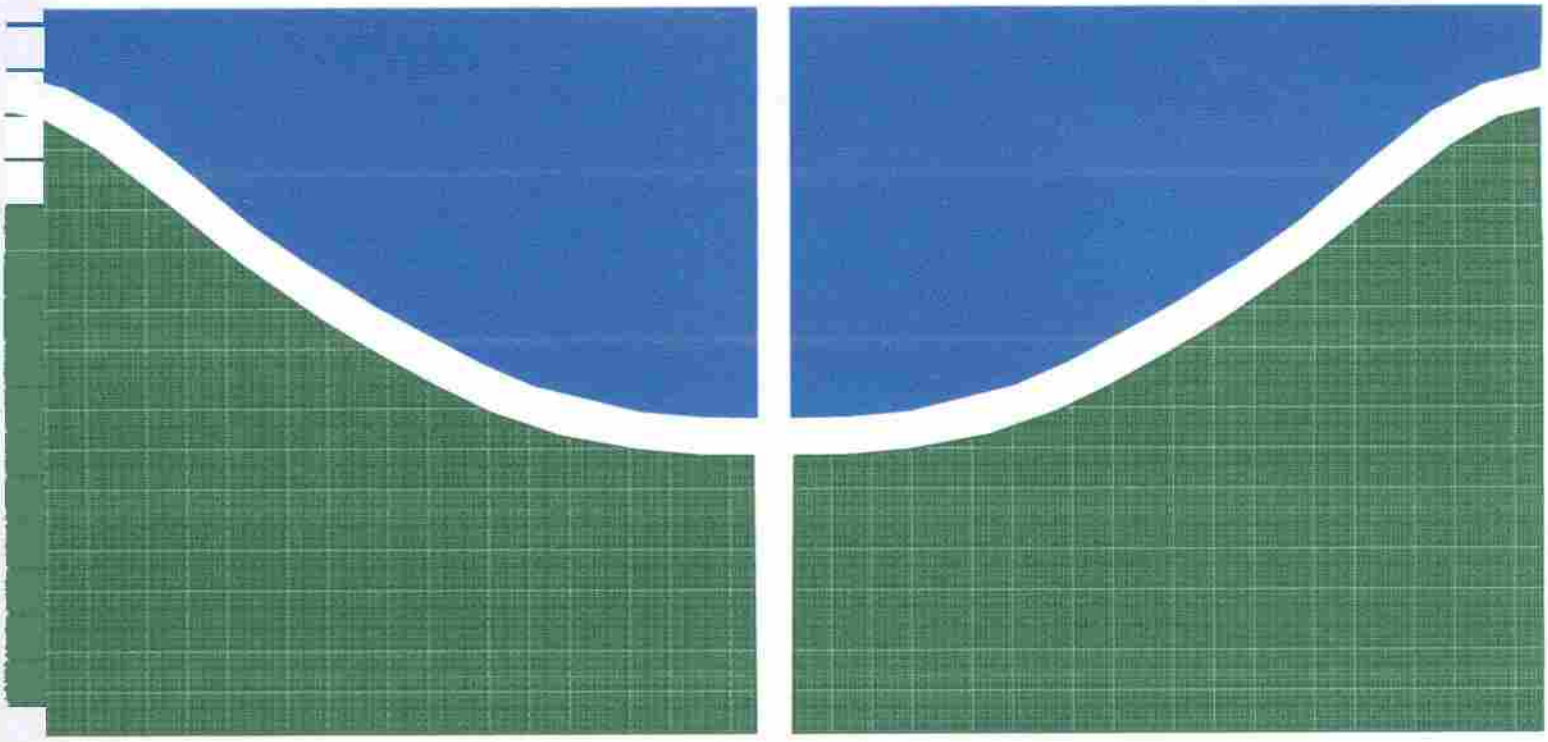


AUDITORIA DE SEGURANÇA DA INFORMAÇÃO NOS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA: MATURIDADE, *COMPLIANCE* E BOAS PRÁTICAS

CLÁUDIO ZUMPICHIATTE MIRANDA

MONOGRAFIA DE ESPECIALIZAÇÃO EM GESTÃO DA SEGURANÇA DA INFORMAÇÃO

FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

AUDITORIA DE SEGURANÇA DA INFORMAÇÃO NOS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA: MATURIDADE, *COMPLIANCE* E BOAS PRÁTICAS

CLÁUDIO ZUMPICHIATTE MIRANDA

ORIENTADORA: PROFESSORA DRA. EDNA DIAS CANEDO

MONOGRAFIA DE ESPECIALIZAÇÃO EM GESTÃO DA SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO: UnBLabRedes.MFE.012/2017
BRASÍLIA, DF: AGOSTO / 2017.

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

AUDITORIA DE SEGURANÇA DA INFORMAÇÃO NOS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA: MATURIDADE, *COMPLIANCE* E BOAS PRÁTICAS

CLÁUDIO ZUMPICHIATTE MIRANDA

MONOGRAFIA DE ESPECIALIZAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ESPECIALISTA EM GESTÃO DA SEGURANÇA DA INFORMAÇÃO.

APROVADO POR:

_____

EDNA DIAS CANEDO
DOUTORA, UNB/ENE (ORIENTADOR)

_____

RAFAEL TIMÓTEO DE SOUSA JÚNIOR
DOUTOR, UNB/ENE (MEMBRO INTERNO - UNB/ENE)

_____

ELIANE CARNEIRO SOARES
MESTRE, UNB/ENE (MEMBRO EXTERNO - SEDF)

_____

BRASÍLIA, DF, AGOSTO DE 2017.

FICHA CATALOGRÁFICA

Miranda, Claudio Zumpichiatte.

Auditoria de Segurança da Informação nos Órgãos da Administração Pública: Maturidade, Compliance e Boas Práticas. [Distrito Federal], 2017.

62 p, 210 x 297mm (ENE/FT/UnB, Especialista, Engenharia Elétrica, 2017).

Trabalho de conclusão de curso - Especialização – Universidade de Brasília, Faculdade de Tecnologia.

1. Segurança da Informação.
2. Auditoria.
3. NBR ISO/IEC 27002:2013.
4. Boas práticas de SI.
5. Normas complementares do GSI

I. ENE/FT/UnB
II. Título (série)

Departamento de Engenharia Elétrica.

REFERÊNCIA BIBLIOGRÁFICA

Miranda, Claudio Zumpichiatte. (2017). Auditoria de Segurança da Informação nos Órgãos da Administração Pública: Maturidade, Compliance e Boas Práticas. Trabalho de conclusão de curso - Especialização, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 62 p.

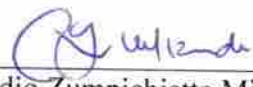
CESSÃO DE DIREITOS

AUTOR: Claudio Zumpichiatte Miranda

TITULO: Auditoria de Segurança da Informação nos Órgãos da Administração Pública: Maturidade, Compliance e Boas Práticas.

GRAU / ANO: Especialista / 2017

É concedida à Universidade de Brasília permissão para reproduzir cópias deste Trabalho de Conclusão de Curso, para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. O autor reserva outros direitos de publicação e nenhuma parte deste Trabalho de Conclusão de Curso pode ser reproduzida sem autorização por escrito do autor.



Claudio Zumpichiatte Miranda

Tel. +55(61) 981479816 / claudio.zumpichiatte@gmail.com

AGRADECIMENTOS

A Deus, pelas oportunidades que me tem concedido.

Aos meus pais, Onicio (*in memorian*) e Eureny, pelo exemplo, amor e dedicação.

À minha esposa Vanessa, pelo amor, companheirismo, inspiração e incentivo a cada dia.

Aos meus filhos Victor e Cecília, inspiração e desafio, presentes de Deus na minha vida.

Aos meus irmãos Marcos, Eduardo e Mauro, amigos e companheiros em todos os momentos da vida.

Aos professores, por mostrar como subir mais um grau do conhecimento.

Aos colegas de trabalho e amigos, pelos incentivo e bons momentos juntos nesta jornada.

À minha orientadora Prof. Drª Edna Dias Canedo pela orientação e paciência.

A verdadeira medida de um homem não é como ele se comporta em momentos de conforto e conveniência, mas como ele se mantém em tempos de controvérsias e desafios.
(Martin Luther King)

RESUMO

Auditoria de Segurança da Informação nos órgãos da administração pública: Maturidade, *Compliance* e Boas Práticas.

A Tecnologia da Informação tornou-se fundamental para que as organizações públicas e privadas atinjam seus objetivos institucionais. Como consequência do uso intensivo de computadores, há o aumento no número de ataques que exploram as vulnerabilidades dos ativos e sistemas de informação. Para reduzir essas vulnerabilidades e os riscos inerentes ao uso de tecnologias impõe-se níveis crescentes de proteção e o uso de controles cada vez mais sofisticados relacionados à Segurança da Informação. A Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. Hoje a legislação e os normativos que tratam de Segurança da Informação (SI) são cada vez mais complexos. Existem mais de 400 princípios, diretrizes e recomendações das normas elaboradas pelo Gabinete de Segurança Institucional, órgão responsável pela normatização das recomendações sobre SI na Administração Pública Federal. A NBR ISO/IEC 27002, dividida em 14 seções, prevê outros 114 controles sobre boas práticas de SI para as organizações. Nesse cenário, é essencial que haja um conjunto mínimo de controles, diretrizes e boas práticas de SI que orientem o gestor de TI. Tal conjunto de controles será útil nas auditorias de Segurança da Informação, realizadas pela própria organização (auditoria interna) e pelos órgãos de controle (auditoria externa). Este estudo chegou a um conjunto de 59 controles considerados muito relevantes para a Segurança da Informação. Esse conjunto de controles será uma ferramenta útil para o gestor de TI no planejamento e execução de projetos, além de auxiliar na racionalização dos custos de implementação da Segurança da Informação.

Palavras-chave: Segurança da Informação, auditoria, NBR ISO 27002:2013, Boas práticas de SI, Normas complementares do GSI.

ABSTRACT

Audit of Information Security in public administration bodies: Maturity, Compliance and Best Practices.

Information Technology has become critical for public and private organizations to achieve their institutional goals. As a consequence of the intensive use of computers, there is an increase in the number of attacks that exploit the vulnerabilities of assets and information systems. To reduce these vulnerabilities and the risks inherent in using technologies, increasing levels of protection and the use of increasingly sophisticated controls related to Information Security are required. Information Security is the protection of information from various types of threats to ensure business continuity, minimize risk to the business, maximize return on investment and business opportunities. Today the legislation and regulations that deal with Information Security (IS) are increasingly complex. There are more than 400 principles, guidelines and recommendations of the standards developed by the Office of Institutional Security, the body responsible for standardizing recommendations on IS in Federal Public Administration. The NBR ISO / IEC 27002, divided into 14 sections, provides another 114 controls on good IS practices for organizations. In this scenario, it is essential that there is a minimum set of controls, guidelines and best IS practices that guide the IT manager. Such a set of controls will be useful in the Information Security audits carried out by the organization itself (internal audit) and the control bodies (external audit). This study reached a set of 59 controls considered very relevant for Information Security. This set of controls will be a useful tool for the IT manager in the planning and execution of projects, besides helping to rationalize the costs of implementing Information Security.

Keywords: Information Security, Auditing, NBR ISO 27002: 2013, Good Information Security practices, GSI complementary standards.

SUMÁRIO

1. INTRODUÇÃO 1
1.1. Motivação 3
1.2. Objetivos do Trabalho 4
1.2.1. Objetivo Geral: 4
1.2.2. Objetivos Específicos: 4
1.3. Metodologia 4
1.3.1. Tipologia da Pesquisa 4
1.3.2. Instrumentos de coleta e de análise adotados na Pesquisa 5
1.4. Organização do Trabalho 6
2. REFERENCIAL TEÓRICO 7
2.1. Auditoria 7
2.1.1. Conceitos e definições 7
2.1.2. Fases de uma auditoria 8
2.1.3. Seleção da auditoria 8
2.1.4. Planejamento da auditoria 10
2.1.5. Execução da auditoria 12
2.1.6. Demais fases da auditoria 12
2.2. Legislação – Segurança da Informação e Comunicações 12
2.3. Visão geral das normas da família NBR ISO/IEC 27000 – Segurança da Informação 15
2.4. Visão Geral da NBR ISO/IEC 27002:2013 – Segurança da Informação e Comunicações 16
2.5. Normas Complementares à IN nº 01 GSI/PR/2008 19
2.5.1. NC 01 e 02 - Metodologia de Gestão de Segurança da Informação 20
2.5.2. NC 03 - Política de Segurança da Informação 21
2.5.2.1. Principais diretrizes e recomendações da NC 03 21
2.5.3. NC 04 - Gestão de Riscos de Segurança da Informação 22
2.5.4. NC 05, 08 e 21 - Incidentes de Segurança em Redes Computacionais 23
2.5.4.1. NC 05 - Equipe de Tratamento e Resposta e gerenciamento de Incidentes de Segurança em Redes de Computadores 23
2.5.4.2. NC 08 - Gerenciamento de Incidentes de Segurança em Redes de Computadores 25
2.5.4.3. NC 21 - Preservação de evidências de incidentes de Segurança em Redes 27
2.5.5. NC 06 - Gestão de Continuidade de Negócios 28

2.5.6. NC 07 - Controles de Acesso Relativos à Segurança da Informação 29
2.5.6.1. Diretrizes da NC 07 30
2.5.7. NC 09 - Recursos criptográficos em Segurança da Informação e Comunicações 32
2.5.8. NC 10 - Inventário e Mapeamento de Ativos de Informação 33
2.5.9. NC 11 - Avaliação de conformidade nos aspectos relativos à Segurança da Informação 34
2.5.10. NC 12 - Uso de dispositivos móveis 35
2.5.11. NC 13 - Gestão de mudanças nos aspectos relativos à Segurança da Informação 36
2.5.12. NC 14 - Computação em Nuvem 37
2.5.13. NC 15 - Uso de redes sociais 37
2.5.14. NC 16 - Desenvolvimento e Obtenção de Software Seguro 38
2.5.15. NC 17 - atuação e adequações para profissionais da área de Segurança da Informação 40
2.5.16. NC 18 - Atividades de ensino em Segurança da Informação 40
2.5.17. NC 19 - Segurança da Informação em Sistemas Estruturantes da Administração Pública 41
2.5.18. NC 20 - Segurança da Informação no Tratamento da Informação 42
3. RESULTADOS DA PESQUISA 45
3.1. Como foi elaborado o questionário 45
3.2. Como foi realizada a pesquisa 48
3.3. Consolidação e análise dos resultados 49
3.4. Conjunto mínimo de controles de Segurança da Informação 54
4. CONCLUSÕES 61
4.1. TRABALHOS FUTUROS 62
REFERÊNCIAS BIBLIOGRÁFICAS 63

LISTA DE TABELAS

1. Tabela 2.1 - Modelo de Matriz de Planejamento.
2. Tabela 2.2 – Modelo de Matriz de Achados
3. Tabela 2.3 – Normas da Família NBR ISO/IEC 27000.
4. Tabela 2.4 – Seções da Norma NBR ISO/IEC 27002:2013.
5. Tabela 2.5 – Normas Complementares à IN GSI/PR nº 1, de 13.06.2008.
6. Tabela 2.6 – Modelos de Implementação de ETIR.
7. Tabela 2.7 – Anexo A da NC nº 20/IN01/DSIC/GSIPR.
8. Tabela 3.1 – Total de princípios, diretrizes e recomendações das normas complementares à IN nº 01 GSI/PR/2008.
9. Tabela 3.2 – Correlação entre NC, NBR ISO/IEC 27002:2013 e questionário.
10. Tabela 3.3 – Consolidação dos resultados – Controles selecionados.
11. Tabela 3.4 – Consolidação dos resultados – Implementação dos Controles.
12. Tabela 3.5 – Controles de SI selecionados como "muito relevantes" na pesquisa.
13. Tabela 3.6 – 28 Controles de SI selecionados como "relevantes" na pesquisa.

