UNIVERSIDADE DE BRASÍLIA
CENTRO DE DESENVOLVIMENTO SUSTENTÁVEL

A SEGURANÇA DA INFORMAÇÃO NO CNPq: Alinhamento à legislação e às boas práticas vigentes

Fábio Cezar de Oliveira

Orientadora: Profª. Drª. Isabel Teresa Gama Alves

Dissertação de Mestrado

Brasília-DF: Dezembro/2013

Oliveira, Fábio Cezar
A Segurança da Informação no CNPq: Alinhamento à legislação e às boas práticas vigentes / Fábio Cezar de Oliveira.
Brasília, 2013. 142 p. : il.

Dissertação de Mestrado. Centro de Desenvolvimento Sustentável. Universidade de Brasília, Brasília.

1. Política de Segurança da Informação. 2.Segurança da Informação. 3. Conformidade. I. Universidade de Brasília. II. CDS.

_____
Fábio Cezar de Oliveira

UNIVERSIDADE DE BRASÍLIA
CENTRO DE DESENVOLVIMENTO SUSTENTÁVEL

A SEGURANÇA DA INFORMAÇÃO NO CNPq: Alinhamento à legislação e às boas práticas vigentes

Fábio Cezar de Oliveira

Dissertação de Mestrado submetida ao Centro de Desenvolvimento Sustentável da Universidade de Brasília, como parte dos requisitos necessários para a obtenção do Grau de Mestre em Mestrado Profissional de Política e Gestão de Ciência e Tecnologia.

Aprovado por:

Profª. Drª. Isabel Teresa Gama Alves (CDS-UnB)
(Orientadora)

Prof. Dr. Marcelo Felipe Moreira Persegona (CDS-UnB)
(Examinador Interno)

Dr. Roberto Muniz Barretto de Carvalho (CNPq)
(Examinador Externo)

Brasília – DF, 16 de dezembro de 2013.

Dedico esta dissertação

À minha Mãe e ao meu Pai (em memória),
fundamentais para minha jornada até aqui.

À minha filha Mariana,
minha inspiração maior para prosseguir.

AGRADECIMENTOS

A Deus, porque tem sido a minha força e o meu refúgio nas horas de angústia, e pela graça de me conceder o privilégio de viver este momento.

Aos meus pais que, mesmo diante das lutas e dificuldades, nunca deixaram de incentivar a educação dos filhos, plantando em mim, também, essa vontade.

À minha filha Mariana, por todo amor e carinho que me dedica, pelo companheirismo, pelo cuidado, e pela compreensão diante das minhas ausências durante esse período de pesquisa.

À Minha irmã Zan, ao meu irmão Jim, e aos meus sobrinhos Ana, Larissa e Lukas, que mesmo distantes, me sustentaram com o seu incentivo, o seu amor, e as suas orações.

À minha orientadora Professora Isabel Teresa Gama Alves, pela disponibilidade em me conduzir neste processo, pelas palavras tranquilizadoras nos meus momentos de ansiedade.

Ao Professor Marcelo Persegona, que me despertou a ideia de desenvolver esse tema, pela disposição em me atender sempre que necessário, compartilhando o seu conhecimento e me transmitindo a sua confiança no sucesso do meu trabalho.

À minha amiga/irmã Leonara Rocha, pelo apoio em todos os momentos, principalmente, nos mais difíceis.

Aos professores, pela dedicação, respeito e amizade com que nos trataram, tornando muito prazerosa a nossa convivência.

Aos colegas do mestrado, pelo prazer de caminharmos juntos e pelas amizades verdadeiras surgidas a partir desse convívio.

Aos colegas da CGETI, em especial ao meu chefe Guilherme Reis, que desde o início apoiou a idéia deste projeto, e ao José Henrique, pelo apoio técnico concedido, sempre que necessário.

Ao CNPq, pela oportunidade que tem dado aos seus servidores de buscar conhecimento, e pela oportunidade que me foi dada de desenvolver este projeto, que espero possa ser aplicado em benefício de todos.

RESUMO

Este trabalho tem por finalidade apresentar um estudo de conformidade das atividades de Segurança da Informação e Comunicações do CNPq com as normas vigentes relativas ao tema. Realiza a análise de um conjunto de normas baixadas pelo Governo Federal e, também, de publicações especializadas do mercado, relativas à Segurança da Informação e Comunicações, fazendo um mapeamento de todos os controles determinados e sugeridos no escopo dessas publicações ou dessas normas, e, a partir dos subsídios fornecidos pela pesquisa, propõe a criação de um instrumento de verificação periódica de conformidade. Como resultado, apresenta os percentuais de conformidade encontrados no período de estudo, em relação a cada Norma estudada e, também, relativos a cada área que compõe o universo da Segurança da Informação e Comunicações, apresentando uma série de recomendações que visam melhorar a gestão de Segurança da Informação e Comunicações no CNPq. Indica, também, que o modelo utilizado no estudo pode servir de base para a criação desse instrumento proposto de verificação de conformidade.

Palavras-chave: Política de Segurança da Informação; Gestão de Segurança da Informação; Segurança da Informação; Conformidade.

ABSTRACT

This study has the purpose of presenting a CNPq Information and Communications Security compliance activities study, according to the current regulations on the subject. It analyzes the set of norms issued by the Federal Government. It also examines specialized market publications regarding Information and Communications Security, and maps out all the controls determined and suggested in the scope of these publications or these regulations. Based on the resources provided by this survey, it proposes the creation of an instrument for periodic compliance verification. As a result, it presents the compliance percentages encountered during the study period, pertaining to each norm studied, and also, in relation to each area that composes the world of Information and Communications Security, offering a series of suggestions, with the objective of improving the management of Information and Communications Security at CNPq. It also demonstrates that the model utilized in the study can serve as the basis for the creation of this proposed compliance verification instrument.

Keywords: Information Security Policy; Information Security Management; Information Security; Compliance.

SUMÁRIO

INTRODUÇÃO

O objetivo desta dissertação é analisar a adequação das ações de Gestão de Segurança da Informação e Comunicações no Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, verificando a sua conformidade com a legislação vigente, e com as principais publicações de boas práticas do mercado de Segurança da Informação, como as normas ISO/IEC 27002:2005 e ISO/IEC 27001:2006[1], que a partir deste ponto serão referenciadas apenas como Norma 27002 e Norma 27001. Também busca apresentar um modelo de instrumento que seja prático e eficaz para a aferição e o acompanhamento periódico do grau de conformidade, e oferecer subsídios para o planejamento e execução de ações que contribuam para melhorias na consolidação da política em Segurança da Informação e Comunicações da instituição.

A forma de verificação sugerida é a construção de um modelo contendo um conjunto de tabelas com os controles determinados nessas normas legais e manuais referenciados acima, em forma de uma *check list*. O Governo Federal tem recomendado fortemente que sejam seguidos os controles contidos na Norma 27001 e também, por intermédio do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), tem editado e publicado Instruções Normativas, que contêm um conjunto de Normas Complementares, com determinações específicas para os órgãos da Administração Pública Federal (APF), a respeito de cada tema relevante relacionado à Gestão de Segurança da Informação e Comunicações.

Essas determinações têm representado um grande desafio, no contexto atual da Gestão da Informação, para qualquer organização que se disponha a implementar uma Política de Segurança da Informação e Comunicações. Nos casos dos órgãos da APF, há uma determinação para que, em curto e em médio prazo, não apenas se reforce a infraestrutura física, lógica e normativa, mas que se crie uma cultura de Segurança da Informação, capaz de entender e acompanhar a evolução natural da informação na Web, um ambiente absolutamente sem barreiras físicas, e de proteger os ativos institucionais.

Daí este estudo torna-se necessário e obrigatório para o CNPq, considerando três principais fatores: primeiro fator consiste no fato de o CNPq ter uma quantidade significativa de sistemas, aplicações e informações em ambiente Web, e buscar continuamente implementar procedimentos adequados em Segurança da Informação; segundo é o grande

[1] As Normas 27001:2006 e 27002:2005 integram a família 27000, voltadas para a gestão de Segurança da Informação e Comunicações, publicadas pela *ISO (International Standards Organization) / IEC (International Electrotechnical Commission).*

interesse que o assunto tem despertado no âmbito do Governo Federal, que instituiu e tem aprimorado uma Política de Segurança da Informação e Comunicações, para os órgãos da APF; e, por fim, uma forte motivação para este estudo está no fato de não existir no CNPq, um instrumento de avaliação periódica da conformidade da Segurança da Informação (SI) em relação à legislação vigente e às boas práticas do mercado.

Para a validação do modelo de verificação de conformidade foram selecionadas, do conjunto de normas legais e publicações de boas práticas vigentes, algumas normas que trazem controles determinados no seu escopo e que têm sido considerados de maior importância e urgência pelos órgãos de gestão de Segurança da Informação e Comunicações do Governo Federal. Neste estudo foram selecionados os controles contidos na Instrução Normativa nº 01 (IN01) do GSI/PR, de 13 de junho de 2008, e em cinco normas escolhidas a partir do conjunto das 18 normas complementares da IN01, e também os controles contidos na Norma 27001, de certificação em Segurança da Informação, que tem servido de base para a política de Segurança da informação e Comunicações do Governo Federal e cuja observância vem sendo recomendada aos órgãos da APF.

Objetivo Geral

Contribuir para a melhoria da Segurança da Informação e Comunicações no CNPq, no que se refere à segurança física das instalações, equipamentos e documentos; à segurança lógica de sistemas e informações institucionais; e à segurança pessoal com relação à cultura organizacional e a processos internos.

Objetivos específicos

1. Contextualizar o ambiente atual da Tecnologia da Informação e Comunicações (TIC) do CNPq.
2. Analisar como o Governo Federal tem definido suas políticas de Segurança da informação para a administração federal.
3. Realizar levantamento de fatos históricos da TIC no CNPq.
4. Analisar como a Segurança da Informação vem sendo praticada e implementada no CNPq.
5. Levantar requisitos legais sobre Segurança da Informação para aperfeiçoamento da Política de Segurança da Informação do CNPq.
6. Estudar a conformidade da Segurança da Informação do CNPq em relação à legislação vigente.

7. Fornecer subsídios para a criação de um instrumento de avaliação da conformidade da Segurança da Informação do CNPq com a legislação vigente.
8. Fornecer subsídios para a implementação de melhorias na Gestão de Segurança da Informação do CNPq.

Metodologia

A metodologia utilizada foi a análise documental, consistindo de pesquisa bibliográfica, pesquisa documental dos serviços de TIC do CNPq, estudo da legislação vigente de Segurança da Informação e das publicações de boas práticas (Certificações) em Segurança da Informação, o mapeamento dos controles de conformidade existente nesses instrumentos, e a realização das verificações de conformidade junto aos gestores e aos profissionais de Segurança da Informação do CNPq.

Os documentos analisados, referentes à Tecnologia da Informação e Comunicações, compreendem registros de procedimentos efetuados de segurança e suporte como *backups, logs* de acesso à rede; registros de administração de banco de dados; *logs* de tráfego de emails; documentação de sistemas; documentação de auditorias de segurança; Plano Diretor de Tecnologia da Informação (PDTI); registros de incidentes; mapeamento das áreas físicas; documentação e licenças de software; análise dos procedimentos de proteção à rede, como instalação e gerenciamento de antivírus, de *firewall*, de *anti-span*; registros de bloqueios a sites maliciosos, dentre outros procedimentos, formais e informais que compõem o conjunto de ações que hoje garantem a continuidade do acesso à informação informatizada.

A legislação vigente compreende os instrumentos legais que definem o que deve ser implementado pelas instituições federais em relação à Segurança da Informação, enquanto que as certificações trazem recomendações das melhores práticas de mercado, bem como análise da Política de Segurança da Informação e Comunicações (POSIC) do CNPq e suas normas complementares em vigor.

Estrutura da Dissertação

A dissertação está estruturada em três capítulos. O primeiro procura apresentar conceitos e princípios que envolvem o ambiente de Segurança da Informação (SI) e responder o que é SI, qual a sua abrangência e a sua importância para as organizações. Procura fazer uma análise da Segurança da Informação no mundo e no Brasil, mostrando a

sua evolução e a sua ambientação no contexto tecnológico atual. Por fim, busca mostrar a importância que o Governo Federal tem dispensado ao assunto e às medidas para implementação de uma política permanente de Segurança da Informação no âmbito da APF. O capítulo constitui o referencial teórico sobre o tema.

O segundo capítulo demonstra os fatos históricos importantes em Tecnologia da Informação no CNPq, desde o inicio das suas atividades em Brasília, enfatizando os momentos de mudança tecnológica, e as atividades de Segurança da Informação relacionadas com cada período, desde a época da instalação do seu primeiro Centro de Processamento de Dados (CPD), com processamento centralizado, evoluindo para a tecnologia de distribuição do processamento em rede interna, e chegando ao momento atual com a implementação da maioria de suas aplicações em ambiente Web. Apresenta as mudanças que concorreram para a adoção de uma Política de Segurança da Informação e Comunicações (POSIC) e como essa política vem sendo implementada.

O terceiro capítulo propõe a análise dos procedimentos de Segurança da Informação no CNPq e o estudo da legislação brasileira em Segurança da Informação, e seleciona desse conjunto de leis, aquelas que trazem determinações de controles específicos para a gestão da Segurança da Informação. Analisa também a Norma 27001, com o seu conjunto de controles, que tem sido utilizada pelo Governo Federal na construção de sua Política de Segurança da Informação e Comunicações e cuja observação tem sido recomendada aos órgãos da APF. A partir dessas análises apresenta o estudo de conformidade do CNPq em relação a essas normas e propõe o instrumento de verificação periódica de conformidade com a legislação vigente.

Apresenta ainda, o quadro de conformidade do CNPq com o conjunto de normas selecionado para o estudo. Primeiramente, mostra a conformidade com cada uma das normas selecionadas e, também, mostra a conformidade com as principais áreas relativas à Segurança da Informação, e valida o instrumento proposto para verificação periódica de conformidade. A partir desse quadro, procura responder o que pode ser feito para alinhar a POSIC do CNPq à legislação vigente e às boas práticas de mercado. Faz uma análise dos resultados e os apresenta como subsídios para apoiar o aprimoramento da Gestão de Segurança da Informação no CNPq, demonstrando áreas já contempladas com algumas ações e outras carentes de ações efetivas, que devem ser considerados pela instituição em sua estratégia de implementar a sua POSIC, bem como uma cultura plena em Segurança da Informação e Comunicações.

A dissertação apresenta em sua conclusão a análise geral dos resultados do trabalho, mostrando a eficácia do instrumento utilizado e propondo que seja aperfeiçoado com a inclusão de novos parâmetros que possam fornecer mais informações de apoio à Gestão de Segurança da Informação e Comunicações. Enfatiza os pontos críticos levantados na pesquisa e faz um conjunto de recomendações que vão desde a implementação de ações que estabeleça a conformidade em itens verificados na pesquisa, até ações estratégicas para aperfeiçoamento da Política de Segurança da Informação e Comunicações do CNPq.

1. SEGURANÇA DA INFORMAÇÃO, PARA QUÊ E PARA QUEM?

Este capítulo trata da conceituação de segurança da informação e de sua contextualização no ambiente atual de Tecnologia da Informação e Comunicações (TIC), procurando apresentar as evidências de sua importância na continuidade das atividades das organizações, protegendo seus ativos relevantes e, também, garantindo a privacidade das pessoas.

Descreve a evolução da Segurança da Informação e Comunicações (SIC) ao longo do tempo, mostrando que garantir integridade, disponibilidade e confiabilidade de informações sempre constituiu um desafio para as organizações, principalmente em ambientes de Tecnologia da Informação e Comunicações (TIC), onde essa preocupação sempre esteve mais presente e que teve uma evolução constante, desde os primeiros Centros de Processamento de Dados, no tempo em que implementar segurança se restringia a manter um ambiente físico adequado e uma infraestrutura capaz de garantir o armazenamento seguro dos dados, até o contexto atual, em que a atividade de SIC ganha um espaço cada vez mais formal na Gestão da informação e se estabelece como uma área cada vez mais importante dentro das organizações, e que atrai cada vez mais atenção e investimentos.

No capítulo também é demonstrado, que nesse contexto atual constitui-se um grande desafio diário para gestores, garantir a proteção adequada para os seus ativos de informação contra ataques externos, em um mundo de virtualidade crescente, interconectado e sem barreiras físicas.

Faz parte do escopo de estudo a Política de Segurança da Informação e Comunicações (POSIC) do Governo Federal e os esforços que têm sido dispensados na implantação de POSICs nos órgãos que compõem a Administração Pública Federal (APF). É apresentado um histórico de ações que demonstram essa determinação do Governo, como a criação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e o seu Departamento de Segurança da Informação e Comunicações (DSIC), responsável pela elaboração e publicação de normas legais específicas para assuntos relativos à segurança da informação, e que tem determinado a implementação de controles contidos nessas normas, bem como recomendado a adoção de boas práticas do mercado, com o objetivo de regulamentar o uso da informação no âmbito da APF.

1.1. O QUE É SEGURANÇA DA INFORMAÇÃO?

Ainda que nos pareça uma ideia fácil de compreender, conceituar Segurança da Informação de forma exata não tem sido, até agora, uma tarefa fácil para os estudiosos no assunto. Marciano (2006) destaca que a literatura especializada traz, com abundância, conceitos que demonstram o que a Segurança da Informação faz, mas que não definem o que ela realmente é.

Antes de fazer um aprofundamento na conceituação de Segurança da Informação, tentando evidenciar os aspectos e as características mais importantes que a delimitam e assim chegar à compreensão de sua concepção e contextualização atual, é preciso compreender o conceito de Informação ou as dimensões que este conceito alcança nos dias atuais, e para efeito neste estudo, conhecer também como o Governo Federal define, para aplicação de sua POSIC no âmbito da APF, o que seja informação.

1.1.1. INFORMAÇÃO

Há registros na história, que desde os tempos pré-históricos a informação faz parte do cotidiano do homem, exercendo uma grande importância para sua organização social e sua sobrevivência. Essa importância estava explícita nas práticas relativas à sobrevivência humana, seja de um individuo em sua relação isolada com o meio ambiente, ou dos agrupamentos sociais de então, como tribos, clãs e aldeias, que mesmo antes do surgimento da escrita, procuravam transmitir o que sabiam de uma geração a outra, seja de forma oral ou pela demonstração e repetição das práticas cotidianas, ou ainda em desenhos grafados em cavernas ou pedras. Seguindo a história, observa-se que a informação sempre esteve presente na transformação ou evolução das sociedades, até os dias atuais, e com isso o desafio de proteger a sua integridade, de garantir a sua autenticidade e de utilizá-la ou disseminá-la de forma eficiente.

Porém, é no século XX, principalmente a partir do surgimento e da evolução dos computadores, do desenvolvimento das comunicações, e do aumento da interatividade entre pessoas e organizações, que a informação ganha uma importância ainda maior na sociedade. Afirmações como “informação é poder” ou “quem tem a informação tem o poder” ou ainda “o segredo é a alma do negócio” trazem embutida a percepção dessa importância e fazem parte de uma visão generalizada na sociedade, e assim, pessoas intuitivamente seguram ou disseminam informação de acordo com os seus objetivos. Essa importância levou ao surgimento de uma nova ciência, a Ciência da Informação, que dentre outras

preocupações, como o aperfeiçoamento da classificação, a guarda e a recuperação da informação, tem procurado, desde o seu surgimento, aperfeiçoar o conceito de Informação.

A sua complexidade e sua interdisciplinaridade são analisadas por Capurro e Hjorland (2007), e o que se percebe é que cada área do conhecimento trata a informação e busca defini-la de maneira aplicada. Em Tecnologia da Informação, por exemplo, é muito comum a confusão entre dado e informação. Date (2003) ao tratar de sistemas de banco de dados, afirma que a finalidade primordial de um sistema computadorizado é armazenar informação, logo em seguida ressalta a importância de distinguir dado e informação. A rigor, os bancos de dados armazenam dados e as regras dos sistemas geram informação a partir deles.

Le Coadic (1996), em *A Ciência da Informação*, define o conhecimento como o ato de conhecer, ato pelo qual o espírito apreende um objeto, e define informação como o conhecimento gravado, uma definição que contempla o aspecto físico da informação, porém, Pinheiro (2004) acrescenta que a informação de que trata a Ciência da Informação pode se apresentar de várias formas, como em um diálogo entre cientistas, em uma comunicação informal, em uma inovação, em uma patente, em práticas sociais, em um objeto ou numa fotografia, gravados ou não em uma base de dados.

Essa percepção de Pinheiro (2004) é corroborada em Araújo (2010), quando ele mostra os três aspectos da informação apresentados evolutivamente por Capurro e na segunda metade do século XX. O primeiro é o aspecto físico, enfatizando a dimensão material da informação, como um símbolo gravado em um tipo de suporte. O segundo aspecto é o cognitivo, apresentado nos anos 1970, no qual a percepção da informação não depende apenas do que está gravado ou de seu suporte, mas também do repertório de conhecimento de quem obtém a informação, e nos anos 1990, Capurro apresenta a informação como um fenômeno social. Nesse modelo a informação é apresentada como uma construção coletiva e intersubjetiva (CAPURRO, 2003 *apud* ARAUJO, 2010).

Ao considerar os esforços da Ciência da Informação, por meio século, em buscar uma definição do que seja Informação, podemos concluir que não é tarefa fácil reduzir o conceito a uma definição simples, que contemple todas as suas implicações, e exposta essa complexidade, busca-se para este estudo, um conceito aplicado ao seu objetivo, dentro do contexto de Segurança da Informação.

O conceito utilizado pelos gestores de SIC no âmbito da APF é o apresentado pela Norma 27002 que a considera um ativo importante para a manutenção dos negócios de qualquer organização:

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização, e conseqüentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectvidade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades.
>
> (ABNT NBR ISO/IEC 27002:2005, p. ix)

Essa definição traz em seu escopo, termos como “ativo” e “negócios”, que são habitualmente usados no mercado privado e pode nos parecer inadequados para se referir às atividades de uma instituição pública. Porém, o Governo Federal tem adotado essas terminologias ao disseminar a sua política de Segurança da Informação e Comunicações no âmbito da APF e, assim, esses termos aparecerão durante todo este trabalho. Ativo aparecerá sempre significando aquilo que tem valor para a instituição e Negócios significando as atividades fim da instituição.

1.1.2. SEGURANÇA DA INFORMAÇÃO

O que é segurança? A maioria das pessoas é capaz de responder a esta pergunta sem recorrer a livros ou a dicionários. Segurança é um conceito que está presente no cotidiano da sociedade atual como antagônico de violência ou de perda. Mas para buscar a conceituação de Segurança da Informação vale repassar pela definição do termo Segurança. O Dicionário Houaiss de Língua Portuguesa nos traz 15 definições para esse termo, das quais destaco três, de caráter mais abrangente:

> 1. Estado, qualidade ou condição de uma pessoa ou coisa que está livre de perigos, de incertezas, assegurada de danos e riscos eventuais, afastada de todo mal;
> 2. Estado, condição ou caráter daquilo que é firme, seguro, inabalável, ou daquele com quem se pode contar ou em quem se pode confiar inteiramente;
> 3. Conjunto de processos, de dispositivos, de medidas de precaução que asseguram o sucesso de um empreendimento, do funcionamento preciso de um objeto, do cumprimento de algum plano.
>
> HOUAISS (Dicionário da Língua Portuguesa, *on-line*)

O mais importante a se destacar nessas definições, e em outras semelhantes, é a mesma ideia de proteção a alguém ou a alguma coisa, ou de estar protegido de uma ação danosa de alguém ou de algo. Podemos observar um caráter de pró-atividade que nos conduz à ideia de que Segurança não se limita à reação a agressões ou a ações danosas de qualquer natureza, mas contempla a ideia de estar preparado para garantir proteção àquilo que se quer segurar.

Esse caráter pró-ativo também está presente no conceito de Segurança da Informação. Ao estabelecer a sua Política de Segurança da Informação e Comunicações para órgãos e entidades da Administração Pública Federal, o Governo Federal adotou a seguinte definição de Segurança da Informação:

> Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenadas, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.
>
> (Decreto Lei nº 3.505/2000)

A Norma 27002, em sua definição de Segurança da Informação, enfatiza a importância da informação para as atividades das organizações e a necessidade de protegê-la: "É a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócios" (ABNT ISO/IEC 27002:2005, p. ix).

1.1.2.1. Princípios Básicos em Segurança da Informação

Essa proteção torna-se cada vez mais necessária nos dias atuais em um ambiente que a informação se encontra armazenada em uma grande variedade de mídias e com muita liberdade de acesso e movimentação. Para garantir às organizações a certeza de uma gestão de Segurança da Informação eficiente, alguns princípios básicos devem ser observados. A Norma 27002 enumera três princípios básicos da segurança da informação: disponibilidade, integridade, e confidencialidade, conceituados abaixo, com a ajuda de Laureano (2005), POSIC/CNPq (2013) e Manual de Boas Práticas em Segurança da Informação/TCU (2007):

- **D**isponibilidade: É o que garante que a informação esteja disponível a pessoas ou processos, devidamente autorizados, sempre que for requerida. Este princípio está relacionado à continuidade dos negócios da organização, garantindo a não interrupção de fornecimento de informação a quem precisar.
- **I**ntegridade: É o princípio relacionado à fidedignidade da informação. É a propriedade de que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental.
- **C**onfidencialidade: A informação somente pode ser acessada por pessoas explicitamente autorizadas; É a proteção da informação para impedir que pessoas não autorizadas tenham acesso à mesma. O aspecto mais importante deste item é garantir a identificação e autenticação das partes envolvidas.

Em sua política de Gestão de Segurança da Informação e Comunicações, o Governo Federal considera outra propriedade com um principio básico da Segurança da Informação, definida a seguir:

- **A**utenticidade: Consiste na garantia da veracidade da fonte da informação.

Assim, o Governo tem apresentado esses princípios aos órgãos da Administração Pública Federal, na forma do acrônimo DICA, como os quatros princípios básicos da Segurança da Informação, a serem observados em suas políticas e procedimentos referentes à geração, guarda e disseminação da informação institucional.

Outros autores como Laureano (2005), Dias (2000), bem como o Manual de Boas Práticas em Segurança da Informação do TCU, apresentam, ainda, mais uma propriedade considerada como um princípio básico – o Não Repúdio:

- Não repúdio: Garante que ao ser executada qualquer operação de modificação, acesso, envio ou recepção de uma informação, esta não pode ser negada.

1.1.2.2. Áreas de atuação da Segurança da Informação

Esses princípios apresentados são essenciais para a implantação de uma gestão eficiente de SI e é muito importante que cada organização identifique e priorize quais são os seus requisitos mais importantes para proteção e continuidade dos negócios da instituição. Dias (2000), além de evidenciar a observância dos princípios, relaciona algumas perguntas importantes a serem feitas ao implementar um programa eficiente de SI:

> O que proteger? Contra que ou quem? Quais são as ameaças mais prováveis? Qual a importância de cada recurso? Qual o grau de proteção desejado? Quanto tempo, recursos financeiros e humanos se pretende gastar para atingir os objetivos de segurança desejados? Quais expectativas dos usuários e clientes em relação à segurança de informações? Quais as conseqüências para a instituição se seus sistemas e informações forem corrompidos ou roubados?
>
> (DIAS, 2000, p. 44)

Uma gestão eficaz de Segurança da Informação e Comunicações (SIC) pressupõe esse planejamento e a implementação de controles eficientes para atingir as metas dele decorrentes. A Norma 27001 traz em seu escopo controles agrupados em 11 áreas diversas que também têm sido consideradas pelo Governo Federal, ao instruir seus órgãos subordinados quanto aos procedimentos referentes à gestão de SIC. Ao estabelecer um planejamento para gestão de SIC, é imprescindível considerar algumas áreas essenciais para essa gestão, tais como:

a) Política de Segurança da Informação e Comunicações (POSIC)

A formulação de uma política para gestão de SIC é o primeiro passo na execução do planejamento para uma boa gestão de SIC. Ela deve conter as diretrizes que nortearão as ações de segurança e deve estar alinhada à missão do órgão. Deve ter o patrocínio da alta direção da instituição e ser capaz de envolver todo o corpo de trabalhadores da instituição para o desenvolvimento de uma cultura de SIC.

Além das diretrizes e ações estratégicas contidas em seu escopo, a POSIC deverá conter normas complementares que aborde cada assunto relativo à Segurança da Informação e Comunicações, que sejam aplicáveis ao negócio da instituição.

b) Segurança em Desenvolvimento de Sistemas

Esta é uma área que vem sendo muito observada e que tem atraído muito investimento de organizações públicas e privadas. O processamento centralizado ou distribuído em redes internas (LAN)[2] deu lugar aos sistemas Web[3] onde a aplicação fica muito mais exposta, bem com o tratamento da informação. Isso exige que se pense, *a priori,* em procedimentos especiais de segurança de dados e de códigos quando houver necessidade. O mercado tem provido os construtores de softwares com estudos sobre falhas de software, fraquezas exploradas por pessoas ou sistemas maliciosos, e com controles mínimos que devem ser implementados durante a construção ou no momento da compra de um novo aplicativo.

O Governo tem recomendado que as instituições da Administração Pública Federal observem esses procedimentos de segurança em desenvolvimento, aquisição e manutenção de sistemas. Essas recomendações vêm a partir dos órgãos de controle, que têm incluído em suas auditorias, verificações a respeito do assunto e sugerido que se observe boas práticas contidas em publicações tais como as listas da *Common Weakness Enumeration* mantida por *The MITRE Corporation*[4] (CWE/MITRE) e as listas do *Open Web*

[2] *LAN – Local Área Network* ou Rede Local.
[3] *Web* – Forma simplificada de se referir à rede que conecta computadores por todo mundo, a *World Wide Web (WWW)*
[4] MITRE é uma organização sem fins lucrativos que opera centros de pesquisa e desenvolvimento patrocinados pelo governo federal dos Estados Unidos da América (www.mitre.org)

Application Security Project - OWASP[5], bem como, que nos contratos de construção de aplicações esteja explícito o que se está controlando.

c) Segurança em Recursos Humanos

Este é considerado, por muitos autores, como o ponto mais sensível para se implementar uma política eficaz de SIC, porque não depende apenas de aplicação de recursos financeiros ou de melhorar uma infraestrutura de segurança com *firewalls, anti-virus* e outras barreiras tecnológicas, mas implica mudar a cultura em relação ao tratamento da informação. Um princípio observado em Segurança da Informação e Comunicações é aquele que diz que "uma corrente é tão forte quanto o seu elo mais fraco" e o aspecto humano tem sido considerado o ponto mais vulnerável na gestão de informação. Agentes maliciosos estão atentos aos recursos de segurança das organizações e muitas vezes investem suas forças de ataque usando a Engenharia Social, que consiste em explorar as fraquezas, a confiança ou a ingenuidade das pessoas em relação as suas atitudes cotidianas e seus descuidos habituais com a informação.

O que tem sido recomendado é que as organizações invistam em ações de conscientização em relação à importância de resguardar qualquer informação que seja sensível para a continuidade da atividade fim da instituição. Essas ações incluem a realização de eventos sobre o tema e confecção de cartilhas com instruções básicas sobre o tema; a criação de uma política de senhas fortes e instrução aos usuários em como praticá-la; a criação de uma política de mesa limpa, em que não fiquem à mostra informações que possam contribuir para o acesso de outros ativos vitais à instituição; a manutenção de uma política de tela limpa, em que o computador não fique aberto, como uma porta de entrada para o acesso a informações sensíveis, e que tenha mecanismos de travar automaticamente quando ficar um determinado tempo sem uso. Esses são exemplos de ações que contribuem para implantar uma cultura de valorização da informação.

d) Controles de Acesso

Essa é uma área que tem merecido a atenção das organizações há algum tempo. Um controle eficaz de acesso, tanto lógico quanto físico, contribui bastante para que outras áreas de segurança implementem com efetividade suas soluções. Um conjunto de

[5] OWASP é uma comunidade aberta, sem fins lucrativos, dedicada a capacitar as organizações para conceber, desenvolver, adquirir, operar e manter aplicações que podem ser confiáveis (www.owasp.org)

procedimentos deve ser adotado para garantir segurança no acesso a áreas restritas ou a ativos da instituição.

Em relação ao Acesso Lógico deve ser definido o acesso, de tal forma que um usuário acesse apenas o que ele precisa para a execução do seu trabalho. É o estabelecimento de uma política de acesso mínimo, sugerida nas boas práticas em Segurança da Informação e Comunicações, adotada pelo DSIC e recomendada, em suas normas legais, aos órgãos da Administração Pública Federal. Outra medida que combina Controle de acesso e gestão de ativos, é a separação de sistemas sensíveis em servidores diversos dos sistemas comuns, de tal forma que haja barreiras adicionais, por meio de *firewalls* e servidores de aplicação. Essas e mais um conjunto de pequenas medidas, associadas às novas tecnologias de Rede e de hardware, aumentam a proteção aos ativos de informação, facilitando a aplicação de outros princípios e a gestão de outros seguimentos de Segurança da Informação e Comunicações.

Em relação ao Acesso Físico, devem ser identificadas quais as áreas sensíveis e inventariados os ativos importantes da organização, a fim de que possam ter uma proteção adequada. Esses ativos devem estar em salas seguras com controles de acesso com tecnologias como biometria ou cartão, para pessoal devidamente autorizado. Em todas as áreas de entrada e saída das instalações físicas da organização deve existir um eficiente sistema de identificação de pessoal, que garanta acesso de acordo com a definição de função do identificado.

