Civil, art. 43.	Responsabilidade objetiva do Estado por dano decorrente da má gestão das informações pelos órgãos e entidades da Administração Pública e pessoas de direito privado prestadoras de serviços públicos.
Constituição Federal, art. 37, § 7º.	Necessidade de regulamentação do acesso a informações privilegiadas.
Consolidação das Leis do Trabalho – CLT, art. 482, alínea “g”.	Proteção das informações sigilosas acessadas no exercício de emprego público (empresas públicas e sociedades de economia mista).
Código de Conduta da Alta Administração, art. 5º, § 4º.	Sigilo das informações fiscais e tributárias das autoridades públicas (sigilo perante terceiros e não em face da Administração

	Pública).
Código de Conduta da Alta Administração, art. 14, inciso II.	Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.
Decreto nº 1.171, de 22 de junho de 1994 (Código de Ética do Servidor Público), alínea "h" do inciso XV da Seção II.	Proteção da integridade das informações públicas.
Decreto nº 1.171, de 22 de junho de 1994 (Código de Ética do Servidor Público), alínea "l" do inciso XV da Seção II.	Proteção da disponibilidade das informações públicas.
Decreto nº 1.171, de 22 de junho de 1994 (Código de Ética do Servidor Público), inciso X da Seção I.	Proteção da disponibilidade das informações públicas.
Decreto nº 1.171, de 22 de junho de 1994 (Código de Ética do Servidor Público), inciso VII da Seção I.	Proteção da disponibilidade das informações públicas e garantia da publicidade das informações de interesse da coletividade.
Decreto nº 1.171, de 22 de junho de 1994 (Código de Ética do Servidor Público), inciso IX da Seção I.	Proteção da integridade do patrimônio público, a exemplo de equipamentos, materiais, áreas e instalações.
Decreto nº 1.171, de 22 de junho de 1994 (Código de Ética do Servidor Público), alínea "e" do inciso XIV da Seção II.	Disponibilidade das comunicações.
Código de Propriedade Industrial, art. 75.	Sigilo das patentes de interesse da defesa nacional.
Código de Defesa do Consumidor, arts. 43 e 44.	Garantia da integridade e disponibilidade das informações dos consumidores arquivadas em bancos de dados.
Código Penal, art. 151.	Proteção do sigilo, integridade e disponibilidade das informações de caráter pessoal veiculadas através dos meios de comunicação.
Código Penal, art. 152.	Proteção do sigilo e da disponibilidade das informações dos estabelecimentos comerciais.
Código Penal, art. 153.	Proteção do sigilo das informações classificadas constantes nos sistemas ou bancos de dados da Administração Pública.
Código Penal, art. 154.	Proteção do sigilo das informações conhecidas em razão de função, ministério, ofício ou profissão.
Código Penal, art. 184, § 3º.	Proteção da autenticidade.
Código Penal, art. 297.	Proteção da integridade e autenticidade dos documentos públicos.
Código Penal, art. 298.	Proteção da integridade e autenticidade dos documentos particulares.
Código Penal, art. 305.	Proteção da disponibilidade e integridade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 307.	Proteção da autenticidade.

Código Penal, art. 313-A.	Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 313-B.	Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 314.	Proteção da disponibilidade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 325.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.
Código Processo Penal, art. 20.	Proteção de informações sigilosas.
Código Processo Penal, art. 207.	Proteção do sigilo profissional.
Código Processo Penal, art. 745.	Proteção de informações sigilosas relacionadas ao condenado.
Código Tributário Nacional, art. 198.	Proteção do sigilo fiscal.
Código de Processo Civil, art. 347, inciso II, c/c art.363, inciso IV.	Proteção da privacidade de seus clientes.
Código de Processo Civil, art. 406, inciso II, c/c art. 414, § 2º.	Proteção da privacidade de seus clientes.
Instrução Normativa SLTI/MP Nº 4, de 12 de novembro de 2010.	Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal.
Lei nº 6.538, de 22 de julho de 1978, art. 41.	Proteção da privacidade de correspondência.
Lei nº 7.170, de 14 de dezembro de 1983, art. 13.	Proteção das informações sigilosas relacionadas à segurança nacional.
Lei nº 7.232, de 29 de outubro de 1984, art. 2º, inciso VIII.	Sigilo dos dados relacionados à intimidade, vida privada e honra, especialmente dos dados armazenados através de recursos informáticos.
Lei nº 7.492, de 16 de julho de 1986, art. 18.	Proteção das informações sigilosas no âmbito das instituições financeiras ou integrantes do sistema de distribuição de títulos mobiliários.
Lei nº 8.027, de 12 de abril de 1990, art. 5º inciso I.	Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.
Lei nº 8.027, de 12 de abril de 1990, art. 5º, parágrafo único, inciso V.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.
Lei nº 8.112, de 11 de dezembro de 1990, art. 116, inciso VIII.	Sigilo das informações produzidas ou conhecidas no exercício de cargo ou função pública.
Lei nº 8.112, de 11 de dezembro de 1990, art. 132, inciso IX.	Proteção das informações sigilosas acessadas no exercício de cargo ou função pública.
Lei nº 8.137, de 27 de dezembro de 1990, art. 3º, inciso I.	Proteção da disponibilidade de informações para manutenção da ordem tributária.

Lei nº 8.429, de 02 de junho de 1992, art. 11, incisos III, IV e VII.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público, bem como garantia de publicidade das informações de interesse coletivo ou geral que devem ser divulgadas por ato oficial.
Lei nº 8.429, de 02 de junho de 1992, art. 13.	Disponibilidade de informações pessoais do agente público para o Poder Público e veracidade dos dados.
Lei nº 8.443, de 16 de julho de 1992, art. 86, inciso IV.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.
Lei Complementar nº 75, de 20 de maio de 1993, art. 8º incisos II e VIII, §§ 1º e 2º.	Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.
Lei nº 8.625, de 12 de fevereiro de 1993, art. 26, inciso I, alínea "b" e inciso II.	Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.
Lei nº 8.906, de 04 de julho de 1994, art. 7º, inciso XIX.	Proteção da privacidade do cliente do advogado.
Lei nº 9.100, de 29 de julho de 1995, art. 67, incisos VII e VIII.	Proteção da integridade e autenticidade dos sistemas informatizados e das informações neles armazenadas.
Lei nº 9.279, de 14 de maio de 1996, art. 195, inciso XI.	Proteção da privacidade das pessoas jurídicas, relacionado ao sigilo de suas informações.
Lei nº 9.296, de 24 de julho de 1996, art. 10.	Sigilo dos dados e das comunicações privadas.
Lei nº 9.472, de 16 de julho de 1997, art. 3º, inciso V.	Sigilo das comunicações.
Lei nº 9.472, de 16 de julho de 1997, art. 3º, inciso VI.	Proteção de informações pessoais de caráter sigiloso.
Lei nº 9.472, de 16 de julho de 1997, art. 3º, inciso IX.	Proteção de informações pessoais de caráter sigiloso.
Lei nº 9.504, de 30 de setembro de 1997, art. 72.	Proteção da integridade das informações de caráter eleitoral e dos equipamentos.
Lei nº 9.605, de 12 de fevereiro de 1998, art. 62.	Disponibilidade e integridade de dados e informações.
Lei nº 10.683, de 28 de maio de 2003, art. 6º.	Todos os aspectos da segurança da informação.
Lei nº 10.703, de 18 de julho de 2003, arts. 1º, 2º e 3º.	Disponibilidade de dados cadastrais para fins de investigação criminal e sigilo nas demais hipóteses.
Decreto nº 4.801, de 06 de agosto de 2003, art. 1º, inciso X.	Todos os aspectos da segurança da informação.
Decreto nº 5.483, de 30 de julho de 2005, arts. 3º e 11.	Disponibilidade de informações pessoais do agente público para o Poder Público e dever de sigilo por parte da Controladoria-Geral da União.
Decreto nº 5.687, de 30 de janeiro de 2006,	Disponibilidade das informações públicas ou

arts. 10 e 13 do Anexo.	administrativas e sigilo das informações pessoais constantes nos registros públicos.
Decreto nº 6.029, de 1º de janeiro de 2007, art. 1º, inciso II.	Disponibilidade das informações constantes nos registros públicos.
Decreto nº 6.029, de 1º de janeiro de 2007, art. 10.	Sigilo da identidade do denunciante e sigilo do processo para proteção da honra e da imagem do investigado antes da prolação da decisão pela Comissão de Ética.
Decreto nº 6.029, de 1º de janeiro de 2007, art. 13.	Sigilo do processo administrativo por infração ética antes da prolação da decisão e publicidade após o término e aplicação das penalidades.
Decreto nº 6.029, de 1º de janeiro de 2007, art. 22.	Disponibilidade, integridade e autenticidade das informações constantes no banco de dados mantido pela Comissão de Ética Pública.

Quadro II – Quadro de legislação específica de caráter federal relacionada à SIC

Regulamento	**Assunto**
Lei nº 7.232, de 29 de outubro de 1984.	Dispõe sobre a Política Nacional de Informática, e dá outras providências.
Lei nº 8.248, de 23 de outubro de 1991.	Lei nº 8.248, de 23 de outubro de 1991. Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.
Lei nº 9.296, de 24 de julho de 1996.	Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal que dispõe sobre a violação do sigilo de dados e das comunicações telefônicas.
Lei nº 9.472, de 16 de julho de 1997.	Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais.
Lei nº 9.507, de 12 de novembro de 1997.	Regula o direito de acesso a informações e disciplina o rito processual do habeas data.
Lei nº 9.609, de 19 de fevereiro de 1998.	Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.
Lei nº 9.883, de 7 de dezembro de 1999.	Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências.
Lei nº 8.159, de 8 de janeiro de 1991.	Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências.
Lei Complementar nº 105, de 10 de janeiro de 2001.	Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.
Medida Provisória nº 2.200-2, de 24 de agosto de 2001.	Institui a Infra-Estrutura de Chaves Públicas Brasileira –ICP–Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.
Lei nº 10.973, de 2 de dezembro de	Dispõe sobre incentivos à inovação e à pesquisa

2004.	científica e tecnológica no ambiente produtivo e dá outras providências.
Lei nº 11.111, de 5 de maio de 2005.	Regula o direito à informação e ao acesso aos registros públicos.
Lei nº 11.419, de 19 de dezembro de 2006.	Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências.
Decreto nº 2.295, de 4 de agosto de 1997.	Regulamenta o disposto no art. 24, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Neste caso o processo deverá ser sigiloso, excetuando-se a publicidade das compras governamentais.
Decreto nº 2.556, de 20 de abril de 1998.	Regulamenta o registro previsto no art. 3º da Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.
Decreto nº 3.294, de 15 de dezembro de 1999.	Institui Programa Sociedade da Informação, com objetivo de viabilizar a nova geração da Internet e suas aplicações em benefício da sociedade brasileira.
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.
Decreto de 18 de outubro de 2000.	Cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, e dá outras providências.
Decreto nº 3.714, 3 de janeiro de 2001.	Dispõe sobre a remessa por meio eletrônico de documentos a que se refere o art. 57-A do Decreto nº 2.954, de 29 de janeiro de 1999, e dá outras providências.
Decreto nº 3.996, de 31 de outubro de 2001.	Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.
Decreto nº 4.073, de 3 de janeiro de 2002.	Regulamenta a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.
Decreto nº 4.376, de 13 de setembro de 2002.	Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, e dá outras providências.
Decreto nº 4.522, de 17 de dezembro de 2002.	Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais – SIDOF, e dá outras providências.
Decreto nº 4.553, de 27 de dezembro de 2002.	Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.
Decreto nº 4.689, de 7 de maio de 2003.	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação – ITI, e dá

	outras providências.
Decreto nº 4.829, de 3 de setembro de 2003.	Dispõe sobre a criação do Comitê Gestor da Internet no Brasil – CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.
Decreto de 29 de outubro de 2003.	Institui Comitês Técnicos do Comitê Executivo do Governo Eletrônico e dá outras providências.
Decreto nº 5.301, de 9 de dezembro de 2004.	Institui a Comissão de Averiguação e Análise de Informações Sigilosas, dispõe sobre sua s atribuições e regula seu funcionamento.
Decreto nº 5.450, de 31 de maio de 2005.	Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.
Decreto nº 5.563, de 11 de outubro de 2005.	Regulamenta a Lei nº 10.973, de 02 de dezembro de 2004, que dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo, e dá outras providências.
Decreto nº 5.584, de 18 de novembro de 2005.	Dispõe sobre o recolhimento ao Arquivo Nacional dos documentos arquivísticos públicos produzidos e recebidos pelos extintos Conselho de Segurança Nacional – CSN, Comissão Geral de Investigações – CGI e Serviço Nacional de Informações – SNI, que estejam sob a custódia da Agência Brasileira de Inteligência – ABIN.
Decreto nº 5.772, de 8 de maio de 2006, art. 8º.	Institui na estrutura regimental do Gabinete de Segurança Institucional da Presidência da República o Departamento de Segurança da Informação e Comunicações com diversas atribuições na área de segurança da informação e comunicações.
Decreto nº 6.605, de 14 de outubro de 2008.	Dispõe sobre o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira – CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva – COTEC.
Instrução Normativa nº 1 do GSI, de 13 de junho de 2008.	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
Resolução nº 58 do INPI, de 14 de julho de 1998.	Estabelece normas e procedimentos relativos ao registro de programas de computador.
Resolução nº 59 do INPI, de 14 de julho de 1998.	Estabelece os valores das retribuições pelos serviços de registro de programas de computador.
Resolução nº 338 do STF, de 11 de abril de 2007.	Dispõe sobre classificação, acesso, manuseio, reprodução, transporte e guarda de documentos e processos de natureza sigilosa no âmbito do STF.
Resolução nº 140 do TST, de 13 de setembro de 2007.	Regulamenta, no âmbito da Justiça do Trabalho, a Lei nº 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial.
Resolução nº 22.718 do TSE, de 28 de fevereiro de 2008, arts. 18 e 19.	Regula a propaganda eleitoral na internet em campanha nas eleições de 2008.

Quadro III – Quadro de normas técnicas relacionadas à SIC

Regulamento	**Assunto**
ISO/IEC TR 13335-3:1998.	Esta norma fornece técnicas para a gestão de segurança na área de tecnologia da informação. Baseada na norma ISO/IEC 13335-1:1996 e TR ISO/IEC 13335-2:1997. As orientações são projetadas para auxiliar o incremento da segurança na TI.
ISO/IEC GUIDE 51:1999.	Esta norma fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos. É aplicável a qualquer aspecto de segurança relacionado a pessoas, propriedades, ao ambiente, ou a uma combinação de um ou mais destes (por exemplo, somente pessoas; pessoas e propriedades; pessoas, propriedades e o ambiente).
ISO/IEC GUIDE 73:2002.	Esta norma fornece definições genéricas de termos de gestão de riscos para a elaboração de normas. Seu propósito é ser um documento genérico de alto nível voltado para a preparação ou revisão de normas que incluam aspectos de gestão de riscos.
ABNT NBR ISO IEC 27002:2007.	Esta norma é equivalente à ISO/IEC 17799:2005. Consiste em um guia prático que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos de controle e os controles definidos nesta norma têm como finalidade atender aos requisitos identificados na análise/avaliação de riscos.
ABNT NBR ISO/IEC 27001:2005.	Esta norma é usada para fins de certificação e substitui a norma Britânica BS 7799-2:2002. Aplicável a qualquer organização, independente do seu ramo de atuação, define requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação.

ANEXO B: PSIC DO MINISTÉRIO DO TURISMO

PORTARIA Nº 108, DE 22 DE MAIO DE 2013.

Institui a Política de Segurança da Informação e Comunicação POSIC, no âmbito do Ministério do Turismo.

O MINISTRO DE ESTADO DO TURISMO, no uso da atribuição que lhe confere o art. 87, parágrafo único, inciso II, da Constituição,

R E S O L V E:

Art. 1º Fica instituída, no âmbito do Ministério do Turismo, a Política de Segurança da Informação e Comunicação - POSIC, com vistas a estabelecer as diretrizes, critérios e suporte administrativo e definir tratamento a ser dado às informações produzidas, processadas ou transmitidas e armazenadas no ambiente convencional ou no ambiente de tecnologia.

CAPÍTULO I

OBJETIVO

Art. 2º A Política de Segurança da Informação e Comunicações - POSIC tem por objetivo implantar diretrizes, responsabilidades, competências e princípios de Segurança da Informação e Comunicações - SIC no âmbito do Ministério do Turismo, limitando sua exposição a níveis de risco aceitáveis, com vistas a garantir a Disponibilidade, a Integridade, a Confidencialidade e a Autenticidade - DICA das informações que suportam os objetivos estratégicos deste Ministério, bem como a conformidade, padronização e normatização das atividades de Gestão de Segurança da Informação e Comunicações - GSIC.

Art. 3º As diretrizes de SIC devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e estrutura do Ministério, enquanto a GSIC deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de SIC.

CAPÍTULO II

ABRANGÊNCIA

Art. 4º Esta POSIC e suas Normas Complementares aplicam-se a todas as unidades e à entidade vinculada ao Ministério, bem como aos servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, execute atividades vinculadas a este Ministério.

Art. 5º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo Ministério devem atender a esta POSIC.

CAPÍTULO III

CONCEITOS E DEFINIÇÕES

Art. 6º No âmbito da POSIC considera-se:

I - Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade [NC07/IN01/DSIC/GSIPR, 2010, p. 2];

II - Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização [NC04/IN01/DSIC/GSIPR, 2013, p. 2];

III - Ativo: tudo aquilo que possui valor para o órgão ou entidade da Administração Pública Federal;

IV - Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso [NC04/IN01/DSIC/GSIPR, 2013, p. 3];

V - 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 [IN01/DSIC/GSIPR, 2008, p. 2];

VI - Capacitação em SIC: saber o que é Segurança da Informação e Comunicações aplicando em sua rotina pessoal e profissional, servindo como multiplicador sobre o tema, aplicando os conceitos e procedimentos na Organização como gestor de SIC. [DSIC/GSIPR];

VII - Capacitação: visa à aquisição de conhecimentos, capacidades, atitudes e formas de comportamento exigido para o exercício das funções;

VIII - Classificação da Informação: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;

XIX - Comitê de Segurança da Informação e Comunicações: instância estratégica responsável por tratar e deliberar a respeito de temas na área de Segurança da Informação e Comunicações [NC03/IN01/DSIC/GSIPR, 2009, p. 2];

X - Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado [IN01/DSIC/GSIPR, 2008, p. 2];

XI - Conscientização em SIC: saber o que é Segurança da Informação e Comunicações aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema [DSIC/GSIPR];

XII - Continuidade de Negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido [NC06/IN01/DSIC/GSIPR, 2009, p. 3];

XIII - Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso [NC07/DSIC/GSIPR, 2010, p. 3];

XIV - CTIR.GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de

Segurança de Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República [NC05/IN01/DSIC/GSIPR, 2009 p. 3];

XV - Custodiante: responsável por armazenar e preservar as informações que não lhe pertencem, refere-se a qualquer indivíduo ou estrutura do órgão ou entidade da APF que tenha a responsabilidade formal de proteger um ou mais ativos de informação, como é armazenado, transportado e processado, ou seja, é o responsável pelos contêineres dos ativos de informação. Consequentemente, o custodiante do ativo de informação é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de Segurança da Informação e Comunicações comunicadas pelos proprietários dos ativos de informação [NC10/DSIC/GSIPR, 2012, p. 2];

XVI - Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade [IN01/DSIC/GSIPR, 2008, p. 2];

XVII - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores [NC05/IN01/DSIC/GSIPR, 2009 p. 3];

XVIII - Estrutura de GSIC: Grupo responsável pela gestão e execução da Segurança da Informação e Comunicações – SIC;

XIX - Evento: ocorrência identificada de um sistema, serviço ou rede, que indica 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 [ISO/IEC TR 18044: 2004];

XX - 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 os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos [NC04/IN01/DSIC/GSIPR, 2013, p.3];

XXI - 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 física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações [IN01/DSIC/GSIPR, 2008, p. 2];

XXII - Gestor de Segurança da Informação e Comunicações: servidor responsável pelas ações de Segurança da Informação e Comunicações no âmbito do Ministério do Turismo [NC03/IN01/DSIC/GSIPR, 2009, p. 2];

XXIII - Incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores [NC05/IN01/DSIC/GSIPR, 2009, p. 3];

XXIV - Informação Estratégica: toda a informação corporativa relativa à administração, planejamento, estrutura, gestão, relações internas e externas, novos produtos e tecnologias, serviços e contratos;

XXV - Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental [IN01/DSIC/GSIPR, 2008, p. 2];

XXVI - Nível de Segurança Adequado: são métricas de seguranças estabelecidas para uma rede ou sistema, depois de identificado o potencial de ameaça;

XXVII - Política de Segurança da Informação e Comunicações (POSIC): documento aprovado pela autoridade responsável do órgão ou entidade da APF, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da Segurança da Informação e Comunicações [NC03/IN01/DSIC/GSIPR, 2009, p. 2];

XXVIII - Proprietário da Informação: pessoa ou setor que produz a informação, capaz de estimar em que nível de criticidade cada uma se enquadra;

XXIX - Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações [IN01/DSIC/GSIPR, 2008, p. 2];

XXX - Recursos Criptográficos: sistemas, programas, processos e equipamentos isolados ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

XXXI - 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 [NC04/IN01/DSIC/GSIPR, 2013, p.3];

XXXII - Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar à disponibilidade, a integridade, a confidencialidade e a autenticidade das informações [IN01/DSIC/GSIPR, 2008, p. 2];

XXXIII - Segurança de Operações e Comunicações: definição de parâmetros responsáveis pela manutenção do funcionamento de serviços, sistemas e da infraestrutura que os suporta;

XXXIV - Sensibilização em SIC: ações que visão identificar, recomendar, criar e implementar programas de conscientização, a fim de proporcionar melhorias e mudanças na atitude e na educação organizacional quanto à importância da segurança da informação em todos os níveis do órgão;

XXXV - Sistemas Estruturantes: conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente;

XXXVI - Terceiro: Quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao Ministério, envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;

XXXVII - Usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade [NC07/DSIC/GSIPR, 2010, p. 3]; e

XXXVIII - Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação [NC04/IN01/DSIC/GSIPR, 2013, p.4].