LISTA DE FIGURAS

1. Figura 2.1 – Processo de Gestão de Riscos.

LISTA DE ACRÔNIMOS

1. BCI - Business Continuity Institute
2. Comptia - *Computing Technology Industry Association*
3. DRI International - *Disaster Recovery Institute International*
4. Ec-Council - *Electronic Commerce Consultants*
5. EXIN - *Examinations Institute*
6. GIAC - *Global Information Assurance Certification*
7. IRCA - *International Register of Certificated Auditors*
8. ISACA - *Information Systems Audit and Control Association*
9. ISC²- *International Information Systems Security Certification Consortium, Inc.*
10. OGC - *Office of Government Commerce*
11. RAB - Registrar *Accreditation Board*
12. SANS - *SysAdmin Audit Networking and Security*

1. INTRODUÇÃO

Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava guardar os documentos em algum lugar e restringir o acesso físico. Com as mudanças tecnológicas e o uso de computadores, a estrutura de segurança ficou mais sofisticada, englobando vários tipos de controles (TCU, 2012). A tecnologia da informação (TI) tornou-se então fundamental para que as organizações públicas e privadas atinjam seus objetivos institucionais. Por isso, ao se pensar em Tecnologia da Informação (TI) em uma organização, com o foco em segurança, deve-se ter em mente os conceitos de informação, vulnerabilidade, ativos, riscos e Segurança da Informação (SI).

Para a norma da ABNT NBR ISO/IEC 17799 (2005, pág. 9), a informação "é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e precisa ser adequadamente protegida". A informação pode existir em diversas formas: impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos.

A Norma complementar nº 10/IN01/DSIC/GSIPR, do Gabinete de Segurança Institucional, define "vulnerabilidade" como o conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de SI. Já "riscos de SI" são o potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

Define ainda "Ativos de Informação" como os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Ainda segundo a norma da ABNT NBR ISO/IEC 17799 (2005), "Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

Assim, é necessário que as ações de TI desenvolvidas pelos entes públicos, os ativos de TI e as informações armazenadas estejam protegidos, garantindo a correta aplicação dos

recursos empregados e a entrega dos serviços à população com qualidade, eficiência e eficácia.

A tarefa de gerir a SI de uma organização, pública ou privada, em um ambiente computacional altamente interconectado é um grande desafio, que se torna mais difícil à medida que novos produtos, aplicativos e serviços são lançados. Devido ao dinamismo da evolução das tecnologias é necessário que as organizações públicas estejam preparadas e adaptadas para essas mudanças.

De um lado temos o uso intensivo de TI e de novas tecnologias. De outro, a necessidade de proteção dos ativos contra as ameaças. Nesse cenário, cresce a preocupação dos administradores na busca de um nível adequado de segurança em relação à segurança dos sistemas e das informações armazenadas.

Na busca dessa solução foram criadas e aperfeiçoadas legislações, normativos e boas práticas que tratam especificamente deste tema. Segundo Vieira (2014), existe uma grande quantidade de leis, decretos e normas que disciplinam a Segurança da Informação no Brasil. Em caminho oposto existe a percepção da falta de alinhamento entre o que é disciplinado legalmente e o que é posto em prática pelas organizações.

Na maioria das organizações públicas, percebe-se a carência em processos e capacitação dos gestores nas melhores práticas em SI, além da falta de cultura organizacional, o que dificulta a implementação de controles suficientes e eficientes.

A Segurança da Informação é alcançada pela implementação de um conjunto adequado de controles, políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a Segurança da Informação da organização sejam atendidos (NBR ISO/IEC 27002:2013).

Diante desse quadro, é essencial que uma organização identifique os seus requisitos de SI. São três as principais fontes para verificação destes requisitos (NBR ISO/IEC 27002:2013):

a) avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócio da organização. Por meio da avaliação de riscos, são identificadas as ameaças aos ativos e as vulnerabilidades destes, e realizada uma

estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio.

b) a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, e o seu ambiente sociocultural.

c) os conjuntos particulares de princípios, objetivos e os requisitos do negócio para o manuseio, processamento, armazenamento, comunicação e arquivo da informação, que uma organização tem que desenvolver para apoiar suas operações.

1.1. Motivação

Hoje a legislação e os normativos que tratam de Segurança da Informação são cada vez mais complexos. Além dos várias portarias, decretos e leis que tratam do assunto, temos mais de 400 princípios, diretrizes e recomendações das normas elaboradas pelo Gabinete de Segurança Institucional, órgão responsável pela normatização das recomendações sobre SI na Administração Pública Federal. Temos ainda os 114 controles da NBR ISO/IEC 27002, divididos em 14 seções, que tratam das boas práticas de SI para as organizações públicas e privadas.

Nesse cenário, é essencial que haja um conjunto mínimo de controles, diretrizes e boas práticas em SI que orientem o gestor de TI. Tal conjunto de controles será útil nas auditorias de SI, na elaboração das "questões de auditoria (vide item 2.1.4 – Planejando uma auditoria)", realizadas pela própria organização (auditoria interna) e pelos órgãos de controle (auditoria externa). Será também uma ferramenta útil para o gestor de TI no planejamento e execução de projetos, além de auxiliar na racionalização dos custos de implementação de SI.

A delimitação de um conjunto mínimo de controles, diretrizes e boas práticas em SI, proporcionará uma orientação segura para a administração pública e para as organizações em geral, e possibilitará verificar o *status* de seu Sistema de Gestão da SI (*maturidade*) e a conformidade (*compliance*) com as principais normas existentes.

1.2. Objetivos do Trabalho

1.2.1. Objetivo Geral:

Delimitar um conjunto mínimo de controles, diretrizes e boas práticas em Segurança da Informação, que proporcione uma orientação prática para a administração pública, e que auxilie as atividades de auditoria realizada pela própria organização (auditoria interna) e pelos órgãos de controle (auditoria externa).

1.2.2. Objetivos Específicos:

(1) Verificar o *compliance* (conformidade) à legislação e aos normativos de SI.

(2) Investigar as boas práticas de SI implementadas nos entes públicos e que possam ser replicadas em outros órgãos.

(3) Realizar uma revisão bibliográfica sobre a legislação, normativos e boas práticas de SI.

(4) Apresentar um conjunto de controles, diretrizes e boas práticas em Segurança da Informação que aperfeiçoe a ação dos órgãos públicos, auxiliando as auditorias internas e externas.

1.3. Metodologia

1.3.1. Tipologia da Pesquisa

O presente estudo utilizou uma metodologia quali-quantitativa, transversal (realizado em um determinado instante de tempo), onde as unidades de análise foram os órgãos e entidades públicos, mais especificamente, as diretorias ou coordenações de tecnologia da informação desses órgãos.

Foi construída uma amostra a partir dos órgãos e entidades da administração pública sediados no Distrito Federal, com reconhecido destaque em suas áreas finalísticas de atuação: órgãos de controle, tribunais superiores, tribunal do poder judiciário, empresas públicas, organização militar, minstério ligado ao Poder Executivo Federal.

A delimitação destas unidades de análise que possuem boa representatividade visa superar as dificuldades de generalização dos resultados imposta pela metodologia. Foram enviados, por meio eletrônico, 10 questionários com correspondência explicativa (Apêndice 3) a gestores e usuários avançados de TI destes órgãos, e devolvidos 07 questionários preenchidos, perfazendo 70% de retornos.

1.3.2. Instrumentos de coleta e de análise adotados na Pesquisa

Como instrumentos de coleta de dados, a pesquisa não se limitou a uma única tipologia de coleta. Foram incorporados aspectos da revisão documental, pesquisa bibliográfica, realização de questionário e levantamento de opinião com gestores TI.

Preliminarmente, foi realizado um levantamento do referencial bibliográfico referente ao tema Segurança da Informação. A pesquisa documental teve como base principalmente os manuais de auditorias dos tribunais de contas e a legislação e normas ABNT correlatas. Tendo em vista a carência na literatura quanto aos tópicos maturidade, *compliance* e boas práticas em Segurança da Informação, foi utilizada a abordagem metodológica da pesquisa qualitativa como instrumento para melhor conhecer os fatos, programas, processos e as atividades correspondentes ao objeto de pesquisa.

O documento base para elaboração do questionário (Apêndice 2) foram as 21 normas complementares do Gabinete de Segurança Institucional – GSI (normas de Segurança da Informação detalhadas em recomendações de segurança) à IN Nº 01 GSI/PR/2008 e os 114 controles contidos na NBR ISO/IEC 27002:2013. Foram então criadas categorias de acordo com a interseção destes 114 controles com as normas do GSI. O questionário teve como objetivo selecionar um conjunto mínimo de controles de SI em relação aos controles implementados nas organizações públicas e em relação ao grau de relevância de cada controle de acordo com a percepção do usuário avançado/gestor de TI.

Para a análise das normas e controles foi utilizado o processo de categorização, que segundo Bardin (2002 p.147) "é uma operação de classificação de elementos constitutivos de um conjunto, por diferenciação e seguidamente, por reagrupamento segundo a analogia, com os critérios previamente definidos". Para isso é necessário o trabalho intensivo de análise do que cada um deles tem em comum. Uma boa categorização deverá conter cinco qualidades (Ibidem, 2002 p. 147):

a) Exclusão mútua: o elemento não deverá existir em outra categoria, não deverá existir ambiguidade;
b) Homogeneidade: a categoria deverá ser organizada sobre um único princípio;
c) Pertinência: o conteúdo deverá corresponder ao material de análise ou da investigação;
d) Objetividade e fidelidade: as partes diferentes do objeto da mesma categoria deverão ser codificadas da mesma forma se submetidos a várias análises; e

e) Produtividade: a categorização "fornece resultados férteis: em índices de inferência, em hipóteses novas e em dados exatos" (BARDIN, 2002 p.148).

Diehl (2004) enfatiza que a abordagem qualitativa apresenta maior liberdade teórico-metodológica para realizar seu estudo. Os limites de sua iniciativa são fixados pelas condições exigidas a um trabalho científico, mas ela deve apresentar estrutura coerente, consistente, originalidade e nível de objetivação capaz de merecer a aprovação dos cientistas num processo intersubjetivo de apreciação.

Por meio dessa abordagem, busca-se ter maior familiaridade com o problema, com vistas a torná-lo explícito. Destaca-se que a pesquisa qualitativa é exploratória e útil quando o pesquisador não conhece as variáveis importantes a examinar. Esse tipo de técnica pode ser necessário ou porque o tópico é novo, ou porque nunca foi abordado com uma determinada amostragem ou grupo de pessoas. Outra vantagem do estudo qualitativo é a utilização de uma pequena amostra observada de um modo mais profundo, diminuindo os custos da pesquisa e permitindo a geração de hipóteses pertinentes a problemas complexos (FERREIRA et al, 2002).

O método qualitativo, contrapondo o método quantitativo, não emprega um referencial estatístico como base do processo de análise de um problema. Esse método privilegia os dados qualitativos das informações disponíveis. De acordo com Patton, 1980, e Glazier, 1992, (*apud* DIAS, 2000, p. 1), os dados qualitativos são compostos, dentre outros aspectos, por "citações das pessoas a respeito de suas experiências" e "descrições detalhadas de fenômenos e comportamentos"

Para análise dos dados coletados através do questionário, utilizou-se de estatística descritiva (descrever e sumarizar o conjunto de dados) e gráficos para os dados numéricos. Desse modo, buscou-se reunir as experiências pesquisadas para promover o melhor entendimento quanto ao tema deste trabalho.

1.4. Organização do Trabalho

Este estudo foi dividido em cinco capítulos, o primeiro apresentou a introdução do tema e os objetivos deste estudo. O segundo capítulo trata do referencial teórico e dos conceitos necessários ao entendimento do tema: auditoria e tipos de auditorias; legislação e normas de Segurança da Informação. O terceiro capítulo trará a avaliação proposta neste trabalho. E por fim, o quarto capítulo trata das conclusões deste estudo.

2. REFERENCIAL TEÓRICO

Este capítulo tem como foco a revisão dos principais conceitos de auditoria, legislação e normativos de Segurança da Informação. Com o intuito de abranger o tema em um cenário amplo e ao mesmo tempo, ser possível a separação dos conceitos, assuntos correlatos e similares, foi realizado uma divisão dos assuntos em tópicos específicos.