Esses controles são essenciais para que o trânsito de pessoas dentro da organização não se torne um fator de risco para a segurança da informação institucional.

e) Gestão de Continuidade de Negócios

A Gestão da Continuidade de Negócios é um dos assuntos mais importantes quando se trata de Segurança da Informação e Comunicações, aliás, traz no se próprio nome essa importância, ou seja, os negócios não podem parar. Para isso é preciso que se conheça bem o negócio da organização e tenha um planejamento que preveja o que fazer em caso de alguma crise ou desastre que tenha a capacidade de provocar uma descontinuidade nas atividades da organização.

As boas práticas de SIC têm estabelecido que é essencial a elaboração de um Plano de Continuidade de Negócios (PCN) e que esse Plano seja revisado periodicamente para

contemplar mudanças que sejam significativas em relação às estratégias da organização. Esse plano deve estar alinhado aos interesses estratégicos da organização e é de responsabilidade da alta direção do órgão.

Um PCN deve conter um conjunto de, pelo menos, três planos específicos que funcionam como um manual de procedimentos em caso de ocorrência de um incidente significativo para a continuidade das atividades da organização:

1) Plano de Administração de Crises.
2) Plano de Recuperação de Desastres.
3) Plano de Continuidade Operacional.

f) Gestão de Riscos

A *Federation of European Risk Management Associations (FERMA)*, citando a Norma ISO/IEC Guide 73 que trata do gerenciamento de risco, traz um conceito de risco que pode ser traduzido como uma combinação de probabilidade de um evento e suas conseqüências. A simples existência de uma organização com suas atividades estabelece a possibilidade da ocorrência de situações positivas ou negativas, que representam oportunidades ou ameaças ao sucesso dessas atividades.

A Gestão de Riscos inclui algumas atividades essenciais para o seu sucesso, como a identificação dos riscos inerentes à atividade da organização, o tratamento ou a aceitação desses riscos, de acordo com as estratégias da organização. Os riscos devem ser identificados e classificados em função do grau de probabilidade de ocorrência, se baixo, médio ou alto, e em termos de valor para a organização.

Na Gestão de Riscos, uma vez identificados e valorados os riscos, pode-se fazer um planejamento em que riscos sejam tratados ou não. A decisão de não tratar um determinado risco deve estar embasado em justificativa, que mostre a pouca influência da ocorrência de um evento associado a esse risco para as atividades da organização. Qualquer decisão em relação à gestão de risco deve estar alinhada às decisões estratégicas da organização.

A atenção à gestão desses assuntos em destaque, dentre outros, associados a monitoramentos cotidianos, garante grande parte da segurança dos ativos de informação que sejam sensíveis à continuidade e sucesso das atividades da organização.

1.2. A EVOLUÇÃO DA SEGURANÇA DA INFORMAÇÃO

As pessoas em geral relacionam, intuitivamente, os termos Informação e Segurança da Informação à Tecnologia da Informação e Comunicações. Porém, muito antes do surgimento do computador ou mesmo da teorização dos sistemas de informação, já havia uma preocupação em organizar, guardar e disseminar o conhecimento adquirido ou produzido, bem como, a preocupação em preservá-lo. Como já afirmamos, a informação sempre esteve presente na história do homem e na sua transformação através dos séculos e, portanto, precede o computador e a Tecnologia da Informação e Comunicações (TIC).

De fato, o surgimento do computador em conjunto com o aprimoramento das telecomunicações na primeira metade do século XX é, sem dúvida, um divisor de águas no relacionamento de pessoas e organizações com a informação. Não somente pela capacidade de armazenamento, de processamento dos dados, e da produção de informação que tinham essas máquinas, comparado com qualquer invento anterior, mas também pela aplicabilidade que em pouco tempo descobriu-se para essas máquinas que passaram a ter, em poucas décadas, uma importância vital para a sociedade, principalmente para as organizações, sejam governamentais, educacionais e científicas, ou comerciais.

Desde então, como conseqüência, o que se viu, também, foi o aumento da preocupação com a proteção a informações geradas e a dados armazenados. Isso nada mais é do que um olhar com o foco na segurança das informações, ainda que essa preocupação não apresentasse as formalidades e contornos que essa área tem assumido no contexto atual da Tecnologia da Informação.

O primeiro período da era dos computadores tem como marco o surgimento do *Electronic Numerical Integrator and Computer (ENIAC)*, considerado o primeiro computador a ser construído, pois ele representou uma revolução em termos de velocidade de cálculo e capacidade para realizar aplicações científicas complexas. Mas, foi o *Electronic Discrete Variable Automatic Computer (EDIVAC)*, seu sucessor, construído na mesma década, que utilizou uma arquitetura que foi, e continua sendo, modelo de quase todos os projetos de computadores subsequentes: a arquitetura de von Neumann[6] (FONSECA, 2007). Ele já utilizava o sistema binário e já utilizava programas armazenados juntamente com os dados.

[6] John von Neumann (1903-1957), matemático húngaro, propôs uma arquitetura de computadores na qual programas e dados pudessem ser armazenados no mesmo espaço de memória, uma inovação para a época que continua presente nos computadores atuais.

Nesse primeiro período, de computadores gigantes que ocupavam uma enorme área de instalação e pesavam toneladas, o que era exigido em termos de Segurança era um robusto e caro sistema de arrefecimento, por que essas máquinas eram muito sensíveis às variações de temperatura, e tinham a necessidade de manutenções freqüentes, principalmente pela queima das válvulas. Em um segundo momento, mesmo com a utilização transistores, essas máquinas ainda permaneciam muito sensíveis à interferência climática. O essencial era ter o controle do ambiente físico, com sala dedicada à sua instalação e uma climatização adequada para evitar a queima de circuitos.

Com a evolução do Circuito Integrado, surgem os computadores de terceira geração, na década de 1960, utilizando essa tecnologia (FONSECA, 2007). Os computadores eram construídos em quantidades maiores, em tamanhos menores e com maior capacidade de processamento. O software também evoluía e surgiam linguagens de programação bem mais aplicáveis à construção de sistemas comerciais. Os CPDs ainda eram tradicionais e os controles de segurança já contemplavam a realização de *backups*, além dos controles ambientais já existentes. As máquinas ainda eram muito sensíveis às variações climáticas.

O período de domínio dos grandes computadores, com processamento centralizado, se estende até o final da década de 1970, e nesse período a informação continuou a ser registrada, processada e mantida isoladamente, em ambientes protegidos por paredes físicas, seja em computador ou fora dele. As medidas de segurança se restringiam a controles de desastres físicos como incêndios, inundações, umidade excessiva, temperatura, que implicava organizar ações de proteção, como *backups* e controle no acesso de pessoas não autorizadas aos ambientes de manutenção das informações. Os sistemas eram em sua maioria grandes geradores de relatórios, ainda com uma característica totalmente operacional. Nesse período, a indústria de software começa a se desenvolver, dissociada da indústria de hardware.

Nas décadas de 1970 e de 1980, surgem os Sistemas de Gerenciamento de Banco de Dados (SGBDs), que organizam o armazenamento e otimizam a recuperação de informações. Os computadores aumentam exponencialmente as suas capacidades de armazenagem e de processamento de dados o que, além da ampliação do uso comercial dos computadores, contribui, de certa forma, para a implementação de visões gerenciais às bases de dados e para o surgimento dos sistemas de informações gerenciais. O impacto da evolução dos computadores começa a ser visível nas empresas e em produtos, mas o computador ainda é um instrumento invisível no cotidiano das pessoas e essa tecnologia

continua sendo vista como algo reservado a especialistas, e a atividade de computação continua internalizada em Centros de Processamento de Dados (CPD).

Porém, na década de 1970 surge o Microprocessador, considerado uma revolução tecnológica (PEREZ, 2000), que provoca o surgimento dos computadores de quarta geração. Um dos produtos dessa quarta geração é o computador pessoal, com sistemas instalados, que tiravam a computação de dentro dos CPDs e permitiam novas oportunidades de trabalho, aprendizado e lazer. Começa a mudar a relação da sociedade com a Tecnologia da Informação e Comunicações e, extrapolando, com a Informação.

Essa difusão dos microcomputadores provocou um crescimento exponencial da indústria de software comercial, representando um mercado de bilhões de dólares e atingindo milhões de pessoas no mundo inteiro. Com surgimento das redes de banco de dados e da internet, como hoje a conhecemos, há uma mudança do paradigma de relacionamento das pessoas com a informação em rede. O computador deixa, definitivamente, de ser uma ferramenta isolada em instituições e deixa de ser usado apenas por especialistas, e passa a fazer parte do dia-a-dia do cidadão comum. A exposição da informação tornou-se muito maior, assim como os riscos à integridade da informação e à privacidade de seus proprietários (LAUREANO, 2005).

No contexto atual de computação em rede mundial, segurança não se refere apenas à informação contida em bases de dados isoladas, ou a ações de Tecnologia da Informação e Comunicações, inclui também a relação atual do homem com o computador. A dependência do homem em relação ao computador é cada vez mais eminente e ainda que não se perceba, o computador é utilizado o tempo todo, mesmo em atividades cotidianas consideradas banais. A tecnologia de agora e do futuro é a computação móvel, em que se programa e acessa informações por meio de um dispositivo multiuso de mão, como um celular ou um *tablet*, e, nesse contexto, é muito grande o desafio para manter segura a informação em um ambiente tão aberto.

1.3. ATUAÇÃO DO GOVERNO FEDERAL EM SEGURANÇA DA INFORMAÇÃO

O Estado brasileiro tem passado por muitas mudanças por meio de ações de vários governos nas últimas décadas. A velha burocracia, caracterizada pelo acumulo de papel e pela pouca eficiência em suas ações, deu lugar a um estado que utiliza cada vez mais a tecnologia na busca de uma gestão dinâmica e eficaz. Não se pode afirmar que isso se deve

apenas a ações de governos, mas o avanço tecnológico na sociedade em geral contribuiu muito para essa mudança.

Quando olhamos um pouco para trás, podemos observar um certo caos em instituições governamentais, principalmente instituições com grande estrutura e grande capilaridade, com a movimentação de grande volume de informações. É muito difícil imaginar a existência de controles eficientes de informações, sigilosas ou não, em um contexto desses. Devido a isso, não é incomum ouvir histórias de perdas causadas por ineficiência de controles pelo Governo.

Muitas fraudes, envolvendo a coisa pública, que hoje são descobertas e são noticiadas à sociedade diariamente e que, em muitos casos, se chega à punição dos envolvidos, no passado encontravam um ambiente propício para a perpetuação de suas práticas, porque a sociedade não tomava conhecimento e os órgãos e as ferramentas de controle eram bem menos eficientes. Os governos não se preocupavam tanto com a transparência de suas ações e a sociedade não dispunha de mecanismos eficientes de acompanhamento e controle.

Governos sucessivos, a partir dos anos 1980, procuraram investir na informatização dos órgãos federais e em sistemas de acompanhamento de abrangência nacional, principalmente para o controle orçamentário e financeiro e também para órgãos com programas de atendimento à população. Por muitos anos, mesmo com o aumento da informatização, a grande maioria dos sistemas era composta de sistemas administrativos, com pouca informação gerencial e nenhuma visibilidade pela sociedade.

Na era pré-internet, o conhecimento das ações de governo se dava por publicações esporádicas, com resultados de ações da presidência, de ministérios e órgãos subordinados, o que limitava bastante o acesso da sociedade a essas informações. As informações ainda ficavam guardadas em suas instituições de origem, em processamento centralizado nos CPDs locais. Era um ambiente de pouca visibilidade, mas de fácil implementação da Segurança da Informação.

Mas, Segurança da Informação não era uma atividade que preocupava a maioria dos órgãos públicos. Esse era um assunto, que quando surgia, relacionava-se à esfera militar ou a órgãos de inteligência ou, ainda, órgãos de controle. Não havia, de um modo abrangente, uma diretriz de governo voltada para a disseminação da ideia que a informação fosse um

bem a ser protegido, ainda que muito já se falava da importância da informação no sucesso dos negócios das empresas.

Com a criação de redes de computadores e a popularização da Internet, surge um complicador na gestão dessa informação sob a responsabilidade dos órgãos públicos. Fica muito evidente a fragilidade dos meios disponíveis para proteger as informações sensíveis das instituições. Gerir informação não se limitava a organizar um bom CPD com alta capacidade de armazenamento e processamento, com rotinas seguras de *backup*, mas já se percebia a necessidade de criar novos mecanismos de segurança para essa informação institucional.

Nesse contexto, a Segurança da Informação passa a ser preocupação de todos, tanto do mercado quanto de governos, e os altos escalões de governo passam a coordenar ações para implementar uma política de SIC em toda a Administração Pública Federal. Essas ações passam tornam-se mais visíveis a partir da criação de uma estrutura de governo que tratava do assunto.

Em 1999, a Casa Militar – que era responsável não somente por assuntos militares, mas também pela proteção de interesses estratégicos do Estado e pela segurança de altas autoridades do governo – passa a se chamar Gabinete de Segurança Institucional da Presidência da República, ainda com um perfil militar e com atribuições relacionadas à defesa do país. Porém, começa a ampliar os seus objetivos e responsabilidades, e a implementar ações relacionadas às informações no âmbito da Administração Pública Federal, por intermédio de seu Departamento de Segurança da Informação e Comunicações (DSIC).

Em 13 de junho de 2000, o decreto 3.505, cria o Comitê Gestor da Segurança da Informação e passa atuar como apoio às elaborações de diretrizes da Política de Segurança da Informação, para os órgãos da Administração Pública Federal.

Atualmente, O DSIC, do Gabinete de Segurança Institucional da Presidência da República tem sido o órgão responsável pela implementação da política de gestão de segurança da informação no âmbito da Administração Pública Federal. Desde 2008, o DSIC tem publicado Instruções normativas e normas complementares, que determinam ações necessárias para a implantação da Política de SIC pelos órgãos da APF. Além disso, mantém equipes que interagem com os órgãos na troca de informações sobre eventos

ligados à SIC. Os órgãos da APF têm, por obrigação, que enviar informações relativas aos incidentes em rede, além das ações que estão sendo implementadas.

Em conjunto com o DSIC, o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), tem promovido ações de capacitação e conscientização em Segurança da Informação e Comunicações, como realização de eventos informativos, congressos com realizações de oficinas, divulgação de cartilhas, dentre outras. Ações que buscam contribuir para a implantação, no âmbito da APF, de uma cultura voltada para a valorização da informação como um ativo essencial para a vida das organizações.

Outro órgão bastante envolvido nas questões de SIC no âmbito do Governo é o Tribunal de Contas da União (TCU), que tem atuado, não apenas com um órgão de controle externo com ações de auditoria nos órgãos públicos, mas também como um disseminador de boas práticas em SIC. Da mesma forma que o SISP tem realizado eventos que contribuem para trocas de experiências, divulgado cartilhas de boas práticas em vários aspectos de Segurança da Informação e Comunicações.

Outros órgãos da esfera federal têm funcionado como parceiros do DSIC nessa busca por uma política de segurança para os órgãos do Governo. O Serviço Federal de Processametno de Dados (Serpro) tem prestado o apoio tecnológico e também divulgado suas práticas em SIC. A Controladoria Geral da União (CGU), órgão de controle que, dentre muitas funções, faz auditorias em órgãos no âmbito do Poder executivo, tem incluído em suas verificações, questionamentos relacionados às determinações do DSIC/GSI-PR e normas legais relativas à Segurança da Informação, e também tem feito sugestões para que os órgãos possam melhorar a segurança em suas atividades, o que se torna também um incentivo a que as instituições da APF implementem com celeridade as suas POSICs.

Nesse contexto de alta conectividade e de grande produção e disseminação de informações, o Governo tem se deparado com um grande desafio que é a questão do acesso à informação. O Governo publicou, em 2011, a Lei de Acesso a Informação, que visa garantir os direitos constitucionais de acesso à informação pública. Qualquer cidadão, sem precisar apresentar motivos, pode ter acesso às informações de qualquer órgão público, desde que não esteja protegida na forma da lei.

O Governo tem, atualmente, discutido a questão dos dados abertos que busca definir e delimitar o acesso às informações disponíveis na Web, para isso reforça ainda mais a

necessidade de gerir a informação com mais critério, observando todas as dimensões dos riscos envolvidos nessa atividade de guarda e disseminação da informação pública.

2. TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES NO CNPq

Este capítulo apresenta um histórico da Tecnologia da Informação e Comunicações (TIC) no CNPq, enfocando o período compreendido desde a transferência de sua Agência Central para Brasília, em meados dos anos 1970, até os dias atuais. Destaca os períodos de mudanças tecnológicas significativas pelos quais passou, mostrando a evolução das tecnologias utilizadas em cada período relativas ao hardware, ao software, à infraestrutura em geral, ao processo de desenvolvimento, às linguagens de programação, às bases de dados, e às metodologias empregadas.

Também discorre sobre os procedimentos relativos à Segurança da Informação e Comunicações que foram adotados pelo CNPq em cada um desses períodos, demonstrando que ações referentes a essa atividade foram implementadas de forma evolutiva – ainda que sem a formalidade e a visibilidade com que a Segurança da Informação e Comunicações é tratada atualmente –, em conformidade com a realidade da gestão da informação de cada período e com os controles pertinentes a cada contexto tecnológico.

Por se tratar de um histórico relativo a uma unidade interna do CNPq, não há uma disponibilidade de publicações substanciais que registre essa evolução no período apresentado. Dessa forma, grande parte das informações contidas neste capítulo foi gerada a partir da experiência e memória particular do autor, com o auxílio de algumas poucas publicações como PDTIs, publicações anuais de fomento, extrações em base de dados e informações contidas na página Web do CNPq, que corroboraram as ideias e os fatos apresentados.

Ao explanar tais fatos, o capítulo aborda procedimentos que vão desde as atividades básicas de segurança – como a realização de *backup* de dados e de sistemas, o controle de temperatura e de umidade, a estabilização da rede elétrica e demais controles de ambiente físico como portas fechadas e permissão de acesso somente para pessoas autorizadas em determinados ambientes, ações que eram praticadas desde os anos 1970 – até os controles implementados no contexto atual da Tecnologia da Informação e Comunicações, especificados e formalizados em uma Política de Segurança da Informação e Comunicações - POSIC, com a realização de auditorias, que garantem a salvaguarda de informações e a navegação segura, em um ambiente com grande conectividade e transferência de informações.

Antes de oferecer essa análise da evolução da Tecnologia da Informação e Comunicações no CNPq, bem como dos respectivos procedimentos de Segurança da Informação e Comunicações, relativos a cada mudança tecnológica evidenciada, o capítulo apresenta um breve histórico da instituição desde a sua criação – no qual se destacam alguns momentos importantes de transformação até chegar ao momento atual –, bem como a sua colocação na estrutura do Governo Federal, os seus sistemas de apoio ao fomento e a sua infraestrutura tecnológica para suportar essas atividades.

2.1. O CNPq: BREVE HISTÓRICO

O CNPq – Conselho Nacional de Desenvolvimento Científico e Tecnológico, criado em 1951, nasceu com o objetivo de coordenar e fomentar a pesquisa científica no País. A ideia de se criar uma agência que estimulasse a pesquisa já existia desde a década de 1930, quando o presidente Getúlio Vargas encomendou a criação de uma instituição que desenvolvesse a pesquisa no setor agropecuário (http://centrodememoria.cnpq.br /Missao2.htm), mas a proposta de criação de uma instituição que atuasse de forma mais abrangente, fomentando o desenvolvimento científico e tecnológico em diversas áreas do conhecimento, ganhou força após a Segunda Guerra Mundial, momento em que muitos países viram a necessidade de uma corrida em busca desse desenvolvimento, a fim de diminuir a dependência científica e tecnológica em relação aos países desenvolvidos, principalmente em física nuclear, em grande evidência no pós-guerra.

A questão nuclear funcionou, sem dúvida, como um catalisador na criação do conselho, ainda que o CNPq tenha sido idealizado para atuar no fomento a diversas áreas do conhecimento. O principal entusiasta de sua criação, e que se tornou o seu primeiro presidente, foi o Almirante Álvaro Alberto que, logo após a guerra, já a partir de 1946, vinha fazendo gestões junto à Academia Brasileira de Ciências, buscando apoio em favor da criação do Conselho. Nesse contexto, foi criada uma comissão com 22 cientistas, em 1949, para elaboração do texto do projeto de criação do Conselho, que resultou na lei 1.310 de 15 de janeiro de 1951, sancionada pelo então presidente Eurico Gaspar Dutra, que criava o Conselho Nacional de Pesquisas, nome original do CNPq, como uma Autarquia ligada diretamente à Presidência da República.

Já na década de 1950, o Conselho, estabelecido em um nível estratégico na Administração Federal, começa a se solidificar como uma importante instituição de fomento à pesquisa e começa a fomentar atividades em pesquisa de pesquisadores já reconhecidos e também, a investir na ampliação do quadro de pesquisadores, fomentando a formação de

recursos humanos qualificados para a pesquisa. A Estrutura organizacional do CNPq começa a crescer com criação de institutos de pesquisa e a incorporação de outros já existentes como o Instituto de Matemática Pura e Aplicada (IMPA), o Museu Paraense Emilio Goeldi (MPEG), Instituto de Bibliografia e Documentação (IBBD), transformado em IBCTI em 1976, o Instituto de Pesquisas Rodoviárias, entre outros. Ainda nessa década, o CNPq deixa as atividades da energia nuclear, que passam a ser executadas pela Comissão Nacional de Energia Nuclear (CNEN), criada em 1954.

Nas décadas seguintes até o fim da década de 1980, o CNPq não somente aumentou a sua estrutura, com a incorporação de outros institutos de pesquisas e a criação de agências regionais de atendimento a instituições e demandantes de bolsas e auxílios, mas também viu crescer a sua importância passando a se incorporar, já na década de 1960, a um grupo de instituições responsáveis pela formulação da política de C&T no país e, em 1972, o CNPq passou a ocupar a posição de órgão central do Sistema Nacional de Desenvolvimento Científico e Tecnológico. Essa atuação da instituição como ator principal na política de C&T no país cresceu até o início dos anos 1980, época da aprovação do III PBDCT, com vigência até 1985, em que o CNPq procurou ampliar o seu papel no cenário da C&T nacional. (Informações extraídas do site do Centro de Memória do CNPq).

Com a criação do Ministério da Ciência e Tecnologia (MCT), em 1985, o CNPq começou a perder o seu espaço na formulação de política de C&T, à medida em que o ministério passava a ocupar esse lugar central, e ainda em 1985, o CNPq deixa a vinculação direta com a Presidência da República e passa se vincular ao MCT. A partir daí, várias funções da instituição foram sendo transferidas gradativamente ao ministério e o CNPq foi se voltando de forma mais intensa à atividade de fomento à Ciência e Tecnologia. (Informações extraídas do site do Centro de Memória do CNPq).

Ainda segundo a página web do Centro de Memória do CNPq, nesse período de transição e ajustes em sua forma de atuação, o CNPq incorporou a Inovação em suas linhas de fomento com a participação da iniciativa privada, e com a inserção cada mais urgente da função social na produção de C,T&I foi instituída, em 1995, a nova missão do CNPq: “Promover e fomentar o desenvolvimento científico e tecnológico e executar pesquisas necessárias ao progresso social, econômico e cultural do País”. (Informações extraídas do site do Centro de Memória do CNPq).

Além dos institutos de pesquisa, o CNPq ainda manteve, até o ano de 1990 quando foram desativadas, quatro agências regionais – no Rio, em Recife, em São Paulo e em

Porto Alegre. Ao final dos anos 1990 o CNPq mantinha uma estrutura com as seguintes unidades vinculadas:

1. Administração Central – Brasília
2. Laboratório Nacional de Luz Sincrontron – LNLS
3. Centro de Tecnologia Mineral – CETEM
4. Instituto de Matemática Pura e Aplicada – IMPA
5. Instituto de Pesquisas da Amazônia – INPA
6. Museu Emílio Goeldi – MPEG
7. Centro Brasileiro de Pesquisas Físicas – CBPF
8. Observatório Nacional – ON
9. Laboratório Nacional de Computação Científica – LNCC
10. Laboratório Nacional de Astrofísica - LNA
11. Instituto Brasileiro de Informação em C&T – IBICT
12. Museu de Astronomia e Ciências Afins – MAST

Em 17 de agosto de 2000, o Decreto nº 3567 transferiu todas essas unidades de pesquisa para o Ministério da Ciência e Tecnologia, e o CNPq ficou reduzido às atividades que eram de competência de sua Agência Central, consolidando-se ainda mais como uma importante agência de fomento, com a adequação de sua missão, explícita no Regimento Interno do CNPq (Portaria n° 816, de 17 de dezembro de 2002): "O CNPq tem por finalidade promover e fomentar o desenvolvimento científico e tecnológico do País e contribuir na formulação das políticas nacionais de ciência e tecnologia".

Não é objeto deste estudo aprofundar na questão da atuação política do CNPq ou mesmo discutir a questão de perda de espaço ou diminuição no orçamento ao longo das duas últimas décadas, mas fazer entender a complexidade do momento atual, no que se refere ao volume de informação envolvido na atividade de fomento, e a complexidade atual dessa atividade, bem como a complexidade das tecnologias que a suportam. O contexto no qual estão inseridas as atividades atuais do CNPq justifica a necessidade de investimento em um ambiente tecnológico que garanta a agilidade, a segurança e a transparência que a sociedade exige de seus entes públicos.

A Tecnologia da Informação e Comunicações do CNPq, desde a transferência do órgão para Brasília, passou por várias mudanças até chegar à concepção atual. Para maior compreensão neste estudo, o período enfocado está dividido em quatro fases, apresentadas a seguir.

2.2. PRIMEIRA FASE: O INÍCIO DAS ATIVIDADES EM BRASÍLIA.

Esta fase, que começa em 1975 e vai até meados da década de 1980, iniciou-se com implantação do Centro de Processamento de Dados (CPD) em Brasília e a implementação de sistemas de suporte às atividades administrativas. Esse CPD era constituído por um computador central, considerado um minicomputador, com poucos terminais ligados diretamente a ele. Nessa época, não havia a concepção de distribuição do processamento em rede, o terminal era ligado diretamente à unidade central do computador, por isso a capacidade de terminais de trabalho era bem limitada.

Apesar de não ser considerado um equipamento de grande porte para os padrões da época, esse computador, de marca Data-General e modelo C-330, mantinha as características de *mainframe*, com processamento centralizado, ocupando uma grande sala com sua unidade de processamento central (CPU), seus dispositivos de armazenamento em disco, e suas unidades de processamento de fita magnética. Essas instalações representavam uma conformidade tecnológica com o que existia de moderno para a época e era capaz de atender às necessidades de então, mas com pouca margem para suportar um crescimento, tanto de processamento quanto de volume de dados armazenados.

Nesse período, o conjunto de sistemas suportados pela Tecnologia da Informação do CNPq era composto basicamente por sistemas administrativos, que suportavam as rotinas administrativas da própria agência central, das agências regionais e dos institutos de pesquisa, vinculados ao CNPq. Os sistemas implementados eram o Sistema de Folha de Pagamento, Sistema de Contabilidade, Sistema Orçamentário e Financeiro, Sistema de Material e Patrimônio, e todo o desenvolvimento, a manutenção e a operação desses sistemas eram feitos em Brasília. As informações dos institutos chegavam por malotes e eram inseridas na base por uma equipe permanente de digitadores.

Além desses sistemas, foram desenvolvidos alguns sistemas de apoio à atividade de fomento. O Sistema de Bolsas e Auxílios, que foi um embrião dos sistemas de fomento posteriores, limitava-se a registrar a demanda por bolsas e auxílios e o resultado final dos julgamentos, muito mais para efetuar o pagamento da concessão do que visando à guarda dessas informações sobre os projetos para uma utilização gerencial mais qualificada. A grande característica do processo de informatização dessas rotinas era a permanência de uma forte interferência manual no processo, com grande parte das atividades de cada rotina permanecendo fora do sistema computadorizado.

Os produtos desses sistemas, tanto os administrativos quanto o de bolsas e auxílios, eram puramente operacional como as folhas de pagamento de bolsistas; os controles orçamentários, financeiros e contábeis; a folha de pagamento de funcionários; o cadastramento dos bens do patrimônio e dos bens em comodato, com atividades básicas de cadastramento e atualização de dados, cálculos, emissão de relatórios. Havia uma forte cultura de utilização de relatórios, tanto na forma de insumo para atividades diárias como na forma de *backups*, talvez pela desconfiança na eficácia dos sistemas e dos arquivos computadorizados em garantir a integridade das informações.

Essa desconfiança e a conseqüente tentativa de garantir segurança e continuidade das atividades é compreensível e muito pertinente, porque se olharmos para trás com a nossa concepção atual de Segurança da Informação, veremos um ambiente totalmente caótico, com controles mínimos não conseguiam garantir confiabilidade, integridade e disponibilidade da informação utilizando apenas o ambiente computacional. A Segurança da Informação estava muito mais ligada à manutenção da infraestrutura e do hardware do que à integridade do software e das informações. A grande preocupação em termos de continuidade das atividades recaia sobre os controles climáticos e instalações, uma vez que esses computadores tinham circuitos ainda muito sensíveis à variação e temperatura e umidade, e a realização de *backups* de sistemas e de dados.

Nessa primeira fase, usava-se uma linguagem de programação única para todos os sistemas, o MUMPS[7], que era uma linguagem ágil para o desenvolvimento, mas frágil em termos de segurança de código e de dados. Não havia separação de ambientes para cada sistema, nem entre ambientes de produção e desenvolvimento, de tal forma que a exposição das informações de um determinado sistema era muito grande, não somente aos analistas e programadores daquele sistema, mas também a todos os outros analistas e programadores, e muito mais grave, até a agentes maliciosos que poderiam praticar ações que iam desde uma modificação de informações até a eliminação de um ou vários registros inteiros de informação. Não havia um método de desenvolvimento e nem um profissional dedicado à administração dos dados, o que tornava o analista ou programador senhor absoluto do seu sistema, utilizando o método ou a falta de método que lhe conviesse.

[7] Massachusetts General Hospital Utility Multi-Programming System (MUMPS), é uma linguagem desenvolvida na década de 1960, a principio, para uso em hospitais ou na área da saúde. Era uma linguagem interpretada, ou seja, não utilizava compiladores para transcrever a linguagem para um código de máquina. A eliminação dessa etapa de compilação agilizava o desenvolvimento.

As informações eram armazenadas em uma estrutura de dados chamada Global. Uma Global se constituía em um arquivo seqüencial estruturado em níveis, em que o próprio programador ou analista calculava suas chaves de acesso, com o objetivo de distribuir a informação de forma a garantir melhor eficiência na sua armazenagem e na sua recuperação. Não existia ainda nesse ambiente uma estrutura de banco de dados com padrões de transações, com confirmação de uma inclusão ou alteração, ou opções para desfazer uma ação equivocada. Uma vez executada a ação, o registro estava alterado de forma definitiva. Não era incomum recorrer-se aos *backups* para buscar a restauração de um registro ou de um arquivo danificado por um erro de programação ou uma ação involuntária.

A estrutura de *backup* era compatível ao existente no mercado de então. Eram feitos *backups* diários, semanais, mensais e anuais, em um processo denominado processamento *batch*[8], rodados à noite e para isso os sistemas ficavam indisponíveis, durante a sua realização. Essa programação de *backup* garantia uma integridade relativa dos arquivos, mas era freqüente a perda de dados ou de versões de programas, o que implicava re-trabalho não apenas dos profissionais de informática, mas também de usuários. Podemos afirmar que esse era um ambiente muito inseguro para as informações digitalizadas e em conseqüência, a continuidade de negócios era garantida por ações extra-sistemas, em uma cultura de guardar pilhas e pilhas de relatórios com espelhos das informações armazenadas.

Aos poucos o próprio crescimento da demanda por fomento e, também, por informações mais qualificadas mostrou a fragilidade desse modelo e a necessidade de melhorar a capacidade de armazenamento de dados com uma tecnologia que não somente facilitasse o trabalho de analistas, de programadores e de suporte, mas também aumentasse a confiança do usuário em relação às informações digitalizadas.

2.3. SEGUNDA FASE: A TECNOLOGIA DE BANCO DE DADOS E OS PRIMEIROS SISTEMAS GERENCIAIS.

A segunda fase inicia-se em meados dos anos 1980, ainda com uma tecnologia de processamento centralizado, mas, além dos sistemas administrativos já existentes, começam a surgir as primeiras ideias de sistemas gerenciais relativos ao fomento. A atualização da infraestrutura de hardware, com a compra de novos computadores,

[8] Processamento *Batch* é o processamento de dados que ocorre em lotes de tarefas enfileiradas, de tal forma que o sistema operacional só processa uma tarefa após o término da tarefa anterior. Geralmente o termo Processamento *Batch* aparece em oposição ao termo Processamento *On-line*.

representa um avanço importante para a instituição, que já começava a perceber o aumento da demanda por suas linhas de fomento. Além disso, a construção de rotinas gerenciais demandava mais espaço em disco e mais capacidade de processamento.