CAPÍTULO IV

PRINCÍPIOS

Art. 7º As ações relacionadas com a Segurança da Informação e Comunicações no Ministério são norteadas pelos seguintes princípios:

I - Responsabilidade: os agentes públicos devem conhecer e respeitar todas as normas de Segurança da Informação e Comunicações do Ministério;

II - Ética: os direitos dos agentes públicos devem ser preservados sem comprometimento da Segurança da Informação e Comunicações;

III - Clareza: as regras de Segurança dos ativos de Segurança da Informação e Comunicações devem ser precisas, concisas e de fácil entendimento;

IV - Privacidade: informação que fira o respeito, à intimidade, à integridade e a honra dos cidadãos não podem ser divulgadas;

V - Eficiência: realizar um trabalho correto, sem erros e de boa qualidade;

VI - Eficácia: realizar um trabalho que atinja totalmente os resultados esperados;

VII - Celeridade: as ações de segurança da informação e comunicações devem oferecer respostas rápidas a incidentes e falhas; e

VIII - Publicidade: dar transparência no trato das informações, observado os critérios legais.

CAPÍTULO V

DIRETRIZES GERAIS

Art. 8º A Política de Segurança da Informação e Comunicações do Ministério rege-se pelas seguintes diretrizes:

I - a Gestão de SIC deve suportar a tomada de decisões, bem como realizar a gestão de conhecimento e de recursos por meio da utilização eficiente e eficaz dos ativos, possibilitando alcançar os objetivos estratégicos do Ministério, assim como otimizar seus investimentos;

II - os custos associados à Gestão da SIC deverão ser compatíveis com os custos dos ativos que se deseja proteger; e

III - as normas e procedimentos de SIC do Ministério, devem considerar, subsidiariamente, normas e padrões aceitos no mercado como referência nos processos de gestão e governança de SIC.

Art. 9º Fica instituída a Estrutura de GSIC do Ministério, composta pelo Comitê de Segurança da Informação e Comunicações – CSIC, pelo Grupo de Trabalho de Segurança da

Informação e Comunicações – GT-SIC e pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, os quais serão responsáveis pelas seguintes atividades:

I - executar os processos de segurança da informação e comunicações;

II - desenvolver, implementar e monitorar estratégias de segurança que atendam aos objetivos estratégicos do Ministério;

III - Avaliar, selecionar, administrar e monitorar controles apropriados de proteção dos ativos de informação;

IV - Desenvolver ações de conscientização dos usuários a respeito da implementação desses controles;

V - Fornecer subsídios visando à verificação de conformidade de segurança da informação e comunicações; e

VI - Promover a melhoria contínua nos processos e controles de GSIC.

Parágrafo único. A Estrutura de GSIC deve definir um Plano Diretor de Segurança da Informação e Comunicações para o Ministério.

Art. 10. Os membros da Estrutura da GSIC devem receber capacitação especializada nas disciplinas relacionadas à SIC.

Art. 11. A GSIC do Ministério deve auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias do Ministério e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

Art. 12. A Estrutura de GSIC deve planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança.

Art. 13. O Ministério, além das diretrizes estabelecidas nesta POSIC, deve também se orientar pelas melhores práticas e procedimentos de SIC recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 14. Os contratos firmados pelo Ministério devem conter cláusulas que determinem a observância da POSIC e seus respectivos documentos.

CAPÍTULO VI

DIRETRIZES ESPECÍFICAS

Art. 15. Para cada uma das diretrizes constantes desta POSIC devem ser elaboradas normas e procedimentos específicos.

CAPÍTULO VII

DA GESTÃO DE ATIVOS

Art. 16. Os ativos da organização são elementos fundamentais para a consecução dos objetivos estratégicos, portanto ações de segurança específicas deverão garantir a proteção adequada dos mesmos, sendo que os níveis de proteção deverão variar de acordo com a criticidade do ativo para o Ministério.

Art. 17. Os ativos de informação devem ter controles de segurança implementados independentemente do meio em que se encontram e deverão ser protegidos contra divulgação não autorizada, modificações, remoção ou destruição, de forma a evitar incidentes de segurança que possam danificar a imagem da instituição e interromper suas operações.

Art. 18. As pessoas que de alguma forma tenham acesso aos ativos de informação da organização devem ser periodicamente conscientizadas, capacitadas e sensibilizadas em assuntos de segurança e de tratamento da informação18, de forma a garantir o entendimento e a prática efetiva da SIC.

Art. 19. Os processos e atividades que sustentam os serviços críticos disponibilizados pelo Ministério devem ser protegidos de forma a garantir a DICA das informações.

Art. 20. Os ativos de informação devem:

I - ser inventariados e protegidos;

II - ter identificados os seus proprietários e custodiantes;

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

IV - ter a sua entrada e saída nas dependências do Ministério autorizadas e registradas por autoridade competente;

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

VI - ser regulamentados por norma específica quanto a sua utilização; e

VII - ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 21. O Ministério deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 22. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 23. Os sistemas de informação e as aplicações do Ministério devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

Art. 24. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite a termo de sigilo e responsabilidade.

CAPÍTULO VIII

DA GESTÃO DE RISCOS

Art. 25. Com o objetivo de reduzir as vulnerabilidades, evitar as ameaças, minimizar a exposição aos riscos e atenuar os impactos associados aos ativos da organização, deverá ser estabelecido processo que possibilite a identificação, a quantificação, a priorização, o tratamento, a comunicação e a monitoração periódica dos riscos.

Art. 26. A Estrutura de GSIC é responsável por estabelecer os processos de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC, cujo processo é contínuo e deve ser aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações – GSIC, levando em consideração o planejamento, execução, análise crítica e melhoria da SIC no Ministério.

CAPÍTULO IX

DA GESTÃO DE OPERAÇÕES E COMUNICAÇÕES

Art. 27. Dada à importância estratégica que os recursos de processamento da informação têm para a consecução dos objetivos deste Ministério, ações de segurança deverão garantir a operação segura e correta desses recursos.

Art. 28. A Estrutura de GSIC deve estabelecer parâmetros adequados, relacionados à SIC, para a disponibilização dos serviços, sistemas e instraestrutura que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais do Ministério.

Art. 29. Com o objetivo de reduzir os riscos associados, o gerenciamento dos serviços terceirizados deverá manter os níveis apropriados de segurança da informação e da entrega dos serviços, devendo os acordos de nível de serviço ser compatíveis com os padrões de mercado e requisitos de segurança.

Art. 30. A troca de informações, tanto internamente, quanto externamente, deverá ser regulada de forma a manter o nível adequado da segurança.

Art. 31. As operações deverão ser adequadamente monitoradas pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais- ETIR, visando detectar o mais cedo possível atividades não autorizadas.

CAPÍTULO X

DO CONTROLE DE ACESSO

Art. 32. A Estrutura de GSIC deve estabelecer normas ou procedimentos que garantam o controle de acesso às informações e às instalações, com o objetivo de evitar a quebra de segurança.

Art. 33. Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 34. Os usuários do Ministério são responsáveis por todos os atos praticados com suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico e assinatura digital.

Art. 35. A identificação do usuário, qualquer que seja o meio e a forma, devem ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

Art. 36. 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.

Art. 37. Os sistemas de informação do Ministério devem ter um Gestor, designado pela autoridade competente, que deve definir os privilégios de acesso às informações.

Art. 38. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de exoneração ou despensa do Ministério.

Art. 39. Os sistemas estruturantes devem possuir normas específicas, no âmbito de sua atuação, que regrem o controle de acesso quanto:

I - ao acesso às suas bases de dados;

II - à extração, carga e transformação de dados; e

III - aos serviços acessíveis via linguagem de programação.

Art. 40. Os sistemas estruturantes devem possuir mecanismos para:

I - revogar as concessões e desativar as contas de acesso do servidor nos casos de exoneração, demissão, aposentadoria e falecimento do servidor;

II - bloquear as contas de acesso do servidor nos casos de licença, afastamento, cessão e disponibilidade do servidor; e

III - tratar os casos de remoção e redistribuição do servidor, segundo as definições constantes na norma de controle de acesso ao sistema.

Art. 41. O Ministério instituirá normas e procedimentos que garantam a segurança da informação em ambientes de computação móvel e de trabalho remoto, com o objetivo de evitar a vulnerabilidade do Sistema de Gestão de Segurança da Informação e Comunicações.

Art. 42. Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.

CAPÍTULO XI

DA SEGURANÇA FÍSICA E DO AMBIENTE

Art. 43. A Estrutura de GSIC deve estabelecer mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências.

Art. 44. As proteções devem estar alinhadas aos riscos identificados.

CAPÍTULO XII

DA SEGURANÇA EM RECURSOS HUMANOS

Art. 45. Os usuários devem ter ciência:

I - das ameaças e preocupações relativas à SIC; e

II - de suas responsabilidades e obrigações no âmbito desta POSIC.

Art. 46. Os usuários devem difundir e exigir o cumprimento da POSIC, das normas de segurança e da legislação vigente acerca do tema.

Art. 47. Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em Segurança da Informação, que alcancem todos os usuários do Ministério, de acordo com suas competências funcionais.

Art. 48. Controle de pessoal:

I - Servidores: é de responsabilidade do titular da unidade administrativa juntamente com a Coordenação-Geral de Pessoas da Diretoria de Gestão Interna - COGEP/DGI/SE; e

II - Colaboradores: é de responsabilidade do titular da unidade administrativa juntamente com a Coordenação-Geral de Recursos Logísticos da Diretoria de Gestão Interna - CGRL/DGI/SE.

Parágrafo único. O Gestor de SIC deve estabelecer controles de perfis, permissões e procedimentos necessários para a salvaguarda da SIC.

CAPÍTULO XIII

DA GESTÃO DE INCIDENTES

Art. 49. Os Incidentes de Segurança da Informação e Comunicações devem ser identificados, monitorados, comunicados e devidamente tratados, em tempo hábil, de forma a garantir a continuidade das atividades e a não intervenção no alcance dos objetivos estratégicos do Ministério.

Art. 50. A Estrutura de GSIC deve instituir metodologias ou normas que estabeleçam processos de gestão para tratamento e respostas a incidentes de segurança, de forma a observar ao disposto no arcabouço técnico normativo do CTIR.GOV.

Art. 51. O Ministério instituirá Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR.

CAPÍTULO XIV

DA GESTÃO DE CONTINUIDADE DO NEGÓCIO

Art. 52. O Ministério instituirá normas e procedimentos que estabeleçam a Gestão de Continuidade do Negócio para minimizar os impactos decorrentes de eventos que causem a indisponibilidade sobre seus serviços, além de recuperar perdas de ativos de informação a um nível estabelecido, por intermédio de ações de prevenção, resposta e recuperação.

Art. 53. A Estrutura de GSIC deve instituir metodologias ou normas que estabeleçam processos de Gestão de Continuidade de Negócio.

CAPÍTULO XV

DA CRIPTOGRAFIA

Art. 54. O uso de recursos criptográficos interfere na DICA, sendo, portanto, responsabilidade do Gestor de SIC a implementação dos procedimentos relativos ao seu uso, no âmbito das informações produzidas e custodiadas no Ministério, em conformidade com as orientações contidas em norma específica.

Art. 55. O usuário é responsável pelo recurso criptográfico que receber, devendo assinar Termo de Responsabilidade pelo seu uso.

CAPÍTULO XVI

DA AUDITORIA E CONFORMIDADE

Art. 56. O uso dos recursos computacionais e de informações disponibilizadas pelo Ministério será monitorado, respeitando os princípios legais.

Art. 57. Deverão ser mantidos procedimentos, tais como: trilha de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para todos os sistemas corporativos e rede interna do Ministério.

CAPÍTULO XVII

DO USO DE E-MAIL

Art. 58. As regras de acesso e utilização serão definidas por normas específicas, em conformidade com esta POSIC e demais orientações e diretrizes de Governo.

CAPÍTULO XVIII

DO ACESSO À INTERNET

Art. 59. O acesso à internet, no ambiente de trabalho do Ministério, será regido por norma específica, em conformidade com esta POSIC e demais orientações governamentais e legislação em vigor.

CAPÍTULO XIX

DA PROPRIEDADE INTELECTUAL

Art. 60. As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual do Ministério não cabendo a seus criadores qualquer forma de direito autoral.

Art. 61. É vedada a utilização de informações produzidas por terceiros para uso exclusivo do Ministério em quaisquer outros projetos ou atividades de uso diverso do estabelecido pelo Ministério, salvo autorização específica pelos titulares das unidades administrativas, nos processos e documentos de sua competência, ou pelo Ministro, nos demais casos.

CAPÍTULO XX

PENALIDADES

Art. 62. Ações que violem a POSIC ou que quebrem os controles de Segurança da Informação e Comunicações serão passíveis de sansões civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

Art. 63. Processo disciplinar específico deverá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta POSIC.

Art. 64. A resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo Comitê de Segurança da Informação e Comunicações - CSIC do Ministério.

CAPÍTULO XXI

COMPETÊNCIA E RESPONSABILIDADE

Art. 65. É de responsabilidade da alta administração deste Ministério prover a orientação e o apoio necessários às ações de SIC, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes.

Art. 66. É de responsabilidade dos demais gestores zelar pelo cumprimento das diretrizes desta Política no âmbito de suas áreas de atuação.

Art. 67. É de responsabilidade de todos que têm acesso aos ativos do Ministério manter níveis de segurança da informação adequados, segundo preceitos desta Política e de suas Normas Complementares.

Parágrafo único. Cabe aos usuários:

I - conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta POSIC, bem como os demais normativos e resoluções relacionados à SIC;

II - obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação; e

III - comunicar os incidentes que afetam a segurança dos ativos de informação e comunicações à ETIR.

Art. 68. Cabe a Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais – ETIR:

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

II - promover a recuperação de sistemas;

III - 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;

IV - realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;

V - analisar ataques e intrusões na rede do Ministério;

VI - executar as ações necessárias para tratar quebras de segurança;

VII - obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

VIII - cooperar com outras equipes de Tratamento e Resposta a Incidentes; e

IX - participar em fóruns, redes nacionais e internacionais relativos à SIC.

Art. 69. O Comitê de Segurança da Informação e Comunicações - CSIC é a instância estratégica responsável por tratar e deliberar a respeito de temas na área de Segurança da Informação e Comunicações no âmbito do Ministério.

Parágrafo único. Cabe ao CSIC:

I - deliberar sobre a implementação das ações de Segurança da Informação e Comunicações no âmbito do Ministério;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação e Comunicações;

III - elaborar e propor alterações na Política de Segurança da Informação e Comunicações;

IV - submeter, para aprovação do Ministro de Estado do Turismo, a Política de Segurança da Informação e Comunicações;

V - propor normas relativas à Segurança da Informação e Comunicações;

VI - designar o Gestor de Segurança da Informação e Comunicações; e

VII - solicitar apurações quando da suspeita de ocorrências de quebras de Segurança da Informação e Comunicações.

Art. 70. O Gestor de Segurança da Informação e Comunicações é o responsável pelas ações de Segurança da Informação e Comunicações no âmbito do Ministério.

Parágrafo único. Cabe ao Gestor de SIC:

I - promover cultura de Segurança da Informação e Comunicações;

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

III - propor recursos necessários às ações de Segurança da Informação e Comunicações;

IV - coordenar o CSIC e a equipe de tratamento e resposta a 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 direto com o Departamento de Segurança da Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da República - GSI/PR para o trato de assuntos relativos à Segurança da Informação e Comunicações;

VII - propor normas relativas à Segurança da Informação e Comunicações;

VIII - apoiar técnica e administrativamente as reuniões e demais atividades do Comitê, incluindo o acompanhamento da execução das resoluções do CSIC;

IX - receber e expedir correspondências e comunicados;

X - selecionar e organizar a legislação e a jurisprudência relativas à Segurança da Informação e Comunicações;

XI - preparar atos a serem baixados pelo Presidente;

XII - informar sobre a tramitação de processos;

XIII - providenciar:

a) elaboração e apresentação das propostas a serem discutidas e homologadas nas reuniões do Comitê; e

b) comunicados e demais documentos administrativos;

XIV - adotar providências para:

a) realização das reuniões, secretariando-as e elaborando as respectivas atas;

b) cumprimento das deliberações do Comitê; e

c) organizar, disponibilizar e manter atualizado o acervo documental correspondente; e

XV - exercer outras atribuições administrativas que lhe forem conferidas pelo Presidente.

Art. 71. Os níveis adequados de segurança dos ativos de informação deverão ser garantidos pelos proprietários e custodiantes diretamente responsáveis pelos mesmos.

CAPÍTULO XXII

ATUALIZAÇÃO

Art. 72. Esta POSIC, bem como todos os instrumentos normativos gerados a partir dela, deverão ser revisados e atualizados sempre que se fizer necessário, não excedendo o período máximo de três anos.

CAPÍTULO XXIII

DISPOSIÇÕES GERAIS

Art. 73. Para a implementação da POSIC no Ministério, são recomendadas as seguintes ações:

I - implantar a POSIC através da aprovação e publicação por parte da autoridade máxima do órgão, demonstrando a todos os servidores e usuários o seu comprometimento;

II - garantir a provisão dos recursos necessários para a implementação da POSIC;

III - promover no órgão, a cultura de Segurança da Informação e Comunicações, por meio de atividades de sensibilização, conscientização, capacitação e especialização; e

IV - esta POSIC, bem como as Normas e Procedimentos de SIC associados, deverão ter ampla divulgação, de forma a garantir que todos entendam suas responsabilidades e estejam de acordo com os preceitos desta Política.

Art. 74. Esta Portaria entra em vigor na data de sua publicação.

GASTÃO VIEIRA

Este texto não substitui o publicado no DOU de 23.5.2013

ANEXO

REFERÊNCIAS NORMATIVAS

Dispositivos legais, aplicáveis à Segurança da Informação e Comunicações:

I - Associação Brasileira de Normas Técnicas - ABNT NBR ISO/IEC 17799: 2005 (27002). Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

II - Constituição da República Federativa do Brasil de 1988;

III - Decreto nº 1.171, de 22 de junho de 1994, que dispõe sobre o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

IV - 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;

V - Decreto nº 7.845, de 14 de novembro de 2012, 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;

VI - Instrução Normativa GSI 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 demais normas complementares; e

VII - Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

ANEXO C: PSIC DO MINISTÉRIO DA SAÚDE

PORTARIA Nº 3.207, DE 20 DE OUTUBRO DE 2010

Institui a Política de Segurança da Informação e Comunicações do Ministério da Saúde.

O MINISTRO DE ESTADO DA SAÚDE, no uso da atribuição que lhe conferem os incisos I e II do parágrafo único do art. 87 da Constituição, e

Considerando a necessidade de estabelecer os direcionamentos e os valores adotados para a gestão de segurança da informação e comunicações no âmbito do Ministério da Saúde;

Considerando a importância que deve ser dada à garantia da integridade, à disponibilidade, à confidencialidade e à autenticidade dos dados e das informações nos mais diversos suportes utilizados por este Ministério;

Considerando as diretrizes do Governo Federal, representado pelo Gabinete de Segurança Institucional da Presidência da República, que recomenda a implantação, o no âmbito de cada órgão da Administração Pública Federal (APF), de processos e de metodologias de segurança da informação e comunicações;

Considerando o 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;

Considerando 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;

Considerando a Lei Nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei Nº 2.848, de 7 de setembro de 1940 (Código Penal), que dispõe sobre a tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

Considerando que segundo o art. 1.016 da Lei Nº 10.406, de 10 de janeiro de 2002 (Código Civil), os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções;

Considerando o Decreto Nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal;

Considerando a Política Nacional de Informação e Informática em Saúde - Proposta versão 2.0 que inclui as deliberações de 12ª Conferência Nacional de Saúde, de 2003;

Considerando o acórdão do Tribunal de Contas da União Nº 461/2004, de 28 de abril de 2004, que dispõe sobre a análise regular de arquivos logs com utilização, sempre que possível, de softwares utilitários específicos, para monitoramento do uso dos sistemas;

Considerando a Portaria Nº 66/SVS/MS, de 10 de dezembro de 2004, que dispõe sobre procedimentos e responsabilidades relativas à divulgação técnico-cientifica de dados e informações da Secretaria de Vigilância em Saúde;

Considerando a Norma NBR ISO/IEC 17799:2005 – Código de Práticas para a Gestão da Segurança da Informação;

Considerando a Instrução Normativa Nº 1, de 13 de junho de 2008, do Conselho de Defesa Nacional e da Secretaria-Executiva, que disciplina a gestão de segurança da informação e comunicações no âmbito da Administração Pública Federal;

Considerando a Portaria Nº 2.466/GM/MS, de 14 de outubro de 2009, que institui o Comitê de Informação e Informática em Saúde (CIINFO) no âmbito do Ministério da Saúde, resolve:

Art. 1º Instituir, no âmbito do Ministério da Saúde, a Política de Segurança da Informação e Comunicações do Ministério da Saúde (POSIC/MS), aprovada pelo CIINFO, e regida pelos objetivos e diretrizes estabelecidos nesta Portaria.