Na seção 2.1 é abordado o tema de auditoria. Na seção 2.2 é abordado os conceitos relacionados à legislação. Na seção 2.3 é abordado o tema visão geral das normas da família NBR ISO/IEC 27000. Na seção 2.4 é apresentado a visão geral da NBR ISO/IEC 27002:2013. Na seção 2.5 são apresentados as principais diretrizes, orientações e recomendações das normas complementares à IN nº 01 GSI/PR/2008.

2.1. Auditoria

2.1.1. Conceitos e definições

Auditoria é processo sistemático, documentado e independente de se avaliar objetivamente uma situação ou condição para determinar a extensão na qual os critérios aplicáveis são atendidos, obter evidências quanto a esse atendimento e relatar os resultados dessa avaliação a um destinatário predeterminado (TCU - Glossário de Termos do Controle Externo, 2012).

Segundo as Normas de Auditoria Governamental (2010), auditoria governamental "é o exame efetuado em entidades da administração direta e indireta, em funções, subfunções, programas, ações (projetos, atividades e operações especiais), áreas, processos, ciclos operacionais, serviços, sistemas e sobre a guarda e aplicação de recursos públicos por outros responsáveis, em relação aos aspectos contábeis, orçamentários, financeiros, econômicos, patrimoniais e operacionais, assim como acerca da confiabilidade do sistema de controle interno".

Ainda segundo as Normas de Auditoria Governamental (2010) este tipo de auditoria é realizado por profissionais de auditoria governamental, por intermédio de (a) levantamentos de informações; (b) análises imparciais; (c) avaliações independentes; e (d) apresentação de informações seguras. Essas informações serão devidamente consubstanciadas em evidências, segundo vários critérios, sendo os principais: legalidade, legitimidade, economicidade, eficiência, eficácia, efetividade, equidade, ética, transparência e proteção do meio ambiente,

além de observar a probidade administrativa e a responsabilidade social dos gestores da coisa pública.

O TCU adota a seguinte classificação para os tipos de auditoria na esfera governamental auditoria de conformidade ou de regularidade e auditoria operacional (Manual de Auditoria Operacional/ TCU, 2010). Já a Controladoria-Geral da União – CGU, classifica a auditoria governamental em: (1) auditoria de avaliação da gestão; (2) auditoria de acompanhamento da gestão; (3) auditoria contábil; (4) auditoria operacional; e (5) auditoria especial (CONTROLADORIA-GERAL DA UNIÃO, Instrução Normativa nº 01/2001, página 32).

Um tipo de auditoria adotada na esfera privada é a auditoria de demonstrações contábeis. Conforme as Normas Brasileiras de Contabilidade – NBC TA 200, este tipo de auditoria consiste no exame objetivo, sistemático e independente, pautado em normas técnicas e profissionais, das demonstrações contábeis com o objetivo de se expressar uma opinião, materializada em relatório ou parecer de auditoria, sobre a adequação desses demonstrativos em relação aos princípios e às normas contábeis e à legislação pertinente.

A NBC TA 200, norma que trata objetivos gerais do auditor independente e a condução da auditoria em conformidade com normas de auditoria, define que o objetivo da auditoria contábil é aumentar o grau de confiança nas demonstrações contábeis por parte dos usuários. Isso é alcançado mediante a expressão de uma opinião pelo auditor sobre se as demonstrações contábeis foram elaboradas, em todos os aspectos relevantes, em conformidade com uma estrutura de relatório financeiro aplicável.

2.1.2. Fases de uma auditoria

Conforme as orientações do TCU para "Avaliação de Programas de Governo" (2016), o ciclo completo de uma auditoria compreende as etapas de seleção, planejamento, execução, análise, elaboração de relatório, comentário do gestor, apreciação, divulgação e monitoramento.

2.1.3. Seleção da auditoria

Segundo o Manual de Auditoria Operacional do TCU (2010), o processo de seleção do objeto da auditoria é o primeiro estágio deste ciclo. Visa selecionar um objeto que ofereça oportunidade para realização da auditoria e que, no caso dos órgãos de controle, contribua para

o aperfeiçoamento da administração pública e forneça à sociedade opinião independente sobre o desempenho da atividade pública.

Segundo as "Normas Internacionais das Entidades Fiscalizadoras Superiores" (ISSAI 200, 2001), o processo de seleção é necessário porque o campo de atuação do controle externo é muito amplo, se comparado aos seus recursos, que são limitados. A equipe de auditoria precisa decidir o que auditar, pois os recursos são limitados.

Por isso é necessário estabelecer critérios de seleção, visando aumentar a probabilidade de atingir objetivos significativos na auditoria. O auditor sempre estará diante do dilema das escolhas estratégicas, e essas escolhas dependerão da experiência e da capacitação da equipe de auditoria. Conforme Intosai – *International Organization of Supreme Audit Institutions* (*apud* Manual de auditoria operacional TCU, 2010), em uma auditoria governamental, alguns critérios de seleção podem ser utilizados, tais como relevância, materialidade e vulnerabilidade.

Em uma auditoria contábil, métodos de amostragem estatística ou não estatística também podem ser utilizados na fase seleção. O auditor deve projetar e selecionar uma amostra de auditoria, aplicar a essa amostra procedimentos de auditoria e avaliar os resultados da amostra, de forma a proporcionar evidência de auditoria suficiente e apropriada (Normas de Auditoria Independente das Demonstrações Contábeis, NBC T, 2009).

A amostra selecionada deve ter uma relação direta com o volume de transações realizadas pela organização objeto de exame, como também com os efeitos na posição patrimonial e financeira da entidade, e o resultado (financeiro) por ela obtido no período (NBC T 11, 2009).

Uma outra técnica utilizada é a seleção baseada em risco, ou como tratado pela literatura, auditoria baseada em riscos. Segundo Cicco (2006), a avaliação de riscos em auditoria identifica, mede e prioriza os riscos para possibilitar a focalização nas áreas auditáveis mais significativas. A auditoria é pautada pela avaliação dos riscos, que é utilizada para identificar as áreas mais importantes em uma organização. A avaliação de riscos pode ser utilizada pelo auditor nas outras fases de uma auditoria, delineando um programa de auditoria capaz de testar os controles mais importantes.

Ainda segundo CICCO (2006), a avaliação de riscos em auditoria ou "Auditoria Baseada em Riscos" engloba todos os tipos de auditoria, pois identifica, mede e prioriza os

riscos para possibilitar a focalização nas áreas auditáveis, imprescindíveis para a operacionalidade da organização.

É importante destacar que em qualquer dos métodos descritos, as possíveis opções implicam escolhas. E por ser um procedimento formal, o método escolhido na seleção deverá estar devidamente fundamentado, e embasado em critérios objetivos.

2.1.4. Planejamento da auditoria

O segundo estágio do ciclo é o planejamento da auditoria, e consiste das seguintes atividades: a) análise preliminar do objeto de auditoria; b) definição do objetivo e escopo da auditoria; c) especificação dos critérios de auditoria; d) elaboração da matriz de planejamento; e) validação da matriz de planejamento; f) elaboração de instrumentos de coleta de dados; g) teste-piloto; h) elaboração do projeto de auditoria (Manual de Auditoria Operacional do TCU, 2010).

No final da fase de planejamento deverá existir um conjunto de informações que norteie as demais fases da auditoria, geralmente sintetizada em uma matriz, chamada de matriz de planejamento. A matriz de planejamento apresenta, para cada questão de auditoria, as informações que serão necessárias para a sua análise; as fontes de obtenção de informações; os procedimentos de coleta e análise das informações; as limitações dela decorrentes; e, os potenciais resultados esperados.

Um dos elementos centrais no planejamento dos trabalhos de auditoria é definir as "questões de auditoria". Uma "questão de auditoria" é uma pergunta (linha da Matriz de Planejamento) que estabelece com clareza o foco de sua investigação, as dimensões e os limites que deverão ser observados durante a execução dos trabalhos. Para cada "questão de auditoria" deverá existir um "critério" de avaliação, ou fonte de informação, que poderá ser uma lei, normativo ou uma boa prática existente no mercado.

O conjunto de controles resultantes desta pesquisa irá auxiliar o trabalho das equipes no planejamento de auditorias de SI, fornecendo os elementos necessários para formulação das "questões de auditoria".

Tabela 2.1 - Modelo de Matriz de Planejamento

Problema: Expressar, de forma clara e objetiva, aquilo que motivou a auditoria.						
Questão de auditoria	**Informações requeridas**	**Fontes de informação**	**Procedimentos de coleta de dados**	**Procedimentos de análise de dados**	**Limitações**	**O que a análise vai permitir**
Especificar os termos- chave e o escopo da questão: -critério -período de abrangência -atores envolvidos -abrangência geográfica	Identificar as informações necessárias para responder à questão de auditoria	Identificar as fontes de cada item de informação	Identificar as técnicas de coleta de dados que serão usadas e descrever os respectivos procedimentos	Identificar as técnicas a ser empregadas na análise de dados e descrever os respectivos procedimentos	Especificar as limitações quanto: -à estratégia metodológica adotada -ao acesso a pessoas e informações -à qualidade das informações -às condições operacionais de realização do trabalho	Esclarecer precisamente que conclusões ou resultados podem ser alcançados

Fonte: Manual de Auditoria do TCU, 2010.

Tabela 2.2 - Modelo de Matriz de Achados

Questão de auditoria (repetir a questão da matriz de planejamento).						
Achado					**Recomendações e determinações**	**Benefícios esperados**
Situação encontrada	**Critério**	**Evidências e análises**	**Causas**	**Efeitos**		
Constatações de maior relevância, identificadas na fase de execução.	Padrão usado para determinar se o objeto auditado atinge, excede ou está aquém do de-sempenho esperado.	Resultado da aplicação dos métodos de análise de dados e seu emprego na produção de evidências. De forma sucinta, devem ser indicadas as técnicas usadas para tratar as informações coletadas durante a execução e os resultados obtidos.	Podem ser relacionadas à operaciona-lização ou à concepção do objeto da auditoria, ou estar fora do controle ou da influência do gestor. A identificação de causas requer evidências e análises robustas. As deliberações conterão as medidas consideradas necessárias para sanear as causas do desempenho insuficiente.	Consequências relacionadas às causas e aos correspondentes achados. Pode ser uma medida da relevância do achado.	Devem ser elaboradas de forma a tratar a origem dos problemas diagnosticados. Sugere-se parcimônia na quantidade de deliberações e priorização para solução dos principais problemas.	Melhorias que se esperam alcançar com a implementação das reco- mendações e determinações. Os benefícios podem ser quantitativos e qualitativos. Sempre que possível, quantificá-los.

Fonte: Manual de Auditoria do TCU, 2010.

2.1.5. Execução da auditoria

Na fase de execução, terceiro estágio do ciclo, a equipe de auditoria realiza os trabalhos de campo e as pesquisas necessárias à coleta de dados, por meio de entrevistas, aplicação de questionários, observação direta, grupos focais, consultas a documentos e bases de dados. Após os trabalhos de campo, é elaborada a matriz de achados, síntese dos resultados obtidos.

2.1.6. Demais fases da auditoria

Os estágios quarto e quinto do ciclo tratam da elaboração do relatório preliminar; do seu encaminhamento ao gestor público, para comentários. O sexto estágio se dá quando da apreciação do relatório.

A etapa de divulgação do relatório, estágio sétimo do ciclo, tem a finalidade de ampliar o conhecimento dos atores externos sobre os resultados das ações avaliadas, contribuindo para aumentar a efetividade do controle, por meio da mobilização no acompanhamento e na apreciação dos objetivos, da implementação e, no caso de de uma auditoria operacional, dos resultados das políticas públicas.

Para aumentar a probabilidade de resolução dos problemas identificados durante a auditoria realiza-se o monitoramento, tratado no oitavo estágio do ciclo, mediante o acompanhamento de um "Plano de Ação", apresentado pelo gestor do órgão auditado, que formaliza as ações que serão tomadas para atender as deliberações.

2.2. Legislação – Segurança da Informação e Comunicações

Segundo SISP (BRASIL, 2017), as organizações públicas devem tomar como base os seguintes normativos a fim de subsidiar a Gestão de Segurança da Informação e Comunicações:

(a) do Departamento de Segurança da Informação e Comunicação;

(b) do Gabinete de Segurança Institucional da Presidência da República – GSI;

(c) o Decreto no 3.505, de 13 de junho de 2000, da Presidência da República, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, e

(d) a Instrução Normativa nº 01/DSIC/GSIPR, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na APF, direta e indireta.

O Decreto nº 3.505/2000 da Presidência da República também definiu que o Gabinete de Segurança Institucional – GSI – é o coordenador do Comitê Gestor da Segurança da Informação, que por sua vez assessora a Secretaria-Executiva do Conselho de Defesa Nacional na consecução das diretrizes da Política de SI na Administração Pública Federal, e avaliar e analisar os assuntos relativos à Segurança da Informação.

A competência do GSI para editar normas advém do Inciso VIII do Decreto nº 3.505/2000:

> *VIII - estabelecer normas, padrões, níveis, tipos e demais aspectos relacionados ao emprego dos produtos que* incorporem *recursos criptográficos, de modo a assegurar a confidencialidade, a autenticidade, a integridade e o não-repúdio, assim como a interoperabilidade entre os Sistemas de Segurança da Informação.*

Conforme disposto no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional, compete ao Departamento de Segurança da Informação e Comunicações – DSIC, estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

O arcabouço normativo de Segurança da Informação e Comunicações (SIC) do GSI abrange 3 instruções normativas (IN):

(a) Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a Gestão de SIC na Administração Pública Federal;

(b) Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013, que dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal;

(c) Instrução Normativa GSI/PR nº 3, de 06 de março de 2013, que dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.

A Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 aprovou as orientações para gestão de SI que deverão ser implementadas pelas organizações públicas, e definiu competências para o Gabinete de Segurança Institucional da Presidência da República - GSI, por intermédio do Departamento de Segurança da Informação e Comunicações, entre elas:

(a) planejar e coordenar as atividades de SI e comunicações na Administração Pública Federal, direta e indireta;

(b) estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta;

(c) operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da Administração Pública Federal, direta e indireta, denominado CTIR.GOV;

(d) elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos em SI; e

(e) orientar a condução da Política de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

A IN nº 01/2008 estabeleceu várias competências às organizações públicas, com destaque para: (1) nomeação do Gestor de Segurança da Informação e Comunicações; (2) instituição e implementação da equipe de tratamento e resposta a incidentes em redes computacionais; (3) instituição do Comitê de Segurança da Informação e Comunicações; (4) aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações; e (5) remessa dos resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações para o GSI.