Essa atualização da infraestrutura melhora significativamente a capacidade de processamento e otimiza, também, o armazenamento e a recuperação da informação. Alguns sistemas começam a utilizar Banco de Dados Relacionais, como tecnologia de dados, em paralelo à maioria dos sistemas que permaneciam na estrutura antiga, utilizando arquivos Globais do sistema MUMPS, já citados. Nessa fase ainda há pouca interação *on-line* do usuário com o computador ou com os sistemas. Predomina-se o processamento *batch*. Os sistemas, principalmente os ligados ao fomento, começam a implementar rotinas com informações gerenciais, porém mantendo as suas rotinas e características operacionais. Com a utilização de Banco de Dados relacional, surgem sistemas que começam a trabalhar com uma maior qualificação da informação, como o Sistema em Linha de Acompanhamento de Projetos (SELAP). O SELAP e o Sistema de Bolsas e Auxílios, já transformado em Sistema Gerencial de Fomento (SIGEF), começam a ganhar características gerenciais, com a produção de informações consolidadas que apoiaram várias publicações do CNPq.

O CNPq começava a criar novas linhas de fomento à pesquisa, bem como a adotar o sistema de concessão de bolsas por cotas[9], e na segunda metade da década de 1980, já se via um grande crescimento na demanda e um aumento na complexidade dos julgamentos e concessão de bolsas e auxílios à pesquisa. Além disso, os sistemas começam a armazenar uma grande quantidade de informações, visando o fornecimento de informações qualitativas do fomento, e isso aumentou o volume de informações guardadas nos bancos de dados. No final dessa década surgiu a ideia de se criar uma base de dados com currículos de pesquisadores e de postulantes a qualquer fomento concedido peloo CNPq e, assim, surge a primeira versão do Banco de Currículos. A capitação das informações era feita em formulários de papel e o CNPq, além de começar a usar essas informações nos editais de fomento, já disponibilizava informações curriculares a universidades e a instituições de

[9] Essa forma de fomento destinava cotas de bolsas aos cursos de mestrado e doutorado no país, seguindo as prioridades de fomento do governo e mediante o mérito de cada curso, de acordo com avaliação periódica feita pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). A responsabilidade de indicação individual de bolsista passava a ser do curso contemplado com as cotas.

pesquisa, por meio da BITNET[10], uma rede precursora da Internet, utilizada no meio acadêmico.

Em relação aos sistemas administrativos, a grande mudança foi a iniciativa do Governo em centralizar em um sistema nacional, todas as atividades referentes aos sistemas Financeiro e de Pessoal, e já no final da década de 1980 implementou-se o Sistema de Administração Financeira (SIAFI) que acrescentou, no caso do CNPq, um grau de complexidade na gestão da área financeira: a dupla alimentação de dados nos sistemas. O Sistema Financeiro interno do CNPq que continuava a operar e o externo (SIAFI), alimentado via Rede Serpro, ambos mantendo características estritamente operacionais. O sistema interno do CNPq utilizava uma estrutura precária com informações ainda armazenadas nos arquivos Globais MUMPS, portanto, sem utilizar a segurança oferecida pela tecnologia de banco de dado relacional. Para a Segurança da Informação cria-se uma situação paradoxal: se por um lado havia a segurança de que as informações da instituição estavam guardadas sob a responsabilidade do Governo federal, por outro a convivência de dois sistemas com a mesma finalidade criava situações de inconsistência que colocava, constantemente, em dúvida a confiabilidade e a integridade da informação.

Surgem os primeiros estudos e experiências na implantação de tecnologias *Workflow*[11] para o sistema de protocolo, visando otimizar a tramitação de documentos, tanto administrativos quanto de fomento. Essa iniciativa vislumbrava, também, a digitalização futura de todos os processos das atividades da instituição, porém, ainda havia uma predominância de papel, formulários de entrada e relatórios de saídas, formando grandes volumes de informação em paralelo às digitalizadas. Uma redundância que, percebe-se ao olhar para trás, representava um risco ao uso adequado da informação. Havia uma grande exposição da informação em circulação sem o devido acompanhamento e descarte seguro, quando necessário, sem que isso representasse uma preocupação para os gestores da época.

Ainda em relação à segurança da informação dessa época, o que se pode dizer é que houve um avanço em relação às instalações, com a aquisição de *no-breaks* e com a melhoria nos controles de temperatura e umidade do ambiente. A ferramenta de *no-break*,

[10] A BITNET foi uma rede criada na década de 1980 e era utilizada na transferência de arquivos entre computadores em instituições educacionais e de pesquisa na América do Norte, América do Sul, Europa e Japão. Na década de 1990 a BITNET foi suplantada pela Internet.

[11] Workflow é a tecnologia que permite a automação de um determinado fluxo de trabalho e a troca de informações interdepartamentais. É bastante utilizada na tramitação de documentos digitalizados.

ainda que com uma pequena capacidade, garantia a sustentação de energia, por um tempo mínimo necessário, para que se encerrasse processamentos em andamento, o que diminuiu bastante a perda de trabalho tanto em dados, como em códigos de programas. Os computadores mais modernos, já não eram tão sensíveis à variação de temperatura e umidade, bem como as mídias utilizadas para armazenamento e para *backups.* A tecnologia de Banco de Dados Relacional tinha procedimentos transacionais que garantiam maior segurança na inclusão, alteração e exclusão da informação, e a perda de dados, bem como a necessidade de se requisitar informações de *backup*, diminuíram sensivelmente.

A tecnologia para realização de *backup* tem uma significativa melhora, para alguns sistemas, mas ainda em mídias limitadas. Ainda podia-se constatar muita perda de dados, com um conseqüente volume de re-trabalho, que também representava uma certa ineficiência em relação à confiabilidade e à integridade da informação.

Como o processamento continuava centralizado em uma única sala, o controle de acesso físico consistia apenas de barreiras como portas e trancas nas salas dos computadores. Havia ainda muita exposição de equipamentos e informações. Essa não era uma preocupação primordial nessa época.

O final dessa década e o início da década de 1990, marcam o momento da convivência com uma diversidade de tecnologias, não somente de softwares, mas também de hardware, com a aquisição dos primeiros microcomputadores.

2.4. TERCEIRA FASE: A DESCENTRALIZAÇÃO DO PROCESSAMENTO

Essa fase inicia-se com a entrada da década de 1990 e sua principal característica é a diversificação da infraestrutura de hardware, que mantém um computador central, mas em paralelo já se começa um processo descentralização, com a compra de microcomputadores e a instalação de uma rede local, com alguns sistemas já sendo construídos utilizando a tecnologia Cliente/Servidor, que descrevendo de forma simplificada, consiste em executar os aplicativo ou sistemas, no microcomputador do usuário (cliente), e ter os recursos de rede e de banco de dados controlados pelo computador instalado no Centro de Dados (Servidor). Começa uma fase de maior interação *on-line* do usuário com os sistemas. O usuário começa a perceber o computador mais próximo de suas atividades.

Foi a fase em que os sistemas, tanto administrativos quanto de fomento, passaram por grandes modificações em seus processos. O Governo aperfeiçoava os controles

implantados no SIAFI e começava a implementar as primeiras rotinas do Sistema de Administração de Pessoal (SIAPE), utilizando a mesma plataforma e mesmo protocolo de comunicação com a Rede Serpro. O SIAPE implementou, inicialmente, as rotinas de pagamento, em que os órgãos da APF enviavam as informações em mídia magnética, no caso do CNPq fitas magnéticas, obedecendo a um cronograma único estabelecido para todo o Brasil.

Para os órgãos que, por não possuir uma infraestrutura própria de TIC, já executavam suas folhas de pagamento utilizando a estrutura do Serpro, a mudança foi mais tranquila, uma vez que já se configurava ali uma dependência tecnológica, mas no caso do CNPq já existia um Sistema de Pessoal com rotinas que iam além das implementadas no SIAPE e isso resultou em um ingrediente a mais na complexidade da gestão do sistema como, por exemplo, a dupla digitação de informações cadastrais e de folha de pagamento.

Ainda no início dessa fase, o CNPq investiu na criação de um formulário eletrônico de currículos, que eram preenchidos e enviados em disquetes para o CNPq e gravados na base de dados de currículos, era uma nova versão do Banco de Currículos conhecida como BCUR, um precursor do Curriculo Lattes que aparecia na década seguinte. Havia uma convivência, nem sempre pacífica, de várias tecnologias tanto de hardware quanto de softwares, que funcionavam em sua maior parte isoladamente, com muito trabalho para se consolidar informações gerenciais.

Ainda nessa década, os sistemas começam a usar a interface Windows e quase todos eram desenvolvidos usando tecnologia Cliente/Servidor. Surgem novos sistemas como o Lattes Fomento, uma evolução do SIGEF, mas que implementa apenas algumas fases do fomento, trabalhando, assim, em paralelo com o sistema antigo, o que representou um complicador para a consolidação de informações do fomento, uma vez que os dados eram armazenados em bases diferentes; o Sistema Integrado de Recursos Humanos (SIRH), substituindo o antigo sistema de Pessoal; o sistema CONFIO, substituindo o antigo sistema financeiro e orçamentário; e o Governo Federal consolida e amplia cada vez mais os seus sistemas de acompanhamento Financeiro e de Pessoal, o SIAFI e SIAPE, respectivamente.

Houve um grande aumento, a cada ano, no numero de bolsas no país, incluindo bolsas de formação e de pesquisa, passando de um patamar de 30.000 bolsas/ano no início da década para um patamar de 45.000 bolsas/ano (Dados aproximados a partir de informações das publicações *O Fomento do CNPq nos Estados e Instituições de pesquisa*,

década de 1990). Esse aumento, em conjunto com o crescimento da base do Curriculo Lattes, representa também, um aumento substancial no volume de dados e no volume de processamento de informação, que passa a exigir uma infraestrutura cada vez mais robusta para suportar essas atividades.

Nessa fase, bem como nas duas anteriores, a maior parte das preocupações com Segurança da Informação restringia-se a questões de infraestrutura e à segurança de dados. Melhorou-se a estrutura de *No-break*, que garantia a continuidade e encerramento seguro das aplicações e uma estrutura de *back-up* que minimizava a perda de dados e de versões de programas. A rede interna era distribuída com roteadores por andar, que facilitava a manutenção. Mas nessa fase o risco de infecção por vírus ou corrupção da informação via softwares maliciosos era quase inexistente, o que faz com que concluamos que os riscos para o mau uso da informação relacionavam-se aos próprios procedimentos dos sistemas, da inftraestrutura e das pessoas.

2.5. QUARTA FASE: A INFORMAÇÃO EM AMBIENTE WEB.

Na quarta e atual fase, que teve início no final da década de 1990, começa a migração definitiva dos sistemas para o ambiente Web. Essa mudança de concepção, visando colocar as atividades de Tecnologia da Informação e Comunicações (TIC) do CNPq no contexto mundial da informação, levou o órgão a investir na mudança substancial de sua infraestrutura de TIC e também no aperfeiçoamento de seu processo de desenvolvimento, aquisição e manutenção de sistemas.

Essa mudança de concepção traz consigo o aumento na complexidade de controlar esse ambiente. A infraestrutura para suportar essas atividades é reforçada com soluções de proteção, que vão além da simples guarda de dados em bancos seguros ou na robustez e qualidade dos programas. Essa infraestrutura inclui servidores de aplicação, servidores de *firewalls*, atualização de *anti-virus,* monitoramento de rede, monitoramento de tráfego de emails. Essas atividades de suporte estão isoladas em sala com acesso restrito de pessoas, controlado por biometria, assim como todos os servidores estão em uma sala cofre com acesso, ainda mais restrito, somente aos gerentes e profissionais relativos à operação e manutenção de hardware.

No momento atual do ambiente de TIC do CNPq, a quase totalidade do processamento de informações relativas à atividade de fomento está em ambiente Web. Formulários de propostas, emissão de pareceres, atualização de currículo *on-line* permitem

a otimização dos julgamentos, constituindo as duas principais plataformas de sistemas do CNPq, a Plataforma Lattes e a Plataforma Carlos Chagas. Muitas funcionalidades de sistemas internos, administrativos, também foram migradas e têm acesso via internet, buscando a padronização de acesso a todos os sistemas.

Atualmente, são 44 sistemas implantados, suportados por uma infra-estrutura de mais de 100 servidores centrais, com aproximadamente 1000 estações de trabalho distribuídas pela instituição. A capacidade de armazenamento instalada é de 200 terabytes. O acesso a esses sistemas é feito através do Portal do CNPq, mas não por uma entrada única, alguns sistemas estão agrupados em plataformas separadas, de acordo com a sua aplicação. Duas grandes plataformas foram desenvolvidas e funcionam como um "guarda chuva'" para aplicações afins: a Plataforma Lattes e a Plataforma Carlos Chagas.

A Plataforma Carlos Chagas funciona como um facilitador para bolsistas e pesquisadores brasileiros e estrangeiros acessarem informações operacionais relativas ao fomento em geral. Ela reúne dados do fomento à bolsas e auxílios, de encaminhamento de projetos, andamento de processos, emissão de pareceres, relatórios técnicos e prestação de contas, entre outras facilidades.

A Plataforma Carlos Chagas suporta anualmente, a submissão de 86.000 propostas, a emissão de 400.000 pareceres diversos, 81.000 indicações de bolsistas (Dados extraídos da Base de dados de fomento, referência Ano 2012).

A Plataforma Lattes integra as bases de dados de Currículos, de Grupos de pesquisa e o Diretório de Instituições em um único Sistema. Ela representa um importante instrumento para o planejamento e ações operacionais do fomento no CNPq. O Currículo Lattes é amplamente utilizado atualmente por instituições de fomento, universidades e institutos de pesquisa de todo o País. A disponibilização da Plataforma na internet é um facilitador para o usuário externo ao CNPq e dão mais transparência às atividades do CNPq.

A Plataforma Lattes conta com três milhões de currículos cadastrados, sofre anualmente cinco milhões de atualizações em currículos, e aproximadamente 500.000 currículos novos são cadastrados (Dados extraídos da Base de dados de currículos, referência Ano 2012).

Os sistemas de fomento da Plataforma Carlos Chagas e da Plataforma Lattes, têm disponibilidade de acesso 24 horas por dia, com acessos provenientes de todas as partes

do mundo. Nesse contexto, torna-se imprescindível aprimorar as atividades que garantam disponibilidade, confiabilidade, integridade e autenticidade da informação. As atividades de proteção a sistemas e informações não se restringem à realização de *backup* ou à manutenção da estrutura física, mas depende de uma série de monitoramentos constantes e do desempenho de atividades diárias que garantam essa proteção. Para suportar atividades que envolvem tais volumes de processamento e de armazenamento de dados, torna-se necessário que se tenha um planejamento eficiente de ações em curto e médio prazo, para atender não somente a demanda imediata por informações, mas, também, prover a infraestrutura necessária no futuro.

Atualmente, o CNPq, além de melhorar a sua estrutura física e o controle do ambiente, investiu na modernização do seu Centro de Dados, com equipes especializadas que monitoram ações em cada área sensível da TI. Essa organização permite não somente uma organização do trabalho de tal forma que facilite o gerenciamento, mas que também contribua para um ambiente seguro para a informação.

Além da organização do processo de desenvolvimento de aplicações, no Centro de Dados essas equipes monitoram, utilizando ferramentas adequadas, todas as atividades relativas às atividades que utilizam a rede do CNPq. Há o monitoramento da Rede com atividades como, verificação de gargalos, de possíveis ataques, de volume de tráfego, manutenção de listas negras com sites proibidos ou perigosos. Há o monitoramento constante do envio de mensagens estabelecendo limite para transmissão de arquivos, controle de padrão para criação das contas, controle de criação e exclusão de conta de email, monitoramento e impedimento de *spans*. A equipe de Banco de Dados controla a capacidade de armazenamento, faz previsões de atualizações necessárias para o futuro, e administra o desempenho do banco de dados.

Todas essas características do parque tecnológico instalado nesta nova sede do CNPq aliadas à complexidade de suas atividades de fomento, implementadas em diversos sistemas, criam um ambiente em que, mais do que atender às determinações do Governo Federal para alinhar-se à sua Política de Segurança da Informação e Comunicações, torna-se necessário a constante preocupação com requisitos de SIC para continuidade e eficiência dos negócios da Instituição.

3. GESTÃO DE SEGURANÇA DA INFORMAÇÃO NO CNPq

Este capítulo apresenta uma análise da gestão de Segurança da Informação e Comunicações no CNPq, contemplando ações que têm sido realizadas ao longo dos últimos três anos na busca de soluções tecnológicas, de melhorias no uso de metodologias, e de ações de governança, visando à melhoria dos serviços prestados, bem como as ações realizadas em observância a orientações e determinações do Governo Federal, a fim de implementar maior segurança para as informações e os processos da instituição. Essa análise considera o período que tem início na mudança do CNPq para a nova sede, em 2010, até o momento atual de gestão da informação no órgão, em um ambiente que pode ser considerado de alta aplicação tecnológica, no qual a quase totalidade da informação sensível para as atividades da instituição está definida e guardada em meio magnético, utilizando uma infraestrutura que se mantém segura para os padrões atuais de mercado.

Apresenta também uma análise da legislação relacionada à Segurança da Informação e Comunicações, consolidada e publicada pelo Governo Federal, e das publicações de boas práticas do mercado em Segurança da Informação. Desse conjunto de normas, algumas servem de base para a proposta de instrumento da conformidade da Segurança da Informação do CNPq, apresentada também neste capítulo.

3.1. ESTUDO DA LEGISLAÇÃO DE SEGURANÇA DA INFORMAÇÃO.

No universo das normas legais do Brasil encontramos inúmeras referências, diretas ou indiretas, ao tema Segurança da Informação. Desde a descrição de garantias individuais na Constituição Federal até o código penal que prevê penas para crimes envolvendo o mau uso da informação alheia. Em função dessa diversidade, o Departamento de Segurança da Informação e Comunicações (DSIC), subordinado ao Gabinete de Segurança Institucional da Presidência da República, realizou um trabalho de catalogação dessas normas que é disponibilizado em um quadro consolidado, em sua página na Web, primeiramente como material de referência aos órgãos da Administração Pública Federal, mas com acesso ao público em geral.

Ainda que o assunto Segurança da Informação, de alguma forma, já seja tratado pelo estado brasileiro há algumas décadas, isso não era feito em forma de uma política abrangente aplicada em todas as esferas governamentais. A ideia que vigorou por muito tempo é que esse assunto se referia as algumas esferas especiais como forças armadas, polícias e órgãos de inteligência, que desempenhavam essas atividades de acordo com o

objetivo de cada instituição sem uma diretriz comum, e mantinham essas atividades relativas ao tema em nichos especializados.

Porém, esse assunto ganhou um ingrediente especial com a popularização da Internet, e Segurança da Informação e temas mais específicos como Guerra Cibernética despertaram as atenções não apenas de militares e setores de inteligência, mas de todo o setor estratégico do Estado brasileiro e também do mercado privado como um todo. Desta forma, o assunto tem ganhado força nos últimos governos, com um crescimento muito grande nos dois últimos mandatos presidenciais, em que o Governo Federal ampliou a sua atuação em Segurança da Informação e Comunicações e nos últimos anos tem fortalecido sua estrutura para a gestão de SI, e tem feito um grande esforço com o objetivo de disseminar e consolidar uma cultura de Segurança da Informação no âmbito da APF.

Para atingir esse objetivo, o Governo Federal tem procurado, por meio do seu Gabinete de Segurança Institucional e, mais precisamente, por meio do DSIC, estudar e catalogar toda a legislação relativa aos assuntos ligados à Segurança da informação, e a partir daí estabelecer regras a serem seguidas pelas instituições da Administração Pública Federal. Em função disso, o DSIC tem publicado um conjunto de normas específicas para tratar o assunto, principalmente normas que regulam, com diretrizes e procedimentos, a atuação de órgãos da Administração Federal no que se refere a guarda, tratamento, classificação e disseminação da informação, observando os princípios da disponibilidade, integridade, confidencialidade e autenticidade.

Além desse conjunto de normas legais, o Governo Federal também recomenda a implementação de ações que estão em conformidade com práticas de sucesso no mercado de Segurança da Informação. Muitas dessas ações já vêm sendo praticadas no âmbito do Governo, mas, na maioria das vezes, de forma desordenada ou desvinculada da Gestão de Segurança da Informação, e por isso o Governo tem recomendado observar ações e controles contidos em publicações de boas práticas em Segurança da Informação, principalmente as Normas 27001 e 27002.

O Governo tem ainda organizado, em ações conjuntas do DSIC e outros órgãos como o MPOG e o TCU, eventos de conscientização e divulgação de práticas já implementadas na esfera governamental, de forma de dar transparência às ações e diminuir a defasagem de conhecimentos sobre o assunto entre os órgãos federais. Mas, a aplicação dos controles contidos nesse conjunto de leis e nos manuais de boas práticas, constitui-se

na principal estratégia do Governo Federal para consolidação de sua política de Segurança da Informação e Comunicações a da Informação.

Para fundamentar este estudo, é tomado como base esse conjunto normas legais e os manuais de boas praticas do mercado de segurança da informação, citados acima e descritos com mais detalhes nos subitens abaixo. Vale lembrar que essa é uma área que se encontra em constante transformação, o que conduz a uma constante evolução das normas e das práticas que envolvem essas atividades. Em conformidade com essa característica de evolução, este trabalho apresenta a construção de um instrumento que também tem como característica permanecer aberto a atualizações futuras, sempre que necessário.

3.1.1. INSTRUÇÃO NORMATIVA Nº 01 DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA (IN01 GSI/PR).

A IN01 GSI/PR, de 13 de junho de 2008, é o principal instrumento legal utilizado pelo Governo Federal para tratar da Gestão de Segurança da Informação e Comunicações no âmbito da APF. Ela traça as diretrizes gerais para implantação da Política de Segurança da Informação e Comunicações, definindo responsabilidades para cada ator envolvido nessa gestão, como o Gabinete de Segurança Institucional da Presidência da República (GSI/PR); o Comitê Gestor de Segurança da Informação e Comunicações (GSIC); e os demais órgãos que compõem a APF, bem como, as suas divisões responsáveis pela gestão de SIC.

A IN01 GSI/PR funciona como uma norma mais genérica, que traz controles referentes à gestão da Segurança da Informação e Comunicações (SIC) de uma forma mais geral, e prevê a vinculação de normas complementares a ela, que tratam de cada assunto específico e relevante para a gestão de SIC nas entidades subordinas ao Governo Federal. Até o momento, foram publicadas 18 normas complementares, que seguem listadas abaixo com suas descrições originais, destinadas a orientar e a determinar ações e controles que devem ser implementados a fim de garantir a conformidade com a Gestão de SIC planejada pelo Governo Federal para os órgãos da APF.

a) Norma complementar n° 01, de 13 de outubro de 2008.

Estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

b) Norma complementar n° 02, de 13 de outubro de 2008.

Define a metodologia de Gestão de Segurança da Informação e Comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

c) Norma complementar n° 03, de 30 de junho de 2009.

Estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (POSIC), nos órgãos e entidades da APF, direta e indireta.

d) Norma complementar n° 04, de 15 de fevereiro de 2013.

Estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC), nos órgãos e entidades da Administração Pública Federal, direta e indireta.

e) Norma complementar n° 05, de 14 de agosto de 2009.

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.

f) Norma complementar n° 06, de 11 de novembro de 2009.

Estabelece diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta.

g) Norma complementar n° 07, de 06 de maio de 2010.

Estabelece 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.

h) Norma complementar n° 08, de 19 de agosto de 2010.

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.

i) Norma complementar n° 09, de 15 de fevereiro de 2013.

Normatiza o uso de recurso criptográfico para a segurança de informações produzidas nos órgãos e entidades da Administração Pública Federal, direta e indireta.

j) Norma complementar n° 10, de 30 de janeiro de 2012.

Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações, dos órgãos e entidades da Administração Pública Federal, direta e indireta.

k) Norma complementar n° 11, de 30 de janeiro de 2012.

Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta.

l) Norma complementar n° 12, de 30 de janeiro de 2012.

Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta.

m) Norma complementar n° 13, de 30 de janeiro de 2012.

Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta.

n) Norma complementar n° 14, de 30 de janeiro de 2012.

Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta.

o) Norma complementar n° 15, de 11 de junho de 2012.

Estabelece diretrizes de Segurança da Informação e Comunicações para o uso das redes sociais, nos órgãos e entidades da Administração Pública Federal, direta e indireta.

p) Norma complementar nº 16, de 21 de novembro de 2012.

Estabelece diretrizes de Segurança da Informação e Comunicações para obtenção de software seguro, nos órgãos e entidades da Administração Pública Federal, direta e indireta.

q) Norma complementar n° 17, de 09 de abril de 2013.

Estabelece diretrizes nos contextos de atuação e adequações para profissionais da área de Segurança da Informação e Comunicações, nos órgão e entidades da Administração Pública Federal, direta e indireta.

r) Norma complementar n° 18, de 09 de abril de 2013.

Estabelece diretrizes para as atividades de ensino em Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta.

3.1.2. NORMA ABNT ISO/IEC 27001:2006.

Essa norma, segundo a descrição que consta em seu próprio texto, foi preparada para prover um modelo que estabelece, implementa, opera, monitora, faz análise critica, mantém e aperfeiçoa um Sistema de Gestão de Segurança da Informação e Comunicações (SGSIC). A norma instrui que é necessário que a organização conheça bem as suas necessidades e os seus objetivos, os seus requisitos de segurança, os processos utilizados e o tamanho e estrutura da organização, para que se possa implementar com sucesso um SGSIC.

A Norma 27001 utiliza uma abordagem de sistema, sugerindo às organizações que enfatizem a importância da Gestão de Segurança da Informação e Comunicações para a continuidade e sucesso dos seus negócios, buscando entender os seus próprios requisitos de segurança e suas necessidades, para estabelecer uma política para Segurança da Informação e Comunicações que seja alinhada aos objetivos e às ações estratégicas da instituição. Reforça, ainda, a importância de uma gestão dos riscos de Segurança da Informação e Comunicações e de monitoração e análise crítica do próprio SGSIC implementado, utilizando o modelo de melhoria continua conhecido como *Plan-Do-Check-Act* (PDCA), ou ciclo de Deming[12] como é definido pela *ITIL Foundation* (*Information Technology Infrastructure Library*).

Apesar de ser uma norma amplamente utilizada por empresas de mercado em relação à Gestão de Segurança da Informação e Comunicações, a Norma nos apresenta requisitos genéricos que podem ser utilizados pelos mais diversos tipos de organização privadas ou públicas, razão pela qual o Governo tem adotado a sua observância pelos seus órgãos subordinados.

[12] PDCA – Planejar-Executar-Verificar-Agir ou em inglês Plan-Do-Check-Act é um método iterativo de gestão de quatro passos de melhoria continua, conhecido por ciclo de Deming por ter sido popularizado pelo Dr. W. Edwards Deming.

3.1.3. NORMA ABNT ISO/IEC 27002:2005.

A norma equivale à norma ISO/IEC 17799:2005 que foi elaborada pelo Comitê Brasileiro de Computadores e Processamento de Dados e a partir de 2007, usando sua nova numeração, passou a integrar à família de normas ISO/IEC 27000 que têm por objetivo apresentar requisitos de sistema de gestão da segurança da informação, gestão de riscos, métricas e medidas, e diretrizes para implementação. É uma publicação de boas práticas que fornece diretrizes e procedimentos detalhados para orientar as atividades de Gestão de Segurança da Informação e Normas de Segurança da Informação nas organizações.

Essa Norma apresenta um detalhamento dos controles apresentados na norma ABNT ISO/IEC 27001:2006 e essas duas normas têm sido utilizadas pelo Governo Federal, como referência para regulamentação da Segurança da Informação no âmbito da Administração Pública Federal, com recomendação para que os órgãos federais observem e implementem os controles nelas sugeridos.

3.1.4. CWE/MITRE – FRAQUEZAS EM DESENVOLVIMENTO DE SOFTWARE – LISTA TOP 25.

A *Common Weakness Enumeration (CWE/MITRE)* fornece uma base ampla com um conjunto de fraquezas de software e propõe ações que pode ajudar no reconhecimento dessas fraquezas relacionadas à arquitetura e ao design. O site CWE contém dados sobre mais de 800 erros de programação, erros de projeto e erros de arquitetura que podem levar a vulnerabilidades exploráveis por agentes maliciosos. Em suas auditorias mais recentes, a Controladoria-Geral da União (CGU) tem recomendado, que os órgãos da Administração Pública Federal explicitem em seus processos de desenvolvimento de aplicações, quais controles referentes a vulnerabilidades de software vêm sendo considerados, e tem sugerido a lista *CWE/MITRE* como referência para a implementação desses controles.

Neste estudo vamos verificar a lista TOP 25 do *CWE/MITRE*, uma publicação bienal que relaciona as 25 fraquezas ou erros mais perigosos em desenvolvimento de software. A última publicação da lista ocorreu em 2011 e reúne a colaboração de vários institutos especialistas em segurança de software, como o SANS com experiência em vetores de ataque, o catálogo do MITRE de fraquezas comuns, a lista Top 10 do *Open Web Application Security Project* (*OWASP)*, dentre outros. Essa lista funciona como referência para designers, arquitetos e programadores envolvidos em desenvolvimento de software, com um

caráter educativo ou de conscientização, em relação a necessidade de observar erros comuns e perigosos antes da entrega de um software.

Além disso, essa lista ajuda também contratantes ou requisitantes de uma aplicação a exigir controles para garantir a construção de softwares mais seguros no atendimento de suas solicitações. Para a Gestão de Segurança da Informação e Comunicações, essa lista, em conjunto com outros controles, ajuda a aumentar a confiabilidade no funcionamento dos softwares que sustentam os negócios da instituição.

3.1.5. OWASP – LISTA TOP 10.

Segundo a autodefinição constante de sua página Web, o *Open Web Application Security Project (OWASP)* é um projeto de uma fundação de nível mundial, sem fins lucrativos, cujo objetivo é contribuir para a melhoria na segurança de desenvolvimento de software. Sua missão é tornar visível a segurança do software de modo que pessoas e organizações de todo o mundo possam tomar conhecimento dos verdadeiros riscos de segurança de software, e usá-lo em suas tomadas de decisão.

A forma de atuação do *OWASP* consiste em reunir e divulgar informações catalogadas e analisadas que forneça subsídios para melhorar e facilitar a avaliação de riscos no momento do desenvolvimento de softwares aplicativos e permita minimizar vulnerabilidades que possam ser exploradas em ataques via internet. A *OWASP Foundation* mantém uma publicação anual chamada *The Top 10 Most Critical Web Application Security Risks* ou “Os 10 riscos mais críticos para a segurança de aplicações Web”, e esta lista tem sido citada pelos órgãos de controle do Governo, como referência para observação de prováveis riscos desenvolvimento de suas aplicações.

3.1.6. LEI N° 11.527 – LEI DE ACESSO À INFORMAÇÃO.

A Lei nº 11.527, de 16 de novembro de 2011, ou Lei de Acesso à Informação (LAI), que entrou em vigor seis meses após a sua publicação 16 de maio de 2012, tem o propósito primordial de regulamentar os preceitos constitucionais relativos ao acesso às informações públicas. A lei garante que cidadãos brasileiros tenham acesso a informações de qualquer ente público tanto do Executivo, como do Legislativo e Judiciário, salvo informações de acesso restrito protegidas pela classificação prevista nesta mesma lei ou protegida por outro instrumento legal em vigor.

A LAI não trata de Segurança da Informação e Comunicações (SIC), pelo menos não com o enfoque que tratam as outras normas citadas aqui. Os controles apresentados nessa norma referem-se mais ao direito de acesso que propriamente à proteção da informação. Ela representa o desafio que instituições governamentais têm que enfrentar em relação à proteção dada ao conjunto de informações em seu poder. Garantir o acesso à informação significa garantir uma informação integra, autêntica, e que esteja disponível quando solicitada, e aí sim, estamos falando de SIC.

3.2. ANÁLISE DOS PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO NO CNPq.

Como já foi visto no capítulo anterior, o CNPq, desde a transferência de sua administração para Brasília em 1976, tem acompanhado as mudanças em Tecnologia da Informação e Comunicações, e ao longo de quase quatro décadas utilizou vários modelos de Centros de Processamento de Dados, com várias tecnologias em hardware e software, sempre buscando acompanhar e incorporar tecnologias e boas práticas ao seu modelo de gerenciamento de Tecnologia da Informação e Comunicações (TIC). A última grande adaptação ocorreu com a mudança da sede do órgão para o seu endereço atual, com uma infraestrutura predial mais moderna, com mais espaço, o que permitiu implementar ambiente atual é o nosso foco de análise neste estudo.

O CNPq tem buscado, há algum tempo, melhorar a segurança de seus sistemas de informação e, por extensão, a segurança das informações concernentes à sua atividade fim, o fomento à Ciência, Tecnologia e Inovação. A mudança para a nova sede, em 2010, representou a oportunidade de implementar novos procedimentos de Gestão de Tecnologia da Informação e Comunicações que melhoram não somente a produtividade dos sistemas implantados, mas também a segurança dos ativos de informação. Foi, também, o momento oportuno para melhorar a infraestrutura, seguindo o que recomenda as boas práticas do mercado de Segurança da Informação e Comunicações (SIC).

O ambiente de rede em que se encontram as aplicações do CNPq, exige que previamente se implemente muitos procedimentos de suporte suficientes para garantir a disponibilidade dessas aplicações, e não apenas isso, mas garantindo também o máximo de confiabilidade nos requisitos implementados e nas informações processadas. Isso tem requerido do CNPq, buscar frequentemente implementar medidas de segurança da informação, ainda que diluídas em vários processos de desenvolvimento e suporte.

O departamento de TIC do CNPq tem buscado melhorar o seu processo de desenvolvimento, com a especificação clara de atividades, definição de funções e especialidades, e o aperfeiçoamento das metodologias empregadas. Tem buscado capacitar e até certificar os servidores em áreas de gerência e governança de TIC, mas, em um contexto de grande terceirização, tem um grande desafio que é fazer com que todas as funções de gestão de TIC sejam ocupadas por servidores do órgão.