Parágrafo único. O Subcomitê de Segurança da Informação e Comunicações, sob orientação do CIINFO deverá disciplinar as seguintes matérias:

I - a criação e manutenção de contas e acesso aos recursos de Tecnologia da Informação e Comunicação (TIC);

II - o uso do correio eletrônico;

III - a segurança para usuários da rede;

IV - a classificação da informação do Ministério da Saúde;

V - a cessão de bases de dados nominais;

VI - o uso da Internet no Ministério da Saúde;

VII - o controle de acesso lógico e remoto;

VIII - a segurança da informação para técnicos;

IX - a segurança para estações de trabalho e equipamentos eletrônicos portáteis;

X - a segurança física de instalações;

XI - a instalação e configuração de aplicações;

XII - o tratamento de mídias e cópia de segurança;

XIII - a segurança para recursos de tecnologia da informação e comunicação;

XIV - a segurança contra código malicioso;

XV - a segurança para acordo de nível de serviço;

XVI - a conformidade legal;

XVII - a segurança em contratos de prestação de serviços;

XVIII - a segregação de função;

XIX - o registro de eventos e trilhas de auditoria;

XX - os procedimentos para custódia de equipamentos; e

XXI - o termo de responsabilidade.

Art. 2º Para efeitos desta Portaria, adotam-se as seguintes conceituações:

I - acesso: possibilidade de consulta ou reprodução de documentos e arquivos;

II - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função no Ministério da Saúde e equipara-se a quem trabalha para empresa prestadora de serviços contratada ou conveniada para a execução de atividade, de qualquer natureza, desenvolvida no âmbito do Ministério da Saúde;

III - ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas [Security Officer - 1 guia oficial para formação de gestores em segurança da informação];

IV - ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

V - ativo de informação: ativo que guarda informações do órgão;

VI - auditoria: atividade com a finalidade de reconstruir um evento relacionado à segurança para auxiliar no exame de suas causas e efeitos;

VII - autenticar: processo que busca verificar a identidade de uma pessoa no momento em que é requisitado um acesso a determinado ambiente ou recurso de tecnologia da informação;

VIII - cessão de bases de dados: ato de disponibilizar cópia, total ou parcial, de dados do Ministério da Saúde, aprovada pelo gestor competente;

IX - ciclo de vida da informação: compreende as fases de criação, manuseio, armazenamento, transporte e descarte da informação, considerando sua confidencialidade, integridade e disponibilidade;

X - classificação da informação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

XI - concedente: responsável pelo fornecimento da base de dados confidenciais pelo Ministério da Saúde;

XII - confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

XIII - conta de acesso: conjunto do "nome de usuário" e "senha" utilizado para acesso aos sistemas informatizados e recursos de TIC;

XIV - controles de segurança: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

XV - custodiante: agente público responsável por zelar pelo armazenamento e pela preservação do ativo sob sua propriedade;

XVI - dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;

XVII - dados confidenciais: dados pessoais que permitam a identificação da pessoa e possam ser associados a outros dados referentes ao endereço, idade, raça, opiniões políticas e religiosas, crenças, ideologia, saúde física, saúde mental, vida sexual, registros policiais, assuntos familiares, profissão e outros que a lei assim o definir, não podendo ser divulgados ou utilizados para finalidade distinta da que motivou a estruturação do banco de dados, salvo por ordem judicial ou com anuência expressa do titular ou de seu representante legal;

XVIII - dados pessoais: representação de fatos, juízos ou situações referentes a uma pessoa física ou jurídica, passível de ser captada, armazenada, processada ou transmitida por meios informatizados ou não;

XIX - disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

XX - documento confidencial: contém informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado;

XXI - evento: ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente conhecida que possa ser relevante para a segurança da informação (ISO/IEC TR 18044:2004);

XXII - gestor da informação: agente público do Ministério da Saúde responsável pela administração das informações geridas nos processos de trabalho sob sua responsabilidade;

XIII - grau de sigilo: gradação de segurança atribuída a dados e informações em decorrência de sua natureza ou conteúdo;

XXIV - incidente de segurança: todo e qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação ou de redes de computadores;

XXV - informação custodiada: informação sob a guarda e responsabilidade de alguém;

XXVI - integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

XXVII - logs: arquivos em computador utilizados para manter registros das atividades executadas por programas e usuários nos computadores e sistemas informatizados;

XXVIII - recursos de TIC: recursos de tecnologia da informação e comunicação que processam, armazenam e transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

XXIX - rede corporativa: conjunto de todas as redes locais sob a gestão do Ministério da Saúde;

XXX - rede local: conjunto de equipamentos interligados localmente com o objetivo de disponibilizar serviços aos usuários de rede do Ministério da Saúde;

XXXI - segurança da informação: preservação da confidencialidade, da integridade e da disponibilidade da informação e, adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas;

XXXII - senha ou palavra-chave: é uma palavra ou uma ação secreta previamente convencionada entre duas partes como forma de reconhecimento, sendo senhas amplamente utilizadas em sistemas de computação para autenticar usuários e permitir-lhes o acesso a informações personalizadas armazenadas no sistema;

XXXIII - sigilo: segredo de conhecimento restrito a pessoas credenciadas; proteção contra revelação não autorizada;

XXXIV - software: programa de computador desenvolvido para executar um conjunto de ações previamente definidas;

XXXV - usuário da rede: qualquer indivíduo ou instituição que tenha acesso autenticado aos recursos da rede corporativa do Ministério da Saúde;

XXXVI - usuário de sistema: qualquer indivíduo ou instituição que tenha acesso autenticado aos sistemas disponibilizados pelo Ministério da Saúde; e

XXXVII - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO I

DOS OBJETIVOS

Art. 3º Constituem objetivos da (POSIC/MS):

I - estabelecer suas diretrizes, a serem seguidas pelo Ministério da Saúde no que diz respeito à adoção de normas e procedimentos relacionados à segurança da informação e comunicações;

II - prover o Ministério da Saúde de normas para a segurança da informação, estabelecendo responsabilidades e diretrizes, bem como atitudes adequadas para manuseio, tratamento, controle e proteção contra a indisponibilidade, a divulgação, a modificação e o acesso não autorizados a dados e informações; e

III - definir um conjunto de instrumentos normativos e organizacionais que capacitem o Ministério da Saúde a assegurar a confidencialidade, a integridade e a disponibilidade dos dados e das informações.

CAPÍTULO II

DAS DIRETRIZES

Art. 4º Política de Informação e Comunicações do Ministério da Saúde (POSIC/MS) rege-se pelas seguintes diretrizes:

I - propriedade da informação:

a) toda informação criada, que for manuseada, armazenada, transportada ou descartada pelos agentes públicos do Ministério da Saúde, no exercício de suas atividades, é de propriedade do órgão e deve ser protegida segundo as diretrizes descritas na POSIC/MS e as regulamentações em vigor;

b) a informação custodiada, que for manuseada, armazenada, transportada ou descartada pelos agentes públicos do Ministério da Saúde, no exercício de suas atividades, deve ser protegida segundo as diretrizes descritas na POSIC/MS e nas demais regulamentações em vigor;

c) quando da obtenção de informação de terceiros, o Gestor da Informação deve providenciar junto ao concedente a documentação formal que atenda aos direitos de acesso antes de seu uso;

d) na cessão de bases de dados nominais custodiadas ou na informação de propriedade do Ministério da Saúde a terceiros, o Gestor da Informação deve providenciar a documentação formal relativa à autorização de acesso às informações

II - classificação da informação:

a) toda informação criada, manuseada, armazenada, transportada ou descartada do Ministério da Saúde deve ser classificada quanto aos aspectos de confidencialidade, integridade e disponibilidade, de forma explícita ou implícita, conforme o Decreto Nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal;

b) um processo de Classificação da Informação deve ser implementado e mantido, em conformidade com a legislação vigente, visando estabelecer os controles de segurança

necessários a cada informação custodiada ou de propriedade do Ministério da Saúde ao longo do seu ciclo de vida;

c) toda informação criada, manuseada, armazenada, transportada, descartada ou custodiada pelo Ministério da Saúde é de sua responsabilidade e deve ser protegida, adequadamente, conforme a classificação das informações;

d) a classificação da informação é atribuição do Gestor da Informação;

III - permissão de acesso:

a) todos os recurso de Tecnologia da Informação e Comunicação (TIC) sob responsabilidade do Ministério da Saúde deve ter um gestor formalmente designado por autoridade competente;

b) o agente público do Ministério da Saúde que utiliza os recursos de TIC deve ter uma conta de acesso, única e intransferível, cuja concessão de acesso será regulamentada em norma específica;

c) os privilégios de leitura, modificação ou eliminação das informações devem ser definidos pelo Gestor da Informação;

d) a autorização, o acesso, o uso da informação e dos recursos de TIC devem ser controlados e limitados ao cumprimento das atribuições de cada agente público do Ministério da Saúde e qualquer outra forma de uso necessita de prévia autorização formal pelo Gestor da Informação;

e) sempre que houver mudanças nas atribuições de determinado agente público do Ministério da Saúde será de responsabilidade da chefia imediata informar os seus privilégios de acesso às informações e aos recursos de TIC para que sejam adequados imediatamente;

f) no caso de exoneração ou demissão, esses privilégios devem ser cancelados;

IV - Gestão de Continuidade de Negócio:

a) deve ser estabelecida a Gestão de Continuidade de Negócio em segurança da informação e comunicações no âmbito do Ministério da Saúde visando reduzir a possibilidade de interrupção causada por desastres ou falhas nos recursos de TIC que suportam as operações do Ministério da Saúde;

b) deve ser estabelecido um processo de gestão de risco com vistas a minimizar possíveis impactos associados aos ativos, processo esse que deve possibilitar a seleção e a priorização dos ativos a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança;

c) as medidas de proteção devem ser planejadas e os custos na aplicação de controles devem ser balanceados de acordo com os danos potenciais de falhas de segurança;

d) toda informação institucional, se eletrônica, deve ser armazenada nos servidores de arquivo da rede local e, se não eletrônica, deve ser mantida em local que a salvaguarde adequadamente;

e) no descarte de informações institucionais devem ser observados as políticas, as normas, os procedimentos internos, a classificação que a informação possui, bem como a temporalidade prevista na legislação;

f) os recursos de TIC disponibilizados para criação, manuseio, armazenamento, transporte e descarte da informação no Ministério da Saúde devem dispor de mecanismos que minimizem os riscos inerentes a problemas de segurança, a fim de evitar ocorrências de incidentes, de forma acidental ou intencional, que afetem os princípios da integridade, da disponibilidade e da confidencialidade das informações;

g) os recursos de TIC utilizados pelo Ministério da Saúde devem ser previamente homologados, identificados individualmente e inventariados, além de possuir documentação mínima e atualizada para o seu uso e estar em conformidade com as normas de segurança especificas;

V - monitoramento:

a) o uso dos recursos de TIC disponibilizados pelo Ministério da Saúde é passível de monitoramento e auditoria, conforme o previsto no item 9.1.4 do acórdão do Tribunal de Contas da União Nº 461 de 28 de abril de 2004, que dispõe sobre a análise regular de arquivos logs com utilização, sempre que possível, de softwares utilitários específicos, para monitoramento do uso dos sistemas, e devem ser implementados e mantidos, sempre que possível, mecanismos que permitam a rastreabilidade desse uso; e

b) a entrada e a saída de ativos de informação nas dependências do Ministério da Saúde devem ser registradas e autorizadas por autoridade competente.

CAPÍTULO III

DA GESTÃO, DO GERENCIAMENTO E DA ABRANGÊNCIA

Art. 5º Compete ao CIINFO aprovar e revisar as diretrizes da POSIC/MS e suas regulamentações, que visam preservar a disponibilidade, a integridade e a confidencialidade das informações do Ministério da Saúde.

Art. 6º Esta política aplica-se ao ambiente de trabalho e aos recursos de TIC, estabelecendo responsabilidades e obrigações a todos os agentes públicos do Ministério da Saúde que tenham acesso às informações ou aos recursos de TIC deste órgão.

Art. 7º As diretrizes de segurança da informação estabelecidas nesta Portaria aplicam-se às informações armazenadas, bem como às que estão sendo transmitidas e devem ser seguidas pelos agentes públicos do Ministério da Saúde, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação.

Art. 8º A POSIC/MS deve ser difundida a todos os agentes públicos do Ministério da Saúde por um processo permanente de Conscientização em Segurança da Informação.

Art. 9º É dever do agente público do Ministério da Saúde conhecer e cumprir a Política de Segurança da Informação e Comunicações.

Art. 10. É condição para acesso aos ativos de informação do Ministério da Saúde a adesão formal aos termos desta Portaria.

Art. 11. O agente público do Ministério da Saúde é responsável pela segurança dos ativos de informação e processos que estejam sob a sua responsabilidade.

Art. 12. Os gestores responsáveis pelos processos inerentes à gestão da segurança da informação devem receber capacitação especializada.

Art. 13. Os contratos firmados pelo Ministério da Saúde devem conter cláusulas que determinem a observância desta política e normas dela derivadas.

Art. 14. Os recursos de TIC disponibilizados pelo Ministério da Saúde devem ser utilizados estritamente dentro do seu propósito.

Parágrafo único. É vedado, a qualquer agente público do Ministério da Saúde, o uso dos recursos de TIC para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias ou religiosas, comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo Ministério da Saúde ou para perpetrar ações que, de qualquer modo, venham a constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, assim como àquelas que atentem contra a moral e a ética ou que prejudiquem o cidadão ou a imagem do órgão.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 15. Os agentes públicos do Ministério da Saúde devem reportar ao Departamento de Informática do SUS (DATASUS) os incidentes que afetam a segurança dos ativos ou o descumprimento da POSIC/MS.

Art. 16. Em casos de quebra de segurança da informação por meio de recursos de TIC, o DATASUS deverá ser imediatamente acionado para tomar as providências necessárias a fim de sanar as causas, podendo, inclusive, determinar a restrição temporária do acesso às informações ou ao uso dos recursos de TIC do Ministério da Saúde.

Art. 17. A utilização da POSIC/MS é recomendada aos órgãos vinculados ao Ministério da Saúde.

Art. 18. A violação das normas de segurança da informação resultará na suspensão temporária ou permanente de privilégios de acesso aos recursos de TIC, em penas e sanções legais impostas por meio de medidas administrativas sem prejuízo das demais medidas cíveis e penais cabíveis.

Art. 19. Os casos omissos serão resolvidos pelo Comitê de Informação e Informática em Saúde (CIINFO/MS).

Art. 20. O Subcomitê de Segurança da Informação e Comunicações, sob orientação do CIINFO, deverá revisar, sempre que necessário, a POSIC/MS e todos os atos normativos dela decorrentes, não excedendo o período máximo de 1 (um) ano.

Art. 21. O Ministro de Estado da Saúde providenciará a edição dos atos que integram a POSIC/MS, nos termos do parágrafo único do artigo 1º, no prazo de 180 (cento e oitenta) dias, a partir da publicação desta Portaria.

Art. 22. Esta Portaria entra em vigor na data de sua publicação.

Art. 23. Ficam revogadas as Portarias DATASUS/MS nºs 207, de 9 de julho de 2008, publicada no Diário Oficial da União nº 137, de 18 de julho de 2008, Seção I, página 50.

JOSÉ GOMES TEMPORÃO

ANEXO D: PSIC DO MINISTÉRIO DA JUSTIÇA

PORTARIA MJ Nº 3.530, DE 3 DE DEZEMBRO DE 2013

Institui a Política de Segurança da Informação e Comunicações do Ministério da Justiça, e dá outras providências.

O MINISTRO DE ESTADO DA JUSTIÇA, no uso das atribuições que lhe conferem o art. 87, parágrafo único, inciso II, da Constituição, e o Decreto nº 6.061, de 15 de março de 2007, e tendo em vista o disposto no Decreto nº 3.505, de 13 de junho de 2000, e na Norma Complementar nº 3, de 30 de junho de 2009, do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, resolve:

Art. 1º Fica aprovada a Política de Segurança da Informação e Comunicações do Ministério da Justiça - POSIC/MJ, na forma do Anexo a esta Portaria.

Art. 2º A POSIC/MJ aplica-se a todos os órgãos e entidades da estrutura organizacional do Ministério da Justiça.

Parágrafo único. Os órgãos e entidades de que trata o caput poderão elaborar políticas setoriais de segurança da informação e comunicações, desde que observados os princípios e as diretrizes gerais da POSIC/MJ.

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

Art. 4º Fica revogada a Portaria nº 3.251, de 19 de dezembro de 2012, do Ministério da Justiça.

JOSÉ EDUARDO CARDOZO

ANEXO

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º A Política de Segurança da Informação e Comunicações do Ministério da Justiça - POSIC/MJ objetiva dotar os órgãos e entidades da estrutura organizacional do Ministério de princípios, diretrizes, critérios e instrumentos aptos a assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados e informações, protegendo-as contra ameaças e vulnerabilidades.

Art. 2º Para efeitos da POSIC/MJ, considera-se:

I - agente público: aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função no Ministério;

II - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado que possa resultar em dano para um sistema, órgão ou entidade da estrutura organizacional do Ministério;

III - ativos de informação: meios de armazenamento, transmissão e processamento de informação, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - 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;

V - confidencialidade: propriedade de que a informação não esteja disponível ou que não tenha sido revelada a pessoa física, sistema, órgão ou entidade não autorizados e não credenciados;

VI - continuidade de serviços: capacidade estratégica e tática de um órgão ou entidade da estrutura organizacional do Ministério de se planejar e responder a incidentes e interrupções de funcionamento, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

VII - disponibilidade: propriedade que assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou por determinado sistema, órgão ou entidade;

VIII - 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 e de implementar a segurança da informação e comunicações no Ministério;

IX - gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para um órgão ou entidade da estrutura organizacional do Ministério e os possíveis impactos no funcionamento de seus serviços e atividades, caso estas ameaças se concretizem;

X - gestão de risco: 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, permitindo equilibrá-los com os custos operacionais e financeiros envolvidos;

XI - incidente de segurança: qualquer evento adverso, confirmado ou suspeito, relacionado à segurança de sistemas de computação ou de redes de computadores;

XII - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XIII - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XIV - Segurança da Informação e Comunicações - SIC: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XV - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação; e

XVI - vulnerabilidade: conjunto de fatores internos ou causas potenciais de um incidente de segurança, que pode ser evitado por uma ação de SIC.

CAPÍTULO II

DO ESCOPO

Seção I

Dos Princípios

Art. 3º A POSIC/MJ é guiada pelos princípios da legalidade, segurança, publicidade, privacidade e ética.

Parágrafo único. Para efeitos da POSIC/MJ, entende-se por:

I - legalidade: observância dos parâmetros legais e regulamentares na implementação das ações de SIC;

II - segurança: proteção dos ativos de informação contra perda, corrupção, destruição, acesso, uso e alteração indevidos ou não autorizados;

III - publicidade: divulgação da POSIC/MJ e de todas as normas complementares aos agentes públicos em exercício no Ministério;

IV - privacidade: proteção do direito individual da pessoa à inviolabilidade de sua intimidade e vida privada e do sigilo de suas comunicações, observado o disposto no art. 31 da Lei nº 12.527, de 18 de novembro de 2011, e nos arts. 55 a 62 do Decreto nº 7.724, de 16 de maio de 2012; e

V - ética: observância do Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto nº 1.171, de 22 de junho de 1994, e demais regras de conduta normativamente delimitadas para os agentes públicos.

Seção II

Das Diretrizes

Art. 4º São diretrizes gerais da POSIC/MJ:

I - estabelecer medidas e procedimentos de tratamento da informação, com o objetivo de viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

II - manter equipe de tratamento e resposta a incidentes em redes computacionais, com objetivo de registrar, analisar e tratar incidentes de SIC por meio da coleta de evidências, investigação de ataques, provimento de assistência local e remota e intermediação da comunicação entre as partes envolvidas;

III - elaborar e implementar plano de gestão de riscos, com o objetivo de reduzir as vulnerabilidades, evitar ameaças, minimizar a exposição aos riscos e atenuar os impactos associados aos ativos de informação do Ministério;

IV - elaborar e implementar plano de gestão de continuidade, com o objetivo de identificar ameaças e possíveis impactos na continuidade dos processos e serviços essenciais para o funcionamento do Ministério;

V - elaborar e implementar mecanismos de auditoria e conformidade, com o objetivo de garantir a exatidão dos registros de acesso aos ativos de informação e avaliar sua conformidade com as normas de SIC em vigor;

VI - implementar controle de acesso lógico aos sistemas de computação e redes de computadores e controle de acesso físico às instalações, com o objetivo de preservar os ativos de informação do Ministério;

VII - definir regras claras e precisas de uso do e-mail institucional, com o objetivo de evitar o uso pelos agentes públicos para fins particulares, com abuso de direito ou violação à imagem do Ministério; e

VIII - controlar o acesso à Internet, com o objetivo de evitar que os recursos computacionais do Ministério sejam utilizados em desrespeito às leis, aos costumes e à dignidade da pessoa humana.