Além dessas 3 instruções normativas, o GSI editou:

(a) 21 normas complementares à IN nº 01 GSI/PR/2008, que estão detalhadas a seguir neste trabalho; e

(b) uma norma complementar à IN nº 02 GSI/PR/2013, que disciplina o Credenciamento de Segurança de Pessoas Naturais, Órgãos e Entidades Públicas e Privadas para o Tratamento de Informações Classificadas.

Além desses normativos, Vieira (2014) compilou a legislação específica de Segurança da Informação, com o foco de subsidiar o trabalho de operadores, técnicos e juristas da área de

segurança da informação. Tal legislação, pela sua abrangência, está fora do escopo deste trabalho.

2.3. Visão geral das normas da família NBR ISO/IEC 27000 – Segurança da Informação

A NBR ISO/IEC 27000 também conhecida como família de normas ISO 27000 é uma série de padrões relacionados à temática de Segurança da Informação. A série oferece melhores práticas e recomendações sobre a gestão da informação, riscos e controles dentro do contexto de uma estratégia global do Sistema de Gestão de Segurança da Informação – SGSI.

Segundo PIRES (2016), a série possui deliberadamente um escopo amplo, que abrange mais do que apenas a autenticidade, confidencialidade, disponibilidade ou questões de segurança técnica. É aplicável a organizações de todos os tamanhos e feitios. Todas as organizações são incentivadas a avaliar os seus riscos de segurança da informação, em seguida, implementar controles de segurança apropriados de acordo com as suas necessidades, usando orientações e sugestões quando aplicado.

Existem diversas normas nas séries da ISO/IEC 27000 (Apêndice 4), e cada uma com um objetivo específico. As normas podem ser adotadas independente do porte ou tipo da organização pública ou privada, e suas diretrizes buscam fazer com que as informações da organização e os sistemas sejam seguros.

Histórico das normas (BASTOS, 2009, pág. 19/20)

- 1988: Primeira versão da BS 7799 parte 2 (BS 7799-2:1998 – Sistema de Gestão da Segurança da Informação – Especificações e guia para uso);
- 1999: revisão da BS 7799 parte 1 (BS 7799-1:1999 – Tecnologia da Informação – Código de prática para gestão da segurança da Informação);
- 2000: primeira versão da norma ISO/IEC 17799 (ISO/IEC 17799:2000) – Tecnologia da Informação – Código de prática para gestão da segurança da informação também referenciada como BS ISO/IEC 17799:2000), a evolução da norma BS7799-1: 1999 transformada em norma ISO;
- 2001: primeira versão da norma no Brasil pela ABNT, NBR ISO/IEC 17799 (NBR ISO/IEC 17799:2001 – Tecnologia da Informação – Código de prática para gestão da segurança da informação);

- 2002: revisão da norma BS 7799 parte 2 (BS 7799-2: 2002 – Sistema de Gestão da Segurança da Informação – Especificações e guia para uso);
- 2005: segunda versão da norma ISO 27001 (ISO/IEC 27001:2005 – Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão da Segurança da Informação – Requisitos), que é a evolução da BS 7799-2:2002 para norma ISO;
- 2006: primeira versão da norma no Brasil pela ABNT, NBR ISO/IEC 27001 (NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão da Segurança da Informação – Requisitos);
- 2008: lançamento da norma ISO/IEC 27005 – Sistema de Gestão de Segurança da Informação – Gestão de Riscos, publicada em 07/07/2008 pela ABNT.

A tabela a seguir traz as normas iniciais da família 2700. No Apêndice 4 encontra-se a tabela com todas as 47 normas da família.

Tabela 2.3 – Normas da família NBR ISO/IEC 27000

Norma	Objetivo
NBR ISO/IEC 27000:2009	Sistema de Gerenciamento de Segurança - objetivos e vocabulários.
NBR ISO/IEC 27001:2013	Sistema de Gestão de Segurança da Informação – Requisitos.
NBR ISO/IEC 27002:2013	Boas Práticas para controles de Segurança da Informação.
NBR ISO/IEC 27003:2011	Guia de implantação do Sistema de Gestão de Segurança da Informação
NBR ISO/IEC 27004:2010	Gestão da Segurança da Informação – Medição.
NBR ISO/IEC 27005: 2011	Gestão de Risco em Segurança da Informação.
ISO/IEC 27006 (inglês)	Requisitos para empresas de auditoria e certificação de Sistemas de Gestão de Segurança da Informação.
NBR ISO/IEC 27007:2012	Diretrizes para auditoria em Sistemas de Gestão de Segurança da Informação.
NBR ISO/IEC 27008:2012	Diretrizes para auditores sobre controle de Segurança da Informação.
ISO/IEC 27009 (inglês)	Norma apoia a indústrias específicas que pretendem trabalhar orientadas às normasda família ISO/IEC 27000.
ISO/IEC 27010 (inglês)	Gestão de segurança da informação para comunicação intersetorial e interorganizacional.
NBR ISO/IEC 27011:2009	Diretrizes para gestão de segurança da informação em organizações de telecomunicação com base na NBR ISO/IEC 27002.
ISO/IEC 27013 (inglês)	Diretrizes para a implementação integrada da ISO/IEC 27001 e ISO/IEC 20000-1.
NBR ISO/IEC 27014:2013	Governança de Segurança da Informação.

Fonte: Bastos, 2009.

2.4. Visão Geral da NBR ISO/IEC 27002:2013 – Segurança da Informação e Comunicações

Esta Norma foi elaborada para as organizações usarem como uma referência na seleção de controles dentro do processo de implementação de um sistema de gestão da segurança da

informação, baseado nos controles da ABNT NBR ISO/IEC 27001 ou como um documento de orientação para as organizações implementarem controles de segurança da informação comumente aceitos (NBR ISO/IEC 27002:2013, pág. 10).

A norma NBR ISO/IEC 27002:2013 fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, consideração os ambientes de risco da segurança da informação da organização.

Esta norma auxilia às organizações que desejam:

a) selecionar controles dentro do processo de implementação de um sistema de gestão da segurança da informação baseado na ABNT NBR ISO/IEC 27001;
b) implementar controles de segurança da informação comumente aceitos;
c) desenvolver seus próprios princípios de gestão da segurança da informação.

A norma está estruturada em 14 seções de controles de segurança da informação (veja tabela 2.4) de um total de 35 objetivos de controles e 114 controles (Apêndice 1).

Cada seção contém um ou mais objetivos de controle e os controles de segurança da informação relacionados. A norma recomenda que cada organização escolha seus controles conforme sua aplicabilidade e regras/processos individuais de negócios da organização. Destaca-se que não existe uma ordem de prioridade entre as seções ou controles.

Estrutura de cada seção principal contém: (a) um objetivo de controle declarando o que se espera que seja alcançado; (b) um ou mais controles que podem ser aplicados para se alcançar o objetivo do controle.

As descrições do controle estão estruturadas da seguinte forma:

a) Controle – define a declaração específica do controle, para atender ao objetivo de controle.
b) Diretrizes para implementação – apresenta informações mais detalhadas para apoiar a implementação do controle e alcançar o objetivo do controle. As diretrizes podem não ser totalmente adequadas ou suficientes em todas as situações e podem, portanto, não atender completamente aos requisitos de controle específicos da organização.
c) Informações adicionais – apresenta mais dados que podem ser considerados, como por exemplo, questões legais e referências normativas. Se não existirem informações adicionais, esta parte não é mostrada no controle.

Segundo Kosutic (2017), existe uma equivalência entre o anexo A da norma ABNT NBR/ISO 27001 e os controles da norma NBR ISO/IEC 27002:2013. O anexo A não esclarece como cada controle pode ser implementado. O propósito da NBR ISO/IEC 27002:2013 – que possui exatamente a mesma estrutura do anexo A da norma NBR ISO/IEC 27001 – é detalhar como cada controle do Anexo A pode ser implemento. Os 114 controles da norma NBR ISO/IEC 27002:2013 estão descritos no Apêndice 1.

Tabela 2.4 – Seções da Norma NBR ISO/IEC 27002:2013

Nº da Seção	Título da Seção	Objetivo
5	Políticas de segurança da informação	Controles sobre como as políticas são escritas e revisadas.
6	Organização da segurança da informação	Controles sobre como as responsabilidades são designadas; também inclui os controles para dispositivos móveis e trabalho remoto.
7	Segurança em recursos humanos	Controles para antes da contratação, durante e após a contratação.
8	Gestão de ativos	Controles relacionados ao inventário de ativos e uso aceitável, e também para a classificação de informação e manuseio de mídias.
9	Controle de acesso	Controles para a política de controle de acesso, gestão de acesso de usuários, controle de acesso a sistemas e aplicações, e responsabilidades dos usuários.
10	Criptografia	Controles relacionados a gestão de chaves criptográficas.
11	Segurança física e do ambiente	Controles definindo áreas seguras, controles de entrada, proteção contra ameaças, segurança de equipamentos, descarte seguro, política de mesa limpa e tela limpa, etc.
12	Segurança nas operações	Vários controles relacionados a gestão da produção de TI: gestão de mudança, gestão de capacidade, software malicioso, cópia de segurança, registro de eventos, monitoramento, instalação, vulnerabilidades, etc.
13	Segurança nas comunicações	Controles relacionados a segurança em rede, segregação, serviços de rede, transferência de informação, mensageiria, etc.
14	Aquisição, desenvolvimento e manutenção de sistemas	Controles definindo requisitos de segurança e segurança em processos de desenvolvimento e suporte.
15	Relacionamento na cadeia de suprimento	Controles sobre o que incluir em acordos e como monitorar os fornecedores.
16	Gestão de incidentes de segurança da informação	Controles para reportar eventos e fraquezas, definindo responsabilidades, procedimentos de resposta e coleta de evidências.
17	Aspectos da segurança da informação na gestão da continuidade do negócio	Controles requisitando o planejamento da continuidade do negócio, procedimentos, verificação e revisão e redundância da TI.
18	Conformidade	Controles requisitando a identificação de leis e regulamentações aplicáveis, proteção da propriedade intelectual, proteção de dados pessoais e revisões da segurança da informação.

Fonte: Kosutic (2017)

2.5. Normas Complementares à IN nº 01 GSI/PR/2008

Neste tópico será apresentado uma visão geral das normas complementares (NC) à IN Nº 01 GSI/PR/2008, destacando as principais diretrizes, orientações e recomendações. A seguir, a tabela com os objetivos das Normas complementares à IN nº 01 GSI/PR/2008.

Tabela 2.5 – Normas complementares à IN GSI/PR nº 1, de 13.06.2008

Nº da Norma Complementar	OBJETIVO
01	Estabelecer 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.
02	Definir a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta.
03	Estabelecer diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (POSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta.
04	Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal.
05	Disciplinar 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.
06	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.
07	Estabelecer as diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
08	Disciplinar 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.
09	Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta.
10	Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta.
11	Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta.
12	Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
13	Estabelece diretrizes para a Gestão de mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF).
14	Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
15	Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes

Tabela 2.5 – Normas complementares à IN GSI/PR nº 1, de 13.06.2008

Nº da Norma Complementar	OBJETIVO
	sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
16	Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta.
17	Estabelece diretrizes nos contextos de atuação e adequações para profissionais da área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).
18	Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).
19	Estabelece padrões mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta.
20	Estabelece as diretrizes de Segurança da Informação e Comunicações para Instituição do processo de tratamento da informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
21	Estabelecer as diretrizes para o registro de eventos, coleta e preservação de evidências de incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

2.5.1. NC 01 e 02 - Metodologia de Gestão de Segurança da Informação

A Norma Complementar nº 01/IN01/DSIC/GSIPR 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. A NC nº 01 é responsável por orientar na elaboração das outras normas complementares, quanto à apresentação, conteúdo e estrutura do texto.

Segundo a Norma Complementar nº 02/IN01/DSIC/GSIPR (item 3.1), a metodologia proposta de gestão de segurança da informação e comunicações para a administração pública baseia-se no processo de melhoria contínua, denominado ciclo "PDCA" (*"Plan-Do-Check-Act"*), referenciado pela norma ABNT NBR ISO/IEC 27001:2006.

Essa metodologia enfatiza o papel do Gestor de Segurança da Informação no planejamento das ações de segurança da informação, pela abordagem da gestão de riscos.

Destaca-se que as ações de segurança da informação e comunicações da organização selecionadas devem ser consideradas para o tratamento de riscos. Além de outras ações que a organização considere necessárias, a NC 02 cita como exemplos de ações de segurança da informação e comunicações:

(a) Política de Segurança da Informação e Comunicações;

(b) Infraestrutura de Segurança da Informação e Comunicações;

(c) Tratamento Da Informação;

(d) Segurança em Recursos Humanos;

(e) Segurança Física;

(f) Segurança Lógica;

(g) Controle de Acesso;

(h) Segurança de Sistemas;

(i) Tratamento de Incidentes;

(j) Gestão de Continuidade;

(k) Conformidade; e

(l) Auditoria Interna.

A NC nº 02/IN01/DSIC/GSIPR recomenda também que a organização realize auditoria interna, ao qual a norma também denomina como auditoria de primeira parte, das ações de segurança da informação e comunicações a intervalos planejados de pelo menos uma vez ao ano.

2.5.2. NC 03 - Política de Segurança da Informação

O Decreto nº 3.505, de 13 de junho de 2000, instituiu a Política de Segurança da Informação no âmbito dos órgãos e entidades da Administração Pública Federal. A Norma Complementar nº 03/IN01/DSIC/GSIPR detalha como deve ser elaborada uma PSI ou POSIC.

2.5.2.1. Principais diretrizes e recomendações da NC 03

A Política de Segurança da Informação e Comunicações declara o comprometimento da alta direção organizacional com vistas a prover diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a gestão de segurança da informação e comunicações nos órgãos ou entidades da Administração Pública Federal, direta e indireta.