Mais recentemente, nos últimos três anos, o CNPq vem implementado algumas novas ações de SIC, que vão ao encontro das recomendações feitas pelo GSI/PR para os órgãos federais. Contratou auditoria externa para um estudo da segurança em seu ambiente de TIC, focando na detecção de incidentes e aplicação de ações corretivas. Melhorou o ambiente físico, preservando servidores de banco de dados e de aplicações em uma área segura, uma sala-cofre. Melhorou a utilização de metodologias de desenvolvimento de aplicativos, com padrão de desenvolvimento e documentação. E assim, criou um ambiente adequado à implementação das determinações do Governo em relação à Segurança da Informação.

O CNPq tem mantido constantes contatos com as áreas de Gestão de Segurança da Informações e Comunicações do Governo Federal e a partir das recomendações e determinações do Governo, o CNPq formalizou a sua área de Segurança da Informação e Comunicações, constituindo uma equipe responsável pela gestão. Nomeou o Gestor de Segurança da Informação e Comunicações, e tem divulgado informações sobre SI, buscando melhorar o conhecimento dos trabalhadores do órgão sobre o assunto.

Foi criado o Comitê de Segurança da Informação e Comunicações (CSIC), que é responsável pela elaboração, acompanhamento e atualização da Política de Segurança da Informação e Comunicações (POSIC), bem como pela elaboração e aprovação de normas complementares à POSIC. O CSIC delibera sobre quaisquer assuntos relacionados à SIC no âmbito do CNPq. O Comitê já está em funcionamento e realiza suas reuniões periodicamente e já publicou a POSIC do CNPq e algumas normas complementares, e tem buscado elaborar e aprovar outras normas complementares determinadas pelo DSIC/GSIPR e já previstas na POSIC do CNPq. Enfim, além dos aspectos tecnológicos e boas práticas gerenciais já observados pelo órgão, o CNPq tem buscado atender ao previsto nas normas publicadas pelo Governo em relação à SIC.

Em relação à segurança de TIC, o CNPq tem procurado se adequar às determinações do Governo Federal e para isso implantou um modelo de Centro de Dados com uma

organização que mantém as atividades em camadas, que não somente torna mais rápida a identificação de problemas e a possível solução, mas aumenta a segurança devido aos processos de monitoramento constantes.

O Centro de Dados do CNPq é equipado com uma sala cofre, onde estão instalados todos os servidores de aplicação e de e-mail, discos rígidos, firewalls, com acesso físico permitido somente aos responsáveis pelo serviço. As equipes que trabalham no gerenciamento de redes são responsáveis por monitorar, utilizando ferramentas instaladas na console central, a rede, os servidores de aplicação, servidores de firewall e de storage. Monitoram trafego na rede, para detecção de motivos de queda de velocidade ou possíveis interrupções em trechos da rede, controlam ataque ou tentativas de violação de segurança; controlam a ocorrência de incidentes e buscam solução de acordo com o previsto nos planos.

A equipe de Administração de Banco de Dados é responsável pelo desempenho do banco e pelo planejamento de capacidade e pela organização física do armazenamento das informações. Uma equipe controla a mensageria e colaboração, com atividades que monitoram o tráfego de emails, listas negras com sites proibidos ou perigosos, tamanho de mensagens, capacidade de armazenamento de mensagens por conta, e arquivos de *logs*, controle de *spans,* dentre outras.

Essa organização facilita o controle das atividades gerais que envolvem o complexo contexto atual de TIC e, também, contribui para a segurança dos ativos de informação da instituição. Essas atividades cotidianas em conjunto com essa boa infraestrutura vão ao encontro do que preconiza a Política de Segurança da Informação proposta pelo Governo Federal, necessitando que sejam acompanhadas seguindo controles determinados, sejam pelas normas do Governo Federal sejam pelas publicações de boas práticas do mercado.

É nesse contexto que proponho um instrumento para aferição periódica da conformidade dos procedimentos implementados no CNPq, com as normas vigentes em Segurança da Informação e Comunicações.

3.3. PROPOSTA DE INSTRUMENTO DE AFERIÇÃO DA CONFORMIDADE DA SEGURANÇA DA INFORMAÇÃO NO CNPq.

A fim de atingir o objetivo deste estudo, que se propõe a realizar aferição da conformidade das ações implementadas no CNPq em Segurança da Informação, foram destacadas

algumas normas, daquele conjunto consolidado pelo Departamento de Segurança da Informação e Comunicações (DSIC), já descritas no item 3.1, que contêm controles explícitos em seu escopo, para serem implementados pelos órgãos da Administração Pública Federal.

A proposta consiste na elaboração de uma *Check list* (Anexo A) com todas as normas que contenham algum tipo de controle especificado em relação à Segurança da Informação e Comunicações (SIC), que tenham sido direcionadas pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSIPR) aos órgãos da Administração Pública Federal (APF), para que fossem observados, quando da implementação de suas POSICs. O mapeamento dos controles das normas em vigor, relativas à SIC, foi realizado no decorrer deste estudo e a proposta do instrumento é que ele absorva os controles das normas que sejam editadas futuramente.

Do conjunto de Normas listadas no item 3.1 foram destacadas inicialmente, para efeito de prova de conceito neste estudo, as seguintes normas: IN 01 GSI/PR e cinco de suas Normas Complementares: a NC02, a NC03, a NC04, a NC06, e a NC07; e a norma ABNT ISO/IEC 27001:2006.

A *Check list* proposta é dinâmica, como dinâmico tem sido a evolução dessa área, e por isso o modelo proposto é um modelo relacional composto de algumas tabelas, com as informações que permitam o acompanhamento das verificações de conformidade a uma periodicidade determinada, e com isso constatar possíveis vulnerabilidades ou determinar quais áreas na instituição carecem de ações ou investimentos. O modelo permite a inclusão futura de novos controles, bem como a exclusão de controles que tenham sido revogados, ou ter a sua aplicabilidade declinada pelo próprio órgão, à medida que o Governo for editando novas normas, na sua busca pelo aperfeiçoamento da gestão de SIC no âmbito da Administração Pública Federal.

Para melhorar a dinâmica de atualização da lista, com inclusão ou exclusão de controles, a proposta sugere a criação de um modelo de dados relacional, com algumas tabelas iniciais:

1) Tabela de Controles – Contem registros com os controles definidos nas normas, com os seguintes atributos: Código do Controle, seqüencial para identificar o controle; Descrição do Controle, descrição de acordo com a norma de origem; Código da Norma, seqüencial para

identificar a Norma que contém aquele controle; e, Código da Área, seqüencial para identificar a área a que se refere aquele controle. Neste modelo foram cadastrados 328 controles. (Tabela completa no Anexo B)

Código do Controle	Descrição do Controle	Código Norma	Código Área
001	Existe uma política de Segurança da Informação aprovada pela direção, publicada e comunicada para todos os funcionários e partes externas relevantes?	01	001
002	Exise um processo de análise crítica da política de SI, em intervalos planejados ou quando mudanças significativas ocorrem, para assegurar a sua contínua pertinência, adequação e eficácia?	01	001
003	A Direção apoia ativamente a segurança da informação dentro da organização, de forma clara, demonstrando o seu comprometimento, definindo atribuições de forma explícita e conhecendo as responsabilidades pela segurança da informação?	01	002
004	As atividades de segurança da Informação são coordenadas por representantes de diferentes partes da organização com funções e papéis relevantes	01	002
. . .	. . .	. . .	. . .
327	Existe uma documentação própria que permita que sejam identificados os perímetros de segurança de cada ativo de informação, por todos que transitarem ou tiverem acesso em tais espaços, em especial às áreas e instalações críticas?	07	007
328	O armazenamento, a veiculação de imagem, vídeo ou áudio, registrados em perímetro de segurança, são regulamentados por normas específicas?	07	007

Tabela 1 - Modelo da Tabela de Controles, no Banco Oracle.
Fonte: Confeccionado pelo autor

2) Tabela de Área - Contem registros com o código e a descrição das áreas a que se referem os controles especificados contidos nas normas. Neste modelo foram identificadas 12 áreas.

Código da Área	Descrição da área
001	Política de Segurança da Informação e Comunicações
002	Gestão de Segurança da Informação e Comunicações
003	Gestão de Ativos
004	Segurança de Recursos Humanos
005	Segurança Física e do Ambiente
006	Gerenciamento das Operações e Comunicações
007	Controle de Acesso
008	Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
009	Gestão de Incidentes de Segurança da Informação
010	Gestão de Continuidade de Negócios
011	Conformidade
012	Gestão de Riscos

Tabela 2 - Modelo da Tabela de Área, no Banco Oracle.
Fonte: Confeccionado pelo autor

3) Tabela de Normas – Tabela de domínio, com registros que contêm o código e a descrição das normas que contêm os controles. Neste modelo foram cadastradas sete normas.

Código da Norma	Descrição da Norma
01	ABNT ISO-IEC 27001:2006
02	Instrução Normativa nº01 GSI/PR
03	Norma Complementar nº 02 - IN01 GSI/PR
04	Norma Complementar nº 03 – IN01 GSI/PR
05	Norma Complementar nº 04 – IN01 GSI/PR
06	Norma Complementar nº 06 – IN01 GSI/PR
07	Norma Complementar nº07 - IN01 GSI/PR

Tabela 3 - Modelo da Tabela de Normas, no Banco Oracle.
Fonte: Confeccionado pelo autor

4) Tabela de Conformidade – Tabela de domínio, com registros que contêm o código e a descrição da conformidade. Estão cadastradas cinco situações de conformidade.

Código da Conformidade	Descrição da Conformidade
01	Sim
02	Não
03	Não se Aplica
04	Não Sei
05	Em Implementação

Tabela 4 - Modelo da Tabela de Conformidade, no Banco Oracle.
Fonte: Confeccionado pelo autor

5) Tabela Histórico de Verificação de Conformidade – Contém os registros com a data da verificação, o código do controle e o código da conformidade nessa data.

Data da Verificação	Código do Controle	Código da Conformidade
01/11/2013	001	01
01/11/2013	002	02
01/11/2013	003	01
01/11/2013	006	02
. . .	. . .	. . .
01/03/2014	001	01
01/03/2014	002	01
01/03/2014	003	01
01/03/2014	006	02

Tabela 5 - Modelo da Tabela de Histórico de Verificação da Conformidade, no Banco Oracle.
Fonte: Confeccionado pelo autor

Este modelo é uma sugestão de implementação que poderá evoluir à medida que a instituição ganhe maturidade na gestão de SIC, ou mesmo ocorram mudanças na estratégia da instituição, mas principalmente, quando o Governo publicar novas normas com novas determinações e controles a serem implementados. As tabelas descritivas completas são apresentadas nos anexos, e os resultados da verificação efetuada para este estudo estão apresentados no tópico seguinte.

3.4. QUADRO DEMONSTRATIVO DA CONFORMIDADE DA SEGURANÇA DA INFORMAÇÃO DO CNPq E A LEGISLAÇÃO VIGENTE.

Após a aplicação do instrumento sugerido neste estudo e a verificação da conformidade do CNPq com as principais normas e publicações de boas práticas em Segurança da Informação e Comunicações, é possível observar algumas características que delimitam a Gestão de SIC em andamento. O que se procura demonstrar neste tópico, como resultado da pesquisa realizada é, além dessa conformidade geral, situação do órgão em relação a cada instrumento normativo separadamente, bem como a situação em relação a cada área de Segurança da Informação.

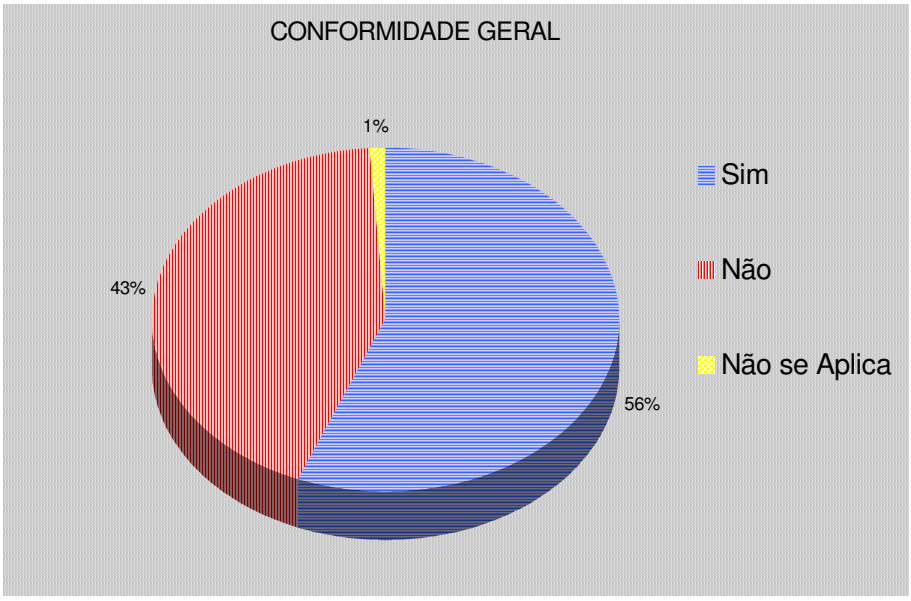

Gráfico 1 – Visão Geral da Conformidade do CNPq com Normas e boas práticas em SI.
Fonte: Confeccionado pelo autor a partir de dados da pesquisa

Os resultados da pesquisa, quando analisados de forma geral sem a separação por norma ou por área de atividade, apresentados no Gráfico 1, demonstram que o CNPq tem uma conformidade mediana que se aproxima de 60%, evidenciando que o órgão vem implementando procedimentos e segue boas práticas, de Segurança da Informação e Comunicações, mas sem podermos afirmar o grau de conformidade que existe em relação às determinações contidas nas Instruções Normativas do Governo Federal.

Por essa visão geral não se pode chegar a uma análise qualitativa do grau de conformidade. Mostra que o CNPq tem uma atividade de Segurança da Informação e Comunicações (SIC) e implementa requisitos relativos a essa atividade, mas deixa claro que há uma boa margem para se avançar no aperfeiçoamento de uma política de SIC, seguindo as determinações do Governo Federal.

É bem verdade que, com o dinamismo dessa área, é quase impossível que se tenha uma conformidade de 100% em relação a todas práticas desejáveis em SIC, mas as instituições governamentais devem, em seus planejamentos, estabelecer metas que contemplem a obediência total aos controles determinados pelo Governo Federal, em suas normas relativas à atividade de SIC, quando aplicáveis. Vale reafirmar aqui que o Governo Federal tem publicado normas com diretrizes, a fim de implementar uma cultura entre as instituições governamentais para que sejam capazes de formalizar uma política com infraestrutura e ações necessárias para uma gestão eficaz de SIC no âmbito de suas atividades.

Uma informação mais qualitativa pode ser encontrada quando detalhamos o levantamento realizado e passamos a analisar os resultados encontrados, separados por Instrumento Normativo ou por área de Segurança da Informação e Comunicações.

3.4.1. ANÁLISE SEPARADA POR INSTRUMENTO NORMATIVO.

Esta análise nos fornece um conjunto de informações que permite que a instituição possa verificar a sua aderência a cada norma vigente relativa à Segurança da Informação e Comunicações (SIC). Em relação à Norma 27001, que abrange 11 áreas diversas de SIC, deve-se buscar aplicar os controles visando estar equiparado com as melhores práticas do mercado de SIC, mas são apenas recomendações, enquanto as normas legais publicadas pelo Governo Federal, que são mais específicas, trazem controles obrigatórios a fim de adequar as ações dos órgãos da Administração Pública Federal à visão do Governo em relação à Segurança da Informação e Comunicações.

a) Análise da conformidade com a Norma 27001

Essa Norma tem sido abundantemente utilizada e citada como referência em certificação e análise de conformidade em Segurança da Informação. Os seus 133 controles, transformados aqui em 141 para melhor aplicabilidade, estão divididos em 11 áreas relativas à Segurança da Informação e Comunicações.

Não se procurou, neste momento, fazer um estudo profundo quando à aplicabilidade de determinados controles. Essa atividade está prevista em norma e, em algum momento o CNPq deverá instituir formalmente uma Declaração de Aplicabilidade em relação a controles necessários em sua política de SIC. Neste momento, foi verificado apenas se o controle estava implementado ou não e apenas para alguns controles, que de forma clara se mostravam incompatíveis com as atividades do CNPq, foi considerada a não aplicabilidade.

Essa Norma, tem sido observada pelo CNPq há alguns anos, e o Gráfico 2 mostra o resultado dessas ações na atualidade. O fato de ser uma norma mais abrangente, cobrindo praticamente todas as áreas envolvidas em SIC, e a análise mostrar um percentual de conformidade, com essa norma, acima de 60%, demonstra que o CNPq tem tido a preocupação em implementar procedimentos de segurança em suas atividades relativas à informação e esse percentual, mediano, constitui um ponto forte em favor da consolidação de uma política de SIC.

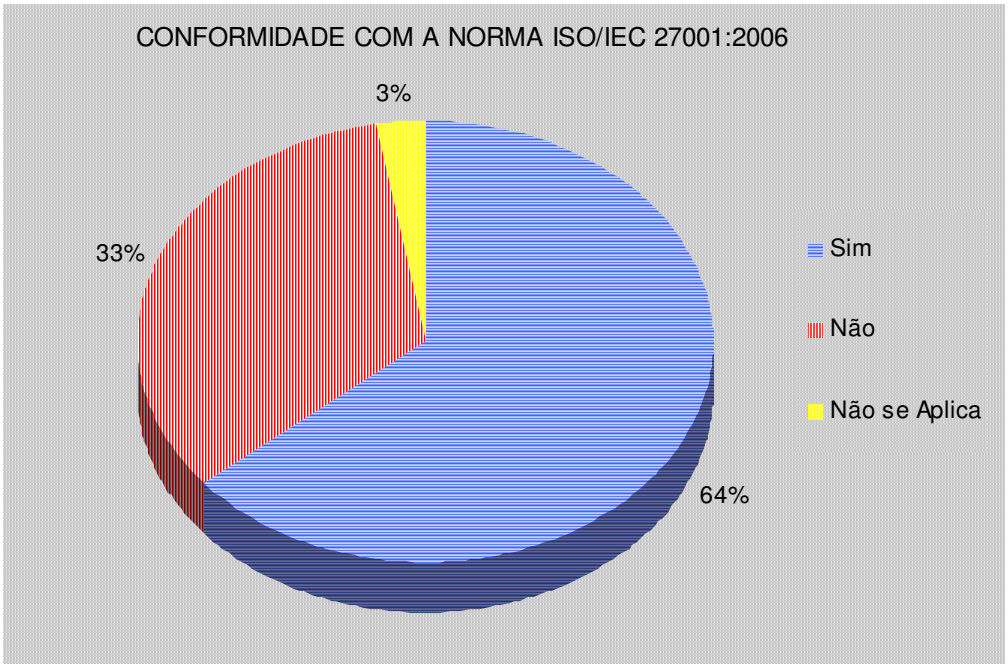

Gráfico 2 – Conformidade com a Norma ISO/IEC 27001:2006
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

b) Análise da conformidade com a Instrução Normativa nº 01 do GSI/PR

A Instrução normativa nº 01 do GSI/PR é o principal instrumento normativo publicado pelo Governo Federal para traçar as diretrizes de implementação da Política de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal

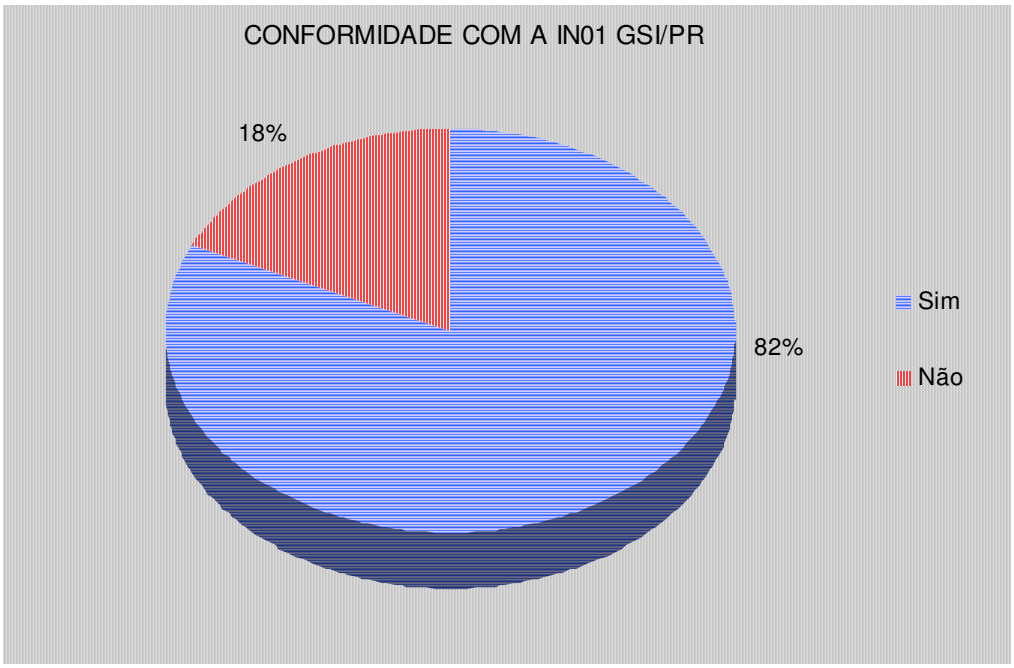

Gráfico 3 – Conformidade com a Instrução Normativa nº 01 GSI/PR
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

O fato de a pesquisa apresentar uma conformidade de 82% demonstra que o CNPq já deu um importante passo para a implementação de sua Política de Segurança da Informação e Comunicações (POSIC), mas, vale lembrar que, essas normas trazem determinações que devem ser cumpridas e o órgão deve buscar, neste caso, atingir 100% de conformidade.

c) Análise da conformidade com a Norma Complementar nº 02 da IN01-GSI/PR

O assunto de que trata essa Norma complementar é a Metodologia de Gestão de Segurança da Informação e Comunicações a ser utilizada pelos órgãos da APF. É uma metodologia baseada no ciclo de Deming, ou PDCA. O estudo da conformidade no CNPq mostra uma baixíssima conformidade com esta norma, que torna evidente que, apesar de o CNPq apresentar uma razoável conformidade com aspectos de segurança, falta a formalização de uma metodologia, que apresente esses procedimentos dentro de um modelo de monitoramento e melhoramento constante. Essa talvez seja uma norma a ser priorizada pelo órgão, para buscar a conformidade.

Mas, antes de buscar a qualquer custo estar em conformidade com as determinações do Governo, ainda que isso seja obrigatório, é muito importante que a instituição aprofunde neste estudo e estabeleça indicadores, que possam auxiliá-la na escolha de quais controles são mais importantes ou mais urgentes para garantir o bom funcionamento das atividades da instituição e também, para implementar a Segurança da Informação, na forma pretendida pelo Governo.

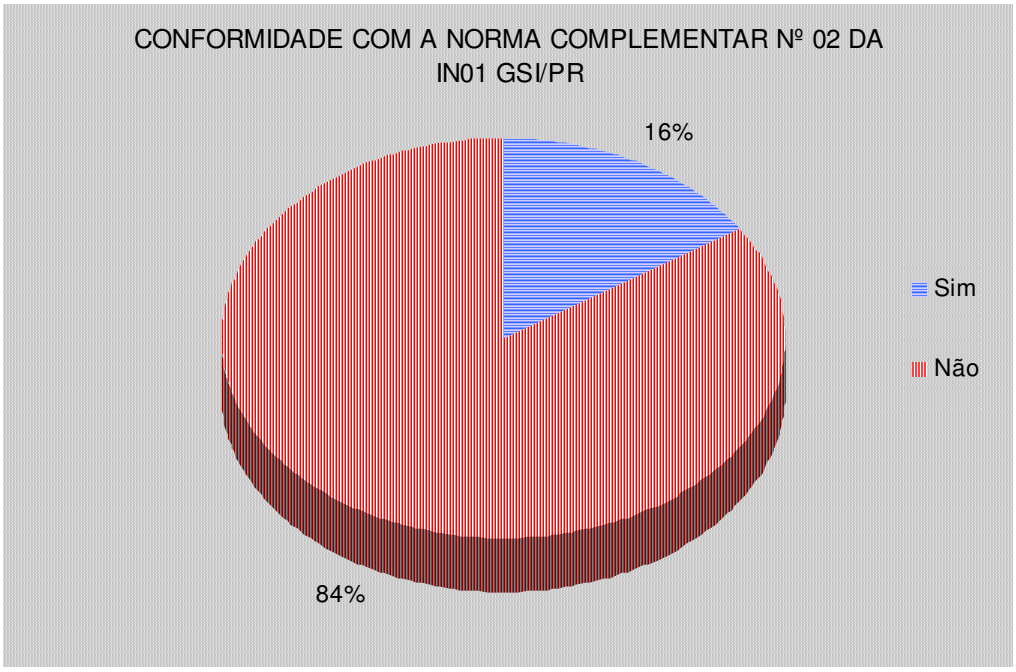

Gráfico 4 – Conformidade com a Norma Complementar nº 02 da IN 01 GSI/PR
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

d) Análise da conformidade com a Norma Complementar nº 03 da IN01-GSI/PR

Esta norma orienta os órgãos da APF em relação à elaboração de suas POSICs. O CNPq já elaborou sua POSIC, e tem observado e aplicado muitas das determinações que ela traz em seu escopo. Criou o Comitê de Segurança da Informação, que tem feito reuniões para discutir pontos importantes para a continuidade da implementação da Política de SIC, como a classificação da informação e as ações para cumprimento da Lei de Acesso à Informação; Aprovou normas complementares à POSIC e tem formado grupos de trabalho que estão discutindo e elaborando novas minutas para a discussão e aprovação; estabeleceu um Gestor para Segurança da Informação e Comunicações; dentre outros.

Os itens da política implementados pelo CNPq, além dos citados acima, contribuem para o grau razoavelmente alto de conformidade apresentado no gráfico 5.

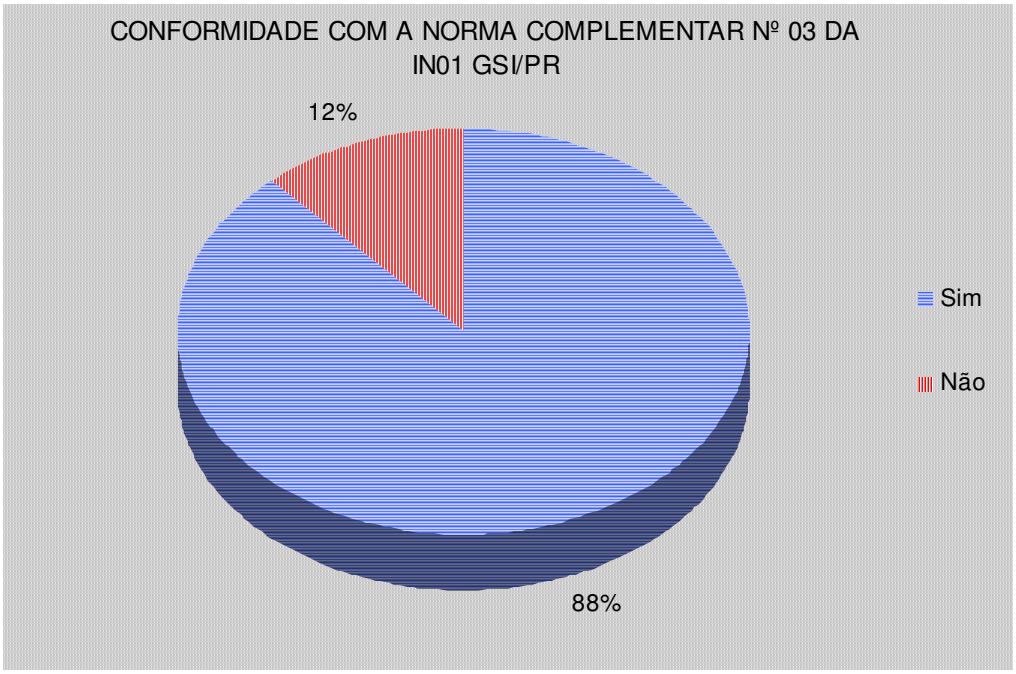

Gráfico 5 – Conformidade com a Norma Complementar nº 03 da IN 01 GSI/PR
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

e) Análise da conformidade com a Norma Complementar nº 04 da IN01-GSI/PR

Esta norma estabelece as diretrizes para os órgãos da APF, instituírem a sua Gestão de Riscos. O risco é inerente a qualquer atividade de uma organização e o mais importante, é que os riscos sejam identificados e possam ser classificados de acordo com a estratégia da instituição. O resultado da pesquisa, mostrada no Gráfico 6, mostra uma não aderência a esta norma. Durante a pesquisa verificou-se que o CNPq tem procedimentos de avaliação de riscos e tratamento de riscos em áreas importantes, mas como a norma trata da

instituição como um todo e determina a formalização de uma gestão de risco para toda a instituição, houve um alto índice de não conformidade.

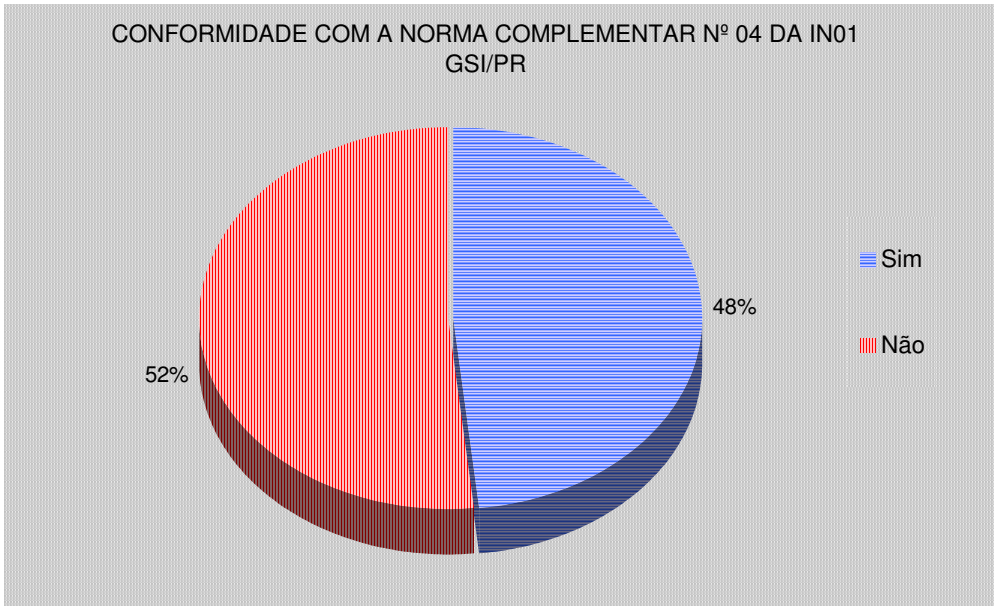

Gráfico 6 – Conformidade com a Norma Complementar nº 04 da IN 01 GSI/PR
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

f) Análise da conformidade com a Norma Complementar nº 06 da IN01-GSI/PR

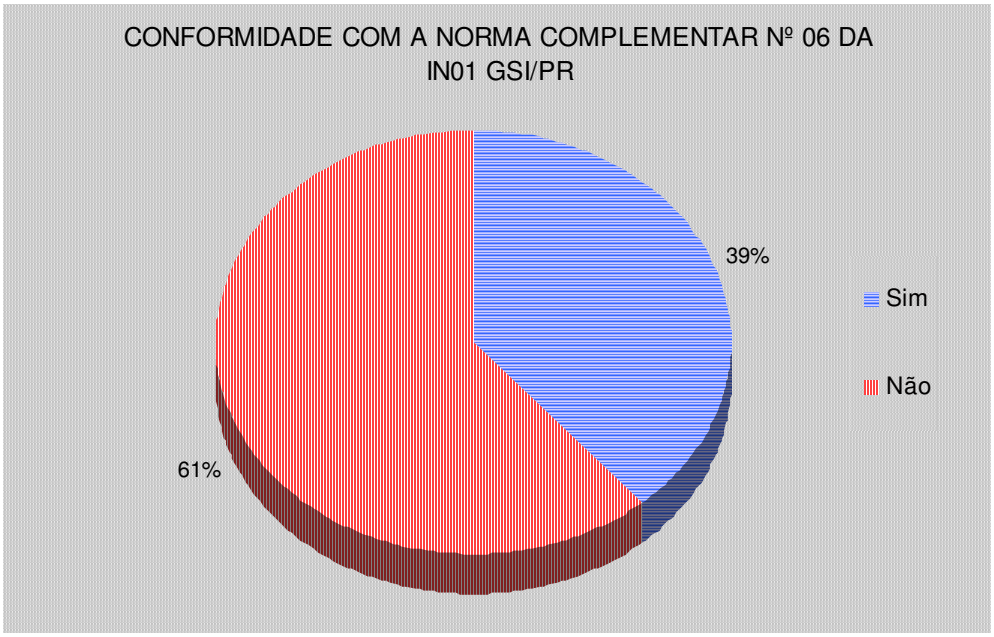

Gráfico 7 – Conformidade com a Norma Complementar nº 06 da IN 01 GSI/PR
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

Outra área importante em Segurança da Informação e Comunicações, e que mereceu uma norma específica do GSI/PR, é Gestão de Continuidade de Negócios (GCN),

cujo resultado do estudo de conformidade no CNPq está demonstrado no Gráfico 7. Em relação à GCN, o que pode-se afirmar é que falta no CNPq a formalização de uma gestão, que crie, monitore e atualize os Planos de Continuidade de Negócios para toda a instituição. Verificou-se que em determinadas áreas, como a área de TIC, existe um plano que foi executado, muitas ações foram executadas e mudanças foram realizadas, mas a norma é mais abrangente e determina que essa gestão seja feita para toda a instituição. Do ponto de vista prático, em uma instituição com um alto grau de informatização, a existência de uma Gestão de Continuidade de Negócios na área de TIC cria uma situação de segurança razoável para toda a casa, porém não considera outros ativos da instituição, tal como determina a norma.

g) Análise da conformidade com a Norma Complementar nº 07da IN01-GSI/PR.