CAPÍTULO III

DAS PENALIDADES

Art. 5º A desobediência às regras da POSIC/MJ e demais normas complementares implicará em sanções administrativas, sem prejuízo da apuração nas esferas cível e penal.

CAPÍTULO IV

DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Seção I

Do Gestor de Segurança da Informação e Comunicações

Art. 6º A implementação da POSIC/MJ ficará a cargo do Gestor de Segurança da Informação e Comunicações, servidor público efetivo designado pelo Secretário-Executivo, cabendo-lhe especialmente:

I - examinar, formular, promover e coordenar as ações de SIC no Ministério, em articulação com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República;

II - acompanhar investigações e avaliações de danos decorrentes de quebras de segurança;

III - propor às autoridades competentes os recursos necessários às ações de SIC no Ministério;

IV - coordenar o Comitê Gestor de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Ministério;

V - divulgar e supervisionar o cumprimento da POSIC/MJ e suas normas complementares;

VI - propor normas e procedimentos relativos à SIC no âmbito do Ministério; e

VII - resolver os casos omissos e as dúvidas surgidas na aplicação da POSIC/MJ e suas normas complementares.

Seção II

Do Comitê Gestor de Segurança da Informação e Comunicações

Art. 7º Fica criado o Comitê Gestor de Segurança da Informação e Comunicações com a competência de:

I - assessorar na implementação das ações de SIC no Ministério;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

III - propor normas e procedimentos internos relativos à SIC, em conformidade com as legislações existentes sobre o tema;

IV - auxiliar na elaboração dos planos de gestão de riscos e de continuidade e na definição das diretrizes de auditoria e conformidade no âmbito do Ministério;

V - revisar a POSIC/MJ sempre que se fizer necessário;

VI - elaborar relatórios periódicos de suas atividades, encaminhando- os ao Secretário-Executivo; e

VII - indicar os integrantes da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

Art. 8º O Comitê será composto por um representante, titular e suplente, de cada órgão e entidade a seguir indicados:

I - Gabinete do Ministro;

II - Comissão de Anistia;

III - Consultoria Jurídica;

IV - Secretaria Executiva;

V - Secretaria de Assuntos Legislativos;

VI - Secretaria Nacional de Justiça;

VII - Secretaria Nacional de Segurança Pública;

VIII - Secretaria de Reforma do Judiciário;

IX - Secretaria Nacional do Consumidor;

X - Secretaria Nacional de Políticas sobre Drogas;

XI - Secretaria Extraordinária de Segurança para Grandes Eventos;

XII - Departamento de Polícia Federal;

XIII - Departamento de Polícia Rodoviária Federal;

XIV - Departamento Penitenciário Nacional;

XV - Defensoria Pública da União;

XVI - Arquivo Nacional;

XVII - Conselho Administrativo de Defesa Econômica; e

XVIII - Fundação Nacional do Índio.

§ 1º Os representantes do Comitê e seus suplentes serão designados mediante ato do Secretário Executivo.

§ 2º A participação no Comitê será considerada serviço público relevante e não ensejará remuneração de qualquer espécie.

§ 3º O Comitê poderá convidar outros técnicos para colaborarem nos trabalhos a serem desenvolvidos, sem direito a voto.

§ 4º As deliberações do Comitê serão tomadas por maioria simples, presente a maioria absoluta de seus membros.

§ 5º O Comitê reunir-se-á a cada dois meses, podendo haver convocação extraordinária, a critério de seu coordenador.

Seção III

Da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais

Art. 9º Fica criada a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, com competência de:

I - registrar, analisar e tratar eventos e incidentes de SIC, por meio da coleta de evidências, investigação de ataques, provimento de assistência local e remota e intermediação da comunicação entre as partes envolvidas;

II - coordenar, analisar e sugerir ações apropriadas para remoção de qualquer arquivo, objeto ou vulnerabilidade que possa causar prejuízos aos sistemas e redes de computadores ou quebra de segurança;

III - disseminar alertas de vulnerabilidades e outras notificações relacionadas à SIC no âmbito do Ministério;

IV - assessorar tecnicamente os órgãos e unidades do Ministério;

V - avaliar o emprego de ferramentas de SIC;

VI - avaliar e analisar riscos atuais e iminentes, bem como propor ações para sua mitigação;

VII - realizar testes para homologação dos sistemas de SIC do Ministério; e

VIII - realizar outras atribuições que lhe forem cometidas pelo Gestor de Segurança da Informação e Comunicações.

Parágrafo único. Os membros da ETIR deverão ter perfil técnico adequado às funções de tratamento de incidentes em redes computacionais.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Art. 10. O acesso à Internet realizado por meio de ativos de tecnologia de informação e comunicações do Ministério deve ser autorizado, identificado e registrado.

Art. 11. Os registros de acessos aos ativos de informação do Ministério devem ser preservados em conformidade à legislação em vigor.

Art. 12. O conteúdo das comunicações, mensagens e arquivos, transitados ou produzidos por meio do correio eletrônico institucional, é considerado propriedade do órgão, não sendo preservada a confidencialidade nos casos de violação da legislação em vigor.

Art. 13. As atribuições da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais serão exercidas pelo Grupo de Atendimento e Tratamento de Incidentes de Segurança da Informação- GATI do Ministério da Justiça.

Art. 14. A POSIC/MJ e suas normas complementares deverão ser revisadas sempre que se fizer necessário, não excedendo o período máximo de dois anos.

ANEXO E: PSIC DO MINISTÉRIO DA DEFESA

MINISTÉRIO DA DEFESA GABINETE DO MINISTRO

PORTARIA NORMATIVA Nº 1.530, DE 14 DE MAIO DE 2013

MINISTÉRIO DA DEFESA

GABINETE DO MINISTRO

DOU de 16/05/2013 (nº 93, Seção 1, pág. 33)

Aprova a Política de Segurança da Informação e Comunicações da Administração Central do Ministério da Defesa e dá outras providências.

O MINISTRO DE ESTADO DA DEFESA, no uso das atribuições que lhe são conferidas pelos incisos I e II do parágrafo único do art. 87 da Constituição, tendo em vista o disposto no Decreto nº 3.505, de 13 de junho de 2000; nos incisos XV e XVII do art. 27; nos incisos II, III, IV e V do art. 31 do Anexo I do Decreto nº 7.974, de 1º de abril de 2013, e em conformidade com o art. 98 da Lei nº 12.702, de 7 de agosto de 2012, resolve:

Art. 1º - Aprovar, nos termos do Anexo a esta Portaria Normativa, a Política de Segurança da Informação e Comunicações (PoSIC), com a finalidade de fornecer diretrizes, critérios e suporte administrativo para a implementação da Segurança da Informação e Comunicações (SIC) no âmbito da Administração Central do Ministério da Defesa (ACMD).

Parágrafo único - A PoSIC se aplica às atividades dos usuários da ACMD e os obriga ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação ou por meio de outros recursos.

Art. 2º - O Centro Gestor e Operacional do Sistema de Proteção da Amazônia (Censipam), o Hospital das Forças Armadas (HFA) e o Centro de Catalogação das Forças Armadas (Cecafa), devido às suas especificidades, serão regidos por Política de Segurança de Informação e Comunicações própria, alinhada, no que couber, à PoSIC anexa a esta Portaria Normativa, a qual deve ser submetida, no prazo de noventa dias, à avaliação e à aprovação do Comitê de Segurança da Informação e Comunicações (CSIC).

Art. 3º - A íntegra da PoSIC da ACMD será disponibilizada no endereço eletrônico www.defesa.gov.br, no Portal do Ministério da Defesa (MD) e também em sua Intranet.

Art. 4º - Esta Portaria Normativa entra em vigor na data de sua publicação.

CELSO AMORIM

ANEXO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA ADMINISTRAÇÃO CENTRAL DO MINISTÉRIO DA DEFESA

1. Escopo

1.1. A Política de Segurança da Informação e Comunicações (PoSIC) tem por objetivo instituir e implementar diretrizes estratégicas, responsabilidades e competências que assegurem a disponibilidade, a integridade, a confidencialidade e a autenticidade (DICA) das informações no âmbito da Administração Central do Ministério da Defesa (ACMD).

1.2. A PoSIC trata do uso e do compartilhamento de dados, informações e documentos no âmbito da ACMD, em todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte), visando à continuidade de seus processos críticos, em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

2. Conceitos e Definições

2.1.Para os efeitos desta Política entende-se por:

a) Assinatura digital: conjunto de dados criptografados, associados a determinado documento/arquivo que foi assinado, destinado a garantir a autenticidade e a integridade das informações constantes do documento, sua autoria e eventuais modificações;

b) Ativo de informação: patrimônio composto por dados, informações e conhecimentos obtidos, gerados e manipulados durante a execução dos sistemas e processos de trabalho;

c) 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 da ACMD;

d) Computação em nuvem: modelo computacional que permite acesso, por demanda e independente da localização, a conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

e) Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

f) Custodiante da informação: usuário que atua em uma ou mais fases do tratamento da informação, ou seja: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, incluindo a sigilosa;

g) Dispositivos móveis: equipamentos portáteis, dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, dentre eles: notebooks, netbooks, smartphones, tablets, pen drives, USB drives, HD externos e cartões de memória;

h) Equipe de tratamento e resposta a incidentes em redes computacionais: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

i) Gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem.

Esse processo fornece estrutura para que se desenvolva uma resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes envolvidas, a reputação e a marca da organização, assim como seus processos e de valor agregado. É o resultado da fusão dos Planos de Contingência e dos Planos de Recuperação de Desastres, que objetiva garantir a recuperação de um ambiente de produção, independentemente de eventos que suspendam suas operações e de danos nos componentes (processos, pessoas, softwares, hardware, infraestrutura etc.) por ele utilizados;

j) 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 física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação e Comunicações (TIC);

k) Gestão de Riscos em 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 os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

l) Gestor de Segurança da Informação e Comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito da ACMD;

m) Infraestrutura crítica de TIC: conjunto dos ativos de tecnologia da informação que afetam diretamente a consecução e a continuidade da informação por meios tecnológicos;

n) Inventário e Mapeamento de Ativos de Informação: processo interativo e evolutivo, composto por três etapas:

a) identificação e classificação de ativos de informação

b) identificação de potenciais ameaças e vulnerabilidades;

c) avaliação de riscos.

o) Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

p) Recurso criptográfico: sistemas, programas, processos e equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

q) Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

r) Termo de Compromisso Individual (TCI): documento formal, a ser assinado pelos usuários da ACMD, por meio do qual é estabelecido vínculo de comprometimento pessoal com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

s) Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

t) Usuários: servidores, militares, terceirizados, colaboradores, consultores, auditores, estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de informação da ACMD, formalizada por meio da assinatura do TCI.

3. Referências

3.1. A PoSIC da ACMD foi elaborada com base nas seguintes referências legais e normativas:

- Lei nº 8.112, de 11 de dezembro de 1990;

- Lei nº 9.983, de 14 de julho de 2000;

- Lei nº 12.527, de 18 de novembro de 2011;

- Decreto nº 3.505, de 13 de junho de 2000;

- Decreto nº 4.553, de 27 de dezembro de 2002;

- Decreto nº 5.482, de 30 de junho de 2005;

- Decreto nº 7.974, de 1º de abril de 2013;

- Instrução Normativa GSI nº 1, de 13 de junho de 2008, e respectivas normas complementares;

- Portaria Normativa nº 142/MD, de 25 de janeiro de 2008;

- Portaria Normativa nº 1.704/MD, de 27 de junho de 2012;

- Norma ABNT NBR/ISO/IEC 27001/2006;

- Norma ABNT NBR/ISO/IEC 27002/2007;

- Decreto nº 7.724, de 16 de maio de 2012;

- Decreto nº 7.845, de 14 de novembro de 2012.

4. Princípios

4.1. A PoSIC da ACMD orienta-se pelos seguintes princípios:

a) Disponibilidade: garante que a informação estará acessível e utilizável por pessoa física, sistema, órgão ou entidade, quando requisitada;

b) Integridade: garante que a informação não será modificada, gravada ou excluída sem autorização ou acidentalmente;

c) Confidencialidade: garante que a informação será acessada apenas por pessoa física, sistema, órgão ou entidade autorizada e credenciada;

d) Autenticidade: garante a identificação de pessoa física, sistema, órgão ou entidade que produziu, expediu, modificou ou excluiu a informação.

4.2. As ações de segurança da informação e comunicações da ACMD são norteadas pelos seguintes princípios:

a) Criticidade: define a importância da informação para a continuidade do negócio da organização;

b) Celeridade: garante respostas rápidas a incidentes e falhas de segurança;

c) Clareza: as regras e a documentação sobre segurança da informação e comunicações devem ser elaboradas de forma clara, precisa, concisa e de fácil entendimento;

d) Ética: preserva o direito do servidor, militar, colaborador, estagiário e prestador de serviços, sem que ocorra o comprometimento da segurança da informação e comunicações;

e) Legalidade: devem ser levadas em consideração as leis, as normas e as políticas organizacionais administrativas, técnicas e operacionais vigentes;

f) Responsabilidade: os usuários são responsáveis pelo cumprimento da Política de Segurança da Informação e Comunicações e devem respeitar a legislação e normas pertinentes à segurança da informação e comunicações.

4.3. São observados, ainda, sem prejuízo dos demais, os princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a APF.

5. Diretrizes Gerais

5.1. Pressupostos básicos

5.1.1. O sucesso das ações nos assuntos de segurança da informação e comunicações está diretamente associado à capacitação científico-tecnológica dos recursos humanos envolvidos, à conscientização do público interno, à qualidade das soluções adotadas e à proteção das informações contra ameaças internas e externas.

5.1.2. A informação é um recurso vital para o adequado funcionamento de toda e qualquer organização, devendo ser tratada como patrimônio a ser protegido e preservado.

5.2. Para cada uma das diretrizes constantes das Seções deste Capítulo devem ser elaboradas normas técnicas específicas, manuais e procedimentos.

5.3. Tratamento da Informação

5.3.1. Toda informação criada, adquirida ou custodiada pelo usuário, no exercício de suas atividades, é considerada bem e propriedade do MD e deve ser protegida segundo as diretrizes descritas nesta PoSIC e demais regulamentações em vigor, com o objetivo de minimizar riscos às atividades e serviços do Órgão e preservar sua imagem.

5.3.2. É expressamente proibido o acesso, a guarda ou o encaminhamento de material discriminatório, malicioso, não ético, obsceno ou ilegal por intermédio de quaisquer meios e recursos de tecnologia da informação disponibilizados pelo MD.

5.3.3. Os ativos de informação devem ser protegidos de forma preventiva, com o objetivo de minimizar riscos às atividades e aos objetivos de negócio do MD.

5.3.4. As informações criadas, armazenadas, manuseadas, transportadas ou descartadas devem ser classificadas segundo o grau de sigilo, criticidade e outros, conforme normas internas e legislação específica em vigor.

5.3.5. Todo usuário deve respeitar a classificação atribuída a uma informação e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

5.3.6. As informações produzidas ou custodiadas pelo MD devem ser descartadas conforme o seu nível de classificação.

5.3.7. Deve ser disponibilizado Sistema de Gestão Eletrônica de Documentos com mecanismos de assinatura digital aderente à legislação em vigor, com a finalidade de mitigar riscos associados à informação impressa.

5.3.8. A manipulação de informações classificadas em qualquer grau de sigilo deve seguir as normas internas e a legislação em vigor.

5.4. Tratamento de Incidentes de Rede

5.4.1 A área de Tecnologia da Informação (TI) do MD manterá Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (Etir), com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

5.5. Gestão de Risco

5.5.1. Os riscos devem ser continuamente monitorados e tratados, de acordo com as vulnerabilidades associadas aos ativos de informação e aos níveis de risco, conforme procedimentos definidos em norma específica sobre gestão de riscos em segurança da informação e comunicações.

5.5.2. Os usuários são responsáveis por adotar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos seus ativos de informação no âmbito da ACMD.

5.5.3. O processo de inventário e mapeamento de ativos de informação deve ser aplicado tanto na gestão de riscos quanto na gestão de continuidade, conforme procedimentos definidos em norma específica sobre o tema.

5.6. Gestão de Continuidade

5.6.1. O MD deve manter processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil.

5.6.2. As informações de propriedade ou custodiadas pelo MD, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança, de forma a garantir a continuidade das atividades do Órgão.

5.6.3. As informações armazenadas em outros meios devem possuir mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

5.7. Auditoria e Conformidade

5.7.1. O MD deve criar e manter registros e procedimentos, como trilhas de auditoria, que possibilitem o rastreamento, o acompanhamento, o controle e a verificação de acessos aos sistemas corporativos e rede interna do MD.

5.7.2. Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de SIC do MD com esta PoSIC e procedimentos complementares, bem como com a legislação específica em vigor.

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

5.7.4. A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

5.7.5. Os resultados de cada ação de verificação de conformidade serão documentados em Relatório de Avaliação de Conformidade.

5.8. Controle de Acesso

5.8.1. O controle de acesso aos sistemas corporativos, o credenciamento de acesso de usuários aos ativos de informação e o acesso às informações em áreas e instalações consideradas críticas devem ser implantados nos níveis físico e lógico definidos em norma específica, em conformidade com as diretrizes desta PoSIC.

5.9. Uso de E-mail (Correio Eletrônico)

5.9.1. O uso de e-mail no âmbito da ACMD deve ser definido em norma específica, com controle do uso e cancelamento de acesso ao correio eletrônico.

5.10. Acesso à Internet

5.10.1. O acesso à rede mundial de computadores (Internet), no âmbito da ACMD, será regido por norma interna, em conformidade com as diretrizes desta PoSIC, orientações governamentais e legislações específicas em vigor.

5.11. Inventário e Mapeamento de Ativos de Informação

5.11.1. O processo de Inventário e Mapeamento de Ativos de Informação deve produzir subsídios tanto para a Gestão de Segurança da Informação e Comunicações, a Gestão de Riscos de Segurança da Informação e Comunicações e a Gestão de Continuidade de Negócios, nos aspectos relacionados à segurança da informação e comunicações, quanto para os procedimentos de avaliação da conformidade, de melhorias contínuas, auditoria e, principalmente, de estruturação e geração de base de dados sobre os ativos de informação.

5.11.2. O processo de Inventário e Mapeamento de Ativos de Informação deve ser dinâmico, periódico e estruturado, para manter a Base de Dados de Ativos de Informação atualizada e, consequentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação e Comunicações.

5.12. Dispositivos Móveis

5.12.1. O uso de dispositivos móveis para acesso aos recursos computacionais no âmbito da ACMD deve ser controlado, com a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário, de acordo com procedimentos definidos em norma específica e em conformidade com as diretrizes desta PoSIC.

5.13. Computação em Nuvem

5.13.1. As ações de segurança da informação e comunicações para a implementação ou a contratação, no âmbito da ACMD, de tecnologias de computação em nuvem devem estar em conformidade com as orientações definidas em norma e legislações específicas em vigor.

5.14. Criptografia

5.14.1. A cifração e a decifração de informações classificadas em qualquer grau de sigilo devem utilizar recurso criptográfico baseado em algoritmo de Estado, conforme procedimentos definidos em norma e legislações específicas em vigor.

5.15. Redes Sociais

5.15.1.O uso institucional das redes sociais deve ser norteado por diretrizes, critérios, limitações e responsabilidades estabelecidas, visando ao uso seguro das redes sociais, conforme procedimentos definidos em norma específica e legislações específicas em vigor.

5.16. Contratação de Serviços

5.16.1. Nos editais de licitação e nos contratos de empresas prestadoras de serviços com a ACMD deverá constar cláusula específica sobre a obrigatoriedade de atendimento às normas desta PoSIC, bem como ser exigida da empresa contratada e do prestador a assinatura do Termo de Compromisso Individual e do Termo de Confidencialidade.

5.16.2. A empresa contratada também deverá demonstrar que possui mecanismos formais, no mínimo iguais aos adotados nesta PoSIC, que assegurem a confidencialidade e a segurança das informações.

5.16.3. Não deve ser adotada como prática a contratação de serviços terceirizados para atuação na Segurança da Informação e Comunicações, bem como na Infraestrutura Crítica de Tecnologia da Informação e Comunicações.

6. Penalidades

6.1. O usuário responderá pelo prejuízo que vier a ocasionar ao MD em decorrência do descumprimento de uma ou mais regras previstas nesta PoSIC.

6.2. A desobediência às regras estabelecidas implicará ao infrator as penalidades previstas em lei, nos âmbitos administrativo, civil, penal e militar.