As diretrizes constantes na Política de Segurança da Informação e Comunicações no âmbito do órgão ou entidade visam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

Recomenda-se que na elaboração da POSIC sejam incluídos os seguintes itens: escopo; conceitos e definições; referências legais e normativas; princípio; diretrizes gerais; e penalidades.

Nas diretrizes gerais da POSIC, recomenda-se estabelecer diretrizes sobre, no mínimo, os seguintes temas, considerando as normas específicas vigentes no ordenamento jurídico:

tratamento da informação; tratamento de incidentes de rede; gestão de risco; gestão de continuidade; auditoria e conformidade; controles de acesso; uso de e-mail; acesso à internet; e. penalidades.

A NC nº 03 recomenda os seguintes procedimentos:

(a) definir a estrutura para a Gestão da Segurança da Informação e Comunicações;

(b) instituir o Gestor de Segurança da Informação e Comunicações do órgão ou entidade;

(c) instituir o Comitê de Segurança da Informação e Comunicações do órgão ou entidade;

(d) instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do órgão ou entidade.

Todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 03(três) anos.

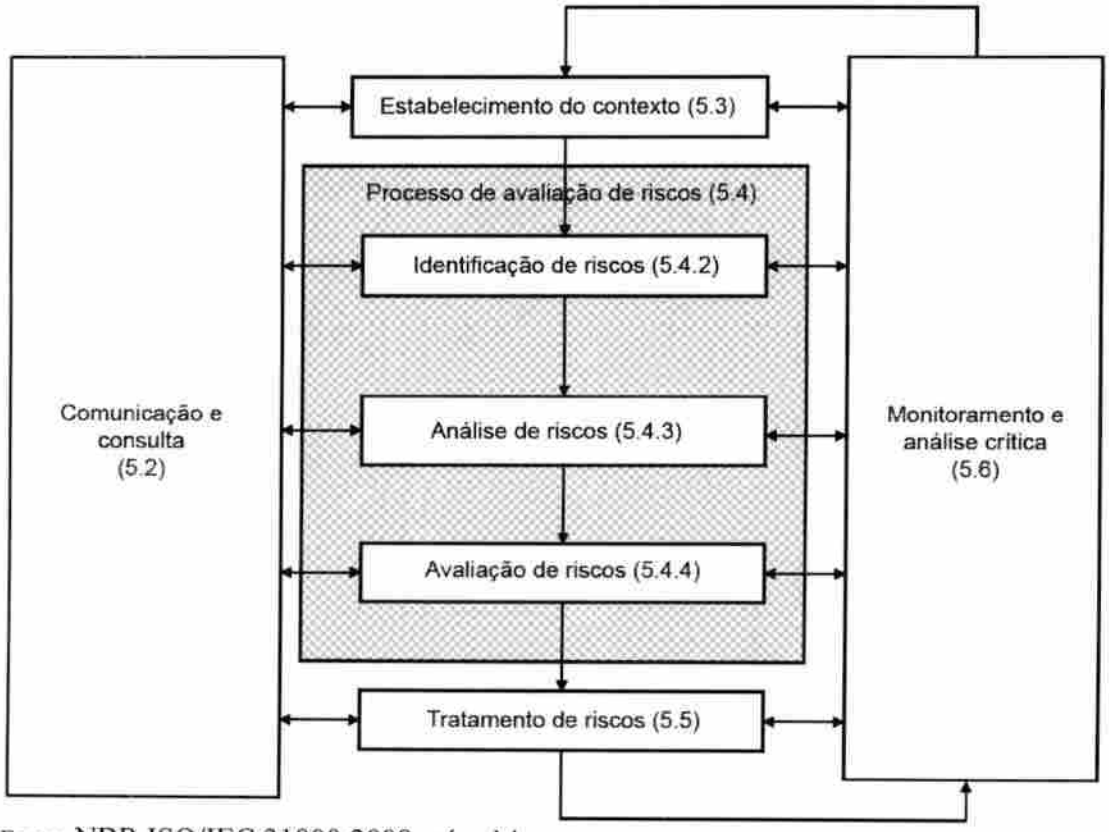
2.5.3. NC 04 - Gestão de Riscos de Segurança da Informação

A NC nº 04/IN01/DSIC/GSIPR, e seu anexo, revisão 01, tem como objetivo estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal - APF, direta e indireta.

A implantação do processo de Gestão de Riscos de Segurança da Informação e Comunicações busca identificar as necessidades da organização em relação aos requisitos de segurança da informação e comunicações, bem como, criar um Sistema de Gestão de Segurança da Informação (SGSI) eficaz.

A NC 04 define "Gestão de Riscos de Segurança da Informação e Comunicações" como o conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos. A figura a seguir resume o conjunto de processos de uma Gestão de Riscos de Segurança da Informação e Comunicações.

Figura 2.1 – Processo de Gestão de Riscos



Fonte: NBR ISO/IEC 31000:2009, pág. 14.

2.5.4. NC 05, 08 e 21 - Incidentes de Segurança em Redes Computacionais

O processo de Gestão da Segurança da Informação e Comunicações abrange as atividades de tratamento e resposta aos incidentes, gerenciamento de incidentes, registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes computacionais, o qual inclui a identificação das causas e o tratamento dos incidentes.

O GSI publicou 3 normas complementares que tratam desses temas, NC´s nº 05, 08 e 21/IN01/DSIC/GSIPR. A seguir, os pontos mais relevantes para a realização deste trabalho de pesquisa.

2.5.4.1. NC 05 - Equipe de Tratamento e Resposta e gerenciamento de Incidentes de Segurança em Redes de Computadores

Considerando a estratégia de segurança da informação composta por várias camadas, uma delas, que vem sendo adotada por diversas instituições, é a criação de Equipes de

Tratamento e Resposta a Incidentes em Redes Computacionais, mundialmente conhecido como CSIRT® (do inglês "*Computer Security Incident Response Team*").

É condição necessária para a criação de uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, que o órgão ou entidade possua a competência formal e respectiva atribuição de administrar a infraestrutura da rede de computadores de sua organização.

A NC 05/IN01/DSIC/GSIPR define "Incidente de segurança" como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores. Define ainda "Tratamento de Incidentes de Segurança em Redes Computacionais" como o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

A NC 05/IN01/DSIC/GSIPR sugere quatro modelos de implementação de ETIR para escolha do órgão ou entidade, devendo fazer sua escolha no modelo que melhor se adequar às suas necessidades e limitações.

Tabela 2.6 – Modelos de implementação de ETIR

Modelo	Definição
Modelo 1 – Utilizando a equipe de tecnologia da informação	A equipe que utilizar este modelo desempenhará suas atividades, via de regra, de forma reativa, sendo desejável, porém que o Agente Responsável pela ETIR atribua responsabilidades para que os seus membros exerçam atividades proativas. Os órgãos ou entidades que inicialmente optarem pela implantação do Modelo 1 deverão, assim que possível, migrar para um dos outros modelos.
Modelo 2 – Centralizado	A equipe composta por pessoal com dedicação exclusiva às atividades de tratamento e resposta aos incidentes em redes computacionais.
Modelo 3 – Descentralizado	A equipe será composta por colaboradores distribuídos por diversos locais dentro da organização, dispersos por uma região ou pelo país inteiro. Essas equipes devem possuir pessoal próprio dedicado às atividades de tratamento e resposta aos incidentes de rede computacionais, podendo atuar operacionalmente de forma independente, porém alinhadas com as diretrizes estabelecidas pela coordenação central.
Modelo 4 – Combinado ou Misto	Trata-se da junção dos modelos descentralizado e centralizado.

2.5.4.2. NC 08 - Gerenciamento de Incidentes de Segurança em Redes de Computadores

Segundo a NC nº 08/IN01/DSIC/GSIPR, o gerenciamento de incidentes de segurança em redes de computadores requer especial atenção da alta administração das organizações públicas. A troca de informações sobre o gerenciamento de incidentes de segurança em redes de computadores entre as ETIR e a Coordenação Geral de Tratamento de Incidentes de Segurança em Redes de Computadores - CGTIR traz as seguintes vantagens:

- promover o intercâmbio científico-tecnológico relacionado a incidentes de segurança em redes de computadores;
- apoiar órgãos e entidades da APF nas atividades de gerenciamento e tratamento de incidentes de segurança em redes de computadores, quando necessário;
- monitorar e analisar tecnicamente os incidentes de segurança em redes de computadores da APF, permitindo a criação de métricas e/ou alertas;
- implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança em redes de computadores da APF;
- apoiar, incentivar e contribuir, no âmbito da APF, para a capacitação no tratamento de incidentes de segurança em redes de computadores.

A NC 08 orienta que a ETIR comunique a ocorrência de incidentes de segurança em redes de computadores ao Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR Gov, conforme procedimentos definidos pelo próprio CTIR Gov, com vistas a permitir que sejam dadas soluções integradas para a administração pública, e para a geração de estatísticas.

O CTIR Gov é o Centro de Tratamento de Incidentes de Redes do Governo e está subordinado ao Departamento de Segurança de Informação e Comunicações - DSIC - do Gabinete de Segurança Institucional da Presidência da República - GSI/PR. Sua finalidade é o atendimento aos incidentes em redes do governo, nos domínios gov.br, jus.br, leg.br, mil.br, mp.br e def.br (CTIR, BRASIL, 2017).

Além do serviço de tratamento de incidentes de segurança em redes de computadores, a ETIR poderá oferecer à sua comunidade um ou mais dos serviços listados a seguir, sem prejuízo de outros requisitados, desde que em consonância com normas e legislações referentes ao gerenciamento de incidentes de segurança em redes de computadores:

- tratamento de artefatos maliciosos;
- tratamento de vulnerabilidades;
- emissão de alertas e advertências;
- anúncios;
- prospecção ou monitoração de novas tecnologias;
- avaliação de segurança;
- desenvolvimento de ferramentas de segurança;
- detecção de intrusão;
- disseminação de informações relacionadas à segurança.

Ainda segundo a NC nº 08/IN01/DSIC/GSIPR, toda ETIR deve observar e adotar, no mínimo, os seguintes aspectos e procedimentos:

(1) Registro de incidentes de segurança em redes de computadores: todos os incidentes notificados ou detectados devem ser registrados, com a finalidade de assegurar registro histórico das atividades da ETIR;

(2) Tratamento da informação: o tratamento da informação pela ETIR deve ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo;

(3) Havendo indícios de ilícitos criminais, as ETIR têm como dever, sem prejuízo do disposto no item 6 desta Norma Complementar e do item 10.6 da Norma Complementar nº 05/IN01/DSIC/GSIPR:

- acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários;
- observar os procedimentos para preservação das evidências exigindo consulta às orientações sobre cadeia de custódia, conforme ato normativo específico a ser expedido;
- priorizar a continuidade dos serviços da ETIR e da missão institucional da organização.

2.5.4.3. NC 21 - Preservação de evidências de incidentes de Segurança em Redes

Segundo a NC nº 21/IN01/DSIC/GSIPR, "coleta de evidências de segurança em redes de computadores" é o processo de obtenção de itens físicos que contém uma potencial evidência, mediante a utilização de metodologia e ferramentas adequadas. Este processo inclui a geração das cópias das mídias, ou coleção de dados que contenham evidências do incidente.

Ainda segundo a NC nº 21/IN01/DSIC/GSIPR, "preservação de evidência de incidentes em redes computacionais" é o processo que compreende a salvaguarda das evidências e dos dispositivos, de modo a garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações.

A NC nº 21/IN01/DSIC/GSIPR define quais são os "Requisitos para adequação dos ativos de informação", os "Procedimentos para coleta e preservação das evidências", os procedimentos para "Comunicação às autoridades competentes", e as "Responsabilidades" relacionadas na preservação de evidências de incidentes.

Ainda segundo a norma, "ativos de Informação" são os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

Das orientações e recomendações destacam-se os seguintes:

(1) requisitos para adequação dos ativos de informação:

a) o horário dos ativos de informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a "Hora Legal Brasileira (HLB)", de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

b) os registros dos eventos previstos no item anterior devem incluir as seguintes informações: a) Identificação inequívoca do usuário que acessou o recurso; b) Natureza do evento, como por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha, etc; c) Data, hora e fuso horário, observando o previsto no item 6.1; e d) Endereço IP (Internet Protocol), identificador do ativo

de informação, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

c) os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (Logs) em formato que permita a completa identificação dos fluxos de dados.

(2) procedimentos para coleta e preservação das evidências:

a) coleta e preservação das mídias de armazenamento dos dispositivos afetados, e de todos os registros de eventos.

b) quando não for possível preservar as mídias, deve-se coletar e armazenar cópia dos arquivos afetados pelo incidente, tais como: Logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original, bem como os metadados desses arquivos, como data, hora de criação e permissões.

c) para a preservação dos arquivos coletados, deve-se gerar um arquivo contendo a lista dos resumos criptográficos de todos os arquivos coletados, acompanhado do arquivo com a lista dos resumos criptográficos e com o resumo criptográfico do arquivo.

(3) após a conclusão do processo de coleta e preservação das evidências do incidente, a NC nº 21 orienta que o responsável pela ETIR deverá elaborar "Relatório de Comunicação de Incidente de Segurança em Redes Computacionais", descrevendo detalhadamente todos eventos verificados.

2.5.5. NC 06 - Gestão de Continuidade de Negócios

A implantação do processo de Gestão de Continuidade de Negócios busca minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou entidade, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

A NC 06/IN01/DSIC/GSIPR define "Gestão da Continuidade" como o processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de

responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado.

A Gestão de continuidade de negócios pode envolver ações mais abrangentes do que as definidas no âmbito da Gestão de Segurança da Informação e Comunicações, especialmente devido aos requisitos estratégicos de continuidade relativos às pessoas, à infraestrutura, aos processos e às atividades operacionais.

A NC 06/IN01/DSIC/GSIPR ainda recomenda que o "Programa de Gestão de Continuidade de Negócios" de uma organização pública seja composto, no mínimo, pelos Planos de Gerenciamento de Incidentes - PGI; de Continuidade de Negócios – PCN; de Recuperação de Negócios - PRN, de acordo com as suas necessidades específicas, de forma a assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas.