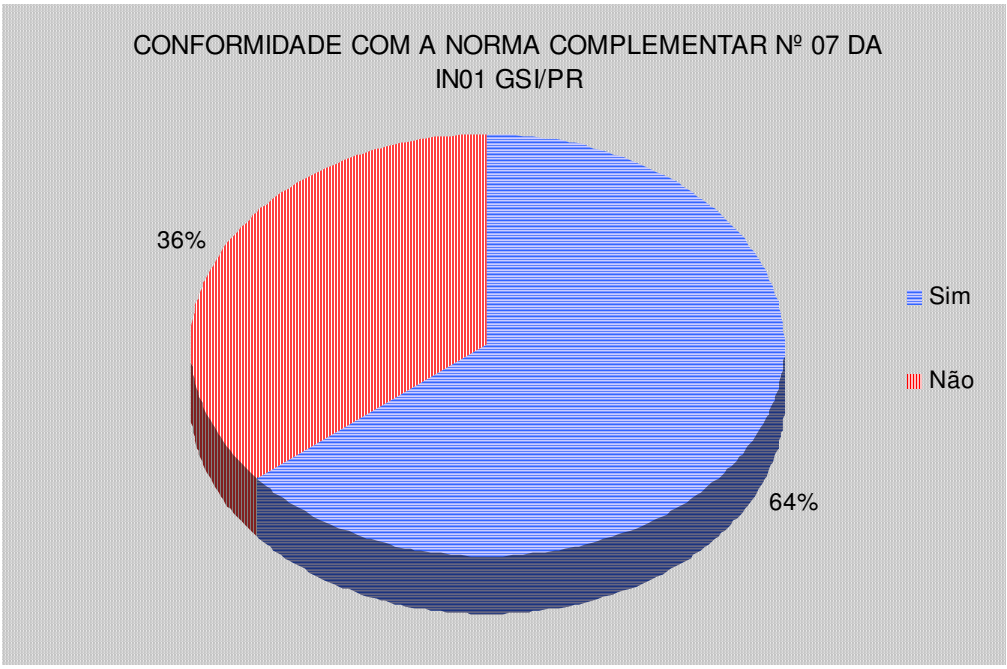

Gráfico 8 – Conformidade com a Norma Complementar nº 07 da IN 01 GSI-PR
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

A área de Controle de Acesso tem sido tratada com grande preocupação tanto pelo mercado quanto por governos, e o Governo Federal tem tentado conscientizar as instituições no âmbito de sua administração e implantarem controles eficientes, tanto lógicos como físicos, para proteção de seus ativos. Acontecimentos recentes em relação à espionagem internacional demonstraram que a implementação de controles rígidos em relação ao acesso de informações, não se restringe a áreas militares ou a órgãos de inteligência, mas a toda informação que esteja sobre a guarda de entes públicos de um modo geral.

Neste estudo, ficou demonstrado que o CNPq tem controles lógicos em conformidade com a norma e controles físicos eficientes em áreas seguras, mas falta avançar esses controle sobre outras áreas da instituição e ainda mais, falta a formalização desses procedimentos para estar em conformidade com as determinações do Governo Federal.

3.4.2. ANÁLISE SEPARADA POR ÁREA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES.

Este instrumento permitiu uma análise separada por área de Segurança da Informação e de uma certa forma, há uma concordância ou redundância com os resultados encontrados nas análises das normas específicas do GSI/PR. Isso se justifica, porque o Governo tem buscado orientar as instituições da APF, normatizando cada assunto referente à Gestão de SIC.

Mas essa análise é importante, porque oferece ao gestor uma visão que permite que ele priorize suas ações de acordo com o que é crítico para a sua organização e também de acordo com o que está alinhado à missão e às estratégias da organização. O que se observa nos resultados da pesquisa, apresentados nos 12 Gráficos seguintes, é que a política do CNPq não tem avançado de forma harmônica, estando bastante conforme em algumas áreas e bem atrasado na conformidade com outras áreas.

a) Análise da conformidade com a Política de Segurança da Informação e Comunicações.

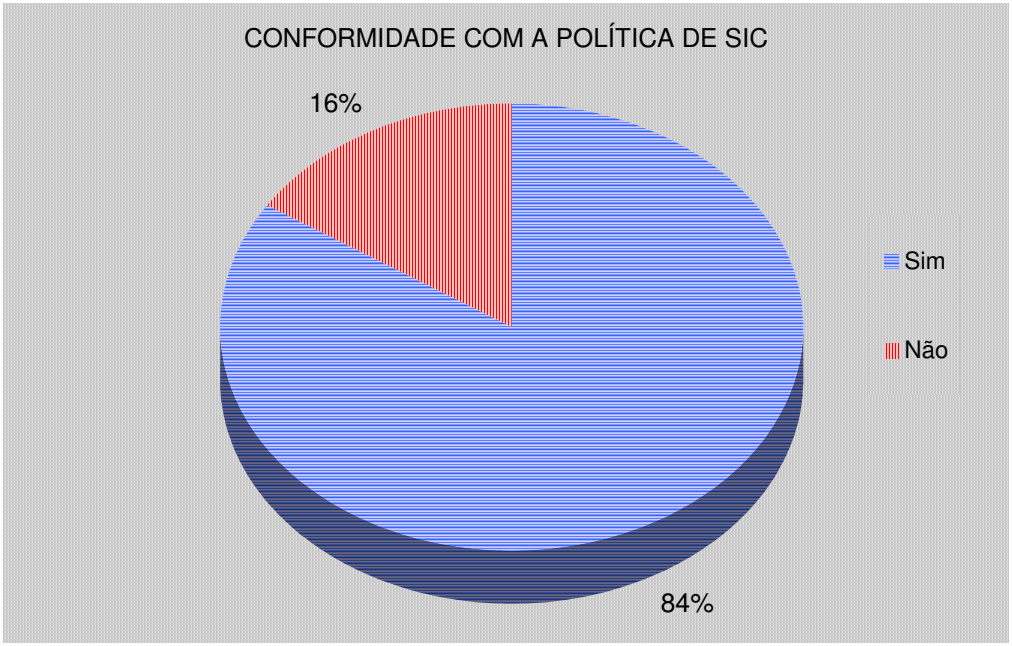

Gráfico 9 – Conformidade com a Política de Segurança da Informação e Comunicações
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

b) Análise da conformidade com a Gestão de Segurança da Informação e Comunicações.

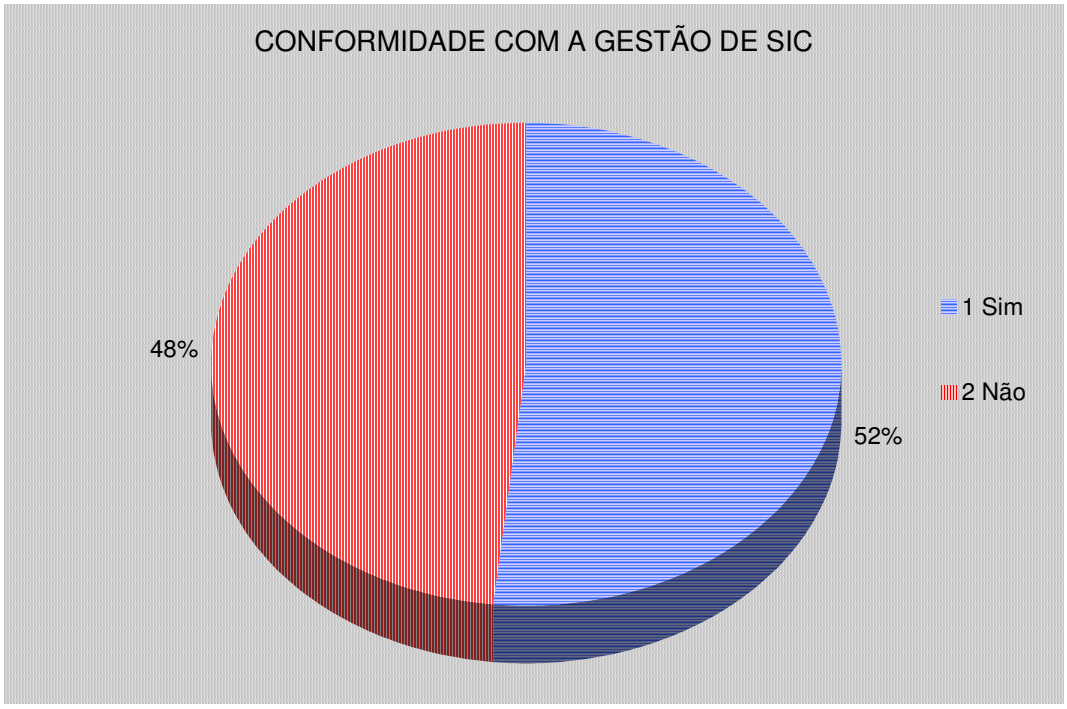

Gráfico 10 – Conformidade com a Gestão de Segurança da Informação e Comunicações
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

c) Análise da conformidade com a Gestão de Ativos.

Gráfico 11 – Conformidade com a Gestão de Ativos
Fonte: Confeccionado pelo autor a partir de dados da pesquisa

d) Análise da conformidade com a Segurança em Recursos Humanos.

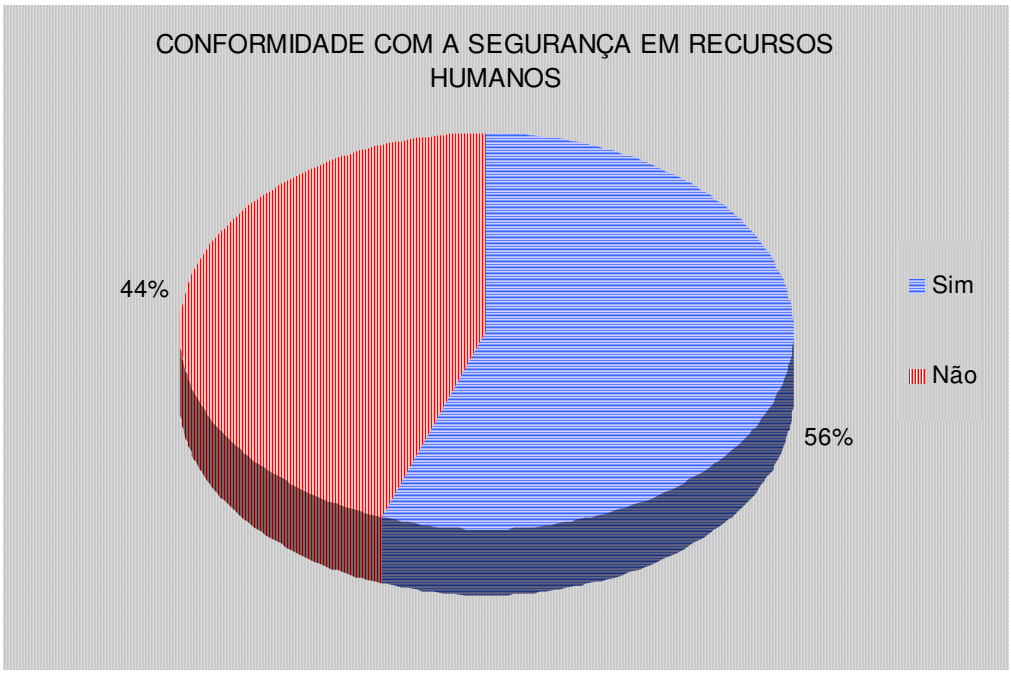

Gráfico 12 – Conformidade com a Gestão de Recursos Humanos
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

e) Análise da conformidade com a Segurança Física e do Ambiente.

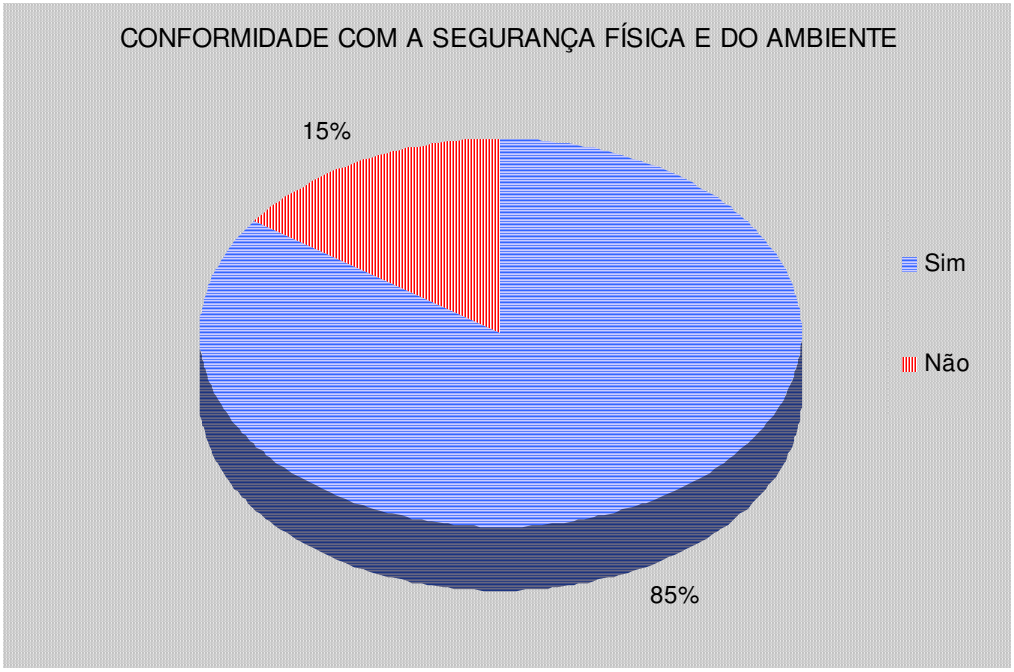

Gráfico 13– Conformidade com Gestão de Segurança Física e do Ambiente
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

f) Análise da conformidade com o Gerenciamento das Operações e Comunicações.

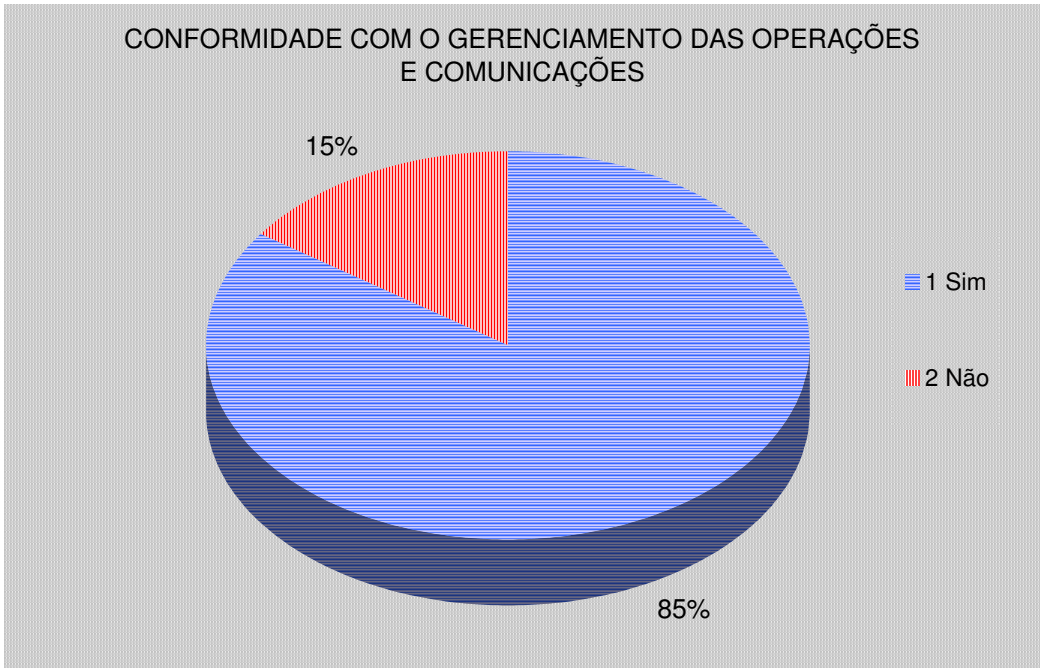

Gráfico 14 – Conformidade com o Gerenciamento das Operações e Comunicações
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

g) Análise da conformidade com o Controle de Acesso.

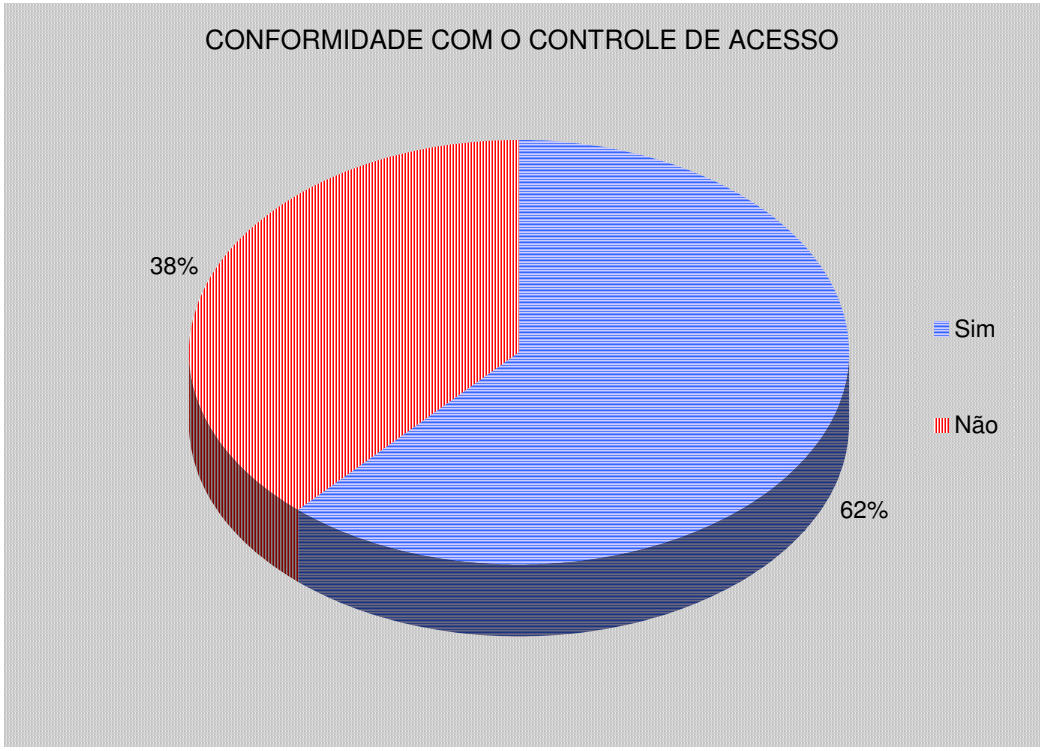

Gráfico 15 – Conformidade com o Controle de Acesso.
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

h) Análise da conformidade com Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação.

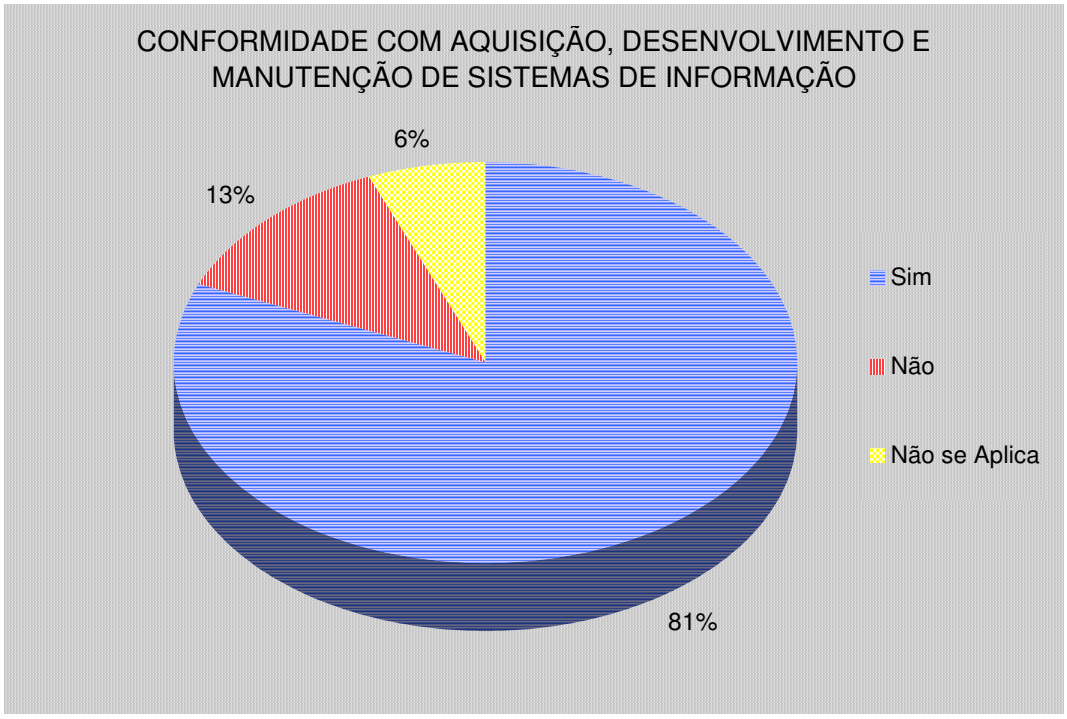

Gráfico 16 – Conformidade com a Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação.
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

i) Análise da conformidade com a Gestão de Incidentes de Segurança da Informação.

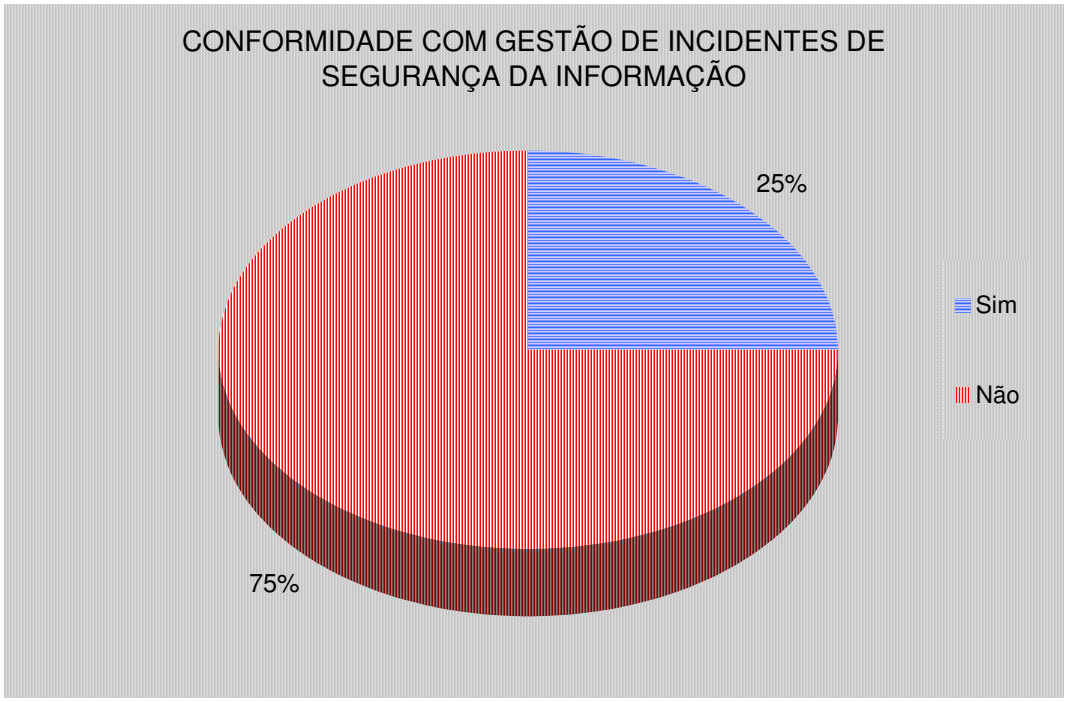

Gráfico 17 – Conformidade com a Gestão de Incidentes de Segurança da Informação.
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

j) Análise da conformidade com a área de Gestão de Continuidade de Negócios.

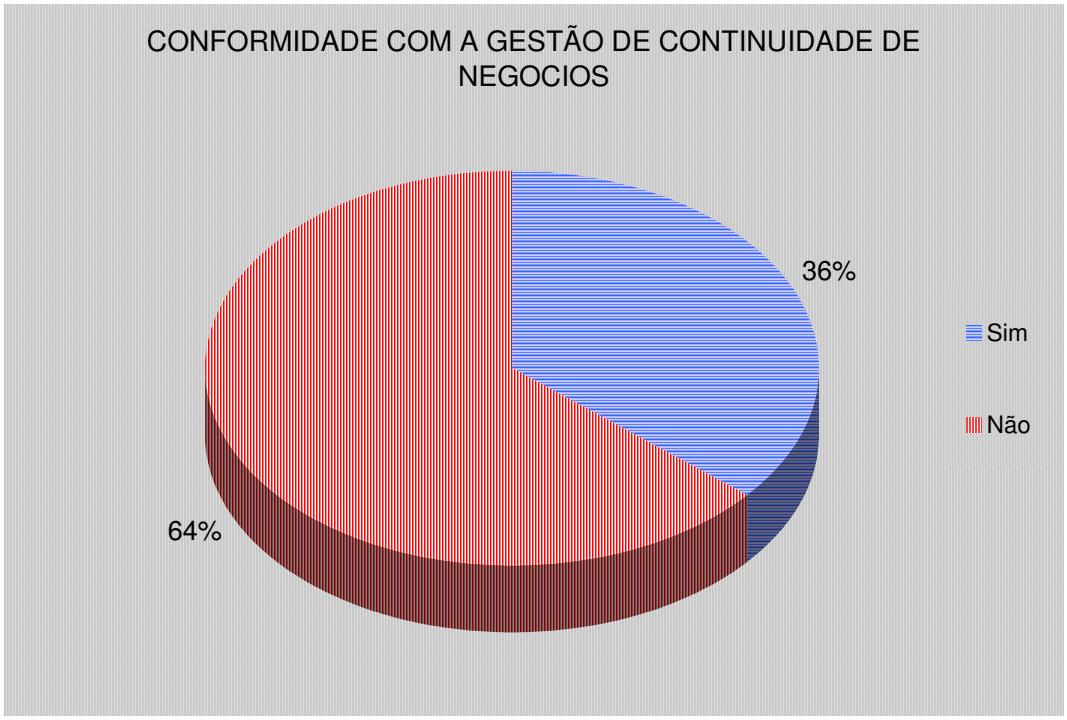

Gráfico 18– Conformidade com a Gestão de Continuidade de Negócios.
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

k) Análise da conformidade com a área de Conformidade.

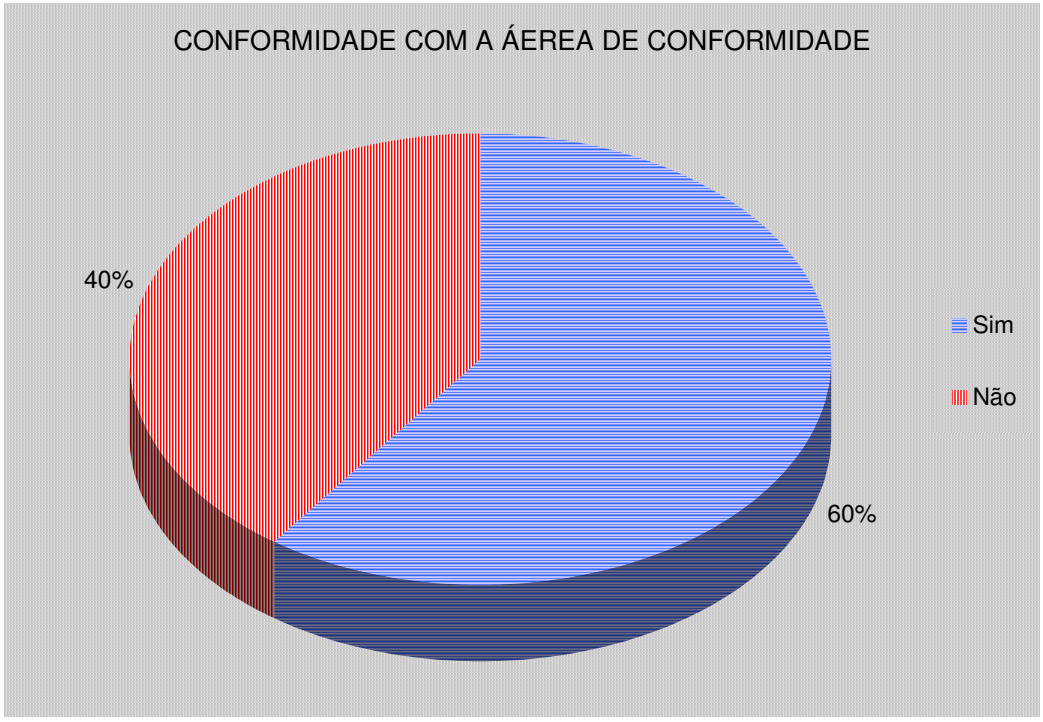

Gráfico 19– Conformidade com a Área de Conformidade.
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

l) Análise da conformidade com a área de Gestão de Riscos.

Gráfico 20 – Conformidade com a Gestão de Riscos
Fonte: Confeccionado pelo autor a partir de dados da pesquisa.

Os resultados apresentados acima mostram que o CNPq tem um bom caminho a ser percorrido na busca pela implementação plena de sua Política de Segurança da Informação e Comunicações. Mostram que existe uma conformidade mediana na maioria das áreas e até uma alta conformidade em áreas importantes, em que a instituição já implementou formalmente ações, como a institucionalização da POSIC e a formalização da área de Gestão da Segurança da Informação, mas apresenta uma pouca conformidade em áreas importantes, como Gestão de Riscos, Gestão de Continuidade de Negócios, e Gestão de Tratamento de Incidentes em Rede, que já se traduz como uma indicação em quais áreas os gestores do CNPq devem destinar suas atenções. Não que alguma área abordada não seja importante, mas essas áreas têm merecido muita atenção tanto do Governo Federal como do mercado de Segurança da Informação em geral.

Isso não significa que essas atividades não estejam implementadas no órgão ou que a informação esteja em um ambiente inseguro na mesma proporção da não conformidade com essas áreas, mas significa, principalmente, que as ações precisam ser adequadas ao que está determinado nas normas do Governo Federal e recomendado por várias instituições do mercado por meio de seus manuais de boas práticas em Segurança da Informação e Comunicações. Essa adequação otimiza o controle e facilita a gestão.

3.5. SUBSÍDIOS PARA MELHORIAS NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO DO CNPq.

A realização deste estudo trouxe à luz, detalhes das atividades de Segurança da Informação e Comunicações do CNPq. Ainda que os resultados estejam apresentados aqui de forma consolidada, eles, em conjunto com o previsto no planejamento da instituição, dão uma indicação de quais áreas da organização precisam de um olhar especial e com que urgência isso deve ocorrer.

Os resultados consolidados mostram com bastante clareza a situação da conformidade nas diversas áreas que norteiam o universo da Segurança da Informação e Comunicações, mas a pesquisa armazenada na tabela de histórico de verificações contém mais detalhes que estão à disposição dos gestores para a análise de especificidades. Isso pode contribuir muito para ações focadas ou bem específicas em determinado controle ou grupo de controles, quando necessário.

O mapeamento dos controles oriundos de várias fontes e armazenados em uma base de dados proprietária representa uma independência em relação a profissionais externos, quando se quiser fazer uma verificação de conformidade. Essa é uma contribuição importante, porque, ainda que se tenha que contratar auditorias externas periódicas, o fato de conter uma série histórica de verificações internas nos conduz a uma contratação mais específica, que tende a ter mais qualidade e possivelmente ser menos onerosa para a instituição.

Esse mapeamento e as aplicações dos controles mapeados mostraram pontos fortes e pontos fracos do CNPq em relação a áreas relativas à Gestão de SIC, e algumas áreas merecem destaque por serem vitais para a manutenção e sucesso das atividades do órgão e para a conformidade com a política do Governo Federal.

Assim, uma das contribuições que o estudo fornece é a demonstração da pouca conformidade do CNPq em relação à Gestão de Riscos, e as informações coletadas a partir da verificação mostram que o CNPq precisa investir em uma formalização da sua Gestão de Riscos. Essa Gestão deve constituir uma equipe que deverá trabalhar na identificação dos Riscos existentes nas atividades da instituição, não somente de TIC, mas do órgão como um todo. Esses riscos devem ser valorados em função das prioridades e as estratégias da Instituição, bem como pelas necessidades de atendimento às normas vigentes. Baseado nessa valoração a direção do órgão pode tomar decisões de aceitação ou não dos riscos.