7. Competências e Responsabilidades

7.1. Gestor de Segurança da Informação e Comunicações:

7.1.1. Planejar e coordenar a execução das ações de SIC;

7.1.2. Definir estratégias para a implementação desta PoSIC e normas complementares;

7.1.3. Supervisionar e analisar a efetividade dos processos, procedimentos, sistemas e dispositivos de SIC;

7.1.4. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e adotar as medidas administrativas necessárias à aplicação de ações corretivas;

7.1.5. Encaminhar os fatos apurados, decorrentes de quebras de segurança, para a aplicação das penalidades previstas;

7.1.6. Gerenciar a análise de risco;

7.1.7. Verificar se os procedimentos de Segurança da Informação e Comunicações (SIC) estão sendo aplicados de forma a atender à conformidade com legislações vigentes a respeito do assunto e normativos internos específicos;

7.1.8. Providenciar a divulgação interna e permanente desta PoSIC.

7.2. Comitê de Segurança da Informação e Comunicações:

7.2.1. Atualizar a Política de Segurança da Informação e Comunicações;

7.2.2. Propor grupos de trabalho para tratar de temas e sugerir soluções específicas sobre a segurança da informação e comunicações;

7.2.3. Propor, analisar e aprovar normas relativas à segurança da informação e comunicações, em conformidade com as legislações vigentes sobre o tema;

7.2.4. Propor um programa de Gestão de Continuidade de Negócios, com vistas a minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do MD, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

7.3. Setor de Tecnologia da Informação:

7.3.1. Planejar, coordenar, supervisionar, executar e controlar a execução das atividades de TIC relacionadas com as diretrizes desta PoSIC;

7.3.2. Elaborar, implementar e atualizar normas internas específicas em conformidade com esta PoSIC e demais diretrizes do Governo;

7.3.3. Criar e manter a ETIR, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores;

7.3.4. Manter registros e procedimentos como trilhas de auditoria e outros que assegurem o rastreamento, o acompanhamento, o controle e a verificação de acesso a todos os sistemas corporativos e das redes computacionais do MD;

7.3.5. Criar e manter a Assessoria de Segurança da Informação e Comunicações (ASSIC), com a responsabilidade de apoiar o Gestor de Segurança da Informação e Comunicações no cumprimento de suas atribuições;

7.4. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais:

7.4.1. Facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

7.4.2. Promover a recuperação de sistemas;

7.4.3. Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de rede por meio de verificações de conformidade;

7.4.4. Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

7.4.5. Analisar ataques e intrusões na rede do MD;

7.4.6. Executar as ações necessárias para tratar quebras de segurança;

7.4.7. Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

7.4.8. Cooperar com outras equipes de Tratamento e Resposta a Incidentes.

7.5. Setor de Recursos Humanos:

7.5.1. Comunicar ao Gestor de SIC, por meio de memorando, a ausência ou o desligamento de pessoal do MD;

7.5.2. Definir, nas descrições de cargos e funções, as responsabilidades pela manutenção das ações de SIC, bem como colher a assinatura do Termo de Compromisso Individual que envolva o manuseio dos ativos de informação;

7.5.3. Promover a ambientação de todo o pessoal, civil e militar, nomeado e/ou designado para a ACMD, por meio de treinamento e capacitação, com vistas a permitir acesso aos sistemas corporativos e às informações nos níveis físico e lógico, definidos em norma específica, em conformidade com as diretrizes desta PoSIC.

7.6. Usuário:

7.6.1. Acessar a rede de dados do MD somente após tomar ciência das normas de SIC e assinar o TCI;

7.6.2. Tratar a informação digital como patrimônio do MD e como recurso que deva ter seu sigilo preservado;

7.6.3. Utilizar as informações digitais disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso da MD exclusivamente para o interesse do serviço;

7.6.4. Preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las;

7.6.5. Não tentar obter acesso à informação cujo grau de sigilo não seja compatível com a sua Credencial de Segurança (Cred-Seg) ou cujo teor não tenha autorização ou necessidade de conhecer;

7.6.6. Não se fazer passar por outro usuário usando a identificação de acesso (login) e senha de terceiros;

7.6.7. No caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o sigilo das informações e documentos sigilosos a que teve acesso;

7.6.8. Não compartilhar, transferir, divulgar ou permitir o conhecimento das suas autenticações de acesso (senhas) utilizadas no ambiente computacional do MD por terceiros;

7.6.9. Responder, perante o MD, por acessos, tentativas de acesso ou uso indevido da informação digital, realizados com a sua identificação ou autenticação;

7.6.10. Não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;

7.6.11. Não transferir qualquer tipo de arquivo que pertença ao MD para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;

7.6.12. Estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço são expressamente proibidos no ambiente computacional do MD;

7.6.13. Estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional do MD pode ser auditada;

7.6.14. Estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e que qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional da ACMD deve obedecer a esse preceito;

7.6.15. Ao assinar o TCI, o usuário declara, formalmente, ter pleno conhecimento e aceitar expressamente, sem reservas, os termos desta PoSIC.

7.7. Custo diante da Informação:

7.7.1. Cumprir e zelar pela observância integral das diretrizes desta PoSIC e demais normas e procedimentos decorrentes;

7.7.2. Zelar pela disponibilidade, integridade, confidencialidade e autenticidade das informações e recursos em qualquer suporte sob sua custódia, conforme condições estabelecidas nesta PoSIC e demais normas e procedimentos decorrentes, mediante assinatura do TCI;

7.7.3. Participar de capacitação e treinamento em segurança da informação e comunicações, quando convocado;

7.7.4. Utilizar os recursos que lhe foram concedidos somente para o fim a que se destinam;

7.7.5. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;

7.7.6. Preservar a classificação do grau de sigilo a documentos, dados e informações dos quais tiver conhecimento em decorrência do exercício de suas funções;

7.7.7. Comunicar prontamente ao seu Chefe imediato e ao Gestor de Segurança da Informação e Comunicações qualquer incidente de que tenha conhecimento ou situações que comprometam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações e recursos em qualquer suporte sob sua custódia.

8. Divulgação

8.1. A PoSIC e suas atualizações, após publicação, deverão ser divulgadas amplamente aos usuários da ACMD e disponibilizadas no Portal do MD e também em sua Intranet.

9. Atualização

9.1. A atualização desta PoSIC e instrumentos normativos adicionais obedecerão aos seguintes critérios:

9.1.1. Política - Nível de Aprovação: Ministro de Estado da Defesa. Periodicidade de atualização: sempre que se fizer necessário, não excedendo o período máximo de três anos;

9.1.2. Normas - Nível de Aprovação: Comitê de Segurança da Informação e Comunicações. Periodicidade de atualização: sempre que se fizer necessário, não excedendo o período máximo de dois anos;

9.1.3. Procedimentos - Nível de Aprovação: Responsável pela área envolvida. Periodicidade de atualização: sempre que se fizer necessário, não excedendo o período máximo de um ano.

10. Anexos

10.1. Termo de Compromisso Individual.

10.2. Termo de Confidencialidade.

ANEXO I

MINISTÉRIO DA DEFESA

SECRETARIA DE ORGANIZAÇÃO INSTITUCIONAL DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES

TERMO DE COMPROMISSO INDIVIDUAL

Pelo presente instrumento, eu, _____, CPF nº _____, Carteira de Identidade nº _____, expedida pelo _____ em _____, lotado (a) no (a) _____, neste Ministério, na qualidade de USUÁRIO (A) da rede de computadores ou CUSTODIANTE de informações da Administração Central do Ministério da Defesa, DECLARO TER CONHECIMENTO da Política de Segurança da Informação e Comunicações (PoSIC) da ACMD, segundo a qual, sem restar qualquer dúvida de minha parte, devo:

a) tratar a informação como patrimônio do MD;

b) utilizar as informações e os recursos, em qualquer suporte sob minha custódia, exclusivamente no interesse do serviço do MD;

c) manter a confidencialidade das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las;

d) utilizar as credenciais de acesso (login e senha) e os recursos computacionais, em conformidade com a PoSIC da ACMD e procedimentos estabelecidos em normas específicas do Órgão;

e) no caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, observar a confidencialidade das informações sigilosas acessadas;

f) responder perante o MD pelo uso indevido das minhas credenciais de acesso, no âmbito administrativo e, se for o caso, perante a Justiça, no âmbito penal e civil.

Estou ciente de meu compromisso individual no Ministério da Defesa e assumo a responsabilidade pelas consequências decorrentes da não observância do disposto no presente Termo e na legislação vigente.

Brasília - DF, de de .

_____

Assinatura

(Usuário)

_____

Assinatura

(Representante da Assessoria de Segurança da Informação e Comunicações)

ANEXO II

MINISTÉRIO DA DEFESA

SECRETARIA DE ORGANIZAÇÃO INSTITUCIONAL

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES

TERMO DE CONFIDENCIALIDADE

A _____, inscrita no CNPJ sob o nº _____, sediada _____, por intermédio de seu representante legal, Sr(a). _____, portador(a) da Cédula de Identidade no _____, expedida pela(o) _____ e CPF nº _____, DECLARA que, para fins da execução do contrato no _____, comprometemo-nos a manter em sigilo, ou seja, não revelar ou divulgar as informações confidenciais ou de caráter não público recebidas durante e após a prestação dos serviços nas instalações do Ministério da Defesa, tais como: informações técnicas, operacionais, administrativas, econômicas, financeiras e quaisquer outras informações, escritas ou verbais, fornecidas ou que venham a ser de nosso conhecimento, sobre os serviços licitados, ou que a eles se referem.

A violação dos termos deste instrumento resultará na aplicação das penalidades cabíveis ao infrator, cíveis e criminais, nos termos da lei, obrigando-lhe, ainda, a isentar e/ou indenizar o Ministério da Defesa de todo e qualquer dano, perda, prejuízo ou responsabilidade, em virtude

de demandas, ações, danos, perdas, custas e despesas que porventura venha a sofrer como resultado da violação do disposto neste instrumento.

_____

Local e Data

_____

Nome, Cargo e Assinatura do Representante da Licitante

ANEXO F: PSIC DO MINISTÉRIO DA CULTURA

Portaria nº 119/2011/MinC

PORTARIA Nº 119, DE 5 DE DEZEMBRO DE 2011

Institui a Política de Segurança da Informação e Comunicações do Ministério da Cultura e o Sistema de Segurança da Informação e Comunicações e dá outras providências.

A MINISTRA DE ESTADO DA CULTURA, no uso da atribuição que lhe confere o inciso II do parágrafo único do art. 87 da Constituição Federal, e considerando o disposto no inciso VII do art. 5º da Instrução Normativa nº 1, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República, resolve:

Art. 1º Instituir a Política de Segurança da Informação e Comunicações do Ministério da Cultura – POSIC/MinC, estabelecendo diretrizes para o tratamento das informações produzidas, processadas, transmitidas ou armazenadas neste Ministério e em seus sistemas de informação.

CAPÍTULO I

DOS PRINCÍPIOS E OBJETIVOS

Art. 2º A POSIC/MinC está fundada no pressuposto de que a informação é um ativo de valor para a eficiente prestação dos serviços públicos, devendo ser adequadamente utilizada e protegida contra ameaças e riscos, sem prejuízo para a transparência da administração pública para com o cidadão.

Parágrafo único. Para efeitos de segurança da informação, as informações produzidas, adquiridas ou custodiadas sob responsabilidade do MinC são consideradas parte do seu patrimônio e como tal devem ser protegidas.

Art. 3º A segurança da informação e das comunicações são um conjunto de práticas e princípios que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

§ 1º Confidencialidade é a característica da informação pela qual ela não esteja presumidamente disponível ou revelada a pessoas, sistemas, órgãos ou entidades não autorizados e credenciados.

§ 2º Integridade é a característica da informação indicativa de que ela não foi destruída ou modificada desde sua elaboração.

§ 3º Disponibilidade é a característica indicativa de que a informação está acessível e utilizável sob demanda por uma determinada pessoa, sistema, órgão ou entidade.

§ 4º Autenticidade é a característica que comprova que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa, sistema, órgão ou entidade.

§ 5º Entende-se por Quebra de Segurança toda ação ou omissão que resulte em comprometimento da segurança da informação ou das comunicações, afetando-as em sua confidencialidade, integridade, disponibilidade ou autenticidade.

Art. 4º São objetivos da POSIC/MinC:

I – instituir o Sistema de Segurança da Informação do Ministério da Cultura;

II – dotar o Ministério da Cultura de instrumentos jurídicos, normativos e organizacionais que capacitem científica, tecnológica e administrativamente seus agentes, de modo a assegurar a segurança da informação e das comunicações;

III – eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação; e

IV – nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação.

Art. 5º As normas, procedimentos e ações de segurança da informação do Ministério da Cultura decorrentes desta Política de Segurança da Informação e Comunicações obedecerão aos seguintes princípios:

I – interoperabilidade entre os sistemas de informação;

II – continuidade dos processos e serviços essenciais para o funcionamento deste Ministério;

III – qualidade na prestação de serviços;

IV – publicidade da informação, salvo quando estritamente necessário para assegurar a privacidade e a intimidade do cidadão, ou para garantir a segurança do Estado e da sociedade, nos termos da lei;

V – garantia de confidencialidade, autenticidade, integridade e disponibilidade da informação; e

VI – privacidade das comunicações telefônicas e telemáticas.

CAPÍTULO II

DO SISTEMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 6º O Sistema de Segurança da Informação e Comunicações do Ministério da Cultura – SISIC/MinC – regula-se pela presente Política, bem como por Normas e Procedimentos de Segurança dela decorrentes.

§ 1º As Normas de Segurança estabelecerão padrões de tratamento de informações e obrigações gerais aos seus usuários, regulando os seguintes assuntos, entre outros:

I – modelos de gestão da informação;

II – gerenciamento de riscos;

III – tratamento de incidentes de rede;

IV – gestão de continuidade de serviços;

V – acesso a informações, áreas, instalações e sistemas de informação;

VI – classificação da informação;

VII – programas e ações de conscientização e educação em segurança da informação.

§ 2º Os Procedimentos de Segurança detalham, instrumentalizam e operacionalizam as disposições das Normas de Segurança, permitindo sua aplicação direta às atividades do ministério.

Art. 7º Compete ao Secretário-Executivo editar as Normas Gerais de Segurança.

Parágrafo único. Compete ao Diretor de Gestão Interna editar as normas específicas de procedimentos de segurança.

Seção I

Da Organização do Sistema

Art. 8º O SISIC/MinC será coordenado pelo Secretário-Executivo do Ministério da Cultura, cabendo-lhe decidir sobre a implantação de projetos na área de segurança da informação, bem como nos casos de descumprimento das diretrizes da POSIC/MinC e de suas Normas e Procedimentos de Segurança.

Parágrafo único. Compete ao Secretário-Executivo designar o Gestor de Segurança da Informação de que trata o art. 11 e os Responsáveis por Informações de que trata o art. 12 desta Portaria.

Art. 9º O SISIC/MinC contará com um Comitê de Segurança da Informação e Comunicações – CSIC – incumbido de:

I – assessorar na implementação das ações de segurança da informação e comunicações do Ministério da Cultura;

II – receber e analisar notícias de violação da POSIC e suas Normas e Procedimentos, encaminhando-as ao Secretário-Executivo quando for o caso;

III – propor projetos e iniciativas relacionados à melhoria da segurança da informação do MinC;

IV – propor, aos ordenadores de despesa e autoridades superiores, o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação e comunicações;

V – acompanhar o andamento de projetos e iniciativas relacionados à segurança da informação, no âmbito deste Ministério e da Administração Pública Federal; e

VI – propor Normas e Procedimentos de Segurança da Informação e Comunicações às autoridades competentes para expedi-las no âmbito deste Ministério, bem como ajustes e aprimoramentos da POSIC/MinC.

§ 1º O CSIC terá a seguinte composição:

I – Coordenador-Geral de Tecnologia da Informação, que o coordenará;

II – Gestor de Segurança da Informação;

III – um representante da Coordenação-Geral de Gestão de Pessoas;

IV – um representante da Coordenação-Geral de Recursos Logísticos;

V – um representante da Coordenação-Geral de Atendimento, Documentação e Prestação de Contas; e

VI – um representante da Coordenação-Geral de Execução Orçamentária e Financeira.

§ 2º O CSIC reunir-se-á mensalmente, podendo haver convocação extraordinária, a critério do coordenador do Comitê.

§ 3º O Comitê deliberará por maioria simples, devendo as reuniões ser registradas em atas.

§ 4º De acordo com a necessidade, outros profissionais do Ministério da Cultura e convidados externos poderão participar das reuniões na condição de observadores ou colaboradores eventuais.

Art. 10. Será constituída Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) com a incumbência de:

I – realizar ações de análise de vulnerabilidade e estabelecer mecanismos de registro e controle de conformidade das rotinas e sistemas do Ministério da Cultura à POSIC/MinC e suas Normas e Procedimentos de Segurança, comunicando Quebras de Segurança e outras desconformidades ao Gestor de Segurança da Informação;

II – receber, analisar e responder a notificações relacionadas aos incidentes de Quebra de Segurança em computadores no âmbito do Ministério da Cultura, encaminhando-as ao Gestor de Segurança da Informação quando necessário;

III – gerenciar os sistemas de informação do Ministério da Cultura, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários; e

IV – apresentar ao CSIC relatórios periódicos sobre riscos relacionados à segurança da informação e comunicações, acompanhados de proposta de aperfeiçoamento dos sistemas de informação deste Ministério, quando for o caso;

Parágrafo único. A composição e rotinas de trabalho da ETIR serão definidas em Normas e Procedimentos de Segurança específicos.

Art. 11. A execução do SISIC/MinC ficará a cargo do Gestor de Segurança da Informação, servidor responsável pelas ações de segurança da informação e comunicações no âmbito do Ministério da Cultura, cabendo-lhe especialmente:

I – supervisionar o cumprimento e promover a divulgação da POSIC/MinC e suas Normas e Procedimentos;

II – requisitar informações às Unidades específicas do Ministério da Cultura;

III – coordenar a ETIR, bem como a realização de testes e averiguações em sistemas e equipamentos;

IV – prover todas as informações de gestão de segurança da informação solicitadas pelo CSIC; e

V – lavrar as atas das reuniões do CSIC.

Art. 12. Cada Unidade organizacional do Ministério da Cultura contará com um servidor designado como Responsável por Informações, que estará encarregado da concessão, manutenção, revisão e cancelamento de autorizações de acesso a instalações e sistemas de informações deste Ministério, bem como a documentos do Órgão ou sob sua guarda.

§ 1º O encargo de Responsável por Informações recairá preferencialmente sobre o Chefe da Unidade ou seu Assessor direto.

§ 2º A Norma de Segurança especificará as unidades que deverão contar com seus próprios Responsáveis por Informações.

Art. 13. Cabe ao Responsável por Informações:

I – elaborar matriz que relacione cargos em comissão e funções gratificadas sob sua subordinação às autorizações de acesso concedidas, observadas as diretrizes da POSIC/MinC e suas Normase Procedimentos, bem como as disposições dos arts. 37 e 38 do Decreto No-4.553, de 27 de dezembro de 2002, quando se tratar de informações classificadas como sigilosas;

II – manter registro e controles atualizados das liberações de acesso concedidas, determinando, sempre que necessário, a pronta suspensão ou alteração de tais liberações;

III – reavaliar, sempre que necessário, as liberações de acesso concedidas, cancelando aquelas que não forem mais necessárias;

IV – analisar os relatórios da ETIR que sejam levados a seu conhecimento, com o objetivo de identificar desvios em relação à POSIC/MinC e suas Normas e Procedimentos, adotando as ações corretivas necessárias;

V – participar da investigação de incidentes de Quebra de Segurança relacionados a informação sob sua responsabilidade; e

VI – participar, sempre que convocado, das reuniões do CSIC, prestando os esclarecimentos solicitados.

Seção II

Dos Deveres para com a Segurança da Informação e das Comunicações

Art. 14. São deveres dos dirigentes do Ministério da Cultura:

I – cumprir e fazer cumprir a Política, as Normas e os Procedimentos de Segurança da Informação e Comunicações;

II – assegurar que suas equipes possuam acesso e conhecimento da Política, das Normas e dos Procedimentos de Segurança da Informação;

III – propor Procedimentos de Segurança da Informação relacionados às suas áreas de competência, submetendo as propostas aoComitê de Segurança da Informação; e

IV – comunicar imediatamente eventuais casos de violação de segurança da informação ao Comitê de Segurança da Informação e Comunicações ou a qualquer um de seus membros.

Art. 15. São deveres de todo servidor ou colaborador do Ministério da Cultura:

I – cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação deste Ministério;

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

III – assinar os termos de confidencialidade, responsabilidade e outros que venham a ser instituídos por Normas ou Procedimentos de Segurança, formalizando a ciência e o aceite da Política, das Normas e Procedimentos respectivos, bem como assumindo responsabilidade por seu fiel cumprimento;

IV – proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados nos termos da POSIC/MinC e suas Normas e Procedimentos;

V – assegurar que os recursos tecnológicos a sua disposição sejam utilizados apenas para as finalidades aprovadas nos termos da POSIC/MinC, suas Normas e Procedimentos; e

VI – comunicar imediatamente, ao respectivo Responsável por Informação ou ao Gestor de Segurança da Informação, qualquer descumprimento ou violação da POSIC/MinC ou suas Normas e Procedimentos.

Parágrafo único. As Normas de Segurança poderão especificar os colaboradores sujeitos à POSIC/MinC, bem como definir obrigações adicionais a servidores e colaboradores.

CAPÍTULO III

DISPOSIÇÕES GERAIS

Art. 16. A POSIC/MinC e suas Normas e Procedimentos serão disponibilizados para consulta de todos os servidores e colaboradores na rede corporativa deste Ministério, sem prejuízo da publicação oficial.

Parágrafo único. Sem prejuízo da disponibilização a que se refere o caput, a POSIC/MinC será objeto de ampla divulgação a todos os servidores, sendo facultada a divulgação das Normas e Procedimentos de Segurança apenas ao público-alvo nelas definido.

Art. 17. Em caso de Quebra de Segurança, poderá o Gestor de Segurança da Informação, para garantir a continuidade e a normalidade dos serviços de rede, determinar restrições temporárias de acesso a informações ou a recursos computacionais deste Ministério.