Recomenda-se ainda que cada plano seja revisado anualmente e que os contratos firmados com empresas terceirizadas que suportem atividades críticas contenham cláusula segundo a qual as referidas empresas possuam Planos de Continuidade dos seus Negócio.

2.5.6. NC 07 - Controles de Acesso Relativos à Segurança da Informação

Segundo a NC 07, o objetivo do controle é sistematizar a concessão de acesso, a fim de evitar a quebra de segurança da informação e comunicações. A identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para concessão de acesso nos órgãos ou entidades da APF. A identificação dos controles de acesso lógico e físico, nos órgãos ou entidade da APF, é consequência do processo de Gestão de Riscos de Segurança da Informação e Comunicações. A implementação dos controles de acesso está condicionada à prévia aprovação pela autoridade responsável pelo órgão ou entidade da APF.

Para implementar os controles de acesso aprovados é fundamental a elaboração e divulgação de normas, bem como programas periódicos de sensibilização e conscientização em conformidade com a Política de Segurança da Informação e Comunicações dos órgãos ou entidades da APF.

Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras específicas para credenciamento de acesso de usuários aos ativos de informação em conformidade com a legislação vigente, e em especial quanto ao acesso às informações em áreas e instalações consideradas críticas.

2.5.6.1. Diretrizes da NC 07

A NC nº 07/IN01/DSIC/GSIPR traz 43 diretrizes para os controles de acesso lógico categorizadas como:

a) quanto à criação e administração de contas de acesso;
b) quanto à rede corporativa de computadores;
c) quanto aos ativos de informação;
d) quanto às áreas e instalações físicas
e) quanto aos usuários;
f) quanto aos ativos de informação; e
g) quanto ao perímetro de segurança.

Das 43 diretrizes da NC nº 07/IN01/DSIC/GSIPR destacam-se as seguintes:

1. responsabilizar o usuário pela quebra de segurança ocorrida com a utilização de sua respectiva conta de acesso, mediante assinatura de Termo de Responsabilidade.
2. a criação de contas de serviço exige regras específicas vinculadas a um processo automatizado.
3. recomenda-se a utilização de autenticação de multifatores para o controle de acesso lógico, a fim de autenticar a identidade de um usuário e vinculá-lo a uma conta de acesso a ativos de informação. Autenticação de multifatores: utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema.
4. excluir credenciais de acesso à rede corporativa de computadores quando do desligamento do usuário.
5. registrar os acessos à rede corporativa de computadores de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido em cada órgão ou entidade da APF.
6. utilizar mecanismos automáticos para inibir que equipamentos externos se conectem na rede corporativa de computadores.
7. manter, na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados.
8. utilizar a legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro.

9. os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para o uso da internet, do correio eletrônico, sem fio e de mensagens instantâneas.
10. os órgãos ou entidades da APF estabelecem regras para o uso de credenciais físicas, que se destinam ao controle de acesso dos usuários às áreas e instalações sob suas responsabilidades;
11. os órgãos ou entidades da APF definem a necessidade e orientam a instalação de sistemas de detecção de intrusos nas áreas e instalações sob suas responsabilidades;
12. classificar as áreas e instalações como ativos de informação de acordo com o valor, a criticidade, o tipo de ativo de informação e o grau de sigilo das informações que podem ser tratadas em tais áreas e instalações, mapeando aquelas áreas e instalações consideradas críticas;
13. os órgãos ou entidades da APF orientam o uso de barreiras físicas de segurança, bem como equipamentos ou mecanismos de controle de entrada e saída;
14. proteger os ativos de informação contra ações de vandalismo, sabotagem, ataques, especialmente em relação àqueles considerados críticos.
15. implementar área de recepção com regras claras para a entrada e saída de pessoas, equipamentos e materiais;
16. intensificar os controles para as áreas e instalações consideradas críticas em conformidade com a legislação vigente.
17. conscientizar o usuário para adotar comportamento favorável à disponibilidade, à integridade, à confidencialidade e à autenticidade das informações.
18. identificar e avaliar sistematicamente os riscos à segurança da informação e comunicações dos ativos de informação e quais controles devem ser aplicados quanto aos acessos dos usuários;
19. estabelecer formulário específico de Termo de Responsabilidade a ser difundido e assinado individualmente pelos usuários;
20. estabelecer distância mínima de segurança para manutenção das mídias contendo as cópias de segurança (backups);
21. classificar os ativos de informação em níveis de criticidade, considerando o tipo de ativo de informação, o provável impacto no caso de quebra de segurança, tomando

como base a gestão de risco e a gestão de continuidade de negócios relativa aos aspectos da segurança da informação e comunicações da APF,

22. os ativos de informação classificados como sigilosos requerem procedimentos especiais de controles de acesso físico em conformidade com a legislação vigente.
23. definir perímetros de segurança, suas dimensões, equipamentos e tipos especiais de controles de acesso aos ativos de informação;
24. regulamentar, por intermédio de normas específicas de cada órgão ou entidade da APF, o armazenamento, a veiculação de imagem, vídeo ou áudio, registrados em perímetros de segurança.

2.5.7. NC 09 - Recursos criptográficos em Segurança da Informação e Comunicações

A NC nº 09/IN01/DSIC/GSIPR, (Revisão 02) orienta os procedimentos para utilização de recursos criptográficos pela administração pública.

Algoritmo de Estado é definido na NC nº 09 como a função matemática utilizada na cifração e na decifração de informações sigilosas, necessariamente as informações classificadas, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, não comercializável.

Destacam-se as seguintes diretrizes e recomendações da NC nº 09/IN01/DSIC/GSIPR para o uso de "Algoritmo de Estado":

(a) toda a informação classificada, em qualquer grau de sigilo, produzida, armazenada ou transmitida, em parte ou totalmente, por qualquer meio eletrônico, deverá obrigatoriamente ser protegida com recurso criptográfico baseado em algoritmo de Estado;

(b) a cifração e decifração de informações classificadas, em qualquer grau de sigilo, utilizará exclusivamente recurso criptográfico baseado em algoritmo de Estado em conformidade com os parâmetros e padrões mínimos estabelecidos nesta norma;

(c) o canal de comunicação seguro (Rede Privada Virtual - VPN) que interligue redes dos órgãos e entidades da APF, direta e indireta, objetivando a troca de informações classificadas, deve utilizar recurso criptográfico baseado em algoritmo de Estado;

(d) a utilização de recurso criptográfico, baseado em algoritmo de Estado, para cifração e decifração das informações não classificadas é opcional;

(e) o credenciamento de estrangeiros para uso de recurso criptográfico baseado em algoritmo de Estado deve ser submetido ao GSI/PR;

(f) o GSI/PR é o órgão responsável pelo apoio técnico no tocante a atividades de caráter científico e tecnológico relacionadas ao recurso criptográfico baseado em algoritmo de Estado;

(g) o recurso criptográfico, baseado em algoritmo de Estado, deverá ser de desenvolvimento próprio ou por órgãos e entidades da APF, direta ou indireta, mediante acordo ou termo de cooperação, vedada a participação e contratação de empresas e profissionais externos à APF, para tal finalidade.

Segundo a NC nº 09/IN01/DSIC/GSIPR, (Revisão 02), "Algoritmo Registrado" é a função matemática utilizada na cifração e na decifração de informações não classificadas, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, cujo código fonte e método de processo sejam passíveis de controle e auditoria;

Destacam-se as seguintes diretrizes e recomendações da NC nº 09/IN01/DSIC/GSIPR para o uso de "Algoritmo Registrado":

(a) a cifração e decifração das informações sigilosas não classificadas deve utilizar recurso criptográfico, no mínimo, baseado em algoritmo registrado;

(b) o órgão deverá manter sob sua guarda o código fonte e método de processos do algoritmo, bem como implementar os controles adequados, inclusive quanto à auditoria.

2.5.8. NC 10 - Inventário e Mapeamento de Ativos de Informação

Segundo a NC nº 10/IN01/DSIC/GSIPR, o processo de Inventário e Mapeamento de Ativos de Informação tem como objetivo prover o órgão ou entidade da APF de um entendimento comum, consistente e inequívoco de seus ativos de informação; da identificação clara de seus responsáveis - proprietários e custodiantes; de um conjunto completo de informações básicas sobre os requisitos de segurança da informação e comunicações de cada ativo de informação; de uma descrição do contêiner de cada ativo de informação; e da identificação do valor que o ativo de informação representa para o negócio do órgão ou entidade da APF;

Ainda segundo a norma, o processo de "Inventário e Mapeamento de Ativos de Informação" deve produzir subsídios tanto para a Gestão de Segurança da Informação e

Comunicações, como para a Gestão de Riscos de Segurança da Informação e Comunicações, e para a Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações das organizações públicas, quanto para os procedimentos de avaliação da conformidade, de melhorias contínuas, auditoria e, principalmente, de estruturação e geração de base de dados sobre os ativos de informação;

A NC nº 10/IN01/DSIC/GSIPR apresenta uma abordagem sistemática com 3 processos para o "Inventário e Mapeamento de Ativos de Informação". São eles:

(1) identificação e classificação de ativos de informação;

(2) identificação de potenciais ameaças e vulnerabilidades (NC nº 04 DSIC/GSIPR) e

(3) avaliação de riscos (Guia de Referência para a Segurança das Infraestruturas Críticas da Informação – GSI, 2010).

O processo 1 é composto das seguintes fases: (1) coleta de informações gerais dos ativos de informação; (2) detalhamento dos ativos de informação; (3) identificação dos responsáveis, proprietários e custodiantes de cada ativo de informação; (4) caracterização dos contêineres dos ativos de informação; (5) definição dos requisitos de segurança da informação e comunicações dos ativos de informação; e (6) estabelecimento do valor do ativo de informação.

2.5.9. NC 11 - Avaliação de conformidade nos aspectos relativos à Segurança da Informação

A NC nº 11/IN01/DSIC/GSIPR define as diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações. Segundo a ABNT NBR ISO/IEC 17000:2005, "avaliação de conformidade" é a demonstração de que os requisitos especificados relativos a um produto, processo, sistema, pessoa ou organismo são atendidos.

Destaca-se as seguintes diretrizes:

(1) a avaliação de conformidade em SIC deve ser contínua e aplicada visando contribuir com a Gestão de Segurança da Informação e Comunicações das organizações públicas;

(2) a avaliação de conformidade em SIC deve subsidiada por meio da análise e avaliação de riscos e auditorias internas previsto no item 3.3.5 da NC 02/IN01/GSIPR/DSIC;

(3) as não-conformidades relativas ao descumprimento de legislações, normas e procedimentos são consideradas riscos de SIC e devem ser tratadas segundo a NC 04/IN01/GSIPR/DSIC;

(4) os responsáveis pela avaliação de conformidade devem ser capacitadas nas legislações vigentes referentes à segurança da informação e comunicações; e

(5) a avaliação de conformidade de SIC tomará, no mínimo, como base no inventário e mapeamento de ativos de informação da organização, visando manter a disponibilidade, integridade, confidencialidade e autenticidade das informações.

2.5.10. NC 12 - Uso de dispositivos móveis

Para fins de utilização dos dispositivos móveis pelas organizações públicas, a NC 12/IN01/DSIC/GSIPR classifica os usuários desses dispositivos em três grupos:

(a) agentes públicos com dispositivos móveis corporativos.

(b) agentes públicos com dispositivos móveis particulares.

(c) usuários visitantes com dispositivos móveis.

As diretrizes mais relevantes da NC nº 12/IN01/DSIC/GSIPR sobre o uso de dispositivos móveis são:

a) os dispositivos móveis de computação fornecidos pelos órgãos e entidades da APF devem ser cadastrados, garantindo sua identificação única, bem como a do usuário responsável pelo uso;

b) os agentes públicos não devem instalar aplicativos ou recursos não disponibilizados pelo setor responsável sem permissão;

c) é necessária a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário, bem como do dispositivo às conexões de rede e recursos disponíveis;

d) é recomendada a adoção de mecanismos que garantam a proteção e sigilo dos dados armazenados nos dispositivos em casos de extravio;

e) os agentes públicos devem ser orientados a respeito dos procedimentos de segurança acerca dos dispositivos que lhes forem disponibilizados, mediante a assinatura de Termo de Uso e Responsabilidade do órgão ou entidade a que pertencem, não sendo admitida a alegação de seu desconhecimento nos casos de uso indevido;

f) é necessária a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário, bem como do dispositivo às conexões de rede e recursos disponíveis;

g) os agentes públicos devem ser orientados a respeito dos procedimentos de segurança acerca dos dispositivos móveis e dos recursos que lhes forem disponibilizados, mediante a assinatura de Termo de Uso e Responsabilidade do órgão ou entidade a que pertencem, não sendo admitida a alegação de seu desconhecimento nos casos de uso indevido;

h) devem ser estabelecidos procedimentos de controle e concessão de acesso a visitantes que durante a permanência em instalações de órgãos e entidades da APF, necessitem conectar seus dispositivos móveis à rede da entidade;

i) a concessão de uso deve estar vinculada à conscientização do usuário sobre as normas internas de uso da rede, podendo o órgão ou entidade da APF estabelecer critérios próprios;

j) informações classificadas somente podem ser armazenadas em dispositivos móveis removíveis que possibilitem a aplicação de controles compatíveis com seu nível de classificação.

2.5.11. NC 13 - Gestão de mudanças nos aspectos relativos à Segurança da Informação

Segundo a NC 13/IN01/DSIC/GSIPR, "Gestão de mudanças" é o processo de gerenciamento de mudanças, de modo que ela transcorra com mínimos impactos no âmbito da organização, visando viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

A NC nº 13/IN01/DSIC/GSIPR recomenda-se que o processo de gestão de mudanças seja composto, no mínimo, pelas fases de "descrição", "avaliação", "aprovação", "implementação" e "verificação", de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

A norma orienta ainda que o Gestor de Mudanças observe se o processo de gestão de mudanças contempla os seguintes procedimentos:

a) identificação e registro de todas as etapas das mudanças;

b) correta alocação dos recursos disponíveis;

c) planejamento e testes das mudanças;

d) comunicação dos detalhes das mudanças para todas as pessoas envolvidas; e

e) procedimentos de recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.