Caberá a equipe de Gestão de Riscos tratar ou não os riscos de acordo com a decisão da direção, mas seja qual for a decisão, é importante que esses riscos estejam especificados.

Em relação à Gestão da Continuidade de Negócios, outra área importante de SIC, a pesquisa mostrou a necessidade de formalização da Gestão de Continuidade e Negócios (GCN). Essa gestão deve elaborar um Programa de Continuidade de Negócios, que deve ser atualizado a um período determinado, incluído Plano de Administração de Crises, Plano de Recuperação de Desastres e um Plano de Continuidade Operacional. Esses planos devem ser atualizados em um tempo determinado ou quando mudanças significativas ocorrerem. A equipe formada para essa gestão, deve se responsabilizar pela observação da necessidade de atualizações e de elaborações de planos de continuidade que auxiliem a gestão de SIC no âmbito do CNPq. O CNPq realizou a elaboração de um Plano de Continuidade de Negócios em 2009, mas contemplando somente a área de TIC, e este estudo mostra a necessidade de uma Gestão de Continuidade de Negócios aplicada a cada área da instituição.

A área de Conformidade tem sido muito evidenciada no mercado, e não somente o mercado de TIC. Empresas que atuam no mercado, em áreas diversas, buscam conformidade com padrões estabelecidos para agilizarem sua gestão e garantir qualidade de serviços. No caso do CNPq e de outros órgãos da Administração Pública Federal, e em relação à Segurança da Informação, busca-se conformidade com determinações do Governo e boas práticas, como já foi dito anteriormente. O Governo elaborou uma norma específica determinando ações para que os órgãos da APF façam estudos de conformidade. Este estudo vai ao encontro dessas determinações e constata que o CNPq não tem feito essas verificações e precisa implementar ações de verificação de conformidade como esta.

A conformidade traz benefícios como a agilização de tarefas, busca rápida de soluções de problemas, implementar padrões a serem seguidos por todos que resulta em aumento da segurança na obtenção de resultados, e constitui-se, portanto, em um importante princípio para a melhoria dos processos institucionais. Este estudo deixa evidente a necessidade de se continuar fazendo estudos de conformidade e da implementação de um processo continuo para este fim.

O estudo mostrou, também, que muitas ações de SIC têm sido efetuadas diariamente pelo CNPq, porém, mostrou uma não conformidade muito grande com a metodologia proposta pelo Governo. O que os resultados sugerem é a necessidade de

instituição formal dessa ou de outra metodologia e que ela seja baseada no processo de melhoria continua (PDCA).

Outra área importante mostrada na pesquisa é o Tratamento de Incidentes em Redes computacionais. O Governo determinou a criação de uma Equipe de Tratamento e Resposta a Incidentes em Rede (ETIR) em cada órgão e que essa equipe esteja em constante contato com a ETIR do GSI/PR. O CNPq tem alguns procedimentos para tratamento de incidentes, mas o este estudo mostra que o CNPq não criou a sua ETIR e que suas ações de tratamento de incidentes deve se adequar ao que determina a Norma do GSI/PR.

Em Segurança de Recursos Humanos, as verificações de controle apontam para a necessidade de mudança de cultura da instituição em relação à Segurança da Informação e Comunicações. O que o Governo pretende ao tratar dessa área é instituir uma cultura de valorização da informação em poder de cada um. Que trabalhadores tenham disciplina em observar se não estão negligenciando, no seu dia-a-dia, o trato com a informação que pode ser cara para si e para a instituição. As ações implementadas no CNPq que estão em conformidade com as normas analisadas, referem-se mais aos procedimentos legais como contratação e exclusão de trabalhador, a direitos e a exclusão de acesso, mas pouco foi realizado em relação à condução da mudança de cultura em Segurança da Informação e Comunicações.

Esses pontos levantados, que posteriormente podem ser detalhados e extrapolados, fornecem uma visão que pode contribuir para o estabelecimento de metas em busca da melhoria da Gestão de SIC. A facilidade de aplicação dessa pesquisa e a sugestão do instrumento, ainda que em seu estágio de concepção, podem constituir-se em um aliado para os gestores de cada área da instituição monitorar a conformidade de seus procedimentos e ações, com o que é desejado pela instituição e o que deve ser obedecido legalmente.

CONCLUSÃO

A atividade de Segurança da Informação e Comunicações consolidou-se nos últimos anos como uma importante área a ser gerenciada, a fim de garantir o sucesso de empreendimentos organizacionais. Empresas têm investido cada vez mais em estruturas, métodos e processos, que contemplem a garantia de disponibilidade, integridade e confiabilidade da informação. Isso justifica as ações do Governo Federal em implementar uma política de Segurança da Informação e Comunicações (SIC) para toda a Administração Pública Federal (APF).

O CNPq como uma instituição da APF, tem procurado, nesses últimos anos, acompanhar as ações do Governo relativas ao assunto e implementar o que tem sido recomendado e determinado, em relação a práticas relativas à SIC. O órgão possui uma boa infraestrutura de Tecnologia da Informação e Comunicações que com a implantação de padrões de mercado garante uma boa segurança para ativos de informação informatizados. Com o alto grau de informatização da instituição, essa segurança de TIC se configura como um bom começo para a implementação de uma política ampla de SIC.

Com o objetivo de aumentar a eficiência e implementar uma gestão de melhoria contínua, o CNPq tem buscado a conformidade com boas práticas em várias atividades referentes à informação e este estudo, de alguma forma, está nesse contexto de adequação almejada pela instituição. O que se viu, é que existem atividades que estão de acordo com o previsto para uma boa gestão de SIC, mas sem as formalidades exigidas pelo Governo Federal.

O estudo procurou conceituar Segurança da Informação sob a ótica do Governo Federal que a trata como um ativo importante a ser protegido. Para chegar ao conceito, procurou-se definir informação e entender a sua complexidade no contexto mundial atual. Mostrou a evolução da Segurança da Informação até os dias de hoje e como essa atividade torna-se complexa em um contexto de alta conectividade e grande atividade de processamento de informação.

Tudo isso, para mostrar como o Governo Federal tem definido sua Política de Segurança da Informação e Comunicações, e como tem procurado instrumentar os órgão da Administração Pública Federal com normas e procedimentos necessários à implantação dessa política.

Também apresentou um histórico da Tecnologia da Informação e Comunicações do CNPq, descrevendo os vários contextos tecnológicos pelos quais passou, a fim de demonstrar como o atual contexto é múltiplas vezes mais complexo que contextos anteriores e como se torna imprescindível que a Instituição implemente ações de segurança, pelo alto grau de informatização de suas atividades sensíveis, relativas, principalmente, às atividades de fomento.

A pesquisa de conformidade do CNPq com algumas normas editadas pelo Governo Federal e com a Norma 27001, realizada no período entre 01 de setembro de 2013 e 30 de setembro de 2013, mostrou a realidade do CNPq em relação ao que determina o Governo para seus órgãos subordinados. Ainda que não tenham sido mapeados os controles de todas as normas, o estudo mostrou dados importantes para subsidiar o CNPq em sua gestão de SIC. Esse conjunto, composto pela Norma 27001 e por seis normas do GSI/PR, foi escolhido, em conjunto com o Gestor de SIC do CNPq, por representar assuntos prioritários para qualquer instituição que pretenda implementar um mínimo de segurança para suas informações.

Como a Norma 27001 já abrange 11 áreas relativas à atividade de Segurança da Informação e Comunicações, e o Governo tem usado essa norma, dentre outras, para embasar a elaboração e publicação de suas normas legais, o estudo ganhou uma consistência que empresta confiabilidade aos resultados encontrados. Porém, além dos números apresentados, o estudo teve o objetivo de testar a eficácia de um modelo de pesquisa e guarda dos dados encontrados, que possa subsidiar, cotidianamente, gestores das diversas áreas do CNPq na verificação da conformidade de suas atividades com o que é determinado pelo Governo.

O modelo mostrou-se dinâmico e a expectativa é que ele sofra evoluções, com o acréscimo de novos atributos, à medida que o CNPq e suas áreas de gestão, bem como o corpo de trabalhadores do órgão, amadureçam seus conhecimentos, práticas e cultura em Segurança da Informação e Comunicações, e possam contribuir com novas dimensões a serem exploradas por um instrumento que o utilize. A ideia de guardar as verificações em tabelas do banco de dados relacional tem por objetivo, agilizar a recuperação das informações referentes às verificações realizadas, e a explorar a facilidade de associar novas tabelas e novos atributos, ou ainda, de considerar novas dimensões para o modelo, enfim, algo que possa evoluir junto com o crescimento da maturidade da instituição em relação a essas atividades.

A partir da realização da pesquisa e da análise dos controles aplicados, bem como dos resultados encontrados, surgiram algumas constatações que nos possibilitam recomendar algumas ações em curto prazo, para melhorar a conformidade com as normas legais e boas práticas do mercado de SIC, e também para incrementar o modelo ora apresentado:

1) Continuar o cadastramento de controles existentes nas demais normas do Governo Federal e em outras normas que recomendem boas práticas, para ampliar o universo de verificação de conformidade.
2) Realizar novas rodadas de verificação, com o devido registro dos resultados na tabela histórico de verificações, em prazos de no máximo seis meses, pelos próximos dois anos.
3) Estabelecer metas de conformidade, a partir dos resultados das séries de verificações, a fim de conseguir gradativamente a melhoria da conformidade geral em SIC.
4) Procurar construir indicadores qualitativos para estabelecer a aplicabilidade ou não de controles em atividades da instituição, quando essa aplicabilidade for facultativa.
5) A partir dos indicadores de aplicabilidade, fazer uma declaração formal de aplicabilidade desses controles. A declaração de aplicabilidade é um dos controles contidos na Norma 27001.
6) Realizar um inventário dos ativos de todas as áreas da instituição e criar um modelo de cadastramento e atualização desses ativos, a fim de que eles possam ser monitorados e atualizados de forma eficiente.
7) Estabelecer uma política de Gestão de Risco, e buscar a criação de indicadores para a classificação de riscos, nos critérios sugeridos pelas boas práticas: Baixo, Médio e Alto.
8) Ampliar a Gestão de Continuidade de Negócios, para todas as áreas da Instituição, considerando os ativos geridos em cada área.
9) Aperfeiçoar o modelo e a partir dele, construir ou adquirir um instrumento ou uma ferramenta de gestão de conformidade.

Esse conjunto de recomendações iniciais visa à melhoria da conformidade e também à melhoria da gestão de SIC de um modo geral e, se observadas, poderão contribuir para estabelecer um novo patamar de conformidade do CNPq com as determinações e recomendações do Governo em relação à SIC.

A pesquisa mostrou que mesmo executando ações tecnológicas de alto nível e mesmo implementando procedimentos em Segurança da Informação e Comunicações, é necessário a observação de controles estabelecidos e, em muitos casos, já testados pelo mercado, para melhorar a conformidade com o que é desejável para Segurança da Informação e Comunicações. E mostrou que, com um instrumento simples de verificação de conformidade pode-se contribuir com informações importantes para a tomada de decisão dos gestores, em relação ao aumento dessa conformidade.

Enfim, este estudo procurou atender às características primordiais de um Mestrado Profissional e os resultados apresentados, mais do que servir de referência a outros estudos, podem ter uma aplicabilidade imediata e contribuir para o aperfeiçoamento das atividades relativas ao tema, no âmbito do CNPq.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 27002:2005. **Tecnologia da informação - Técnicas de Segurança - Código de prática para a gestão da segurança da informação**. 2ª edição. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2005.

ABNT NBR ISO/IEC 27001:2006. **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos.** Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2006.

ABNT NBR ISO/IEC Guia 73:2005. **Gestão de riscos – Vocabulário - Recomendações para uso em normas.** Associação Brasileira de Normas Técnicas. Rio de Janeiro. 2005

ARAÚJO, Carlos Alberto A. **O conceito de informação na ciência da informação**. Informação & Sociedade, v. 20, n. 3, p. 95-105, 2010.

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.

_____. **Instrução Normativa GSI nº 1, de 13 de Junho de 2008**. Disciplina a Gestão da Segurança da Informação e Comunicações na Administração Pública Federal.

_____. **Norma Complementar nº 2 da IN01 GSI/PR, de 13 de outubro de 2008**. Define a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da Administração Pública Federal.

_____. **Norma Complementar nº 3 da IN01 GSI/PR, de 30 de junho de 2009**. Estabelece 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.

_____. **Norma Complementar nº 4 da IN01 GSI/PR, de 15 de fevereiro de 2013**. Estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal.

_____.**Norma Complementar nº 6 da IN01 GSI/PR, de 11 de novembro de 2009**. Estabelece diretrizes para a Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal.

_____. **Norma complementar n° 07 da IN01 GSI/PR, de 06 de maio de 2010**. Estabelece 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.

_____. **Lei nº 12.527, de 18 de novembro de 2011**. 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.

CAPURRO, Rafael; HJORLAND, Birger. **O conceito de informação**. Perspectivas em Ciência da Informação, Belo Horizonte,v.12, n.1, p. 148-207, jan./abr. 2007.

CNPq. **História**. Disponível em http: <www.cnpq.br/web/guest/o-cnpq>. Acessado em 30/09/2013.

_____. **História do CNPq**. Disponível em <http://centrodememoria.cnpq.br>. Acessado em 30/09/2013.

_____. **O CNPq e a Formação de Recursos Humanos de C&T para o Brasil**. Estatísticas de Bolsas no País e no Exterior, 1980-85. Brasília: CNPq, 1996. 114 p.

_____. **O Fomento do CNPq nos Estados e Instituições de Pesquisa, 1997**. Brasília: CNPq, 1998. 340 p.

_____. **O Fomento do CNPq nos Estados e Instituições de Pesquisa, 1999**. Brasília: CNPq, 2000. 329 p.

_____. **O Fomento do CNPq nos Estados e Instituições de Pesquisa, 2001**. Brasília: CNPq, 2002. 424 p.

_____. **Política de Segurança da Informação e Comunicações - POSIC**. Publicada no DOU de 24/10/2012, Seção 1, página 6.

DATE, C. J. **Introdução a sistemas de banco de dados**/ C.J.Date: tradução de Daniel Vieira – Rio de Janeiro: Elsevier, 2003 – (9ª reimpressão)

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. 1ª. Edição, AXCEL BOOKS, 2000

FERMA. **A risk management standard**. Disponível em: http://www.ferma.eu/wp-content /uploads/2011/11/a-risk-management-standard-portuguese-version.pdf. Acessado em 30/09/2013.

FONSECA FILHO, C. **História da computação**: **O caminho do Pensamento e da Tecnologia.** Porto Alegre: EDIPUCRS, 2007, 205 p.

HOUAISS, Antônio. In: **Dicionário da Lingua Portuguesa On-line**. Disponível em: http://intranet.cnpq.br/index.htm. Acessado em julho de 2013.

LAUREANO, Marcos A. P. **Gestão de Segurança da Informação**. Disponível em http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf. Acessado em junho/2013.

LE COADIC, Yves-Francois. **A Ciência da Informação**; Tradução de Maria Yêda F. S. de Filgueiras Gomes – Brasília, DF: Briquet de Lemos/Livros, 1996.

MARCIANO, João Luiz P. **Segurança da Informação - uma abordagem social**. Tese (Tese de Doutorado) - Departamento de Ciência da Informação e Documentação da Universidade de Brasília, Brasília, DF, Julho 2006.

PEREZ,Carlota.**Technological revolutions and techno-economic paradigms**. In Cambridge Journal of Economics 2010, Vol. 34, pp. 185–202.

PINHEIRO, Lena Vânia R. **Informação - Esse Obscuro Objeto da Ciência da Informação**. IBICT/Coordenação de Ensino e Pesquisa, Doutora em Comunicação e Cultura, UFRJ/ECO. Artigo Disponível em: <http://ridi.ibict.br/bitstream/123456789/31/1/Morpheus2004Pinheiro. pdf>. Acessado em: junho/2013.

TCU. **Boas práticas em segurança da informação** / Tribunal de Contas da União. – 3. ed. – Brasília :TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2008. 70 p.