Art. 18. Os casos omissos da POSIC/MinC que não sejam objeto de Norma ou Procedimento específico serão estudados pelo CSIC, para eventuais propostas na forma do inciso VI do art. 9º deste Instrumento Normativo.

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

ANNA MARIA BUARQUE DE HOLLANDA

ANEXO G: PSIC DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GABINETE DO MINISTRO

PORTARIA Nº 853, DE 5 DE SETEMBRO DE 2013

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

GABINETE DO MINISTRO

DOU de 06/09/2013 (nº 173, Seção 1, pág. 7)

Aprova a Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação (Posic/MCTI).

O MINISTRO DE ESTADO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, no uso de suas atribuições e considerando o disposto no art. 5º da Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, resolve:

Art. 1º - Aprovar a Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação (Posic/MCTI).

CAPÍTULO I

DO ESCOPO

Seção I

Do Objetivo

Art. 2º - A Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação (Posic/MC-TI) alinha-se às estratégias do Ministério e objetiva garantir a disponibilidade, integridade, confidencialidade e autenticidade (Dica) das informações produzidas ou custodiadas pelo Ministério independentemente do meio onde estejam registradas.

Art. 3º - A Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação (Posic/MC-TI) define as diretrizes, competências e responsabilidades relativas ao uso e compartilhamento de dados, informações e documentos em conformidade com a Legislação vigente, as normas técnicas pertinentes, os valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 4º - Integram também a Posic/MCTI, os documentos que a complementam, destinados à proteção da informação e à disciplina de sua utilização.

Seção II

Da Abrangência

Art. 5º - A Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação (Posic/MC-TI) aplica-se aos órgãos de assistência direta e imediata ao Ministro de Estado; aos órgãos específicos singulares e às unidades descentralizadas do Ministério e deve ser observada em todos os ambientes informatizados e/ou convencionais aqui elencados, devendo ser seguida por todos que, de alguma forma, executem atividades vinculadas a este Ministério.

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

Art. 6º - Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo Ministério devem atender a esta Política.

Art. 7º - Esta Política também se aplica, no que couber, ao relacionamento do Ministério com outros órgãos e entidades públicos ou privados.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 8º - Para efeitos desta Portaria entende-se por:

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

II - agente público: todo aquele que exerce cargo, emprego ou função no Ministério da Ciência, Tecnologia e Inovação, ainda que transitoriamente com ou sem remuneração, por nomeação, designação, contratação ou qualquer outra forma de vínculo (servidores públicos, militares, servidores temporários regidos pela Lei nº 8.745/1993 e empregados públicos regidos pela Lei nº 9.962/2000, e colaboradores);

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

IV - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (Ref.: NC04/IN01/DSIC/GSIPR/2013);

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

VI - ativo classificado: ativo de informação com informação classificada;

VII - ativo de informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio. Inclui meios

de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VIII - ativo sob restrição de acesso: ativo de informação com informação institucional não pública ou com informação de acesso transitoriamente restrito;

IX - auditabilidade: atributo que garante a rastreabilidade dos diversos passos de um processo informatizado, identificando os participantes, ações e horários de cada etapa;

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

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

XII - colaborador: pessoa jurídica ou pessoa física que desempenhe atividade de interesse do MCTI, realize estágio ou preste serviço, em caráter permanente ou eventual;

XIII - Comitê de Segurança da Informação e Comunicações - CSIC: comitê instituído no âmbito dos órgãos de assistência direta e imediata ao Ministro de Estado, dos órgãos específicos singulares e das unidades descentralizadas do MCTI, por meio da Portaria MCTI nº 384, de 30 de maio de 2012, com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do Ministério;

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

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

XVI - custodiante do ativo de informação: aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

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

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

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

XX - documento classificado: documento com informação classificada;

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

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

XXIII - Gestor de Segurança da Informação e Comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito do MCTI;

XXIV - Gestor do Ativo de Informação: autoridade legal responsável pela concessão de acesso a terceiros (pode ser a autoridade marcadora, a autoridade classificadora ou a autoridade instituidora do processo);

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

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

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

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

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

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

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

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

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

XXVIII - informação sob restrição de acesso: informação institucional não pública ou informação de acesso transitoriamente restrito;

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

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

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

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

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

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

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

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

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

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

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

XL - usuário: agente público, auditores e quaisquer outros entes que podem acessar ativos de informação do MCTI mediante autorização de gestores de ativos; vulnerabilidade: conjunto

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

CAPÍTULO III

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 9º - Esta Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação (Posic/MCTI) observa a legislação e normas específicas destacando-se:

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

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

III - Lei nº 9.962, de 22 de fevereiro de 2000, que disciplina o regime de emprego público do pessoal da Administração Federal Direta, Autárquica e Fundacional, e dá outras providências;

IV - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências;

V - Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

VI - Decreto nº 4.073, de 3 de janeiro de 2002, que regulamenta a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados; VII. Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei 12.527, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;

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

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

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

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

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

XIII - Instrução Normativa nº 1, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá providencias;

XIV - Instrução Normativa nº 2, de 5 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal;

XV - Instrução Normativa nº 3, de 6 de março de 2013, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal;

XVI - Norma Complementar nº 3 da IN 1, de 30 de junho de 2009, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

XVII - Norma Complementar nº 4 da IN 1, de 15 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GR-SIC) nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta;

XVIII - Norma Complementar nº 5 da IN 1, de 14 de agosto de 2009, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais (Etir) nos órgãos e entidades da Administração Pública Federal;

XIX - Norma Complementar nº 6 da IN 1, de 11 de novembro de 2009, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a gestão de continuidade de negócios em segurança da informação e comunicações;

XX - Norma Complementar nº 7 da IN 1, de 6 de maio de 2010, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações;

XXI - Norma Complementar nº 9 da IN 1, de 15 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República, que estabelece orientações específicas para o uso de recursos criptográficos em segurança da informação e comunicações;

XXII - Portaria nº 14, de 21 de outubro de 2011, da Secretaria Executiva do Ministério da Ciência, Tecnologia e Inovação, que designa o Gestor de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação;

XXIII - Portaria nº 27, de 3 de fevereiro de 2012, do Ministério do Planejamento, Orçamento e Gestão, que aprova a atualização da Política de Segurança da Informação e Comunicações do Ministério do Planejamento Orçamento e Gestão;

XXIV - Portaria nº 383, de 30 de maio de 2012, do Gabinete do Ministro do Ministério da Ciência, Tecnologia e Inovação, que institui o Comitê Executivo de Tecnologia da Informação (CETI);

XXV - Portaria nº 384, de 30 de maio de 2012, do Gabinete do Ministro do Ministério da Ciência, Tecnologia e Inovação, que institui o Comitê de Segurança da Informação e Comunicações (CSIC);

XXVI - Portaria nº 165, de 30 de novembro de 2012, da Subsecretaria de Planejamento, Orçamento e Administração do Ministério da Ciência, Tecnologia e Inovação, que institui a Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS);

XXVII - Portaria nº 293, de 1º de abril de 2013, do Gabinete do Ministro do Ministério da Ciência, Tecnologia e Inovação, que institui a Política de Gestão Documental no âmbito do MCTI;

XXVIII - NBR ISO/IEC 27001:2006: Sistemas de Gestão de Segurança da Informação;

XXIX - NBR ISO/IEC 27002:2007: Código de Prática para a Gestão da Segurança da Informação.

CAPÍTULO IV

DOS PRINCÍPIOS

Art. 10 - A segurança da informação e comunicações do Ministério da Ciência, Tecnologia e Inovação deve obedecer aos princípios do acesso, da disponibilidade, da integridade, da confidencialidade, da autenticidade, da legalidade, da privacidade, da auditabilidade, e do não repúdio.

CAPÍTULO V

DAS DIRETRIZES GERAIS

Art. 11 - A segurança da informação e comunicações tem como principal diretriz a proteção da informação, garantindo a continuidade do negócio, minimizando seus riscos, maximizando o retorno sobre os investimentos e as oportunidades pertinentes. (Ref. ISO/IEC 27002:2006).

Art. 12 - As diretrizes de segurança da informação e comunicações devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e a estrutura do Ministério.

Art. 13 - As diretrizes de segurança da informação e comunicações descritas nesta Política devem ser observadas por todos os usuários que executem atividades vinculadas a este Ministério durante todas as etapas do tratamento da informação, a saber: produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Art. 14 - O cumprimento desta Política, bem como dos normativos que a complementam deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente instituído pelo Comitê de Segurança da Informação e Comunicações (CSIC), buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

Art. 15 - O Ministério deve observar as diretrizes estabelecidas nesta Política e deve se orientar pelas melhores práticas e procedimentos de segurança da informação e comunicações recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 16 - O Ministério deve criar, gerir e avaliar critérios de tratamento da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

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

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

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

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

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

CAPÍTULO VI

DAS DIRETRIZES ESPECÍFICAS

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

Seção I

Da Gestão da Segurança da Informação e Comunicações

Art. 21 - A Gestão de Segurança da Informação e Comunicações (GSIC) deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de segurança da informação e comunicações.

Art. 22 - A Gestão da Segurança da Informação e Comunicações (GSIC) deve compreender ações e métodos que visem a estabelecer parâmetros adequados, relacionados à segurança da informação e comunicações, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais do Ministério.

Parágrafo único - De forma a promover a gestão e fomentar os aspectos de segurança da informação, o Ministério deve:

I - definir uma Estrutura para a Gestão de Segurança da Informação e Comunicações (GSIC);

II - instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (Etir);

III - instituir Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS) em todos os seus órgãos e unidades;

IV - estabelecer a CPADS como órgão de assessoramento permanente do Comitê de Segurança da Informação (CSIC), sem prejuízo das atribuições propostas no artigo 34 do Decreto nº 7.724, de 16 de maio de 2012.

Seção II

Da Propriedade da Informação

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

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

Seção III

Dos Controles de Acesso

Art. 25 - Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.

Art. 26 - Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 27 - Todos os sistemas de informação do Ministério, automatizados ou não, devem ter um custodiante do ativo da informação, formalmente designado pelo gestor do ativo de informação, que deve definir os privilégios de acesso às informações, observando a legislação em vigor.

Art. 28 - O usuário é responsável por todos os atos praticados com suas identificações, entre as quais se destacam: nome do usuário na rede, carimbo, crachá, endereço de correio eletrônico e assinatura digital. O usuário responderá pela segurança dos ativos; dos processos que estejam sob sua responsabilidade e por todos os atos executados com suas identificações, salvo se comprovado que o fato ocorreu sem o conhecimento ou consentimento do usuário.

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

Art. 29 - A autorização, o acesso e o uso da informação e dos recursos de tecnologia da informação e comunicações devem ser controlados e limitados ao necessário para o cumprimento das atividades de cada usuário. Qualquer outra forma de autorização, acesso ou uso necessitará de prévia autorização do gestor do ativo de informação, observando-se a legislação em vigor.

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

Art. 30 - Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento do Ministério.

Seção IV

Da Gestão de Ativos da Informação

Art. 31 - Os ativos de informação devem:

I - ser inventariados e protegidos;

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

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

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

a) ativos em suporte físico, ostensivos ou com restrição de acesso, deverão ter sua tramitação registrada em sistema de protocolo corporativo;

b) ativos em suporte físico sob restrição de acesso somente poderão ser apensados ao sistema de protocolo corporativo caso estejam criptografados;

c) ativos em suporte digital poderão ser tramitados por meio de sistema de protocolo corporativo ou por correio eletrônico;

d) ativos em suporte digital sob restrição de acesso somente poderão ser tramitados por sistema de protocolo ou por correio eletrônico quando criptografados e com autorização de seu gestor:

I - cópias digitais de ativos sob restrição de acesso para mecanismos de armazenamento de qualquer tipo estarão sujeitos às mesmas regras e restrições de seus originais;

II - ativos classificados, para tramitar eletronicamente, deverão ter autorização expressa da autoridade classificadora, posto que sua tramitação pode gerar cópia eletrônica do ativo;

III - ativos de informação sob restrição de acesso devem ser tramitados de forma segura, de maneira a garantir que seu conteúdo somente possa ser visto pelo destinatário autorizado, conforme especificado na Seção IV do Capítulo III do Decreto nº 7.845, de 14 de novembro de 2012.

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

VI - ser regulamentados por norma específica quanto a sua utilização e movimentação;

VII - ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 32 - Os gestores do ativo de informação devem estabelecer regras e mecanismos que visem à manutenção de uma base de conhecimento sobre a realização de atividades no Ministério, observadas as normas de segurança da informação e comunicações.

Art. 33 - Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 34 - Os sistemas de informação e as aplicações do Ministério devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

Art. 35 - O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite a Termo de Responsabilidade, observando a legislação em vigor.

Seção V

Da Gestão Arquivística de Documentos Eletrônicos

Art. 36 - A Gestão Arquivística de Documentos Eletrônicos tem por objetivo a produção/criação, uso/acesso, avaliação e destinação (arquivamento ou descarte) dos documentos eletrônicos autênticos e fidedignos.

Art. 37 - Os documentos eletrônicos produzidos no âmbito do Ministério terão garantia de autoria, autenticidade e integridade asseguradas, nos termos da lei, mediante utilização de assinatura eletrônica.

Seção VI

Da Gestão Arquivística de Correio Eletrônico

Art. 38 - As mensagens de correio eletrônico de caráter institucional deverão ser reconhecidas como documento de arquivo, dotadas das qualidades inerentes a este, quais sejam: organicidade, unicidade, confiabilidade, autenticidade e acessibilidade, pois aquelas, também, refletem as ações e as competências e servem de apoio às funções e às atividades do Ministério, logo deverão estar sob o alcance desta Política.

Seção VII

Da Preservação dos Documentos em Meio Eletrônico

Art. 39 - O tratamento arquivístico inclusive descarte de documentos eletrônicos deve observar procedimentos definidos na legislação.

Parágrafo único - A gestão de documentos eletrônicos orienta-se pelos critérios da integridade e da disponibilidade das informações produzidas e custodiadas no âmbito do Ministério, respeitados os requisitos legais e os princípios de segurança da informação.

Art. 40 - Os documentos constantes da base de dados corporativa devem ser armazenados em equipamentos e mídias que permitam acesso com celeridade compatível com as necessidades do negócio no âmbito do Ministério.

Art. 41 - Ato do Ministro definirá Plano de Preservação de Documentos Eletrônicos, a partir de proposta formulada pelo Comitê de Segurança da Informação e Comunicações (CSIC), ouvida a Comissão Permanente de Avaliação de Documentos (CPAD).

Parágrafo único - O Plano de Preservação de Documentos Eletrônicos deve conter, entre outros elementos, a política de cópias de segurança (backup) e de recuperação em casos de perda de informação, bem como de retenção de versões de documentos eletrônicos.

Seção VIII

Da Classificação da Informação

Art. 42 - Informações geradas, adquiridas ou custodiadas pelo Ministério podem possuir classificação para indicar a necessidade, a prioridade e o nível esperado de proteção quanto ao seu tratamento. Quando classificadas serão observadas as exigências das atividades da instituição, considerando as implicações que um determinado grau de classificação trará para os seus objetivos institucionais e observando a legislação em vigor.

§ 1º - Todo usuário deve ser capaz de identificar a classificação atribuída a uma informação tratada pelo Ministério e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

§ 2º - A classificação deve auxiliar os gestores na priorização de ações e investimentos para a correta aplicação de mecanismos de tratamento.

Seção IX

Da Guarda e Tramitação de Ativo de Informação sob Restrição de Acesso

Art. 43 - Ativos de informação sob restrição de acesso devem ser armazenados em local que garanta sua acessibilidade apenas a usuário autorizado.

§ 1º - Se o ativo estiver em suporte impresso, deverá ser armazenado em arquivo com proteção de acesso.

§ 2º - Se o ativo estiver em meio eletrônico, deve ser armazenado criptografado, utilizando-se o algoritmo de Estado.

Seção X

Da Segurança Física e do Ambiente

Art. 44 - O Comitê de Segurança da Informação e Comunicações (CSIC) deve estabelecer mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências.

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

Seção XI

Da Segurança em Recursos Humanos

Art. 45 - Os usuários devem ter ciência:

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

II - de suas responsabilidades e obrigações no âmbito desta Política.

Art. 46 - Todos os usuários devem difundir e exigir o cumprimento desta Política, de seus documentos complementares, das normas de segurança e da legislação vigente acerca do tema.

Art. 47 - Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os usuários do Ministério, de acordo com suas competências funcionais.

Seção XII

Da Gestão de Riscos

Art. 48 - As áreas responsáveis por ativos de informação devem implantar processos contínuos de gestão de riscos, os quais serão aplicados na implementação e operação da gestão da segurança da informação e comunicações.

Parágrafo único - A gestão de riscos de TI deve avaliar os riscos relativos à segurança dos ativos de informação e a conformidade com exigências regulatórias ou legais.

Seção XIII

Da Continuidade de Negócio

Art. 49 - O Comitê de Segurança da Informação e Comunicações (CSIC) deverá instituir, formalmente, grupo de trabalho com objetivo de propor, manter e periodicamente testar medidas de gestão da continuidade e recuperação da informação, visando reduzir para um nível aceitável ou previamente definido a possibilidade de interrupção ou o impacto causado por desastres nos recursos de tecnologia da informação e comunicações que suportam os processos vitais do Ministério, até que se retorne à normalidade.

Seção XIV

Do Tratamento de Incidentes de Rede

Art. 50 - O Comitê de Segurança da Informação e Comunicações (CSIC) deverá instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), em conformidade com a Norma Complementar nº NC05/IN01/DSIC/GSIPR.

Seção XV

Da Criptografia

Art. 51 - O uso de recursos criptográficos interfere na disponibilidade, integridade, confidencialidade e autenticidade das informações, sendo, portanto, responsabilidade do Comitê de Segurança da Informação e Comunicações (CSIC) a implementação dos procedimentos relativos ao seu uso, no âmbito das informações geradas, adquiridas ou custodiadas sob a responsabilidade do Ministério, em conformidade com as orientações contidas em norma específica.

Art. 52 - O usuário é responsável pelo recurso criptográfico que receber, devendo assinar Termo de Sigilo e de Responsabilidade por seu uso.

Seção XVI

Da Auditoria e Conformidade

Art. 53 - A autorização, o acesso e o uso da informação e dos procedimentos de auditoria devem ser executados nos recursos de tecnologia da informação e comunicações.

Art. 54 - Deve ser realizada, com periodicidade mínima de três anos, verificação de conformidade das práticas de segurança da informação e comunicações do Ministério com esta Política, com suas normas e com seus procedimentos complementares, bem como com a legislação específica de segurança da informação e comunicações.

Art. 55 - A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o Ministério.

Art. 56 - A verificação da conformidade será realizada de forma planejada, mediante calendário de ações aprovado pelo CSIC.

Art. 57 - O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos identificados ou percebidos.

Art. 58 - Nenhum órgão ou unidade, abrangidos por esta Política, poderá permanecer sem verificação de conformidade de suas práticas de segurança da informação e comunicações por período superior a 3 (três) anos.

Art. 59 - A execução da verificação de conformidade será realizada por grupo de trabalho formalmente instituído pelo Comitê de Segurança da Informação e Comunicações (CSIC), podendo, com a prévia aprovação deste, ser subcontratada no todo ou em parte.

Art. 60 - É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

Art. 61 - A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

Art. 62 - Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo Gestor de Segurança da Informação e Comunicações ao gestor do ativo de informação do órgão ou unidade verificada, para ciência e tomada das ações cabíveis.

Seção XVII

Do Plano de Investimentos em Sic do MCTI

Art. 63 - Os investimentos em SIC serão realizados de forma planejada e consolidados em um plano de investimentos.

Art. 64 - O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco.

Art. 65 - Os investimentos em segurança da informação e comunicações deverão estar prevista na Lei Orçamentária Anual (LOA).

Art. 66 - O plano de investimentos, assim como a correspondente proposta orçamentária, serão aprovados no âmbito do Comitê de Segurança da Informação e Comunicações (CSIC) e submetidos à aprovação do Secretário-Executivo do Ministério.

Art. 67 - Caso a dotação concedida na Lei Orçamentária Anual (LOA) seja inferior à solicitada na proposta orçamentária, ou haja limitação na execução orçamentária, caberá ao Comitê de Segurança da Informação e Comunicações (CSIC) realizar a correspondente revisão do plano de investimentos.

Seção XVIII

Da Relação com Terceiros

Art. 68 - Nos editais de licitação, nos contratos, contratos de gestão, convênios, acordos e instrumentos congêneres de cooperação técnica com entidades prestadoras de serviços para o Ministério deverá constar cláusula específica sobre a obrigatoriedade de observância a esta Política, bem como deverá ser exigida, da entidade contratada, a assinatura do Termo de Responsabilidade.

Art. 69 - O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta Política, bem como suas normas e procedimentos complementares aos seus empregados e prepostos envolvidos em atividades no Ministério.