2.5.12. NC 14 - Computação em Nuvem

A NC nº 14/IN01/DSIC/GSIPR tem como objetivo estabelecer diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nas organizações públicas.

A NC 14 define um modelo de computação em nuvem com cinco características essenciais, três modelos de serviço e quatro modelos de implementação. São elas:

(1) características essenciais: "Autosserviço por demanda"; "Amplo acesso à rede"; "Agrupamento de recursos"; e "Elasticidade; Medição de Serviços";

(2) modelos de serviço: "Software em Nuvem como um Serviço (*Software as a Service – SaaS*"; "Plataforma em Nuvem como um Serviço (*Plataform as a Service - PaaS*)"; "Infraestrutura em Nuvem como um Serviço (*Infrastructure as a Service - IaaS*)"; e

(3) modelos de implementação: " Nuvem Própria"; "Nuvem Comunitária"; "Nuvem Pública"; e "Nuvem Híbrida".

2.5.13. NC 15 - Uso de redes sociais

A NC nº 15/IN01/DSIC/GSIPR tem como foco o uso institucional das redes sociais nos aspectos relacionados à Segurança da Informação e Comunicações, podendo a organização pública expandir a abrangência de sua norma Interna de "Uso Seguro das Redes Sociais" para ações que vão além da SIC, como por exemplo, estratégia de comunicação social e processo de gestão de conteúdo.

Princípios e diretrizes recomendados pela norma:

(1) a normatização interna de uso seguro das redes sociais deve:

a) estar alinhada tanto à Política de Segurança da Informação e Comunicações (POSIC) quanto aos objetivos estratégicos do órgão ou entidade;

b) estabelecer diretrizes, critérios, limitações e responsabilidades na gestão do uso seguro das redes sociais, por usuários que tenham permissão para administrar perfis institucionais ou que possuam credencial de acesso para qualquer rede social, a partir da infraestrutura das redes de computadores; e

c) considerar os requisitos legais de segurança da informação e comunicações.

(2) perfis institucionais mantidos nas redes sociais devem, preferencialmente, ser administrados e gerenciados por equipes integradas exclusivamente por servidores ou empregados públicos federais ocupantes de cargo efetivo; e

(3) é vedada a terceirização completa da administração e da gestão de perfis da organização pública nas redes sociais.

2.5.14. NC 16 - Desenvolvimento e Obtenção de Software Seguro

A NC nº 16/IN01/DSIC/GSIPR traz os seguintes conceitos e definições para entendimento de suas diretrizes:

a) **análise dinâmica:** tipo de teste de software que verifica seu comportamento externo em busca de anomalias ou vulnerabilidades. A análise dinâmica ocorre por meio de interações com o software em execução;

b) **análise estática:** tipo de teste de software que verifica sua lógica interna em busca de falhas ou vulnerabilidades. A análise estática ocorre por meio da verificação do código-fonte ou dos binários;

c) requisitos de segurança: conjunto de necessidades de segurança que o software deve atender, sendo tais necessidades influenciadas fortemente pela política de segurança da organização, compreendendo aspectos funcionais e não funcionais;

d) os **aspectos funcionais** descrevem comportamentos que viabilizam a criação ou a manutenção da segurança e, geralmente, podem ser testados diretamente. Na maioria dos casos, remetem a mecanismos de segurança como, por exemplo, controle de acesso baseado em papéis de usuários (administradores, usuários comuns, etc.), autenticação com o uso de credenciais (usuário e senha, certificados digitais, etc.), dentre outros; e

e) os **aspectos não funcionais** descrevem procedimentos necessários para que o software permaneça executando suas funções adequadamente mesmo quando sob uso indevido. São exemplos de requisites não funcionais, dentre outros, a validação das entradas de dados e o registro de logs de auditoria com informações suficientes para análise forense.

Principais diretrizes para o desenvolvimento e aquisição de software seguro por sua organização:

a) previsão formal por sua organização de requisitos relacionados à segurança da informação;

b) requisitos para que na construção do software suas mensagens de erro não revelem detalhes da sua estrutura interna;

c) possuir controles da qualidade no desenvolvimento/aquisição de software ou procedimentos (p. ex.: análise estática e/ou análise dinâmica do software) com a finalidade de verificar o atendimento dos requisitos de segurança do software;

d) possuir procedimentos para configurar adequadamente o software desenvolvido/adquirido quando este passar para o ambiente de produção. São exemplos: todo código de teste, de "backups" ou arquivos desnecessários, de informações sigilosas nos comentários de código e das contas criadas para teste devem ser removidos;

e) existir procedimento formal para que a segurança da informação seja integrada nos métodos de gerenciamento de projeto da organização, e para assegurar que os riscos de segurança da informação estejam identificados e considerados como parte de um projeto;

f) estabelecer definições sobre a custódia de código-fonte e manutenção do software em caso de falha da empresa contratada;

g) definir regras e procedimentos operacionais para a contratada quanto à liberação de acesso aos recursos tecnológicos e ao ambiente físico ou lógico de sua organização, caso seja necessário;

h) definir as regras para transferência do conhecimento sobre o software desenvolvido/adquirido de modo a permitir a sua manutenção, de forma independente, por sua organização;

i) prever no instrumento contratual correspondente os procedimentos de segurança, como os descritos acima; e

j) os ambientes de desenvolvimento, teste e produção estarem separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.

2.5.15. NC 17 - atuação e adequações para profissionais da área de Segurança da Informação

A NC nº 17/IN01/DSIC/GSIPR traz recomendações para a atuação, treinamento e certificações dos profissionais da área de Segurança da Informação e Comunicações (SIC).

Destacam-se as seguintes recomendações:

(1) estabelecer ciclo de palestras, seminários, reuniões e outros eventos que contribuam para o constante processo de compartilhamento e absorção do conhecimento nos domínios da SIC;

(2) promover a troca de conhecimento e experiências no contexto e domínios de SIC por meio de grupos de trabalho formalmente instituídos, seguindo preferencialmente os temas propostos no ANEXO B da NC nº 17/IN01/DSIC/GSIPR;

(3) designar, sempre que solicitado, profissionais da área de SIC para integrar os grupos de trabalho citados acima;

(4) designar profissionais da área de SIC para participarem da elaboração do planejamento estratégico e da programação orçamentária do órgão ou entidade a qual mantenham vínculo;

(5) estabelecer no planejamento estratégico e tático ações que contemplem os aspectos de formação educacional, retenção e compartilhamento do conhecimento em SIC.

(6) prover a capacitação dos profissionais de SIC, em âmbito interno e externo, preferencialmente alinhada às certificações profissionais e aos temas recomendados na NC nº 17/IN01/DSIC/GSIPR; e

(7) estabelecer políticas de incentivo ao estudo e à pesquisa, bem como a produção e aquisição de obras literárias e normas técnicas de SIC e áreas correlatas.

2.5.16. NC 18 - Atividades de ensino em Segurança da Informação

A NC nº 18/IN01/DSIC/GSIPR tem como objetivo estabelecer as diretrizes para as atividades de ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).

Atividades de ensino em segurança da informação e comunicações recomendadas pela NC nº 18:

(1) os Agentes Públicos deverão receber orientações/instruções em Segurança da Informação e Comunicações no período de ambientação, formação inicial ou continuada em seus órgãos ou entidades, por meio de atividades de ensino de sensibilização, conscientização, capacitação e especialização;

(2) as Escolas de Governo, de formação inicial e/ou continuada deverão ministrar o tema SIC em suas atividades de ensino tomando por base esta Norma Complementar;

(3) recomenda-se que os órgãos e entidades da APF invistam na formação continuada dos profissionais da área de Segurança da Informação e Comunicações por meio de cursos de extensão e especialização.

O Apêndice 6 traz o quadro com as certificações recomendadas pela NC nº 18/IN01/DSIC/GSIPR.

2.5.17. NC 19 - Segurança da Informação em Sistemas Estruturantes da Administração Pública

A NC nº 19/IN01/DSIC/GSIPR tem como objetivo estabelecer padrões mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal, direta e indireta.

Conforme definição da NC nº 19/IN01/DSIC/GSIPR, Sistema Estruturante é um sistema com suporte de tecnologia da informação fundamental e imprescindível para planejamento, coordenação, execução, descentralização, delegação de competência, controle ou auditoria das ações do Estado, além de outras atividades auxiliares, desde que comum a dois ou mais órgãos da Administração e que necessitem de coordenação central.

Segundo Serpro (BRASIL, 2017), os sistemas estruturadores são mecanismos de organização por temas da administração pública federal, sendo previstos no Decreto-Lei nº 200/67. Os sistemas estruturantes, por sua vez, são a forma tecnológica que dá suporte ao funcionamento destes sistemas estruturadores. Como exemplo, cita o SIPEC, sistema estruturador que cuida do pessoal civil da administração, e que recebe o apoio de um sistema estruturante eletrônico, o SIGEPE.

A NC nº 19 recomenda que os padrões de segurança dos sistemas estruturantes deverão incorporar, gradativamente, controles de segurança da informação e comunicações, no mínimo, no que tange aos seguintes aspectos:

(1) planejamento, concepção e manutenção do sistema;

(2) infraestrutura;

(3) controle de acesso e identidades;

(4) tratamento de incidentes; e

(5) política e conformidade

2.5.18. NC 20 - Segurança da Informação no Tratamento da Informação

Segundo a Norma Complementar nº 20/IN01/DSIC/GSIPR, "Revisão 01", toda informação institucional dos órgãos e entidades da Administração Pública em qualquer suporte, materiais, áreas, comunicações e sistemas de informação institucionais, é patrimônio do Estado brasileiro e deve ser tratada segundo as diretrizes da Norma nos termos da legislação pertinente em vigência.

Sendo assim, o tratamento da informação ao longo de seu ciclo de vida deve ser realizado de modo ético e responsável pelos agentes públicos dos órgãos e entidades. O tratamento da informação deve ser feito conforme atos normativos de SIC, assegurando-se os requisitos da disponibilidade, da integridade, da confidencialidade e da autenticidade da informação em todo seu ciclo de vida.

A informação institucional dos órgãos e entidades da APF deve ser tratada visando as suas funções administrativas, informativas, probatórias e comunicativas, e considerados os princípios de acesso a informação dispostos pela

A legislação federal que trata do processo de tratamento da informação:

1. Lei nº 12.527/2011 – Regula o acesso as informações previsto na Constituição Federal (inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216).
2. Decreto nº 7.724/2012 – Regulamenta a Lei nº 12.527, de 18 de novembro de 2011.
3. Decreto nº 7.845/2012 – Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

A NC nº 20 DSIC/GSI/PR traz vários procedimentos quanto à "Produção e Recepção", "Organização", "Uso e disseminação" e "Destinação" das informações classificadas. Destacam-se os seguintes procedimentos:

a) é responsabilidade das organizações públicas verificar se as informações por eles produzidas ou custodiadas se enquadram em quaisquer hipóteses de sigilo

especificadas na Lei 12.527/2011 ou em legislações específicas – tais como aquelas referentes aos sigilos legal, fiscal e bancário, ao segredo industrial ou de justiça, a fim de adotar as medidas cabíveis quanto ao seu tratamento;

b) na fase de registro e armazenamento, deverão ser realizadas as marcações e adotadas as demais medidas de salvaguarda das informações sigilosas nos termos da Lei 12.527/2011 ou de outras legislações específicas, bem como informações pessoais;

c) as informações sigilosas classificadas, produzidas e armazenadas em meios eletrônicos, devem utilizar criptografia compatível com o grau de sigilo, conforme a legislação vigente;

d) no armazenamento de informações classificadas em grau de sigilo secreto ou ultrassecreto, deverá ser utilizado cofre ou estrutura que ofereça segurança equivalente;

e) no caso das demais informações sigilosas, o armazenamento deve ser realizado em ambiente com acesso controlado;

f) a informação classificada deve ser produzida e custodiada utilizando criptografia baseada em algoritmo de estado compatível com o grau de sigilo, conforme padrões mínimos estabelecidos na NC 09 DSIC/GSI/PR;

g) os órgãos e entidades da APF devem instituir as medidas necessárias para garantir a segurança e o adequado tratamento das informações registradas e armazenadas em repositórios digitais institucionais, a fim de permitir o acesso, a recuperação e a preservação dessas informações;

h) recomenda-se a regulamentação do uso de impressoras e copiadoras, definindo diretrizes para a impressão/cópia de documentos que contenham informação sigilosa e pessoal;

i) os órgãos e entidades da APF devem definir medidas e procedimentos para que os fluxos de distribuição das informações assegurem a continuidade das medidas de salvaguarda de informações sigilosas conforme a Lei 12.527/2011 ou de acordo com legislações específicas, bem como de informações pessoais relativas à intimidade, vida privada, honra e imagem detidas pelos órgãos e entidades da APF; e

a) o acesso às áreas, instalações e materiais que contenham informações classificadas em qualquer grau de sigilo, ou que demandem proteção, que demande proteção, deve ser normatizado internamente.

Tabela 2.7 - Anexo A da NC nº 20/IN01/DSIC/GSIPR

QUADRO EXEMPLIFICATIVO DE TIPOS DE INFORMAÇÃO		
TIPO	**DESCRIÇÃO**	
1. OSTENSIVA	Transparência Ativa	
	Transparência Passiva	
2. SIGILOSA CLASSIFICADA EM GRAU DE SIGILO	2.1	Reservada: Prazo máximo de restrição de acesso de 5 anos
	2.2	Secreta: Prazo máximo de restrição de acesso de 15 anos
	2.3	Ultrassecreta: Prazo de restrição de acesso de 25 anos, prorrogável por uma única vez, e por período não superior a 25 anos, limitado ao máximo de 50 anos o prazo total da classificação.
3. SIGILOSA PROTEGIDA POR LEGISLAÇÃO ESPECÍFICA (As hipóteses legais de restrição de acesso à informação elencadas neste item não são exaustivas)	3.1	Sigilos Decorrentes de Direitos de Personalidade
	3.1.1	Sigilo Fiscal
	3.1.2	Sigilo Bancário
	3.1.3	Sigilo Comercial
	3.1.4	Sigilo Empresarial
	3.1.5	Sigilo Contábil
	3.2	Sigilos de Processos e Procedimentos
	3.2.1	Acesso a Documento Preparatório
	3.2.2	Sigilo do Procedimento Administrativo Disciplinar em Curso
	3.2.3	Sigilo do Inquérito Policial
	3.2.4	Segredo de Justiça no Processo Civil
	3.2.5	Segredo de Justiça no Processo Penal
	3.3	Informação de Natureza Patrimonial
	3.3.1	Segredo Industrial
	3.3.2	Direito Autoral e Propriedade Intelectual de Programa de Computador
	3.3.3	Propriedade Industrial
4. PESSOAL	4.1.	Pessoal Prazo máximo de restrição de acesso 100 anos, independente de classificação de sigilo e quando se referir à intimidade, vida privada, honra e imagem das pessoas.