Anexo A – Check List

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
001	Existe uma política de Segurança da Informação aprovada pela direção, publicada e comunicada para todos os funcionários e partes externas relevantes?	
002	Exise um processo de análise crítica da política de SI, em intervalos planejados ou quando mudanças significativas ocorrem, para assegurar a sua contínua pertinência, adequação e eficácia?	
003	A Direção apoia ativamente a segurança da informação dentro da organização, de forma clara, demonstrando o seu comprometimento, definindo atribuições de forma explícita e conhecendo as responsabilidades pela segurança da informação?	
004	As atividades de segunrança da informação são coordenadas por representantes de direrentes partes da organização, com funções e papéis relevantes?	
005	As responsabilidades pela Segurança da Informação estão claramente definidas?	
006	A Instituição definiu e Implementou um processo de gestão de autorização para novos recursos de processamento da informação	
007	Os requisitos de confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação SÃO identificados e analisados criticamente, de forma regular?	
008	São mantidos contados com autoridades relevantes em Segurança da Informação?	
009	São mantidos contados com grupos de interesses especiais ou outros foruns especializados em Segurança da Informação?	
010	O enfoque da instituição para gerenciar e implementar a Segurança da Informação É analisado criticamente, de forma independente, periodicamente ou quando ocorrem mudanças significativas relativas a implementação de SI?	
011	Os Riscos para os recursos de processamento da informação e para a informação da organização oriundos de processos do negócio que envolvam as partes externas SÃO identificados e os Controles apropriados são implementados antes da concessão de acesso?	
012	Os requisitos de segurança da informação identificados SÃO considerados antes da concessão de acesso aos ativos ou às informações da Instituição?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
013	Os acordos com terceiros para acesso, processamento, comunicação ou gerenciamento de recursos de processamento da informação ou da informação da instituição COBREM todos os requisitos relevantes de SI	
014	Os acordos com terceiros para acrescimo de produtos ou serviços aos recursos de processamento da informação COBREM todos os requisitos relevantes de SI?	
015	Os ativos da Instituição estão claramente identificados?	
016	A Instituição mantém um inventário estruturado dos seus ativos importantes?	
017	Todas as informações e ativos da instituição, associados com os recursos de processamento da informação, têm um responsável designado por uma parte definida da instituição?	
018	As regras de permissão de uso de informações e de ativos associados aos recursos de processamento da informação, ESTÃO identificadas e documentadas?	
019	As regras de permissão de uso de informações e de ativos associados aos recursos de processamento da informação, ESTÃO implementadas?	
020	As Informações estão classificadas considerando o seu Valor, os Requisitos Legais, a Sensibilidade e Criticidade para a Instituição?	
021	Foi definido e implementado um conjunto apropriado de procedimentos para rotular e tratar a informação, de acordo com o esquema de classsificação adotado pela instituição?	
022	Os papéis e responsabilidades pela Segurança da Informação tanto de funcionários, como de fornecedores e terceiros, ESTÃO definidos e documentados de acordo com a Política de Segurança da Informação da Instituição?	
023	São feitas verificações de controle de candidatos a emprego, fornecedores e terceiros, de acordo com a legislação vigente e a ética, e considerando os requisitos de negócio, a classificação da informação a serem acessadas e aos riscos envolvidos?	
024	A instituição implementou a assinatura de um termo, no momento da contratação tanto de Funcionários, como de fornecedores e de terceiros, onde estão explicitas as responsabilidades de contratados e da instituição, em relação à Segurança da Informação?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
025	A Direção da Instituição solicita claramente, no momento da contratação, a funcionários, fornecedores e terceiros que pratiquem a Segurança da Informação de acordo com o estabelecido nas políticas e procedimentos da Instituição?	
026	A Instituição promove treinamento apropriado em conscientização a funcionários, fornecedores e terceiros, bem como atualizações regulares nas políticas de procedimentos organizacionais relevantes às suas funções?	
027	Existe um processo disciplinar formal para os funcionários que tenham cometido uma violação da Segurança da Informação?	
028	As responsabilidades para realizar o encerramento de um contrato de trabalho ESTÃO claramente definidas e atribuidas?	
029	No encerramento ou mudança de contrato ou atividades, tanto Servidores, como fornecedores e terceiros procedem formamalmente à devolução dos ativos da instituição que estejam em sua posse?	
030	Os direitos de acesso de servidores, fornecedores e terceiros a informações e a recursos de processamento de informação SÃO retirados em caso de encerramento de contrato ou de atividade, ou SÃO ajustados em caso de mudança de atividades?	
031	A Instituição tem delimitado áreas seguras, com barreiras adequadas, em locais que contenham informações e recursos de processamento da informação?	
032	As áreas seguras SÃO protegidas por controles apropriados de entrada para assegurar que somente pesoas autorizadas tenham acesso?	
033	A Instituição projetou a segurança física para salas e instalações?	
034	A Instituição projetou e aplica proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem?	
035	A Instituição projetou e aplica proteção física e diretrizes para o trabalho em áreas seguras?	
036	A Instituição controla pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos de entrada, para evitar o acesso não autorizado a recursos de processamento de informação?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
037	Os equipamentos estão instalados em locais protegidos de ameaças e perigos do meio ambiente, bem como de oportunidades de acesso não autorizado?	
038	Os equipamentos SÃO protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades?	
039	Os cabeamentos de energia e de telecomunicações que trasportam dados ou dá suporte aos serviços de informações SÃO protegidos contra interrupções ou danos?	
040	Os equipamentos TÊM manutenção com a periodicidade adequada, de forma a assegurar a sua disponibilidade e integridade permanente?	
041	EXISTE medidas de segurança para equipamentos que operem fora das dependências da Instituição, de forma a minimizar riscos?	
042	Os equipamentos que possuem mídias de armazenamento de dados SÃO examinados antes do descarte, para garantir a remoção de dados sensíveis ou softwares licenciados?	
043	É preparada uma autorização prévia para retirada de equipamentos, informações ou softwares da instituição?	
044	Os procedimentos de operação dos recursos de processamento da informação SÃO documentados, mantidos atualizados e disponíveis a todos o usuários que deles necessitem?	
045	As modificações nos recursos de processamento da informação e sistemas SÃO controlados?	
046	Funções e áreas de responsabilidades SÃO segregadas visando a redução das oportunidades de modificação ou uso indevido, não autorizado ou não intencional, dos ativos da organização?	
047	Os recursos de desenvolvimento, teste e produção ESTÃO separados em ambientes específicos para reduzir o risco de acesso ou modificações não autorizadas aos sistemas em produção?	
048	EXISTEM garantias que os controles de segurança, definições de serviço e os níveis de entrega, constantes dos acordos de entrega de serviços, sejam implementados, executados e mantidos pelo terceiro?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
049	Os serviços, relatórios e registros fornecidos por terceiro SÃO regularmente monitorados e analisados criticamente?	
050	SÃO executadas auditorias regulares nos serviços terceirizados?	
051	As mudanças no provisionamento dos serviços de terceiros, incluindo manutenção e melhorias em Segurança da Informação, SÃO gerenciadas levando-se em conta a criticidade dos sistemas e processos de negócios envolvidos e reanálise/reavaliação de riscos?	
052	A utilização dos recursos É monitorada e sincronizada para garantir o desempenho requerido do sistema?	
053	SÃO feitas projeções para as necessidades de capacidade futura de forma a manter o desempenho requerido do sistema?	
054	EXISTEM critérios estabelecidos para aceitação de novos sistemas, atualizações e novas versões?	
055	SÃO efetuados testes apropriados dos sistemas durante o seu desenvolvimento e antes de sua aceitação?	
056	EXISTEM controles implementados para detecção, prevenção e recuperação, para proteção contra códigos maliciosos?	
057	EXISTEM procedimentos de conscientização de usuários para prevenção contra códigos maliciosos?	
058	EXISTEM controles implementados para garantir que códigos móveis autorizados operem de acordo com a política de Segurança da Informação definida pela instituição, e para que códigos móveis não autorizados tenham sua execução impedida?	
059	SÃO efetuadas e testadas regularamente, cópias das informações e softwares, de acordo com uma política definida de geração de cópias de segurança?	
060	As Redes da Instituição são adequadamente gerencias e controladas, de forma a garantir a proteção contra ameaças e manter a segurança das informações, de sistemas e de aplicações?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
061	As características de segurança, de níveis de serviço e de requisitos de gerenciamento dos serviços SÃO devidamente identificados e incluidos nos acordos de serviço de Rede, em contratos mantidos pela instituição?	
062	EXISTEM procedimentos implementados para o gerenciamento de mídias removíveis?	
063	EXISTEM procedimentos formais para o descarte de mídias, de forma segura e protegida, quando não forem mais necessárias?	
064	EXISTEM procedimentos estabelecidos para o tratamento e o armazenamento de informações, de modo a protegê-las contra a divulgação não autorizada ou o uso indevido?	
065	EXISTEM procedimentos formais de proteção da documentação de sistemas contra acessos não autorizados?	
066	EXISTEM Políticas, procedimentos e controles estabelecidos e formalizados visando a proteção na troca de informações em todos os tipos de recursos de comunicação?	
067	EXISTEM acordos estabelecidos para a troca de informações e software entre a instituição e entidades externas?	
068	EXISTEM procedimentos de proteção contra acesso não autorizado, uso impróprio ou alteração indevida, durante o transporte externo aos limites físicos da organização, para mídias contendo informação,?	
069	EXISTE proteção adequada para o tráfego de mensagens eletrônicas no âmbito da instituição?	
070	EXISTEM políticas e procedimentos desenvolvidos e implementados para proteger as informações associadas com a interconexão de sistemas de informações do negócio da instituição?	
071	EXISTE proteção adequada para as informações envolvidas em comércio eletrônico transitando sobre a rede da instituição, contra atividades fraudulentas, disputas contratuais, divulgação e modificações não autorizadas?	
072	EXISTEM procedimentos seguros nas transações on-line para proteção das informações, de forma a prevenir transmissões incompletas, erros de roteamentos,e alterações, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
073	As Informações disponibilizadas em sistemas com acesso público ESTÃO protegidas contra modificações não autorizadas?	
074	Os Registros de auditoria (Log) contendo atividades dos usuários, exceções e outros eventos de segurança da informação, que possam auxiliar em auditorias, SÃO produzidos e mantidos adequadamente por um período definido na política da instituição?	
075	EXISTEM procedimentos estabelecidos para o monitoramento regular do uso dos recurso de processamento da informação, com análise critica dos resultados?	
076	EXISTE proteção adequada para os recursos e informações de registros (log) contra falsificação e acesso não autorizado?	
077	As atividades dos administradores e operadores do sistema SÃO registradas?	
078	As falhas ocorridas SÃO registradas e analisadas, e as ações apropriadas de correção são adotadas?	
079	EXISTE sincronização, de acordo com uma hora oficial, dos relógios de todos os sistemas de processmento de dados relevantes, dentro da instituição ou dentro do domínio de segurança?	
080	EXISTE uma política de controle de acesso estabelecida, documentada e analisada criticamente, em concordância com os requisitos de acesso dos negócios e também da Segurança da Informação?	
081	EXISTE um procedimento formal de registro e cancelamento de usuário, que garanta e revogue acessos em todos os sistemas de informação e serviços?	
082	A concessão e o uso de privilégios SÃO restritos e controlados?	
083	EXISTE um processo de gerenciamento formal para concessão de senhas de acesso?	
084	O gestor de acesso CONDUZ regularmente análise crítica dos direitos de acesso dos usuários, por meio de um processo formal?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
085	EXISTE uma orientação aos usuários para seguir boas práticas de Segurança da Informação, tanto na composição da senha quanto no seu Uso?	
086	EXISTE orientação para que usuários protejam adequadamente equipamentos não monitorados pela rede?	
087	EXISTE um controle automático que bloqueia automaticamente a tela do computador quando estiver ocioso por um determinado tempo (política de tela limpa)?	
088	EXISTE Orientação e conscientização dos usuários para que mantenham a mesa limpa de papéis e midias de armazenamento removíveis?	
089	EXISTE um controle para que usuários recebam acesso somente aos serviços que tenham sido especificamente autorizados a usar?	
090	SÃO utilizados métodos apropriados de autenticação para controlar o acesso de usuários remotos?	
091	A autenticação de conexões vindas de localizações e equipamentos específicos É feita considerando a identificação automática de equipamentos?	
092	Os acessos físico e lógico SÃO controlados no diagnóstico e configuração de portas remotas?	
093	Os grupos de serviço de informação, usuários e sistemas de informação SÃO segregados em redes?	
094	A capacidade de conexão de usuários É calculada e restringida de acordo com a política de controle de acesso e os requisitos das aplicações de negócio?	
095	EXISTE um controle de roteamento para assegurar que conexões não violem a política de controle de acesso das aplicações do negócio?	
096	O acesso aos sistemas operacionais É controlado por um procedimento seguro de log-on?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
097	EXISTE um identificador único para cada usuário se autenticar, utilizando uma técnica de autenticação adequada?	
098	Os sistemas de gerenciamento de senha SÃO interativos e asseguram a construçãao de senhas de qualidade?	
099	O uso de programas utilitários que podem sobrepor os controles dos sistemas de aplicações É restrito e estritamente controlado?	
100	EXISTE procedimento que garanta que os terminais inativos são desconectados após um período definido de inatividade?	
101	SÃO utilizadas restrições nos horários de conexão para proporcionar segurança adicional pra aplicações de alto risco?	
102	O acesso à informação e às funções dos sistemas de aplicações por usuários e pessoal de suporte É restringido de acordo com a política de controle de acesso?	
103	EXISTE um ambiente computacional isolado para sistemas sensíveis?	
104	EXISTE uma política formal para regular o uso de recursos de computação e comunicação móveis, visando a proteção contra riscos para a segurança da informação?	
105	EXISTE uma política, planos operacionais e procedimentos desenvolvidos e implementados para atividades de trabalho remoto?	
106	Os requisitos para controles de segurança SÃO especificados nas especificações de requisitos de negócios, para novos sistemas de informação ou melhorias em sistemas existentes?	
107	Os dados de entrada de aplicações SÃO validados para garantir que são corretos e apropriados?	
108	As checagens de validação SÃO incorporadas nas aplicações, com o objetivo de detectar qualquer corrupção de informações, por erros ou por ações deliberadas?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
109	Os requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações SÃO identificados e os controles apropriados SÃO identificados e implementados?	
110	Os dados de saída das aplicações SÃO validados para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias?	
111	EXISTE uma política desenvolvida e implementada para o uso de controles criptográficos visando a proteção da informação?	
112	EXISTE um processo de gerenciamento de chaves implementado para apoiar o uso de técnicas criptográricas pela organização?	
113	EXISTEM procedimentos implementados para controlar a instalação de software em sistemas operacionais?	
114	Os dados de teste SÃO selecionados com cuidado, protegidos e controlados?	
115	EXISTE controle para restringir o acesso a código-fonte de programas?	
116	A implementação de mudanças É controlada utilizando procedimentos formais de controle de mudanças?	
117	Quando sistemas operacionais são mudados, as aplicações críticas de negócios SÃO analisadas criticamente e testadas, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança?	
118	EXISTEM restrições para mudanças em pacotes de software, limitando-se às mudanças necessárias que são estritamente controladas?	
119	As oportunidades para vazamento de informações SÃO prevenidas?	
120	A instituição SUPERVISIONA e MONITORA o desenvolvimento terceirizado de software?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
121	As informações sobre vulnerabilidades técnicas dos sistemas de informação em uso SÃO obtidas em tempo hábil, avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados?	
122	Os eventos de Segurança da Inforamação SÃO relatados através dos canais apropriados da direção, o mais rapidamente possível?	
123	Os funcionários, fornecedores e terceiros de sistemas e serviços de informação SÃO instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade em sistemas ou serviços?	
124	ESTÃO estabelecidas as responsabilidades e procedimentos de gestão, para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação?	
125	ESTÃO estabelecidos mecanismos para permitir que tipos, quantidades e custos dos incidentes de sergurança da informação sejam quantificados e monitorados?	
126	Quando de uma ação legal envolvendo incidente em segurança da informação, as evidências SÃO coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição ou jurisdições pertinentes?	
127	EXISTE um processo de gestão, mantido para assegurar a Continuidade do negócio por toda a instituição e que contemple os requisitos de Segurança da Informação necessários à continuidade do negócio da Instituição?	
128	ESTÃO identificados os eventos que podem causar interrupções aos processos de negócio, bem como a propabilidade e impacto de tais interrupções e as consequências para a segurança da informação?	
129	Os planos de continuidade relativos à SI foram desenvolvidos e implementados para assegurar a disponibilidade da informação no nível e na escala de tempo requeridos, após a ocorrência de interrupções ou falhas dos processos críticos do negócio?	
130	A instituição MANTÉM uma estrutura básica dos planos de continuidade do negócio para assegurar que todos planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção?	
131	Os planos de continuidade do negócio SÃO testados e atualizados regularmente de forma a assegurar sua permanente atualização e efetividade?	
132	Todos os requisitos estatutários, regulamentares e contratuais relevantes, e o enfoque da instituição para atender a esses requisitos ESTÃO definidos, documentados e mantidos atualizados para cada sistema de informação da Instituição?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
133	EXISTEM procedimentos apropriados implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no o uso de material com direitos de propriedade intelectual e no uso de produtos de software proprietários?	
134	EXISTE proteção de registros importantes contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estaturários, contratuais e do negócio?	
135	A privacidade e a proteção de dados ESTÃO assegurada conforme exigido nas legislações relevantes, regulamentações e, se aplicável, nas cláusulas contratuais?	
136	Os usuários SÃO regularmente, dissuadidos de usar os recursos de processamento da informação para propósitos não autorizados?	
137	Os controles de criptografia SÃO usados em conformidade com leis, acordos e regulamentações relevantes?	
138	EXISTE garantia, por parte dos gestores, que todos os procedimentos de segurança dentro de sua área de responsabilidade sejam executados corretamente para atender à conformidade com as normas e políticas de segurança da informação?	
139	Os sitemas de informação SÃO periodicamente verificados quanto à sua conformidade com as normas de segurança da informação implementadas?	
140	Os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais SÃO cuidadosamente planejados e acordados para minimizar os riscos de interrupção dos processos do negócio?	
141	O acesso às ferramentas de auditoria de sistemas de informação É protegido para prevenir qualquer possibilidade de uso impróprio ou comprometimento?	
142	A Instituição possui uma unidade para coordenar as ações de segurança da informação e comunicações?	
143	A Instituição aplica as ações corretivas e disciplinares cabíveis nos casoa de quebra de segurança?	
144	A Instituição especificou em seu orçamento, recursos para as ações de segurança da informação e comunicações?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
145	A Instituição constituiu um Gestor de Segurança da Informação e Comunicações	
146	A Instituição instituiu e implementou a ETIR - Equipe de Tratamento e Resposta a Incidentes em redes computacionais?	
147	A Instituição instituiu o Comitê de Segurança da Informação e Comunicações?	
148	A Instituição aprovou sua Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações?	
149	A Instituição remete os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações para o GSI?	
150	A Instituição segue os requisitos metodológicos, definidos pelo GSI-PR, para implementação da Gestão de Segurança da Informação e Comunicações?	
151	A Instituição está preparada para receber sugestões de melhorias ou denúncias de quebra de Segurança da Informação, no âmbito de sua atuação?	
152	O Comitê de Segurança da Informação e Comunicações - CSIC tem assessorado na implementação das ações de segurança da informação e comunicações?	
153	O CSIC tem atuado na constituição de grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações?	
154	O CSIC tem analisado a Política de Segurança da Informação e Comunicações e proposto alterações quando necessárias?	
155	O CSIC porpõe normas complementares relativas à Segurança da Informação e Comunicações?	
156	O Gestor de Segurança da Informação e Comunicações tem promovido a cultura de Segurança da Informação e Comunicações na Instituição?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
157	O Gestor de Segurança da Informação e Comunicações acompanha as insvestigações e as avaliações dos danos decorrentes de quebras de segurança?	
158	O Gestor de Segurança da Informação e Comunicações propõe a alocação dos recursos necessários às ações de Segurança da Informação e Comunicações?	
159	O Gestor de Segurança da Informação coordena o CSIC?	
160	O Gestor de Segurança da Informação coordena o ETIR?	
161	O Gestor de Segurança da Informação realiza e acompanha estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações?	
162	O Gestor de Segurança da Informação mantém contato direto com o DSIC pra o trato de assuntos relativos à Segurança da Informação e Comunicações?	
163	O Gestor de Segurança da Informação atua junto ao CSIC na proposição de normas relativas à segurança da informação e comunicações?	
164	A gestão de Segurança da Informação da Instituição está baseada no processo de melhoria contínua (PDCA)?	
165	O escopo e os limites onde serão desenvolvidas as ações de Segurança da Informação ESTÃO definidos?	
166	Os objetivos a serem alcançados com as ações de Segurança da Informação e Comunicações ESTÃO definidos, considerando as expectativas ou diretrizes formuladas pela autoridade decisória da Instituição?	
167	FOI definida uma metodologia de Gestão de Riscos que seja adequada ao escopo, limites e objetivos definidos?	
168	FORAM identificados os níveis de riscos aceitáveis e os critérios para sua aceitação, considerando decisões superiores e o planejamento estratégico da instituição?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
169	Os ativos da instituição e seus responsáveis FORAM adequadamente identificados?	
170	As vulnerabilidades de cada ativo institucional FORAM identificadas?	
171	Os impactos que perdas de Disponibilidade, Integridade, Confidencialidade e Autenticidade podem causar nesses ativos FORAM identificados?	
172	Na Análise de Riscos, os impactos para a Missão da Instituição, relativos a falhas de segurança que resulte na perda de Disponibilidade, Integridade, Confidencialiade ou Autenticidade dos ativos da instituição ESTÃO identificados?	
173	Na Análise de Riscos, ESTÁ identificada a probabilidade real de ocorrência de falhas de segurança, considerando as vulnerabilidades prevalecentes, os impactos associados aos ativos identificados e as ações de segurança da informação já implementadas?	
174	Os níveis de Riscos ESTÃO claramente estimados?	
175	ESTÃO determinados quais riscos são aceitáveis e quais requerem tratamento utilizando os critérios de aceitação definidos?	
176	As opções para tratamento de riscos ESTÃO bem estabelecidas considerando alternativas como a aplicação de novas ações de SIC, a aceitação consciente e objetiva de riscos, o impedimento de riscos, e a transferência de riscos a outras partes?	
177	As ações de Segurança da Informação e Comunicações consideradas necessárias para o tratamento de riscos ESTÃO selecionadas?	
178	Os riscos residuais propostos TÊM a aprovação formal de autoridade decisória da instituição?	
179	EXISTE uma autorização da autoridade decisória da instituição para implementar ações de segurança da Informação e comunicações selecionadas mediante Declaração de Aplicabilidade?	
180	Na Declaração de Aplicabilidade, ESTÃO claros os objetivos e os recursos para cada ação de segurança da informação e comunicações selecionada e as razões para sua seleção?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
181	Na Declaração de Aplicabilidade, ESTÃO claros os objetivos de cada ação de Segurança da Informação e Comunicações já implementadas pela instituição?	
182	Na Declaração de Aplicabilidade, EXISTE um resumo das decisões relativas à gestão de riscos?	
183	Na Declaração de Aplicabilidade, ESTÃO as justificativas de possíveis exclusões de ações de Segurança da Informação e Comunicações sugeridas pelo Gestor de Segurança da Informação e Comunicações e não autorizadas pela autoridade decisória da instituição?	
184	EXISTE um plano de metas formulado para cada objetivo das ações de SIC aprovadas na fase de planejamento em ordem de prioridade, com atribuição de responsabilidades, prazos para execução e custos estimados?	
185	É formalizada uma autorização da autoridade decisória da instituição para implementação do plano de metas com garantia de alocação dos recursos planejados?	
186	EXISTE uma garantia de implementação do plano de metas autorizado?	
187	EXISTE indicadores mensuráveis para medir a eficácia das ações de segurança da informação e comunicações nas metas aprovadas?	
188	EXISTEM ações de capacitação e treinamento de pessoal para desempenho adequado de suas responsabilidades atribuídas nos planos de metas?	
189	EXISTEM ações de conscientização de todo o efetivo da instituição quanto à importância de Segurança da Informação e Comunicações?	
190	SÃO mantidos registros sobre habilidades, experiências e qualificações do efetivo da instituição em relação à Segurança da Informação e Comunicações?	
191	O Gestor de Segurança da Informação e Comunicações GERENCIA a execução das ações de SIC?	
192	O Gestor de Segurança da Informação e Comunicações GERENCIA os recursos empenhados para o desenvolvimento das ações de Segurança da Informação e Comunicações?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
193	SÃO implementados procedimentos capazes de permitir a pronta detecção de incidentes de Segurança da Informação e Comunicações e uma pronta resposta?	
194	EXISTEM procedimentos de avaliação e análise crítica para detectar erros nos resultados de processamento?	
195	EXISTEM procedimentos de avaliação e análise crítica para detectar incidentes de Segurança da Informação e Comunicações?	
196	EXISTEM procedimentos de avaliação e análise crítica para determinar se as ações de SIC se ações delegadas ou executadas por Tecnologia da Informação e Comunicações estão sendo executadas conforme planejado?	
197	EXISTEM procedimentos de avaliação e análise crítica para determinar a eficácia das ações de Segurança da Informação e Comunicações adotadas, usando indicadores?	
198	SÃO realizadas análises críticas regulares, a intervalos planejados de pelo menos uma vez por ano?	
199	SÃO verificados se os requisitos ou pressupostos estabelecidos pelo planejamento organizacional e as diretrizes expedidas pela autoridade decisória da instituição foram atendidos?	
200	A avaliação/análise de riscos É atualizada pelo menos uma vez por ano?	
201	EXISTE a condução de auditoria interna, também denominada de auditoria de primeira parte, das ações de SIC, pelo menos uma vez por ano?	
202	SÃO realizadas atualizações dos planos de SIC, considerando os resultados da avaliação e análise crítica?	
203	A autoridade decisória É informada de possíveis impactos na eficácia da Missão da Instituição?	
204	EXISTE um procedimento formal de proposta à autoridade decisória, da necessidade de implementar as melhorias identificadas?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
205	As ações corretivas e preventivas SÃO executadas de acordo com a identificação de não conformidade real ou potencial?	
206	As melhorias SÃO comunicadas à autoridade decisória da Instituição?	
207	O Gestor de SIC assegura-se que as melhorias atinjam os objetivos pretendidos?	
208	Existe uma POSIC, elaborada considerando a natureza e finalidade da instituição, alinhada com a missão da instituição e ao seu planejamento estratégico?	
209	Os objetivos e abrangência da POSIC estão claramente definidos no seu Escopo?	
210	No texto da POSIC estão os conceitos e definições untilizados para evitar dificuldades de interpretação e ambiguidades de significados?	
211	Estão relacionadas as referências legais e normativas utilizadas na elaboração da POSIC?	
212	Está explícito um item com os principios que regem a Segurança da informação na instituição?	
213	Foram estabelecidas as diretrizes gerais contendo no mínimo os temas: Tratamento da Informação; Tratamento de incidentes de rede; gestão de risco; gestão de continuidade; auditoria e conformidade; controles de acesso; uso de email; e acesso à internet?	
214	Estão previstas as penalidades para os casos de violação da POSIC ou de quebra de segurança?	
215	Foi definida uma estrutura para a Gestão de Segurança da Informação e Comunicações, na instituição?	
216	Foi instituido um Gestor de Segurança da Informação e Comunicações na instituição, com a descrição clara de suas responsabilidades, conforma descrito no item 5.3.7.2 da NC03 da IN01?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
217	Foi Instituido o Comitê de Segurança da Informação e Comunicações da istituição, e descritas a suas atribuições conforme descrito no item 5.3.7.3 da NC03 da IN01?	
218	Foi Instituida a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da entidade?	
219	Ficou estabelecida a periodicidade para revisão da POSIC e suas normas complementares?	
220	A POSIC foi redigida de forma objetiva, simples, e de fácil leitura e entendimento?	
221	A POSIC foi publicada e assinada pela autoridade máxima da instituição?	
222	Existe garantia de recursos para implementação da POSIC da istituição?	
223	Foram implementadas ações que promovam a cultura de Segurança da Informação e Comunicações na instituição?	
224	A POSIC foi publicada e divulgada para todos os trabalhadores da instituição?	
225	As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC considera prioritariamente os objetivos estratégicos, os processo, os requisitos legais e a estrutura do órgão?	
226	As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC estão alinhadas à POSIC do órgão?	
227	O processo de GRSIC é continuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações?	
228	O processo de GRSIC está alinhado ao modelo PDCA?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
229	A GRSIC oferece subsídios para suportar o Sistema de Gestão de Segurança da Informação e Comunicações e a Gestão de Continuidade de Negócios?	
230	Foi definido o escopo de aplicação da GRSIC?	
231	Foi adotada uma metodologia de GRSIC que atenda aos objetivos, diretrizes gerais e o escopo definido contemplando, no mínimo, os critérios de avaliação e aceitação de risco?	
232	Foi realizado um inventário e mapeamento dos ativos de informação, no âmbito do escopo estabelecido, e conforme as diretrizes da NC10/IN01?	
233	Os riscos associados ao escopo definido são identificados considerando as ameaças envolvidas?	
234	Os riscos associados ao escopo definido são identificados considerando as vulnerabilidades existentes nos ativos de informação?	
235	Os riscos associados ao escopo definido são identificados considerando as ações de SIC já adotadas	
236	Os riscos levantados são estimados, considerando os valores ou níveis pra a probabilidade e para a consequência do risco associados à perda de disponibilidade, integridade, confidencialidade e autenticidade nos ativos considerados?	
237	Os riscos são avaliados, determinando se são aceitáveis ou se requerem tratamento?	
238	Os riscos que requeiram tratamento são relacionados, sendo priorizados de acordo com os critérios estabelecidos pelo órgão ou entidade?	
239	As formas de tratamento dos riscos são determinadas considerando as opções de reduzir, evitar, tranferir ou reter o risco, observando a eficácia das ações de SIC já existentes?	
240	As formas de tratamento dos riscos são determinadas considerando as opções de reduzir, evitar, tranferir ou reter o risco, observando as restrições organizacionais, técnicas e estruturais?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
241	As formas de tratamento dos riscos são determinadas considerando as opções de reduzir, evitar, tranferir ou reter o risco, observando os requisitos legais?	
242	As formas de tratamento dos riscos são determinadas considerando as opções de reduzir, evitar, tranferir ou reter o risco, observando a análise custo/beneficio?	
243	É elaborado um plano para tratamento de riscos relacionando as ações de SIC, responsáveis, prioridades e prazos de execução necessários à sua implantação?	
244	Os resultados do processo executado são verificados considerando o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação?	
245	São executadas as ações de SIC incluídas no Plano de Tratamento de Riscos aprovado?	
246	O processo de GRSIC é monitorado e analisado de forma a mantê-lo alinhado às diretrizes gerais estabelecidas e às ncecessidades do órgão?	
247	Os riscos são monitorados e analisados criticamente, a fim de verificar mudanças nos critérios de avaliação e aceitação de riscos?	
248	Os riscos são monitorados e analisados criticamente, a fim de verificar mudanças no ambiente?	
249	Os riscos são monitorados e analisados criticamente, a fim de verificar mudanças nos ativos de informação?	
250	Os riscos são monitorados e analisados criticamente, a fim de verificar mudanças nas ações de SIC?	
251	Os riscos são monitorados e analisados criticamente, a fim de verificar mudanças nos fatores do risco?	
252	Durante a fase de monitoramento e análise crítica, a autoridade decisória do órgão é informada da necessidade de implementar as melhorias identificadas?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
253	As ações corretivas ou preventivas aprovadas, são prontamente executadas?	
254	As melhorias são implementadas de forma a assegurar que os objetivos sejam atendidos?	
255	As instâncias superiores são informadas a respeito de todas as fases da gestão de risco, compartilhando as informações entre o tomador da decisão e as demais partes envolvidas e interessadas?	
256	Foi elaborado um Programa de Gestão de Continuidade de Negócios - PGCN?	
257	O PGCN elaboradao contém um documento com as diretrizes do Programa de Continuidde	
258	O PGCN define as atividades críticas do órgão?	
259	O PGCN avalia os riscos a que essas atividades críticas estão expostas?	
260	O PGCN define as estratégias de continuide para atividades críticas?	
261	São desenvolvidos e implementados Planos previstos no Programa de Gestão de Continuidade de Negócios para respostas tempestivas e interrupções?	
262	São realizados exercícios, testes e manutenção periódica dos Planos, promovendo as revisões necessárias?	
263	Existem ações para o desenvolvimento da cultura de Continuidade de Negócios no órgão?	
264	Os procedimentos previstos no Programa de Gestão de Continuidade de Negócios são executados em conformidade com os requisitos de Segurança de Informação e Comunicações?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
265	O Programa de Continuidade de Negócios contém um Plano de Gerenciamento de Incidentes - PGI?	
266	O Programa de Continuidade de Negócios contém um Plano de Continuidade de Negócios - PCN?	
267	O Programa de Continuidade de Negócios contém um Plano de Recuperação de Negócios - PRN?	
268	O Plano de Gerenciamento de Incidentes foi elaborado seguindo a estrutura proposta na NC 06 da IN01 itens 5.4.1	
269	O Plano de Continuide de Negócios foi elaborado seguindo a estrutura proposta na NC 06 da IN01 itens 5.4.2	
270	O Plano de Recuperação de Incidentes foi elaborado seguindo a estrutura proposta na NC 06 da IN01 itens 5.4.3	
271	Os Planos são exercitados e testados periodicamente e os resultados documentados de forma a garantir a sua efetividade?	
272	Os Planos prevêm serem revisados de acordo com a norma: Pelo menos uma vez por ano; ou em função de resultados de testes realizados; ou Após mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes?	
273	As diretrizes estratégicas que norteiam a elaboração do PGCN são aprovadas pela alta direção do órgão?	
274	A alta direção do ógão avalia a relação custo/benefício das estratégias de continuidade propostas e dos Planos que compõem a PGCN e decide sobre sua implementação?	
275	A alta direção garante os recursos necessários para estabelecer, implementar, operar e manter o PGCN?	
276	O Gestor de Continuidade de Negócios ou, na falta deste, o Gestor de Segurança da Informação propõe as diretrizes estratégicas para o PGCN?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
277	O Gestor de Continuidade de Negócios ou, na falta deste, o Gestor de Segurança da Informação avalia o plano de tratamento de riscos?	
278	O Gestor de Continuidade de Negócios ou, na falta deste, o Gestor de Segurança da Informação realiza, periodicamente, a Análise de Impacto nos Negócios - AIN?	
279	O Gestor de Continuidade de Negócios ou, na falta deste, o Gestor de Segurança da Informação propõe melhorias na implantação de novos controles relativos ao PGCN?	
280	O Gestor de Continuidade de Negócios ou, na falta deste, o Gestor de Segurança da Informação supervisiona a elaboração, implementação, testes e atualização dos Planos?	
281	O Gestor de Continuidade de Negócios ou, na falta deste, o Gestor de Segurança da Informação desenvolve a cultura de GCN?	
282	Os Gestores de setores ou processos que contenham atividades críticas para o órgão Elaboram os Planos previstos no PGCN relacionados às atividades críticas?	
283	Os Gestores de setores ou processos que contenham atividades críticas para o órgão Realizam os testes e exercícios dos Planos?	
284	Os Gestores de setores ou processos que contenham atividades críticas para o órgão Avaliam e Aprimoram os Planos a partir dos resultados dos testes e exercícios?	
285	Os Gestores de setores ou processos que contenham atividades críticas para o órgão Administram a contingência quando da interrupção de atividades, com base nos planos desenvolvidos?	
286	Os Gestores de setores ou processos com atividades críticas para o órgão propõem os recursos necessários à implantação e ao desenvolvimento das ações relativas à continuidade das atividades, e para a realização dos testes e dos exercicios dos Planos?	
287	É feito um credenciamento para usuários antes da criação de contas de acesso a ativos de informação?	
288	Os usuários, com exceção de administradores de rede local, têm somente uma conta institucional única, pessoal e intransferível?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
289	Contas de acesso com perfil de administrador, somente são criadas para usuários que executam tarefas específicas de administração de ativos de informação?	
290	Os usuários são responsabilizados pela quebra de segurança, ocorrida com utilização de sua senha, mediante assinatura de termo de responsabilidade?	
291	Existe um processo automatizado com regras definidas, para criação de contas de serviço?	
292	Existem regras de credenciamento, bloqueio e exclusão de contas de acesso de usuários?	
293	Existem regras de credenciamento, bloqueio e exclusão de contas de acesso ao ambiente de desenvolvimento?	
294	O usuário recebe credenciais de acesso à rede corporativa quando de sua contratação?	
295	As credenciais de acesso do usuário é excluida quando de seu desligamento?	
296	Os acesso à Rede corporativa é registrado permitindo a rastreabilidade e a identificação do usuário?	
297	Existe pelo menos um mecanismo implementado, dos que contemplam biometria, tokens, smart cards, a fim de autenticar a identidade do usuário?	
298	São utilizados mecanismos automáticos para inibir que equipamentos externos se conectem na rede corporativa de computadores?	
299	São mantidos na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados?	
300	O acesso remoto, bem como o acesso à informação sigilosas, é regulamentado por legislação específica?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
301	O acesso remoto à rede corporativa é gravado em LOGs para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada?	
302	Existem regras específicas para o uso de rede sem fio?	
303	São utilizadas ferramentas de proteção contra acesso não autorizado aos ativos de informaçã, que favoreça, preferencialmente, a administração de forma centralizada?	
304	As contas ou credenciais de acesso aos ativos de informação são configuradas respeitando-se o princípio do menor privilégio?	
305	São usados ativos de informação homologados, nas aplicações de controle de acesso, de tratamento das informações sigilosas e de criptografia?	
306	Os eventos relevantes, previamente definidos, para a segurança e rastreamento de acesso às informações sigilosas são registrados?	
307	Existem mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.	
308	O uso de ativos de informação sem relação com as atividades relativas ao cargo, função ou atividades públicas são controladas e bloqueadas?	
309	Existem regras para o uso de Internet, do Correio Eletrônico e de Mensagens Instantâneas?	
310	Existem regras para o uso de credenciais físicas, que se destinam ao controle de acesso dos usuários às instalações do órgão?	
311	Foi definida a necessidade de instalação de sistemas de detecção de intrusos em áreas e instalações do órgão?	
312	As áreas e Instalações são classificadas como ativos de informação de acordo com o valor, a criticidade, o tivo de ativo de informação e o grau de sigilo das informações que podem ser tratadas em tais áreas e instalações?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
313	O uso de barreiras físicas de segurança, bem como equipamentos ou mecanismos de controle de entrada e saída são oritentados?	
314	Os ativos de informação, principalmente aqueles considerados críticos, são protegidos contra ações de vandalismo, sabotagem, ataques, etc?	
315	As áreas de recepção do órgão estão preparadas com regras claras de entrada e saída de pessoas, equipamentos e materiais?	
316	Os pontos de entrega e carregamento de material são definidos e o acesso é restrito ao pessoal credenciado?	
317	Os controle de acesso às áreas e instalações consideradas críticas são intensificados de acordo com a legislação vigente?	
318	São difundidas e é exigido o seu cumprimetno a Política de Segurança da Informação e Comunicações, as normas de segurança e a legislação vigente sobre o tema?	
319	Existem ações de conscientização do usuário para adotar comportamento favorável à disponibilidade, à integridade, à confidencialidade e à autenticidade das informações?	
320	Os riscos à Segurança da Informação e Comunicações dos ativos de informação são avaliados sistematicamente e são definidos controles a serem aplicados quanto ao acesso dos usuários?	
321	Existe um formulário específico de Termo de Responsabilidade definido e dinfundido, que deve ser preenchido individualmente pelos usuários?	
322	Existem regras específicas definidas pra autorização de acesso e credenciamento dos usuários em conformidade com a classificação dos ativos de informação?	
323	Existem especificações de distância mínima de segurança para manutenção das mídias contendo as cópias de segurança (backups)?	
324	Os ativos de informação são classificados em níveis de criticidade, considerando o tipo de informação e o provável impacto no caso de quebra de segurança, com base na gestão de Risco e Gestão de continuidade de negócios?	

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO CONFORMIDADE
325	Existe procedimentos especiais de controles de acesso físico, em conformidade com a legislação vigente, para os ativos de informação classificados como sigilosos?	
326	Estão definidos os perímetros de segurança, suas dimensões, equipamentos e tipos especiais de controles de acesso aos ativos de informação?	
327	Existe uma documentação própria que permita que sejam identificados os perímetros de segurança de cada ativo de informação por todos que transitarem ou tiverem acesso em tais espaços, em especial às áreas e instalações críticas?	
328	O armazenamento, a veiculação de imagem, vídeo ou áudio, registrados em perímetro de segurança, são regulamentados por normas específicas?	

Anexo B – Tabela de Controles

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
001	Existe uma política de Segurança da Informação aprovada pela direção, publicada e comunicada para todos os funcionários e partes externas relevantes?	01	001
002	Exise um processo de análise crítica da política de SI, em intervalos planejados ou quando mudanças significativas ocorrem, para assegurar a sua contínua pertinência, adequação e eficácia?	01	001
003	A Direção apoia ativamente a segurança da informação dentro da organização, de forma clara, demonstrando o seu comprometimento, definindo atribuições de forma explícita e conhecendo as responsabilidades pela segurança da informação?	01	002
004	As atividades de segunrança da informação são coordenadas por representantes de direrentes partes da organização, com funções e papéis relevantes?	01	002
005	As responsabilidades pela Segurança da Informação estão claramente definidas?	01	002
006	A Instituição definiu e Implementou um processo de gestão de autorização para novos recursos de processamento da informação	01	002
007	Os requisitos de confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação SÃO identificados e analisados criticamente, de forma regular?	01	002
008	São mantidos contados com autoridades relevantes em Segurança da Informação?	01	002
009	São mantidos contados com grupos de interesses especiais ou outros foruns especializados em Segurança da Informação?	01	002
010	O enfoque da instituição para gerenciar e implementar a Segurança da Informação É analisado criticamente, de forma independente, periodicamente ou quando ocorrem mudanças significativas relativas a implementação de SI?	01	002

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
011	Os Riscos para os recursos de processamento da informação e para a informação da organização oriundos de processos do negócio que envolvam as partes externas SÃO identificados e os Controles apropriados são implementados antes da concessão de acesso?	01	002
012	Os requisitos de segurança da informação identificados SÃO considerados antes da concessão de acesso aos ativos ou às informações da Instituição?	01	002
013	Os acordos com terceiros para acesso, processamento, comunicação ou gerenciamento de recursos de processamento da informação ou da informação da instituição COBREM todos os requisitos relevantes de SI	01	002
014	Os acordos com terceiros para acrescimo de produtos ou serviços aos recursos de processamento da informação COBREM todos os requisitos relevantes de SI?	01	002
015	Os ativos da Instituição estão claramente identificados?	01	003
016	A Instituição mantém um inventário estruturado dos seus ativos importantes?	01	003
017	Todas as informações e ativos da instituição, associados com os recursos de processamento da informação, têm um responsável designado por uma parte definida da instituição?	01	003
018	As regras de permissão de uso de informações e de ativos associados aos recursos de processamento da informação, ESTÃO identificadas e documentadas?	01	003
019	As regras de permissão de uso de informações e de ativos associados aos recursos de processamento da informação, ESTÃO implementadas?	01	003
020	As Informações estão classificadas considerando o seu Valor, os Requisitos Legais, a Sensibilidade e Criticidade para a Instituição?	01	003
021	Foi definido e implementado um conjunto apropriado de procedimentos para rotular e tratar a informação, de acordo com o esquema de classsificação adotado pela instituição?	01	003

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
022	Os papéis e responsabilidades pela Segurança da Informação tanto de funcionários, como de fornecedores e terceiros, ESTÃO definidos e documentados de acordo com a Política de Segurança da Informação da Instituição?	01	004
023	São feitas verificações de controle de candidatos a emprego, fornecedores e terceiros, de acordo com a legislação vigente e a ética, e considerando os requisitos de negócio, a classificação da informação a serem acessadas e aos riscos envolvidos?	01	004
024	A instituição implementou a assinatura de um termo, no momento da contratação tanto de Funcionários, como de fornecedores e de terceiros, onde estão explicitas as responsabilidades de contratados e da instituição, em relação à Segurança da Informação?	01	004
025	A Direção da Instituição solicita claramente, no momento da contratação, a funcionários, fornecedores e terceiros que pratiquem a Segurança da Informação de acordo com o estabelecido nas políticas e procedimentos da Instituição?	01	004
026	A Instituição promove treinamento apropriado em conscientização a funcionários, fornecedores e terceiros, bem como atualizações regulares nas políticas de procedimentos organizacionais relevantes às suas funções?	01	004
027	Existe um processo disciplinar formal para os funcionários que tenham cometido uma violação da Segurança da Informação?	01	004
028	As responsabilidades para realizar o encerramento de um contrato de trabalho ESTÃO claramente definidas e atribuidas?	01	004
029	No encerramento ou mudança de contrato ou atividades, tanto Servidores, como fornecedores e terceiros procedem formamalmente à devolução dos ativos da instituição que estejam em sua posse?	01	004
030	Os direitos de acesso de servidores, fornecedores e terceiros a informações e a recursos de processamento de informação SÃO retirados em caso de encerramento de contrato ou de atividade, ou SÃO ajustados em caso de mudança de atividades?	01	004
031	A Instituição tem delimitado áreas seguras, com barreiras adequadas, em locais que contenham informações e recursos de processamento da informação?	01	005
032	As áreas seguras SÃO protegidas por controles apropriados de entrada para assegurar que somente pesoas autorizadas tenham acesso?	01	005

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
033	A Instituição projetou a segurança física para salas e instalações?	01	005
034	A Instituição projetou e aplica proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem?	01	005
035	A Instituição projetou e aplica proteção física e diretrizes para o trabalho em áreas seguras?	01	005
036	A Instituição controla pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos de entrada, para evitar o acesso não autorizado a recursos de processamento de informação?	01	005
037	Os equipamentos estão instalados em locais protegidos de ameaças e perigos do meio ambiente, bem como de oportunidades de acesso não autorizado?	01	005
038	Os equipamentos SÃO protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades?	01	005
039	Os cabeamentos de energia e de telecomunicações que trasportam dados ou dá suporte aos serviços de informações SÃO protegidos contra interrupções ou danos?	01	005
040	Os equipamentos TÊM manutenção com a periodicidade adequada, de forma a assegurar a sua disponibilidade e integridade permanente?	01	005
041	EXISTE medidas de segurança para equipamentos que operem fora das dependências da Instituição, de forma a minimizar riscos?	01	005
042	Os equipamentos que possuem mídias de armazenamento de dados SÃO examinados antes do descarte, para garantir a remoção de dados sensíveis ou softwares licenciados?	01	005
043	É preparada uma autorização prévia para retirada de equipamentos, informações ou softwares da instituição?	01	005

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
044	Os procedimentos de operação dos recursos de processamento da informação SÃO documentados, mantidos atualizados e disponíveis a todos o usuários que deles necessitem?	01	006
045	As modificações nos recursos de processamento da informação e sistemas SÃO controlados?	01	006
046	Funções e áreas de responsabilidades SÃO segregadas visando a redução das oportunidades de modificação ou uso indevido, não autorizado ou não intencional, dos ativos da organização?	01	006
047	Os recursos de desenvolvimento, teste e produção ESTÃO separados em ambientes específicos para reduzir o risco de acesso ou modificações não autorizadas aos sistemas em produção?	01	006
048	EXISTEM garantias que os controles de segurança, definições de serviço e os níveis de entrega, constantes dos acordos de entrega de serviços, sejam implementados, executados e mantidos pelo terceiro?	01	006
049	Os serviços, relatórios e registros fornecidos por terceiro SÃO regularmente monitorados e analisados criticamente?	01	006
050	SÃO executadas auditorias regulares nos serviços terceirizados?	01	006
051	As mudanças no provisionamento dos serviços de terceiros, incluindo manutenção e melhorias em Segurança da Informação, SÃO gerenciadas levando-se em conta a criticidade dos sistemas e processos de negócios envolvidos e reanálise/reavaliação de riscos?	01	006
052	A utilização dos recursos É monitorada e sincronizada para garantir o desempenho requerido do sistema?	01	006
053	SÃO feitas projeções para as necessidades de capacidade futura de forma a manter o desempenho requerido do sistema?	01	006
054	EXISTEM critérios estabelecidos para aceitação de novos sistemas, atualizações e novas versões?	01	006

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
055	SÃO efetuados testes apropriados dos sistemas durante o seu desenvolvimento e antes de sua aceitação?	01	006
056	EXISTEM controles implementados para detecção, prevenção e recuperação, para proteção contra códigos maliciosos?	01	006
057	EXISTEM procedimentos de conscientização de usuários para prevenção contra códigos maliciosos?	01	006
058	EXISTEM controles implementados para garantir que códigos móveis autorizados operem de acordo com a política de Segurança da Informação definida pela instituição, e para que códigos móveis não autorizados tenham sua execução impedida?	01	006
059	SÃO efetuadas e testadas regularamente, cópias das informações e softwares, de acordo com uma política definida de geração de cópias de segurança?	01	006
060	As Redes da Instituição são adequadamente gerencias e controladas, de forma a garantir a proteção contra ameaças e manter a segurança das informações, de sistemas e de aplicações?	01	006
061	As características de segurança, de níveis de serviço e de requisitos de gerenciamento dos serviços SÃO devidamente identificados e incluidos nos acordos de serviço de Rede, em contratos mantidos pela instituição?	01	006
062	EXISTEM procedimentos implementados para o gerenciamento de mídias removíveis?	01	006
063	EXISTEM procedimentos formais para o descarte de mídias, de forma segura e protegida, quando não forem mais necessárias?	01	006
064	EXISTEM procedimentos estabelecidos para o tratamento e o armazenamento de informações, de modo a protegê-las contra a divulgação não autorizada ou o uso indevido?	01	006
065	EXISTEM procedimentos formais de proteção da documentação de sistemas contra acessos não autorizados?	01	006