CAPÍTULO VII

DAS SANÇÕES

Art. 70 - A não observância desta política e/ou de seus documentos complementares, bem como a quebra de controles de segurança da informação e comunicações, poderá acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

CAPÍTULO VIII

DAS COMPETÊNCIAS E RESPONSABILIDADE

Seção I

Do Comitê de Segurança da Informação e Comunicações

Art. 71 - As competências do Comitê de Segurança da Informação e Comunicações (CSIC) do Ministério da Ciência, Tecnologia e Inovação estão descritas na Portaria MCTI nº 384, de 30 de maio de 2012, a saber:

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

II - minutar Política de Segurança da Informação composta por políticas, diretrizes, normas e procedimentos relativos à segurança da informação e comunicações para o Ministério, em conformidade com as legislações existentes sobre o tema, submetendo-a a Presidência do

Comitê Executivo de Tecnologia da Informação, que a integrará à Política de Informação vigente, submetendo-as à apreciação da autoridade competente;

III - propor alterações na Política de Segurança da Informação e Comunicações;

IV - instituir Grupos de Trabalho, em caráter permanente ou temporário, para tratar de temas específicos relacionados à segurança da informação e comunicações;

V - receber e analisar as comunicações referentes à quebra de segurança, apresentando parecer à autoridade/órgão competente para análise e providências;

VI - apoiar a implementação de programas destinados a conscientização e à capacitação de recursos humanos em segurança da informação e comunicações;

VII - apresentar soluções técnicas de arquitetura e infraestrutura vinculadas à segurança da informação e comunicações;

VIII - elaborar seu regimento interno no prazo de 180 (cento e oitenta) dias, contados da sua instalação e submetê-lo à aprovação do Secretário-Executivo do Ministério;

IX - exercer outras responsabilidades que lhe forem atribuídas em regimento interno.

Seção II

Do Gestor de Segurança da Informação e Comunicações

Art. 72 - As competências do Gestor da Segurança da Informação e Comunicações do Ministério estão descritas na Portaria SEXEC/MCTI nº 14, de 21 de outubro de 2011, a saber:

I - promover cultura de segurança da informação e comunicações;

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

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

IV - coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a 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 direto com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI/PR) para o trato de assuntos relativos à segurança da informação e comunicações;

VII - propor normas e procedimentos relativos à segurança da informação e comunicações.

Seção III

Dos Usuários

Art. 73 - Compete aos usuários do Ministério da Ciência, Tecnologia e Inovação:

I - cumprir fielmente as políticas, as normas, os procedimentos e as orientações de segurança da informação e comunicações do Ministério da Ciência, Tecnologia e Inovação;

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

II - assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação (Posic/MC TI), bem como assumindo responsabilidade por seu cumprimento;

IV - proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pelo Ministério;

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

VI - comunicar imediatamente ao Comitê de Segurança da Informação e Comunicações (CSIC) qualquer descumprimento ou violação desta Política e/ou de seus documentos complementares.

CAPÍTULO IX

DA VIGÊNCIA E ATUALIZAÇÃO

Art. 74 - Esta Política bem como o conjunto de instrumentos normativos gerados a partir dela, será revisada de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de dois anos.

Art. 75 - Esta Portaria entra em vigor na data de sua publicação.

MARCO ANTONIO RAUPP

ANEXO H: PSIC DO MINISTÉRIO DA EDUCAÇÃO

PORTARIA N° 1054 , DE 02 DE AGOSTO DE 2011

O MINISTRO DE ESTADO DA EDUCAÇÃO, INTERINO, no uso das suas atribuições que lhe conferem os incisos I e II do parágrafo único do art. 87 da Constituição Federal e considerando o disposto na Norma Complementar 03/IN01/DSIC/GSI/PR, de 10 de junho de 2009, resolve:

Art. 1º Aprovar a Política de Segurança da Informação e Comunicações - POSIC do Ministério da Educação - MEC.

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 integridade, confidencialidade, disponibilidade e autenticidade das informações custodiadas e de propriedade do MEC, de modo a preservar os seus ativos e sua imagem institucional.

Art. 3º A POSIC trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito do MEC, em todo o seu ciclo de vida - criação, manuseio, divulgação, armazenamento, transporte e descarte, visando à continuidade de seus processos críticos, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 4º Esta POSIC se aplica a todas as unidades da estrutura regimental do MEC, excetuando suas entidades vinculadas.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 5º Para efeitos desta POSIC, estabelece-se os significados dos seguintes termos e expressões:

I. Agente Público: aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, ao MEC;

II. Ativo: aquilo que tem valor – tangível ou intangível - para o MEC (tais como informação, software, equipamentos, instalações, serviços, pessoas e imagem institucional);

III. Autenticidade: propriedade que assegura que os dados ou informações são verdadeiros e fidedignos tanto na origem quanto no destino, permitindo, inclusive, a identificação do emissor e do equipamento utilizado, quando for o caso;

IV. Ciclo de vida da informação: compreende as fases de criação, manuseio, armazenamento, transporte e descarte da informação, considerando sua confidencialidade, integridade e disponibilidade;

V. Classificação da informação: atribuição, pela autoridade competente, de grau de sigilo, disponibilidade e integridade dado à informação, documento, material, área ou instalação;

VI. Comitê de Segurança da Informação e Comunicações: grupo de representantes de unidades do MEC com a responsabilidade deliberativa sobre as ações de segurança da informação e comunicações;

VII. Confidencialidade: propriedade que garante acesso à informação somente a pessoas autorizadas, assegurando que indivíduos, sistemas, órgãos ou entidades não autorizados não tenham conhecimento da informação, de forma proposital ou acidental;

VIII. Criticidade: grau de importância da informação para a continuidade das atividades e serviços do MEC;

IX. Dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;
X. Descarte: eliminação correta de informações, documentos, mídias e acervos digitais;
XI. Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade autorizados;
XII. Gestor da Informação: servidor público do MEC responsável pela administração das informações geridas nos processos de trabalho sob sua responsabilidade;
XIII. Incidente: evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
XIV. Informação Custodiada: informação sob a guarda e responsabilidade do MEC;
XV. Integridade: propriedade de salvaguarda da inviolabilidade do conteúdo da informação na origem, no trânsito e no destino, representando a fidedignidade da informação;
XVI. Recursos computacionais e de comunicação: equipamentos utilizados para armazenamento, processamento e transmissão de dados ou voz;
XVII. Rede corporativa: conjunto de todas as redes locais sob a gestão do MEC;
XVIII. Software: programa de computador desenvolvido para executar um conjunto de ações previamente definidas; e
XIX. Usuário: agente público com acesso autorizado a sistemas, redes de dados ou informações do MEC.

CAPÍTULO III
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 6º Esta POSIC observa a legislação e normas específicas, destacando-se:
I. Decreto nº 7.480, de 16 de maio de 2011, que aprova a estrutura regimental e o quadro demonstrativo dos cargos em comissão do grupo-direção e assessoramento superiores – DAS e das funções gratificadas do Ministério da Educação e dispõe sobre o remanejamento de cargos em comissão.
II. Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;
III. Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;
IV. 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;
V. 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 e dá outras providências;
VI. Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil);
VII. 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;
VIII. Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;
IX. Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da Rede Mundial de Computadores - Internet;
X. Portaria Interministerial nº 140, de 16 de março de 2006, que disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores - internet e dá outras providências;
XI. Decreto nº 6.029, de 1º de fevereiro de 2007, que institui o Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências;
XII. Acórdão do Tribunal de Contas da União nº 461/2004, de 28 de abril de 2004, que dispõe

sobre a análise regular de arquivos logs com utilização, sempre que possível, de softwares utilitários específicos, para monitoramento do uso dos sistemas;
XIII. Instrução Normativa GSI nº 1, 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;
XIV. Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 03 de julho de 2009, que estabelece as diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;
XV. Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 17 de agosto de 2009, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta - APF;
XVI. Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;
XVII. Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009, que disciplina as Diretrizes para Gestão de Continuidade de Negócios nos aspectos relacionados à Segurança da Informação e Comunicações - GCN nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;
XVIII. Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 07 de maio de 2010, que disciplina as diretrizes para implementação de Controles de Acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;
XIX. Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 24 de agosto de 2010, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;
XX. Norma ABNT NBR ISO/IEC 27001:2006 – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos;
XXI. Norma ABNT NBR ISO/IEC 27002:2005 – Técnicas de segurança - Código de práticas para a segurança da informação;
XXII. Norma ABNT NBR ISO/IEC 27005:2008 - Técnicas de segurança - Gestão de riscos de segurança da informação; e
XXIII. E-PING – Padrões de interoperabilidade de Governo Eletrônico, de 16 de dezembro de 2008.

CAPÍTULO IV
DOS PRINCÍPIOS

Art. 7º Esta POSIC observa os seguintes princípios, assim definidos:
I - Responsabilidade: os agentes públicos devem conhecer e respeitar a POSIC do MEC;
II - Ética: os direitos dos agentes públicos devem ser preservados, sem o comprometimento da segurança da informação e comunicações;
III - Celeridade: as ações de segurança da informação e comunicações devem oferecer respostas rápidas a incidentes e falhas de segurança;
IV - Clareza: as regras de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;
V - Privacidade: informação que fira o respeito à intimidade e à honra dos cidadãos não pode ser divulgada;
VI - Publicidade: dar transparência no trato da informação, observados os critérios legais; e

VII – Serão observados ainda, sem prejuízo das demais, outros princípios constitucionais que regem a Administração Pública Federal – APF.

CAPÍTULO V
DAS DIRETRIZES GERAIS
Seção I
Da Gestão da Segurança da Informação e Comunicações

Art. 8º A gestão da segurança da informação e comunicações compreende a preservação dos ativos do MEC quanto aos aspectos de confidencialidade, integridade, disponibilidade e autenticidade, independentemente do meio que se encontrem.

Art. 9º De forma a promover a gestão e fomentar os aspectos de segurança da informação, o MEC deve:

I - Instituir uma estrutura para a gestão de segurança da informação e comunicações;

II - Nomear um gestor de segurança da informação e comunicações; e

III - Estabelecer o comitê de segurança da informação e comunicações.

Seção II
Do Tratamento da Informação

Art. 10º Toda informação criada, adquirida ou custodiada pelo agente público, no exercício de suas atividades para o MEC, é considerada um bem e deve ser protegida pelo Ministério de acordo com as regulamentações de segurança existentes.

Art. 11º As informações devem ser protegidas de acordo com as diretrizes descritas nesta POSIC e demais regulamentações em vigor, com o objetivo de minimizar riscos às atividades e serviços do MEC e preservar sua imagem.

Art. 12º As informações produzidas ou custodiadas pelo MEC devem ser descartadas conforme o seu nível de classificação.

Seção III
Da Relação com Terceiros

Art. 13º Nos editais de licitação, nos contratos ou acordos de cooperação técnica com entidades prestadoras de serviços para o MEC deverá constar cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta POSIC, bem como deverá ser exigida, da entidade contratada, a assinatura do termo de confidencialidade.

Parágrafo único. As particularidades das relações com terceiros deverão ser definidas em norma interna específica.

Seção IV
Da Classificação da Informação

Art. 14º As informações custodiadas ou de propriedade do MEC devem ser classificadas quanto aos aspectos de sigilo, disponibilidade e integridade de forma implícita ou explícita e receber o nível de proteção condizente com sua classificação, conforme normas e legislação específica em vigor.

Art. 15º O gestor da informação é responsável por atribuir o nível de classificação das informações sob sua responsabilidade.

Art. 16º A classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte.

Art. 17º Todo agente público deve ser capaz de identificar a classificação atribuída a uma informação custodiada ou de propriedade do MEC e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

Seção V
Da Sensibilização, Conscientização e Capacitação

Art. 18º O MEC desenvolverá processo permanente de divulgação, sensibilização, conscientização e capacitação dos agentes públicos sobre os cuidados e deveres relacionados à segurança da informação e comunicações.

Seção VI

Da Gestão de Riscos

Art. 19º O MEC deve adotar processo contínuo de gestão de riscos, o qual será aplicado na implantação e operação da gestão de segurança da informação e comunicações.

Seção VII

Da Gestão de Continuidade

Art. 20º O MEC deve manter processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil.

Art. 21º As ações de continuidade do MEC devem ser adotadas por todos os titulares de unidade administrativa, de forma a proteger a reputação e a imagem institucional.

Art. 22º As informações de propriedade ou custodiadas pelo MEC, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança de forma a garantir a continuidade das atividades do Ministério. As informações armazenadas em outros meios devem possuir mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

Seção VIII

Do Tratamento de Incidentes de Rede Computacional

Art. 23º A Diretoria de Tecnologia da Informação - DTI manterá Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

Parágrafo único. A regulamentação da ETIR deve ser realizada por meio de documento de constituição aprovado pelo diretor da DTI do MEC.

Seção IX

Do Uso de Recursos Computacionais e Comunicações

Art. 24º O uso de recursos computacionais e comunicações do MEC pelos agentes públicos deve ser direcionado prioritariamente para realização das atividades profissionais desempenhadas para o Ministério nos limites dos princípios da ética, razoabilidade e legalidade.

Seção X

Da Auditoria e Conformidade

Art. 25º O MEC deve criar e manter registros e procedimentos, como trilhas de auditoria que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas corporativos e rede interna do MEC.

Art. 26º O MEC deve, periodicamente, promover verificação de conformidade às regulamentações de segurança e legislações em vigor.

Seção XI

Dos Controles de Acesso

Art. 27º O MEC deve sistematizar a concessão de acesso como forma de evitar a quebra de segurança da informação e comunicações.

Art. 28º O MEC deve prover mecanismos de controle de acesso como consequência do processo de gestão de riscos de segurança da informação e comunicações.

Art. 29º O acesso às informações custodiadas ou de propriedade do MEC pelos agentes públicos deve ser restrito ao necessário para desempenho de suas funções.

Art. 30º O acesso físico às instalações do MEC deverá ser regulamentado com o objetivo de garantir a segurança dos agentes públicos e a proteção dos seus ativos.

CAPÍTULO VI

DAS PENALIDADES

Art. 31º A não observância a POSIC e normas correlatas sujeitar-se-á às penalidades previstas nas legislações vigentes.

CAPÍTULO VII
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 32º É dever do agente público do MEC conhecer e zelar pelo cumprimento da POSIC.

Art. 33º Os agentes públicos são responsáveis pela segurança dos ativos e processos que estejam sob sua custódia e por todos os atos executados com suas identificações, tais como: crachá, login, senha eletrônica, certificado digital e endereço de correio eletrônico.

Parágrafo único. A identificação do usuário deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o seu reconhecimento.

Art. 34º Independentemente da adoção de outras medidas, o titular da unidade administrativa deverá, de imediato, comunicar todo incidente de segurança que ocorra no âmbito de suas atividades ao gestor de segurança da informação e comunicações.

Art. 35º No caso de incidente na rede corporativa, o comunicado deve ser feito à ETIR do MEC.

Art. 36º Compete aos coordenadores gerais de planejamento e gestão das secretarias do MEC dar o suporte administrativo necessário à gestão da POSIC.

Art. 37º Sempre que necessário, o gestor da informação do MEC providenciará autorização relativa à cessão de direitos sobre as informações de terceiros, antes de utilizá-las.

Art. 38º A cessão de informações do MEC a terceiros, deverá ser submetida previamente, à autorização do gestor da informação.

CAPÍTULO VIII
DA DIVULGAÇÃO

Art. 39º Após a publicação desta POSIC, deverá ser dada ampla divulgação a todos os agentes públicos do MEC, inclusive com publicação permanente na página da intramec.

CAPÍTULO IX
DA ATUALIZAÇÃO E VIGÊNCIA

Art. 40º Esta POSIC deverá ser revisada e atualizada quando identificada necessidade ou a cada 12 meses a contar da data de sua publicação.

Art. 41º Esta Portaria entra em vigor na data de sua publicação.

JOSÉ HENRIQUE PAIM FERNANDES

ANEXO I: PSIC DO MINISTÉRIO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO

MINISTÉRIO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO
GABINETE DO MINISTRO
PORTARIA Nº 795, DE 5 DE SETEMBRO DE 2012

O MINISTRO DE ESTADO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO, no uso de suas atribuições legais, considerando o disposto no art. 5º, inciso VII, da Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, e de acordo com a deliberação de 27 de julho de 2011 do Comitê de Segurança da Informação e Comunicações do Ministério da Agricultura, Pecuária e Abastecimento, resolve:

Art. 1º Aprovar a atualização da Política de Segurança da Informação e Comunicações do Ministério da Agricultura, Pecuária e Abastecimento, na forma do Anexo I desta Portaria.
Art. 2º Esta Portaria entra em vigor na data de sua publicação.
Art. 3º Fica revogada a Portaria nº 106, de 17 de fevereiro de 2009.
MENDES RIBEIRO FILHO

ANEXO I
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - PoSIC
ORIGEM
Ministério da Agricultura, Pecuária e Abastecimento - MAPA
REFERÊNCIA NORMATIVA
Decreto nº 1.171, de 24 de junho de 1994.
Código Civil, Art. 1.016.
Decreto nº 3.505, de 13 de junho de 2000.
Decreto nº 4.081, de 11 de janeiro de 2002.
Decreto nº 4.553, de 27 de dezembro de 2002.
Decreto nº 4.334, de 12 de agosto de 2002.
Instrução Normativa GSI nº 01, de 13 de junho de 2008 e suas respectivas Normas Complementares
Constituição da República Federativa do Brasil, de 5 de outubro de 1988.
Lei nº 8.112, de 11 de Dezembro de 1990.
Código Civil Brasileiro.
Código Penal Brasileiro.
ABNT NBR ISO/IEC 27001:2006.
ISO/IEC 15408:2005.
ISO/IEC Guide 73:2002.
CAMPO DE APLICAÇÃO
Todos àqueles, que direta ou indiretamente, possuem acesso às informações do MAPA.

SUMÁRIO

5. Diretrizes de Segurança
6. Competências e Responsabilidades
7. Penalidades
8. Disposições Finais
9. Vigência
INFORMAÇÕES ADICIONAIS
Não há.

APROVAÇÃO
JORGE ALBERTO PORTANOVA MENDES RIBEIRO FILHO
Ministro de Estado da Agricultura, Pecuária e Abastecimento

1. OBJETIVO

Estabelecer diretrizes, critérios e procedimentos de Segurança da Informação e Comunicações no âmbito do Ministério da Agricultura, Pecuária e Abastecimento (MAPA), visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo Ministério.

2. ABRANGÊNCIA

Estas diretrizes abrangem os seguintes ambientes: Edifício Sede, Superintendências Federais de Agricultura, Pecuária e Abastecimento (SFA), Laboratórios (LANAGRO), Instituto Nacional de Meteorologia (INMET), Comissão Executiva do Plano da Lavoura Cacaueira (CEPLAC), e todos que tenham acesso às informações e aos recursos computacionais do Órgão, inclusive terceirizados, consultores, estagiários e demais colaboradores externos ou eventuais.

3. CONCEITOS E DEFINIÇÕES

Para os efeitos desta Política serão adotados os conceitos e definições descritos no "Dicionário de Referência", que define os termos utilizados nas normas e procedimentos operacionais de Segurança da Informação e Comunicações criados para o âmbito do MAPA. Este dicionário está disponível na Intranet do MAPA, no link Segurança da Informação.

3.1 SIGLA E ABREVIAÇÕES

CSIC - Comitê de Segurança da Informação e Comunicações
CTIR GOV - Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da
Administração Pública Federal
DSIC - Departamento de Segurança da Informação e Comunicações - subordinado ao GSI/PR.
PDCA - do inglês: Plan-Do-Check-Act (Planejar-Fazer-Checar- Agir)
ETIR - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais
GCN - Gestão de Continuidade de Negócios
GSIC - Gestor de Segurança da Informação e Comunicações
GRSIC - Gestão de Riscos de Segurança da Informação e Comunicações
GSI/PR - Gabinete de Segurança Institucional da Presidência da República.
PDSIC - Plano Diretor de Segurança da Informação e Comunicações
POSIC - Política de Segurança da Informação e Comunicações

SIC - Segurança da Informação e Comunicações

4. PRINCÍPIOS

4.1 As ações relacionadas à Segurança da Informação e Comunicações no MAPA são norteadas pelos seguintes princípios:
4.1.1 Responsabilidade: todos os agentes públicos lotados nos ambientes de atuação do MAPA são responsáveis pelo tratamento da informação e pelo cumprimento das normas de segurança da informação e comunicações;
4.1.2 Conhecimento: os agentes públicos a serviço do MAPA tomarão ciência de todas as normas de segurança da informação e comunicações para o pleno desempenho de suas atribuições;
4.1.3 Legalidade: as ações de segurança da informação e comunicações levarão em consideração as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais do MAPA formalmente estabelecidas;
4.1.4 Proporcionalidade: o nível, a complexidade e os custos das ações de segurança da informação e comunicações no MAPA serão adequados ao entendimento administrativo e ao valor do ativo a proteger;
4.1.5 Continuidade: as ações de segurança devem ser planejadas; implantadas, verificadas e, se necessário for, reestruturadas em períodos cíclicos e continuados;
4.1.6 Veracidade: incidentes de segurança devem ser relatados de forma fiel a fim de permitir o adequado tratamento.