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
066	EXISTEM Políticas, procedimentos e controles estabelecidos e formalizados visando a proteção na troca de informações em todos os tipos de recursos de comunicação?	01	006
067	EXISTEM acordos estabelecidos para a troca de informações e software entre a instituição e entidades externas?	01	006
068	EXISTEM procedimentos de proteção contra acesso não autorizado, uso impróprio ou alteração indevida, durante o transporte externo aos limites físicos da organização, para mídias contendo informação,?	01	006
069	EXISTE proteção adequada para o tráfego de mensagens eletrônicas no âmbito da instituição?	01	006
070	EXISTEM políticas e procedimentos desenvolvidos e implementados para proteger as informações associadas com a interconexão de sistemas de informações do negócio da instituição?	01	006
071	EXISTE proteção adequada para as informações envolvidas em comércio eletrônico transitando sobre a rede da instituição, contra atividades fraudulentas, disputas contratuais, divulgação e modificações não autorizadas?	01	006
072	EXISTEM procedimentos seguros nas transações on-line para proteção das informações, de forma a prevenir transmissões incompletas, erros de roteamentos,e alterações, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada?	01	006
073	As Informações disponibilizadas em sistemas com acesso público ESTÃO protegidas contra modificações não autorizadas?	01	006
074	Os Registros de auditoria (Log) contendo atividades dos usuários, exceções e outros eventos de segurança da informação, que possam auxiliar em auditorias, SÃO produzidos e mantidos adequadamente por um período definido na política da instituição?	01	006
075	EXISTEM procedimentos estabelecidos para o monitoramento regular do uso dos recurso de processamento da informação, com análise critica dos resultados?	01	006
076	EXISTE proteção adequada para os recursos e informações de registros (log) contra falsificação e acesso não autorizado?	01	006

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
077	As atividades dos administradores e operadores do sistema SÃO registradas?	01	006
078	As falhas ocorridas SÃO registradas e analisadas, e as ações apropriadas de correção são adotadas?	01	006
079	EXISTE sincronização, de acordo com uma hora oficial, dos relógios de todos os sistemas de processmento de dados relevantes, dentro da instituição ou dentro do domínio de segurança?	01	006
080	EXISTE uma política de controle de acesso estabelecida, documentada e analisada criticamente, em concordância com os requisitos de acesso dos negócios e também da Segurança da Informação?	01	007
081	EXISTE um procedimento formal de registro e cancelamento de usuário, que garanta e revogue acessos em todos os sistemas de informação e serviços?	01	007
082	A concessão e o uso de privilégios SÃO restritos e controlados?	01	007
083	EXISTE um processo de gerenciamento formal para concessão de senhas de acesso?	01	007
084	O gestor de acesso CONDUZ regularmente análise crítica dos direitos de acesso dos usuários, por meio de um processo formal?	01	007
085	EXISTE uma orientação aos usuários para seguir boas práticas de Segurança da Informação, tanto na composição da senha quanto no seu Uso?	01	007
086	EXISTE orientação para que usuários protejam adequadamente equipamentos não monitorados pela rede?	01	007
087	EXISTE um controle automático que bloqueia automaticamente a tela do computador quando estiver ocioso por um determinado tempo (política de tela limpa)?	01	007

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
088	EXISTE Orientação e conscientização dos usuários para que mantenham a mesa limpa de papéis e midias de armazenamento removíveis?	01	007
089	EXISTE um controle para que usuários recebam acesso somente aos serviços que tenham sido especificamente autorizados a usar?	01	007
090	SÃO utilizados métodos apropriados de autenticação para controlar o acesso de usuários remotos?	01	007
091	A autenticação de conexões vindas de localizações e equipamentos específicos É feita considerando a identificação automática de equipamentos?	01	007
092	Os acessos físico e lógico SÃO controlados no diagnóstico e configuração de portas remotas?	01	007
093	Os grupos de serviço de informação, usuários e sistemas de informação SÃO segregados em redes?	01	007
094	A capacidade de conexão de usuários É calculada e restringida de acordo com a política de controle de acesso e os requisitos das aplicações de negócio?	01	007
095	EXISTE um controle de roteamento para assegurar que conexões não violem a política de controle de acesso das aplicações do negócio?	01	007
096	O acesso aos sistemas operacionais É controlado por um procedimento seguro de log-on?	01	007
097	EXISTE um identificador único para cada usuário se autenticar, utilizando uma técnica de autenticação adequada?	01	007
098	Os sistemas de gerenciamento de senha SÃO interativos e asseguram a construçãao de senhas de qualidade?	01	007

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
099	O uso de programas utilitários que podem sobrepor os controles dos sistemas de aplicações É restrito e estritamente controlado?	01	007
100	EXISTE procedimento que garanta que os terminais inativos são desconectados após um período definido de inatividade?	01	007
101	SÃO utilizadas restrições nos horários de conexão para proporcionar segurança adicional pra aplicações de alto risco?	01	007
102	O acesso à informação e às funções dos sistemas de aplicações por usuários e pessoal de suporte É restringido de acordo com a política de controle de acesso?	01	007
103	EXISTE um ambiente computacional isolado para sistemas sensíveis?	01	007
104	EXISTE uma política formal para regular o uso de recursos de computação e comunicação móveis, visando a proteção contra riscos para a segurança da informação?	01	007
105	EXISTE uma política, planos operacionais e procedimentos desenvolvidos e implementados para atividades de trabalho remoto?	01	007
106	Os requisitos para controles de segurança SÃO especificados nas especificações de requisitos de negócios, para novos sistemas de informação ou melhorias em sistemas existentes?	01	008
107	Os dados de entrada de aplicações SÃO validados para garantir que são corretos e apropriados?	01	008
108	As checagens de validação SÃO incorporadas nas aplicações, com o objetivo de detectar qualquer corrupção de informações, por erros ou por ações deliberadas?	01	008
109	Os requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações SÃO identificados e os controles apropriados SÃO identificados e implementados?	01	008

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
110	Os dados de saída das aplicações SÃO validados para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias?	01	008
111	EXISTE uma política desenvolvida e implementada para o uso de controles criptográficos visando a proteção da informação?	01	008
112	EXISTE um processo de gerenciamento de chaves implementado para apoiar o uso de técnicas criptográricas pela organização?	01	008
113	EXISTEM procedimentos implementados para controlar a instalação de software em sistemas operacionais?	01	008
114	Os dados de teste SÃO selecionados com cuidado, protegidos e controlados?	01	008
115	EXISTE controle para restringir o acesso a código-fonte de programas?	01	008
116	A implementação de mudanças É controlada utilizando procedimentos formais de controle de mudanças?	01	008
117	Quando sistemas operacionais são mudados, as aplicações críticas de negócios SÃO analisadas criticamente e testadas, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança?	01	008
118	EXISTEM restrições para mudanças em pacotes de software, limitando-se às mudanças necessárias que são estritamente controladas?	01	008
119	As oportunidades para vazamento de informações SÃO prevenidas?	01	008
120	A instituição SUPERVISIONA e MONITORA o desenvolvimento terceirizado de software?	01	008

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
121	As informações sobre vulnerabilidades técnicas dos sistemas de informação em uso SÃO obtidas em tempo hábil, avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados?	01	008
122	Os eventos de Segurança da Inforamação SÃO relatados através dos canais apropriados da direção, o mais rapidamente possível?	01	009
123	Os funcionários, fornecedores e terceiros de sistemas e serviços de informação SÃO instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade em sistemas ou serviços?	01	009
124	ESTÃO estabelecidas as responsabilidades e procedimentos de gestão, para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação?	01	009
125	ESTÃO estabelecidos mecanismos para permitir que tipos, quantidades e custos dos incidentes de sergurança da informação sejam quantificados e monitorados?	01	009
126	Quando de uma ação legal envolvendo incidente em segurança da informação, as evidências SÃO coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição ou jurisdições pertinentes?	01	009
127	EXISTE um processo de gestão, mantido para assegurar a Continuidade do negócio por toda a instituição e que contemple os requisitos de Segurança da Informação necessários à continuidade do negócio da Instituição?	01	010
128	ESTÃO identificados os eventos que podem causar interrupções aos processos de negócio, bem como a propabilidade e impacto de tais interrupções e as consequências para a segurança da informação?	01	010
129	Os planos de continuidade relativos à SI foram desenvolvidos e implementados para assegurar a disponibilidade da informação no nível e na escala de tempo requeridos, após a ocorrência de interrupções ou falhas dos processos críticos do negócio?	01	010
130	A instituição MANTÉM uma estrutura básica dos planos de continuidade do negócio para assegurar que todos planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção?	01	010
131	Os planos de continuidade do negócio SÃO testados e atualizados regularmente de forma a assegurar sua permanente atualização e efetividade?	01	010

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
132	Todos os requisitos estatutários, regulamentares e contratuais relevantes, e o enfoque da instituição para atender a esses requisitos ESTÃO definidos, documentados e mantidos atualizados para cada sistema de informação da Instituição?	01	011
133	EXISTEM procedimentos apropriados implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no o uso de material com direitos de propriedade intelectual e no uso de produtos de software proprietários?	01	011
134	EXISTE proteção de registros importantes contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estaturários, contratuais e do negócio?	01	011
135	A privacidade e a proteção de dados ESTÃO assegurada conforme exigido nas legislações relevantes, regulamentações e, se aplicável, nas cláusulas contratuais?	01	011
136	Os usuários SÃO regularmente, dissuadidos de usar os recursos de processamento da informação para propósitos não autorizados?	01	011
137	Os controles de criptografia SÃO usados em conformidade com leis, acordos e regulamentações relevantes?	01	011
138	EXISTE garantia, por parte dos gestores, que todos os procedimentos de segurança dentro de sua área de responsabilidade sejam executados corretamente para atender à conformidade com as normas e políticas de segurança da informação?	01	011
139	Os sitemas de informação SÃO periodicamente verificados quanto à sua conformidade com as normas de segurança da informação implementadas?	01	011
140	Os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais SÃO cuidadosamente planejados e acordados para minimizar os riscos de interrupção dos processos do negócio?	01	011
141	O acesso às ferramentas de auditoria de sistemas de informação É protegido para prevenir qualquer possibilidade de uso impróprio ou comprometimento?	01	011
142	A Instituição possui uma unidade para coordenar as ações de segurança da informação e comunicações?	02	002

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
143	A Instituição aplica as ações corretivas e disciplinares cabíveis nos casoa de quebra de segurança?	02	002
144	A Instituição especificou em seu orçamento, recursos para as ações de segurança da informação e comunicações?	02	002
145	A Instituição constituiu um Gestor de Segurança da Informação e Comunicações	02	002
146	A Instituição instituiu e implementou a ETIR - Equipe de Tratamento e Resposta a Incidentes em redes computacionais?	02	002
147	A Instituição instituiu o Comitê de Segurança da Informação e Comunicações?	02	002
148	A Instituição aprovou sua Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações?	02	002
149	A Instituição remete os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações para o GSI?	02	002
150	A Instituição segue os requisitos metodológicos, definidos pelo GSI-PR, para implementação da Gestão de Segurança da Informação e Comunicações?	02	002
151	A Instituição está preparada para receber sugestões de melhorias ou denúncias de quebra de Segurança da Informação, no âmbito de sua atuação?	02	002
152	O Comitê de Segurança da Informação e Comunicações - CSIC tem assessorado na implementação das ações de segurança da informação e comunicações?	02	002
153	O CSIC tem atuado na constituição de grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações?	02	002

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
154	O CSIC tem analisado a Política de Segurança da Informação e Comunicações e proposto alterações quando necessárias?	02	002
155	O CSIC porpõe normas complementares relativas à Segurança da Informação e Comunicações?	02	002
156	O Gestor de Segurança da Informação e Comunicações tem promovido a cultura de Segurança da Informação e Comunicações na Instituição?	02	002
157	O Gestor de Segurança da Informação e Comunicações acompanha as insvestigações e as avaliações dos danos decorrentes de quebras de segurança?	02	002
158	O Gestor de Segurança da Informação e Comunicações propõe a alocação dos recursos necessários às ações de Segurança da Informação e Comunicações?	02	002
159	O Gestor de Segurança da Informação coordena o CSIC?	02	002
160	O Gestor de Segurança da Informação coordena o ETIR?	02	002
161	O Gestor de Segurança da Informação realiza e acompanha estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações?	02	002
162	O Gestor de Segurança da Informação mantém contato direto com o DSIC pra o trato de assuntos relativos à Segurança da Informação e Comunicações?	02	002
163	O Gestor de Segurança da Informação atua junto ao CSIC na proposição de normas relativas à segurança da informação e comunicações?	02	002
164	A gestão de Segurança da Informação da Instituição está baseada no processo de melhoria contínua (PDCA)?	03	002

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
165	O escopo e os limites onde serão desenvolvidas as ações de Segurança da Informação ESTÃO definidos?	03	002
166	Os objetivos a serem alcançados com as ações de Segurança da Informação e Comunicações ESTÃO definidos, considerando as expectativas ou diretrizes formuladas pela autoridade decisória da Instituição?	03	002
167	FOI definida uma metodologia de Gestão de Riscos que seja adequada ao escopo, limites e objetivos definidos?	03	012
168	FORAM identificados os níveis de riscos aceitáveis e os critérios para sua aceitação, considerando decisões superiores e o planejamento estratégico da instituição?	03	012
169	Os ativos da instituição e seus responsáveis FORAM adequadamente identificados?	03	012
170	As vulnerabilidades de cada ativo institucional FORAM identificadas?	03	012
171	Os impactos que perdas de Disponibilidade, Integridade, Confidencialidade e Autenticidade podem causar nesses ativos FORAM identificados?	03	012
172	Na Análise de Riscos, os impactos para a Missão da Instituição, relativos a falhas de segurança que resulte na perda de Disponibilidade, Integridade, Confidencialiade ou Autenticidade dos ativos da instituição ESTÃO identificados?	03	012
173	Na Análise de Riscos, ESTÁ identificada a probabilidade real de ocorrência de falhas de segurança, considerando as vulnerabilidades prevalecentes, os impactos associados aos ativos identificados e as ações de segurança da informação já implementadas?	03	012
174	Os níveis de Riscos ESTÃO claramente estimados?	03	012
175	ESTÃO determinados quais riscos são aceitáveis e quais requerem tratamento utilizando os critérios de aceitação definidos?	03	012

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
176	As opções para tratamento de riscos ESTÃO bem estabelecidas considerando alternativas como a aplicação de novas ações de SIC, a aceitação consciente e objetiva de riscos, o impedimento de riscos, e a transferência de riscos a outras partes?	03	012
177	As ações de Segurança da Informação e Comunicações consideradas necessárias para o tratamento de riscos ESTÃO selecionadas?	03	012
178	Os riscos residuais propostos TÊM a aprovação formal de autoridade decisória da instituição?	03	012
179	EXISTE uma autorização da autoridade decisória da instituição para implementar ações de segurança da Informação e comunicações selecionadas mediante Declaração de Aplicabilidade?	03	002
180	Na Declaração de Aplicabilidade, ESTÃO claros os objetivos e os recursos para cada ação de segurança da informação e comunicações selecionada e as razões para sua seleção?	03	002
181	Na Declaração de Aplicabilidade, ESTÃO claros os objetivos de cada ação de Segurança da Informação e Comunicações já implementadas pela instituição?	03	002
182	Na Declaração de Aplicabilidade, EXISTE um resumo das decisões relativas à gestão de riscos?	03	002
183	Na Declaração de Aplicabilidade, ESTÃO as justificativas de possíveis exclusões de ações de Segurança da Informação e Comunicações sugeridas pelo Gestor de Segurança da Informação e Comunicações e não autorizadas pela autoridade decisória da instituição?	03	002
184	EXISTE um plano de metas formulado para cada objetivo das ações de SIC aprovadas na fase de planejamento em ordem de prioridade, com atribuição de responsabilidades, prazos para execução e custos estimados?	03	002
185	É formalizada uma autorização da autoridade decisória da instituição para implementação do plano de metas com garantia de alocação dos recursos planejados?	03	002
186	EXISTE uma garantia de implementação do plano de metas autorizado?	03	002

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
187	EXISTE indicadores mensuráveis para medir a eficácia das ações de segurança da informação e comunicações nas metas aprovadas?	03	002
188	EXISTEM ações de capacitação e treinamento de pessoal para desempenho adequado de suas responsabilidades atribuídas nos planos de metas?	03	002
189	EXISTEM ações de conscientização de todo o efetivo da instituição quanto à importância de Segurança da Informação e Comunicações?	03	002
190	SÃO mantidos registros sobre habilidades, experiências e qualificações do efetivo da instituição em relação à Segurança da Informação e Comunicações?	03	002
191	O Gestor de Segurança da Informação e Comunicações GERENCIA a execução das ações de SIC?	03	002
192	O Gestor de Segurança da Informação e Comunicações GERENCIA os recursos empenhados para o desenvolvimento das ações de Segurança da Informação e Comunicações?	03	002
193	SÃO implementados procedimentos capazes de permitir a pronta detecção de incidentes de Segurança da Informação e Comunicações e uma pronta resposta?	03	009
194	EXISTEM procedimentos de avaliação e análise crítica para detectar erros nos resultados de processamento?	03	009
195	EXISTEM procedimentos de avaliação e análise crítica para detectar incidentes de Segurança da Informação e Comunicações?	03	009
196	EXISTEM procedimentos de avaliação e análise crítica para determinar se as ações de SIC se ações delegadas ou executadas por Tecnologia da Informação e Comunicações estão sendo executadas conforme planejado?	03	002
197	EXISTEM procedimentos de avaliação e análise crítica para determinar a eficácia das ações de Segurança da Informação e Comunicações adotadas, usando indicadores?	03	002

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
198	SÃO realizadas análises críticas regulares, a intervalos planejados de pelo menos uma vez por ano?	03	002
199	SÃO verificados se os requisitos ou pressupostos estabelecidos pelo planejamento organizacional e as diretrizes expedidas pela autoridade decisória da instituição foram atendidos?	03	002
200	A avaliação/análise de riscos É atualizada pelo menos uma vez por ano?	03	012
201	EXISTE a condução de auditoria interna, também denominada de auditoria de primeira parte, das ações de SIC, pelo menos uma vez por ano?	03	002
202	SÃO realizadas atualizações dos planos de SIC, considerando os resultados da avaliação e análise crítica?	03	002
203	A autoridade decisória É informada de possíveis impactos na eficácia da Missão da Instituição?	03	002
204	EXISTE um procedimento formal de proposta à autoridade decisória, da necessidade de implementar as melhorias identificadas?	03	002
205	As ações corretivas e preventivas SÃO executadas de acordo com a identificação de não conformidade real ou potencial?	03	002
206	As melhorias SÃO comunicadas à autoridade decisória da Instituição?	03	002
207	O Gestor de SIC assegura-se que as melhorias atinjam os objetivos pretendidos?	03	002
208	Existe uma POSIC, elaborada considerando a natureza e finalidade da instituição, alinhada com a missão da instituição e ao seu planejamento estratégico?	04	001

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
209	Os objetivos e abrangência da POSIC estão claramente definidos no seu Escopo?	04	001
210	No texto da POSIC estão os conceitos e definições untilizados para evitar dificuldades de interpretação e ambiguidades de significados?	04	001
211	Estão relacionadas as referências legais e normativas utilizadas na elaboração da POSIC?	04	001
212	Está explícito um item com os principios que regem a Segurança da informação na instituição?	04	001
213	Foram estabelecidas as diretrizes gerais contendo no mínimo os temas: Tratamento da Informação; Tratamento de incidentes de rede; gestão de risco; gestão de continuidade; auditoria e conformidade; controles de acesso; uso de email; e acesso a internet?	04	001
214	Estão previstas as penalidades para os casos de violação da POSIC ou de quebra de segurança?	04	001
215	Foi definida uma estrutura para a Gestão de Segurança da Informação e Comunicações, na instituição?	04	001
216	Foi instituido um Gestor de Segurança da Informação e Comunicações na instituição, com a descrição clara de suas responsabilidades, conforma descrito no item 5.3.7.2 da NC03 da IN01?	04	001
217	Foi Instituido o Comitê de Segurança da Informação e Comunicações da istituição, e descritas a suas atribuições conforme descrito no item 5.3.7.3 da NC03 da IN01?	04	001
218	Foi Instituida a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da entidade?	04	001
219	Ficou estabelecida a periodicidade para revisão da POSIC e suas normas complementares?	04	001

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
220	A POSIC foi redigida de forma objetiva, simples, e de fácil leitura e entendimento?	04	001
221	A POSIC foi publicada e assinada pela autoridade máxima da instituição?	04	001
222	Existe garantia de recursos para implementação da POSIC da istituição?	04	001
223	Foram implementadas ações que promovam a cultura de Segurança da Informação e Comunicações na instituição?	04	001
224	A POSIC foi publicada e divulgada para todos os trabalhadores da instituição?	04	001
225	As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC considera prioritariamente os objetivos estratégicos, os processo, os requisitos legais e a estrutura do órgão?	05	012
226	As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC estão alinhadas à POSIC do órgão?	05	012
227	O processo de GRSIC é continuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações?	05	012
228	O processo de GRSIC está alinhado ao modelo PDCA?	05	012
229	A GRSIC oferece subsídios para suportar o Sistema de Gestão de Segurança da Informação e Comunicações e a Gestão de Continuidade de Negócios?	05	012
230	Foi definido o escopo de aplicação da GRSIC?	05	012

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
231	Foi adotada uma metodologia de GRSIC que atenda aos objetivos, diretrizes gerais e o escopo definido contemplando, no mínimo, os critérios de avaliação e aceitação de risco?	05	012
232	Foi realizado um inventário e mapeamento dos ativos de informação, no âmbito do escopo estabelecido, e conforme as diretrizes da NC10/IN01?	05	012
233	Os riscos associados ao escopo definido são identificados considerando as ameaças envolvidas?	05	012
234	Os riscos associados ao escopo definido são identificados considerando as vulnerabilidades existentes nos ativos de informação?	05	012
235	Os riscos associados ao escopo definido são identificados considerando as ações de SIC já adotadas	05	012
236	Os riscos levantados são estimados, considerando os valores ou níveis pra a probabilidade e para a consequência do risco associados à perda de disponibilidade, integridade, confidencialidade e autenticidade nos ativos considerados?	05	012
237	Os riscos são avaliados, determinando se são aceitáveis ou se requerem tratamento?	05	012
238	Os riscos que requeiram tratamento são relacionados, sendo priorizados de acordo com os critérios estabelecidos pelo órgão ou entidade?	05	012
239	As formas de tratamento dos riscos são determinadas considerando as opções de reduzir, evitar, tranferir ou reter o risco, observando a eficácia das ações de SIC já existentes?	05	012
240	As formas de tratamento dos riscos são determinadas considerando as opções de reduzir, evitar, tranferir ou reter o risco, observando as restrições organizacionais, técnicas e estruturais?	05	012
241	As formas de tratamento dos riscos são determinadas considerando as opções de reduzir, evitar, tranferir ou reter o risco, observando os requisitos legais?	05	012

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
242	As formas de tratamento dos riscos são determinadas considerando as opções de reduzir, evitar, tranferir ou reter o risco, observando a análise custo/beneficio?	05	012
243	É elaborado um plano para tratamento de riscos relacionando as ações de SIC, responsáveis, prioridades e prazos de execução necessários à sua implantação?	05	012
244	Os resultados do processo executado são verificados considerando o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação?	05	012
245	São executadas as ações de SIC incluídas no Plano de Tratamento de Riscos aprovado?	05	012
246	O processo de GRSIC é monitorado e analisado de forma a mantê-lo alinhado às diretrizes gerais estabelecidas e às ncecessidades do órgão?	05	012
247	Os riscos são monitorados e analisados criticamente, a fim de verificar mudanças nos critérios de avaliação e aceitação de riscos?	05	012
248	Os riscos são monitorados e analisados criticamente, a fim de verificar mudanças no ambiente?	05	012
249	Os riscos são monitorados e analisados criticamente, a fim de verificar mudanças nos ativos de informação?	05	012
250	Os riscos são monitorados e analisados criticamente, a fim de verificar mudanças nas ações de SIC?	05	012
251	Os riscos são monitorados e analisados criticamente, a fim de verificar mudanças nos fatores do risco?	05	012
252	Durante a fase de monitoramento e análise crítica, a autoridade decisória do órgão é informada da necessidade de implementar as melhorias identificadas?	05	012

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
253	As ações corretivas ou preventivas aprovadas, são prontamente executadas?	05	012
254	As melhorias são implementadas de forma a assegurar que os objetivos sejam atendidos?	05	012
255	As instâncias superiores são informadas a respeito de todas as fases da gestão de risco, compartilhando as informações entre o tomador da decisão e as demais partes envolvidas e interessadas?	05	012
256	Foi elaborado um Programa de Gestão de Continuidade de Negócios - PGCN?	06	010
257	O PGCN elaboradao contém um documento com as diretrizes do Programa de Continuidde	06	010
258	O PGCN define as atividades críticas do órgão?	06	010
259	O PGCN avalia os riscos a que essas atividades críticas estão expostas?	06	010
260	O PGCN define as estratégias de continuide para atividades críticas?	06	010
261	São desenvolvidos e implementados Planos previstos no Programa de Gestão de Continuidade de Negócios para respostas tempestivas e interrupções?	06	010
262	São realizados exercícios, testes e manutenção periódica dos Planos, promovendo as revisões necessárias?	06	010
263	Existem ações para o desenvolvimento da cultura de Continuidade de Negócios no órgão?	06	010

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
264	Os procedimentos previstos no Programa de Gestão de Continuidade de Negócios são executados em conformidade com os requisitos de Segurança de Informação e Comunicações?	06	010
265	O Programa de Continuidade de Negócios contém um Plano de Gerenciamento de Incidentes - PGI?	06	010
266	O Programa de Continuidade de Negócios contém um Plano de Continuidade de Negócios - PCN?	06	010
267	O Programa de Continuidade de Negócios contém um Plano de Recuperação de Negócios - PRN?	06	010
268	O Plano de Gerenciamento de Incidentes foi elaborado seguindo a estrutura proposta na NC 06 da IN01 itens 5.4.1	06	010
269	O Plano de Continuide de Negócios foi elaborado seguindo a estrutura proposta na NC 06 da IN01 itens 5.4.2	06	010
270	O Plano de Recuperação de Incidentes foi elaborado seguindo a estrutura proposta na NC 06 da IN01 itens 5.4.3	06	010
271	Os Planos são exercitados e testados periodicamente e os resultados documentados de forma a garantir a sua efetividade?	06	010
272	Os Planos prevêm serem revisados de acordo com a norma: Pelo menos uma vez por ano; ou em função de resultados de testes realizados; ou Após mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes?	06	010
273	As diretrizes estratégicas que norteiam a elaboração do PGCN são aprovadas pela alta direção do órgão?	06	010
274	A alta direção do ógão avalia a relação custo/benefício das estratégias de continuidade propostas e dos Planos que compõem a PGCN e decide sobre sua implementação?	06	010

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
275	A alta direção garante os recursos necessários para estabelecer, implementar, operar e manter o PGCN?	06	010
276	O Gestor de Continuidade de Negócios ou, na falta deste, o Gestor de Segurança da Informação propõe as diretrizes estratégicas para o PGCN?	06	010
277	O Gestor de Continuidade de Negócios ou, na falta deste, o Gestor de Segurança da Informação avalia o plano de tratamento de riscos?	06	010
278	O Gestor de Continuidade de Negócios ou, na falta deste, o Gestor de Segurança da Informação realiza, periodicamente, a Análise de Impacto nos Negócios - AIN?	06	010
279	O Gestor de Continuidade de Negócios ou, na falta deste, o Gestor de Segurança da Informação propõe melhorias na implantação de novos controles relativos ao PGCN?	06	010
280	O Gestor de Continuidade de Negócios ou, na falta deste, o Gestor de Segurança da Informação supervisiona a elaboração, implementação, testes e atualização dos Planos?	06	010
281	O Gestor de Continuidade de Negócios ou, na falta deste, o Gestor de Segurança da Informação desenvolve a cultura de GCN?	06	010
282	Os Gestores de setores ou processos que contenham atividades críticas para o órgão Elaboram os Planos previstos no PGCN relacionados às atividades críticas?	06	010
283	Os Gestores de setores ou processos que contenham atividades críticas para o órgão Realizam os testes e exercícios dos Planos?	06	010
284	Os Gestores de setores ou processos que contenham atividades críticas para o órgão Avaliam e Aprimoram os Planos a partir dos resultados dos testes e exercícios?	06	010
285	Os Gestores de setores ou processos que contenham atividades críticas para o órgão Administram a contingência quando da interrupção de atividades, com base nos planos desenvolvidos?	06	010

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
286	Os Gestores de setores ou processos com atividades críticas para o órgão propõem os recursos necessários à implantação e ao desenvolvimento das ações relativas à continuidade das atividades, e para a realização dos testes e dos exercicios dos Planos?	06	010
287	É feito um credenciamento para usuários antes da criação de contas de acesso a ativos de informação?	07	007
288	Os usuários, com exceção de administradores de rede local, têm somente uma conta institucional única, pessoal e intransferível?	07	007
289	Contas de acesso com perfil de administrador, somente são criadas para usuários que executam tarefas específicas de administração de ativos de informação?	07	007
290	Os usuários são responsabilizados pela quebra de segurança, ocorrida com utilização de sua senha, mediante assinatura de termo de responsabilidade?	07	007
291	Existe um processo automatizado com regras definidas, para criação de contas de serviço?	07	007
292	Existem regras de credenciamento, bloqueio e exclusão de contas de acesso de usuários?	07	007
293	Existem regras de credenciamento, bloqueio e exclusão de contas de acesso ao ambiente de desenvolvimento?	07	007
294	O usuário recebe credenciais de acesso à rede corporativa quando de sua contratação?	07	007
295	As credenciais de acesso do usuário é excluida quando de seu desligamento?	07	007
296	Os acesso à Rede corporativa é registrado permitindo a rastreabilidade e a identificação do usuário?	07	007

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
297	Existe pelo menos um mecanismo implementado, dos que contemplam biometria, tokens, smart cards, a fim de autenticar a identidade do usuário?	07	007
298	São utilizados mecanismos automáticos para inibir que equipamentos externos se conectem na rede corporativa de computadores?	07	007
299	São mantidos na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados?	07	007
300	O acesso remoto, bem como o acesso à informação sigilosas, é regulamentado por legislação específica?	07	007
301	O acesso remoto à rede corporativa é gravado em LOGs para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada?	07	007
302	Existem regras específicas para o uso de rede sem fio?	07	007
303	São utilizadas ferramentas de proteção contra acesso não autorizado aos ativos de informaçã, que favoreça, preferencialmente, a administração de forma centralizada?	07	007
304	As contas ou credenciais de acesso aos ativos de informação são configuradas respeitando-se o princípio do menor privilégio?	07	007
305	São usados ativos de informação homologados, nas aplicações de controle de acesso, de tratamento das informações sigilosas e de criptografia?	07	003
306	Os eventos relevantes, previamente definidos, para a segurança e rastreamento de acesso às informações sigilosas são registrados?	07	007
307	Existem mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.	07	003

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
308	O uso de ativos de informação sem relação com as atividades relativas ao cargo, função ou atividades públicas são controladas e bloqueadas?	07	003
309	Existem regras para o uso de Internet, do Correio Eletrônico e de Mensagens Instantâneas?	07	007
310	Existem regras para o uso de credenciais físicas, que se destinam ao controle de acesso dos usuários às instalações do órgão?	07	007
311	Foi definida a necessidade de instalação de sistemas de detecção de intrusos em áreas e instalações do órgão?	07	007
312	As áreas e Instalações são classificadas como ativos de informação de acordo com o valor, a criticidade, o tivo de ativo de informação e o grau de sigilo das informações que podem ser tratadas em tais áreas e instalações?	07	007
313	O uso de barreiras físicas de segurança, bem como equipamentos ou mecanismos de controle de entrada e saída são oritentados?	07	007
314	Os ativos de informação, principalmente aqueles considerados críticos, são protegidos contra ações de vandalismo, sabotagem, ataques, etc?	07	007
315	As áreas de recepção do órgão estão preparadas com regras claras de entrada e saída de pessoas, equipamentos e materiais?	07	007
316	Os pontos de entrega e carregamento de material são definidos e o acesso é restrito ao pessoal credenciado?	07	007
317	Os controle de acesso às áreas e instalações consideradas críticas são intensificados de acordo com a legislação vigente?	07	007
318	São difundidas e é exigido o seu cumprimetno a Política de Segurança da Informação e Comunicações, as normas de segurança e a legislação vigente sobre o tema?	07	007

CODIGO CONTROLE	DESCRICAO CONTROLE	CODIGO NORMA	CODIGO AREA
319	Existem ações de conscientização do usuário para adotar comportamento favorável à disponibilidade, à integridade, à confidencialidade e à autenticidade das informações?	07	007
320	Os riscos à Segurança da Informação e Comunicações dos ativos de informação são avaliados sistematicamente e são definidos controles a serem aplicados quanto ao acesso dos usuários?	07	007
321	Existe um formulário específico de Termo de Responsabilidade definido e dinfundido, que deve ser preenchido individualmente pelos usuários?	07	007
322	Existem regras específicas definidas pra autorização de acesso e credenciamento dos usuários em conformidade com a classificação dos ativos de informação?	07	007
323	Existem especificações de distância mínima de segurança para manutenção das mídias contendo as cópias de segurança (backups)?	07	007
324	Os ativos de informação são classificados em níveis de criticidade, considerando o tipo de informação e o provável impacto no caso de quebra de segurança, com base na gestão de Risco e Gestão de continuidade de negócios?	07	007
325	Existe procedimentos especiais de controles de acesso físico, em conformidade com a legislação vigente, para os ativos de informação classificados como sigilosos?	07	007
326	Estão definidos os perímetros de segurança, suas dimensões, equipamentos e tipos especiais de controles de acesso aos ativos de informação?	07	007
327	Existe uma documentação própria que permita que sejam identificados os perímetros de segurança de cada ativo de informação por todos que transitarem ou tiverem acesso em tais espaços, em especial às áreas e instalações críticas?	07	007
328	O armazenamento, a veiculação de imagem, vídeo ou áudio, registrados em perímetro de segurança, são regulamentados por normas específicas?	07	007