5. DIRETRIZES DE SEGURANÇA

5.1 Adota-se o método PDCA (Plan-Do-Check-Act) como metodologia para implantação e implementação do Sistema de Gestão de Segurança da Informação e Comunicações. O PDCA é referenciado pela norma ABNT NBR ISO/IEC 27001:2006 e adotado como padrão pelo GSI por meio da Norma Complementar nº 02/IN01/DSIC/GSI/PR.
5.2 O Ministro de Estado da Agricultura, Pecuária e Abastecimento compromete-se a prover diretrizes estratégicas, responsabilidades, competências e apoio à implementação do Sistema de Gestão de Segurança da Informação e Comunicações do MAPA.
5.3 Todos os usuários são responsáveis pela segurança dos ativos de informação e comunicações que estejam sob a sua responsabilidade e por todos os atos executados com suas identificações, tais como: usuário e senha de acesso aos recursos do MAPA, crachá, carimbo, endereço de correio eletrônico ou assinatura digital.
5.4 Toda informação deve ser tratada como um patrimônio, devendo ser protegida no acesso, tráfego, uso e armazenamento, de acordo com sua classificação em graus de confidencialidade e criticidade ao MAPA, ao Estado e as pessoas.
5.4.1 Não é permitido comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo Ministério.
5.4.2 A segurança é direcionada contra destruição, modificação ou divulgação indevida das informações - acidental ou intencional - e no impedimento de fraudes.
5.4.3 As informações do Órgão não devem ser expostas na presença de pessoas não autorizadas.
5.4.4 Registros e informações sigilosas devem ser protegidos contra perda, destruição e falsificação, sendo retidos de forma segura para atender requisitos legais e regulamentares.

5.4.5 O acesso às informações e aos recursos necessários para execução de atividades profissionais ao MAPA, serão concedidos ao Agente Público, mediante assinatura de Termo de Confidencialidade e Responsabilidade, observando suas atribuições.
5.5 A identificação do Agente Público - qualquer que seja o meio e a forma - deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.
5.6 Os usuários que tenham acesso às informações confidenciais ou reservadas devem fazê-lo apenas para os fins aprovados pelo respectivo gestor das informações, respeitando as regras de proteção estabelecidas.
5.7 Todos os usuários devem estar capacitados nos procedimentos de segurança e no uso correto da informação e dos recursos tecnológicos de forma a minimizar possíveis riscos de segurança.
5.8 Quando do afastamento ou desligamento do usuário de suas atribuições, faz-se necessário o cancelamento imediato dos direitos de acesso e uso da informação, além do preenchimento de termo de desligamento.
5.9 Os recursos computacionais disponibilizados pelo MAPA devem ser utilizados, de forma exclusiva, dentro dos propósitos institucionais:
5.9.1 É vedado, a qualquer Agente Público, o uso desses recursos para fins pessoais - próprios ou de terceiros, entretenimento, veiculação de opiniões político-partidárias ou religiosas.
5.9.2 Recursos do MAPA não podem ser utilizados para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a qualquer pessoa física ou jurídica, nem veicular opiniões político partidárias.
5.9.3 A utilização de recursos computacionais na rede interna do MAPA é permitida somente mediante homologação e autorização de sua área de tecnologia.
5.9.4 O uso da internet e do email corporativo, no âmbito do MAPA, deve seguir normas específicas e em conformidade a estas diretrizes.
5.10 O uso dos recursos computacionais e de informações disponibilizadas pelo MAPA é passível de monitoramento, respeitando os princípios legais:
5.10.1 Mecanismos que permitam a rastreabilidade desse uso devem ser implementados e mantidos pelo MAPA.
5.10.2 A entrada ou saída de equipamento computacional do Órgão deve ser autorizada e registrada.
5.11 Os contratos firmados pelo MAPA devem conter cláusulas que determinem a observância desta política e de suas normas específicas.
5.12 O MAPA deve implementar e manter um processo de gestão de riscos com vistas a minimizar possíveis impactos associados aos ativos de informação e comunicações:
5.12.1 Esse processo deve possibilitar a seleção e priorização dos ativos a serem protegidos, bem como a definição e implementação de controles para a identificação e tratamento de possíveis problemas de segurança.
5.13 O MAPA deve elaborar, implementar e manter um Programa de Gestão da Continuidade de Negócios, em conformidade a estas diretrizes, considerando os seguintes procedimentos:
a. Definir as atividades críticas do Ministério;
b. Avaliar os riscos a que estas atividades críticas estão expostas;
c. Definir as estratégias de continuidade para as atividades críticas;
d. Desenvolver e implementar os Planos previstos no Programa de Gestão da Continuidade de Negócios para respostas tempestivas a interrupções;
e. Realizar exercícios, testes e manutenção periódica dos Planos, promovendo as revisões necessárias;
f. Desenvolver a cultura de continuidade de negócios no Ministério.

5.14 Os perímetros físicos de atuação do Órgão devem ser adequadamente protegidos, visando à adequada salvaguarda de seus ativos de informação, conforme a classificação de risco de cada ambiente.
5.15 Todo sistema em operação, definido como crítico para os serviços prestados pelo MAPA deve possuir suficiente documentação de forma a garantir sua manutenibilidade, utilização, instalação, configuração, operação e produção, restringindo-se o acesso a essa documentação quando necessário.
5.16 As condições e termos de licenciamento de software e os direitos de propriedade intelectual devem ser respeitados.
5.17 A instalação e uso de sistemas e equipamentos para processamento de informação devem ser previamente homologados e autorizados pela área de tecnologia do Órgão.
5.18 O cumprimento das normas de Segurança da Informação do MAPA será auditado periodicamente, de acordo com os critérios definidos pelo Comitê de Segurança da Informação e Comunicações.
5.19 As medidas de proteção devem ser planejadas e os gastos na aplicação de controles devem ser balanceados de acordo com os danos potenciais de falhas de segurança.
5.20 Os incidentes de segurança - a exemplo de: indícios de fraude; sabotagem; falhas de segurança em processos, sistemas, instalações ou equipamentos - devem ser notificados imediatamente à chefia imediata e ao responsável pela Gestão de Segurança da Informação do MAPA.
5.21 Estas diretrizes estão de acordo com os objetivos, estratégias e necessidades operacionais do Ministério, respeitando a avaliação dos riscos e a análise de custo e benefício à continuidade de suas atividades.
5.22 Estas diretrizes de Segurança da Informação e Comu nicações devem ser conhecidas e seguidas por todos os usuários do órgão, para tanto, devem ser difundidas no MAPA por meio de um processo permanente de conscientização de Segurança da Informação e Comunicações.
5.22.1 Os membros do Comitê, o Gestor, e as Equipes de Segurança da Informação e Comunicações deverão receber regularmente, ao menos uma (01) vez por ano, capacitação especializada em SIC, a fim de garantir a adequada gestão e manutenção destas diretrizes.
5.23 Os diversos níveis gerenciais devem zelar pelo cumprimento destas Diretrizes de Segurança da Informação e Comunicações no âmbito de sua competência.
5.24 O MAPA, além das diretrizes estabelecidas nesta Portaria, deve também, se orientar pelas melhores práticas e procedimentos de segurança da informação, recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

6 COMPETÊNCIAS E RESPONSABILIDADES

6.1 Todos os agentes públicos que necessitem ter acesso às informações devem assinar, antes do início de suas atribuições, termo de responsabilidade e confidencialidade, garantindo o conhecimento e zelo pelo adequado cumprimento desta Política de Segurança da Informação e Comunicações.
6.2 Ao Ministro de Estado da Agricultura, Pecuária e Abastecimento, compete:
a. Coordenar as ações de segurança da informação e comunicações;
b. Aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra de segurança;
c. Propor programa orçamentário específico para as ações de segurança da informação e comunicações;
d. Instituir Comitê de Segurança da Informação e Comunicações;
e. Nomear Gestor de Segurança da Informação e Comunicações;
f. Instituir e manter área e equipe dedicadas à Gestão da Segurança da Informação e Comunicações;

g. Instituir e manter equipe de tratamento e resposta a incidentes em redes computacionais;
h. Aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações;
i. Remeter os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações, sempre que solicitado formalmente, ao GSI/PR.
6.3 Aos membros do Comitê de segurança da informação e comunicações do MAPA, compete:
a. Assessorar na implementação das ações de segurança da informação e comunicações no MAPA;
b. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;
c. Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema;
d. Avaliar e revisar a Política de Segurança da Informação e Comunicações, no mínimo, uma vez a cada 12 meses, visando a sua aderência e concordância aos objetivos institucionais do MAPA e às legislações vigentes;
e. Auditar o cumprimento da Política de Segurança da Informação e Comunicações;
f. Realizar reuniões ordinárias trimestralmente e reuniões extraordinárias quando convocadas pelo coordenador do comitê.
6.4 Ao Gestor de Segurança da Informação e Comunicações compete:
a. Promover a cultura de segurança da informação e comunicações no âmbito do MAPA;
b. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
c. Propor recursos necessários às ações de segurança da informação e comunicações;
d. Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
e. Prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da ETIR e do CSIC, bem como prover a infraestrutura necessária;
f. Convocar as reuniões ordinárias e extraordinárias do CSIC;
g. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
h. 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;
i. Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do MAPA;
j. Comunicar incidentes de segurança ao Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR Gov, conforme procedimentos a serem definidos pelo próprio CTIR Gov, com vistas a permitir que sejam dadas soluções integradas para a APF, além de viabilizar geração de estatísticas.
6.5 À Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais compete:
a. Receber, analisar e responder a notificações e atividades relacionadas aos incidentes de segurança em computadores;
b. Comunicar a ocorrência de incidentes de segurança em redes de computadores ao Gestor de segurança, Registrar todos os incidentes notificados ou detectados, com a finalidade de assegurar registro histórico das atividades da ETIR.

7. PENALIDADES

O não cumprimento das determinações da Política de Segurança da Informação e Comunicações do MAPA, bem como de suas Normas Complementares e Procedimentos Técnicos, sujeitará o infrator às penalidades previstas na Constituição Federal, Código Civil, Código Penal, Lei 8.112; e em regulamentos/normativos internos da Presidência da República e deste Ministério.

8.DISPOSIÇÕES FINAIS

8.1 O Agente Público deve reportar os incidentes que afetam a segurança dos ativos de informação e comunicações ou o descumprimento da Política de Segurança da Informação e Comunicações (POSIC) ao Comitê de Segurança da Informação e Comunicações (CSIC).
8.2 Em casos de quebra de segurança da informação por meios eletrônicos, a Coordenação-Geral de Tecnologia da Informação (CGTI) deverá ser imediatamente acionada para adotar as providências necessárias, podendo inclusive determinar a restrição temporária do acesso às informações e/ou aos recursos computacionais do MAPA.
8.3 Os casos omissos serão analisados e deliberados pelo Comitê de Segurança da Informação e Comunicações do MAPA.
D.O.U., 06/09/2012 - Seção 1

ANEXO J: PSIC DO MINISTÉRIO DO TRABALHO E EMPREGO

PORTARIA Nº 1.047, DE 16 DE JULHO DE 2013

O MINISTRO DE ESTADO DO TRABALHO E EMPREGO - INTERINO, no uso das suas atribuições legais e considerando o disposto na Norma Complementar 03/IN01/DSIC/GSIPR, de 10 de junho de 2009, e deliberações do Comitê de Segurança da Informação e Comunicações - CSIC, resolve:

Art. 1º Aprovar a Política de Segurança da Informação e Comunicações - POSIC do Ministério do Trabalho e Emprego - MTE.

SEÇÃO I

DO ESCOPO

Art. 2º A Política de Segurança da Informação e Comunicações - POSIC objetiva, observando a legislação e normas específicas em vigor, instituir diretrizes estratégicas, responsabilidades e competências, visando assegurar a integridade, confidencialidade, disponibilidade, autenticidade e legalidade dos dados, informações e documentos do MTE, contra ameaças e vulnerabilidades, de modo a preservar os seus ativos, inclusive sua imagem institucional.

Art. 3º A POSIC trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito do MTE, em todo o seu ciclo de duração - criação, manuseio, divulgação, armazenamento, transporte e descarte -, visando à continuidade de seus processos vitais, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 4º Esta POSIC se aplica a todas as unidades da estrutura regimental do MTE, incluindo as unidades descentralizadas, órgãos colegiados, bem como a servidores, prestadores de serviço, colaboradores, fornecedores, estagiários, consultores externos e a quem, de alguma forma, execute atividades vinculadas a este Ministério.

Parágrafo único. Esta Política também se aplica, no que couber, ao relacionamento do MTE com outros órgãos e entidades públicas ou privadas.

SEÇÃO II

DOS CONCEITOS E DEFINIÇÕES

Art. 5º Para efeitos desta POSIC, fica estabelecido o significado dos seguintes termos e expressões:

I - ameaça: conjunto de fatores externos ou causa potencial de um incidente, que pode resultar em dano para um sistema ou para o MTE;

II - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

III - autenticidade: propriedade que assevera que os dados ou informações são verdadeiros e fidedignos tanto na origem quanto no destino, permitindo, inclusive, a identificação do emissor e do equipamento utilizado, quando for o caso;

IV - Comitê de Segurança da Informação e Comunicações: grupo de representantes de unidades do MTE com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações;

V - confidencialidade: propriedade que garante acesso à informação somente a pessoas autorizadas, assegurando que indivíduos, sistemas, órgãos ou entidades não autorizados não tenham conhecimento da informação, de forma proposital ou acidental;

VI - criticidade: grau de importância da informação para a continuidade das atividades e serviços do MTE;

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

VIII - incidente de segurança da informação: evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

IX - integridade: propriedade de salvaguarda da inviolabilidade do conteúdo da informação na origem, no trânsito e no destino, representando a fidedignidade da informação;

X - gestão de continuidade dos negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócios, caso essas ameaças se concretizem;

XI - 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 os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

XII - recursos de tecnologia da informação e comunicações: recursos que processam, armazenam e transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

XIII - resiliência: capacidade de enfrentamento ágil de situações inesperadas e de superação das adversidades para restabelecer processo de normalidade;

XIV - usuário: todo aquele que está autorizado a obter acesso a informações e sistemas; e

XV - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para o MTE, os quais podem ser evitados por uma ação interna de segurança da informação.

SEÇÃO III

DOS PRINCÍPIOS

Art. 6º São princípios desta POSIC:

I - a legalidade, a impessoalidade, a moralidade, a publicidade, a eficiência, a celeridade e a ética na proteção do ativo de informação;

II - a responsabilidade individual na utilização dos ativos de informação; e

III - o respeito à privacidade das informações pessoais.

SEÇÃO IV

DAS DIRETRIZES GERAIS

Art. 7º Compete à Secretaria-Executiva, assessorada pelo Comitê de Segurança da Informação e Comunicações, normatizar a implantação e operacionalização das diretrizes previstas nesta Seção.

Subseção I

Da Gestão da Segurança da Informação e Comunicações

Art. 8º A Gestão da Segurança da Informação e Comunicações não se limita à tecnologia da informação e comunicações, compreendendo as ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos.

Art. 9º A Gestão de Segurança da Informação e Comunicações deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de segurança da informação e comunicações.

Subseção II

Do Tratamento e Classificação da Informação

Art. 10. A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços do MTE.

Art. 11. O MTE deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 12. Todo usuário deve ser capaz de identificar a classificação atribuída a uma informação tratada pelo MTE e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

Subseção III

Da Sensibilização, Conscientização e Capacitação

Art. 13. O MTE desenvolverá processo permanente de divulgação, sensibilização, conscientização e capacitação dos usuários sobre os cuidados e deveres relacionados à segurança da informação e comunicações.

Subseção IV

Da Contratação de Terceiros

Art. 14. Todos os contratos, convênios, acordos e instrumentos congêneres firmados pelo MTE devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta POSIC e das normas dela derivadas.

Parágrafo único. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta POSIC e suas normas complementares aos seus empregados e prepostos envolvidos em atividades no MTE.

Subseção V

Da Gestão de Riscos

Art. 15. As áreas responsáveis por ativos da informação devem implementar processo contínuo de gestão de riscos no âmbito de suas competências, o qual será aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações.

Subseção VI

Da Gestão de Continuidade

Art. 16. Todas as áreas do MTE devem promover a continuidade de suas atividades e serviços do MTE, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil, quando for o caso.

Art. 17. A resiliência do MTE contra possíveis interrupções de sua capacidade em atingir seus principais objetivos deve ser uma prática pró-ativa de todos os titulares de unidade administrativa, de forma a proteger a reputação e a imagem institucional do MTE.

Art. 18. As informações institucionais, se eletrônicas, devem ser guardadas nos ambientes de armazenamento, homologados pela área de tecnologia de informação do MTE e, se não eletrônicas, devem ser mantidas em local que as salvaguardem adequadamente, conforme as exigências legais.

Art. 19. A área de tecnologia da informação do MTE deverá manter Plano de Contingências, gradado de acordo com o grau de probabilidade de ocorrência do evento ou sinistro, estabelecendo o conjunto de estratégias e procedimentos que devem ser adotados em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

Subseção VII

Do Tratamento de Incidentes de Rede Computacional

Art. 20. A área de tecnologia da informação manterá Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, instituída pelo Comitê de Segurança da Informação e Comunicações, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

Subseção VIII

Do Uso dos Recursos de Tecnologia da Informação e Comunicações

Art. 21. Os recursos de tecnologia da informação e comunicações disponibilizados pelo MTE devem ser utilizados de acordo com seu propósito e seu uso deverá ser regulamentado em conformidade com a legislação vigente.

Parágrafo único. É expressamente proibido o acesso, guarda e encaminhamento de material não ético, discriminatório, malicioso, obsceno ou ilegal, por intermédio de quaisquer dos meios e recursos de comunicações disponibilizados pelo MTE.

Subseção IX

Da Auditoria e Conformidade

Art. 22. O cumprimento desta POSIC deve ser avaliado, periodicamente, em conformidade com normas complementares, manuais de procedimentos e legislação específica de segurança da informação e comunicações, buscando a certificação do atendimento dos requisitos de segurança da informação.

Art. 23. A área de tecnologia da informação manterá 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 MTE.

Subseção X

Dos Controles de Acesso

Art. 24. Devem ser instituídas normas que estabeleçam procedimentos, processos e mecanismos de controle de acesso às informações, instalações e sistemas de informação do MTE, com o objetivo de garantir a segurança dos servidores e a proteção dos seus

ativos.

Art. 25. Por questão de segurança, é obrigatório o uso de crachá de identificação para acesso e permanência nas instalações do MTE.

Art. 26. O usuário é responsável pela segurança dos ativos de informação que estejam sob sua responsabilidade e por todos os atos executados com suas identificações, tais como: crachá,

broche institucional, carimbo, login, senha eletrônica, certificado digital, assinatura digital e endereço de correio eletrônico.

Art. 27. Toda informação veiculada eletronicamente será alvo de controle e monitoração, e seu uso deve ser tão somente para fins corporativos relacionados às atividades do MTE.

Subseção XI

Da Propriedade Intelectual

Art. 28. As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual do MTE e não cabe a seus criadores qualquer forma de direito autoral.

Parágrafo único. Os direitos autorais relativos a programas de computador desenvolvidos por servidores ou colaboradores do MTE, durante a vigência de contrato ou de vínculo estatutário, no exercício de suas funções e com recursos do Ministério, pertencerão exclusivamente ao MTE.

Art. 29. É vedada a utilização de informações produzidas por terceiros para uso exclusivo do MTE em quaisquer outros projetos ou atividades de uso diverso do estabelecido pelo Ministério, salvo autorização específica pelos titulares das unidades administrativas, nos processos e documentos de sua competência, ou pelo Ministro, nos demais casos.

SEÇÃO V

DAS PENALIDADES

Art. 30. O usuário responderá disciplinar, civil e/ou penalmente pelo prejuízo que vier a ocasionar ao MTE, em decorrência do descumprimento das regras previstas nesta POSIC e demais normas internas e legislação vigente.

Art. 31. A desobediência às normas estabelecidas implicará na aplicação das sanções previstas em regulamentações internas e legislação em vigor.

SEÇÃO VI

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 32. Compete a Coordenação-Geral de Planejamento e Gestão Estratégica dar o suporte administrativo necessário à gestão da POSIC.

Art. 33. Cabe aos usuários de informações e sistemas do MTE:

I - conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta POSIC, bem como os demais normativos e resoluções relacionados à segurança da informação e comunicações;

II - obedecer aos requisitos de controle especificados pelos gestores da informação;

III - comunicar os incidentes que afetam a segurança dos ativos de informação e comunicações à Equipe de Tratamento e Resposta a incidentes em redes computacionais - ETIR; e

IV - assinar os termos de confidencialidade, responsabilidade e outros que venham ser instituídos por normas ou procedimentos decorrentes desta POSIC.

Art. 34. Independentemente da adoção de outras medidas, o titular da unidade administrativa deverá:

I - comunicar, de imediato, todo incidente de segurança que ocorra no âmbito de sua unidade à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR;

II - conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de segurança da informação e comunicações;

III - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação e comunicações; e

IV - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação e comunicações por parte dos usuários sob sua supervisão.

Art. 35. Cabe às empresas de prestação de serviço contratadas fornecer toda a documentação dos sistemas, produtos e serviços relacionados ao objeto do contrato.

SEÇÃO VII

DA DIVULGAÇÃO

Art. 36. Deverá ser dada ampla divulgação desta POSIC a todos os servidores e colaboradores do MTE, inclusive com publicação permane te na página da intranet do MTE.

Parágrafo único. Cabe ao Gestor de Segurança da Informação e Comunicações providenciar a divulgação interna desta POSIC.

Art. 37. Na apresentação de prestador de serviços contratado será entregue um exemplar desta POSIC.

SEÇÃO VIII

DA ATUALIZAÇÃO

Art. 38. Esta POSIC deverá ser atualizada, no máximo, a cada dois anos, a contar da data de sua publicação.

SEÇÃO IX

DA VIGÊNCIA

Art. 39. Esta POSIC entra em vigor na data de sua publicação.

Art. 40. Fica revogada a Portaria nº 1.327, de 11 de junho de 2010.

PAULO ROBERTO DOS SANTOS PINTO