3. RESULTADOS DA PESQUISA

Este Capítulo tem como foco descrever como o questionário foi elaborado, a pesquisa foi realizada, os dados encontrados e o resultado consolidado.

3.1. Como foi elaborado o questionário

O documento base para elaboração do questionário (Apêndice 2) foram as 21 Normas Complementares (NC) à IN nº 01 GSI/PR/2008, do Gabinete de Segurança Institucional, correlacionadas aos 114 controles contidos na NBR ISO/IEC 27002:2013 (Apêndice 1).

Tabela 3.1 – Total de princípios, diretrizes e recomendações das normas complementares à IN nº 01 GSI/PR/2008

Nº da NC	Descrição	Nº de recomendações /princípios/diretrizes por NC
1	Elaboração, atualização, alteração, aprovação e publicação de normas complementares.	-
2	Gestão de SI.	28
3	Elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação.	10
4	Ciclo completo de um processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC.	23
5	Tipos de estruturas organizacional e de autonomia das Equipes de tratamento e resposta a incidentes.	11
6	Procedimentos para elaboração do Programa de Gestão da Continuidade de Negócios.	15
7	Procedimentos para implementação de controles de acesso relativos à Segurança da Informação e Comunicações.	43
8	Gestão dos serviços de gerenciamento de Incidentes de Segurança em Redes de Computadores.	13
9	Orientações específicas para o uso de recursos criptográficos.	23
10	Orientações sobre o inventário e mapeamento de ativos.	15
11	Avaliação de Conformidade.	11
12	Dispositivos móveis nos aspectos relativos à Segurança da informação.	18
13	Gestão de mudanças.	13
14	Uso de computação em nuvens.	14
15	Uso de redes sociais.	13
16	Desenvolvimento e obtenção de software seguro.	24
17	Atuação e adequações para profissionais da área de SI.	16
18	Atividades de ensino em SI.	5
19	Padrões mínimos de SI para os sistemas estruturantes da Administração Pública Federal.	24
20	Tratamento da informação.	57
21	Coleta e preservação de evidências de incidentes de segurança em redes.	28
TOTAL		404

Inicialmente foram criadas 14 categorias conforme a interseção dos objetivos tratados em cada uma das 21 normas complementares do GSI e nas 14 seções da norma NBR/ISO 27002:2013 (Tabela 3.2 a seguir).

Quatro normas complementares não foram categorizadas:

(a) NC nº 1: critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares.
(b) NC nº 14: computação em nuvem nos aspectos relacionados à Segurança da Informação;
(c) NC nº 18: atividades de ensino em Segurança da Informação; e
(d) NC nº 19: padrões mínimos de Segurança da Informação e Comunicações para os sistemas estruturantes da Administração Pública Federal.

Tais temas tratam de diretrizes específicas para a alta administração (NC nº 01, 18 e 19) ou tratam de temas ainda não implementados ou incipientes nas organizações públicas (NC nº 14).

Após a categorização, foram elaboradas questões que refletissem as recomendações, princípios e diretrizes das normas complementares, reproduzindo o conteúdo das normas em perguntas. Da mesma forma, foram criadas questões a partir dos 114 controles da norma NBR ISO/IEC 27002:2013.

Como algumas das recomendações das normas complementares e como alguns dos controles da norma NBR ISO/IEC 27002:2013 são muito específicos ou "descem" muito ao nível de implementação, foi necessário agregá-los em um maior nível de abstração.

Do confronto entre esses questionamentos foram então elaboradas 54 perguntas e subitens, totalizando 87 itens de verificação do questionário da pesquisa, agregados em 14 temas. A tabela 3.2 mostra a correlação entre as 21 normas complementares do GSI, as 14 seções da NBR ISO/IEC 27002:2013 e o questionário elaborado para a pesquisa.

Tabela 3.2 – Correlação entre NC, NBR ISO/IEC 27002:2013 e questionário

ASSUNTO/TEMA		Nº da Norma Complementar	Seção da NBR ISO/IEC 27002:2013	Questionário 54 Perguntas/ 87 itens de verificação
Estabelecer critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares		1	-	-
Metodologia de Gestão de segurança da informação e comunicações		2	-	-
Política de Segurança da Informação e Comunicações		3	5 - Políticas de SI	1 a 3 (6 itens)
Gestão de Riscos de Segurança da Informação e Comunicações		2, 4	6 - Organização da SI	4 (1 item)
Incidentes de Segurança da Informação	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR	5	6 - Organização da SI	5, 6, 7, 8 e 9 (6 itens)
	Gerenciamento de Incidentes de Segurança em redes de computadores realizado pelas ETIR	8	16 - Gestão de incidentes de SI	
	Registro de eventos, coleta e preservação de evidências de incidentes de Segurança em Redes.	21		
Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações		6	17 - Aspectos da segurança da informação na gestão da continuidade do negócio	10, 11, e 12 (3 itens)
Controles de acesso relativos à Segurança da Informação e Comunicações		7	8.3 Tratamento de mídias 9 Controle de acesso 11 Segurança física e do ambiente 12 Segurança nas operações 13 Segurança nas comunicações 15 Relacionamento na cadeia de suprimento	13 a 30 (35 itens)
Uso de recursos criptográficos em Segurança da Informação e Comunicações		9	10 - Criptografia	31 a 35 (6 itens)
Inventário e Mapeamento de Ativos de Informação		10	8 Gestão de ativos	36 (1 item)
Avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações		11	12.7 Considerações quanto à auditoria de sistemas da informação 18 Conformidade 18.1 Conformidade com requisitos legais e contratuais 18.2 Análise crítica da segurança da informação	37 e 38 (2 itens)

Tabela 3.2 – Correlação entre NC, NBR ISO/IEC 27002:2013 e questionário

ASSUNTO/TEMA	Nº da Norma Complementar	Seção da NBR ISO/IEC 27002:2013	Questionário 54 Perguntas/ 87 itens de verificação
Uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC)	12	6.2 Dispositivos móveis e trabalho remoto	39 a 42 (4 itens)
Gestão de mudanças nos aspectos relativos à Segurança da Informação e Comunicações.	13		43 a 44 (2 itens)
Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC)	14	-	-
Diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais na APF.	15	-	45 (1 item)
Desenvolvimento e Obtenção de Software Seguro	16	6.1.5 SI no gerenciamento de projetos 14 Aquisição, desenvolvimento e manutenção de sistemas	46-itens "a" a "j" (10 itens)
Atuação e adequações para profissionais da área de Segurança da Informação e Comunicações.	17	6.1 Organização interna 7 Segurança em recursos humanos 7.1 Antes da contratação 7.2 Durante a contratação 7.3 Encerramento e mudança da contratação	47 a 52 (8 itens)
Atividades de Ensino em Segurança da Informação e Comunicações	18	-	-
Padrões mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta.	19	-	-
Processo de tratamento da informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.	20	8.2 Classificação da informação	53 e 54 (2 itens)

3.2. Como foi realizada a pesquisa

Para avaliar a percepção dos entrevistados, cada controle foi categorizado em 3 escalas de relevância: (1) pouco relevante; (2) relevante, somente se houver recursos; e (3) muito relevante, independente dos recursos necessários. Tal escala se explica, pois, o gestor encontra-se sempre diante do dilema de qual controle deverá ser implementado frente aos recursos limitados.

Cada controle ainda foi avaliado quanto ao grau de implementação na organização pública. As respostas possíveis foram: (1) "sim, está implementado"; (2) "não foi implementado"; (3) "em parte implementado"; (4) "não se aplica"; e (5) "desconheço".

Para escolha das organizações públicas objeto da pesquisa foi utilizado o critério de destaque da organização no cenário da Administração Pública. Reforçou essa escolha a percepção do pesquisador em suas atividades em auditoria de Tecnologia da Informação quanto à importância das atividades finalísticas ou grau de maturidade da área de TI da organização.

Para aplicação do questionário, foram contatados usuários avançados ou gestores de TI, conhecedores da estrutura de TI de sua organização. Foram enviados 10 questionários por email (Apêndice 3 – correspondência explicativa), sendo que 07 foram respondidos, perfazendo 70 % (setenta por cento) do total.

As dez organizações públicas que participaram dessa pesquisa foram: dois tribunais superiores, três órgãos de controle (federal e distrital), um órgão do legislativo federal, uma empresa pública distrital, uma universidade pública, um ministério do Poder Executivo Federal, e uma organização militar, todos sediados em Brasília no Distrito Federal.

O número de organizações não teve como objetivo servir de amostra para uma inferência estatística, e sim ser exequível pelo objetivo e abrangência deste trabalho. Uma outra dificuldade de realizar a pesquisa em um grupo mais extenso de organizações públicas reside no fato de que alguns gestores não se sentem à vontade em descrever a real situação de suas organizações, principalmente quando questionados sobre controles de Segurança da Informação que deveriam estar implementados conforme os normativos governamentais.

3.3. Consolidação e análise dos resultados

Para consolidação dos resultados, foram tabuladas todas as respostas em uma planilha eletrônica: 87 itens de verificação, 5 escalas, e 7 questionários respondidos; e totalizado o número de ocorrências por controle/item de verificação, conforme os critérios da pesquisa: relevância e implementação do controle.

A relevância de cada controle foi definida pelo somatório da opinião de cada entrevistado. A maior pontuação na escala definia o grau de relevância daquele controle. Em

caso de empate, houve a avaliação individual do controle para verificar a tendência da percepção dos gestores.

A tabela 3.3 a seguir traz a consolidação dos controles selecionados por tema ou categoria. Dos 87 itens de verificação propostos na pesquisa, 59 controles foram categorizados como "muito relevantes", 28 como "relevantes" e nenhum dos 87 controles propostos foram definidos como "pouco relevantes".

Tabela 3.3 – Consolidação dos resultados – Controles selecionados

Tema/Categoria	Total de Controles propostos	Total de Controles selecionados		
		1 - Pouco relevante	2 - Relevante se houver recursos	3 - Muito relevante, independente dos recursos necessários
Políticas de SI	6			6
Gestão de Riscos	1			1
Gestão de incidentes de SI	6		5	1
Gestão de Continuidade da SI	3			3
Controles de Acesso	35		10	25
Uso de recursos criptográficos	6		5	1
Inventário dos ativos	1		1	
Conformidade e auditoria	2		1	1
Dispositivos móveis	4		4	
Gestão de Mudanças	2			2
Redes Sociais	1		1	
Desenvolvimento e aquisição de Software Seguro	10		1	9
Atuação e adequações para profissionais de SI	8			8
Classificação da Informação	2			2
TOTAIS	**87**		**28**	**59**

Em uma análise inicial da tabela 3.3, observa-se que alguns controles propostos foram considerados em sua maioria muito relevantes conforme a percepção dos entrevistados. Entretanto, essa percepção não se concretiza na prática. Muitos controles considerados muito relevantes não estão implementados nas organizações participantes da pesquisa.

A tabela 3.4 a seguir sintetiza a análise quanto aos controles de SI e a sua implementação nas organizações públicas participantes da pesquisa.

Tabela 3.4 – Consolidação dos resultados – Implementação dos Controles

Tema: Políticas de segurança da informação	**Nº de controles propostos: 6**
Relevância verificada: Os 06 controles foram considerados "muito relevantes" - 100%.	
Comentário: 1. 28% das organizações implementaram uma PSI (POSIC) totalmente; 2. 14% tem uma ETIR ou um comitê de gestão de SI; e 3. 28% tem um gestor de SI.	
Tema: Organização da segurança da formação	**Nº de controles propostos: 1**
Relevância verificada: o controle proposto *"Sua organização possui um processo de Gestão de Riscos de Segurança da Informação?"* foi considerado "muito relevante".	
Comentário: 1. 85% das organizações **não possuem** um processo de Gestão de Riscos de SI.	
Tema: Gestão de incidentes de SI	**Nº de controles propostos: 6**
Relevância verificada: 5 controles foram considerados relevantes, se houver recursos. 1 controle foi considerado "muito relevante".	
Comentário: 1. Nenhuma das organizações possuem procedimento formal de coleta e preservação de evidências na ocorrência de um incidente de SI. 2. 28% das organizações possuem seus servidores de hospedagem de página eletrônica com configuração para armazenar registros históricos de eventos (logs) em formato que permita a completa identificação dos fluxos de dados.	
Tema: Continuidade da Segurança da Informação	**Nº de controles propostos: 3**
Relevância verificada: Os 03 controles foram considerados "muito relevantes" - 100%.	
Comentário: 1. 14% das organizações possuem controles de continuidade da segurança da informação que são verificados a intervalos regulares, para garantir que eles sejam válidos e eficazes em situações adversas.	
Tema: Controles de Acesso	**Nº de controles propostos: 35**
Relevância verificada: 25 controles foram considerados "muito relevante". 10 controles foram considerados relevantes, se houver recursos.	
Comentário: 1. 42% das organizações possuem **procedimento** que verifique se os **direitos de acesso** às informações e aos recursos de processamento da informação de todos os funcionários e partes externas **são retirados** logo após o **encerramento** de suas atividades, contratos ou acordos, ou ajustados após a mudança destas atividades. 2. Somente 28% das organizações possuem sistemas de senhas que asseguram a criação de senhas de qualidade. 3. 57% das organizações possuem procedimentos de segurança da informação para o trabalho remoto. 4. Somente 14% das organizações possuem controles contra acesso não autorizado a sua rede e serviços, com mecanismos apropriados de registro e monitoração para gravação e detecção de ações que possam afetar, ou ser relevante para a segurança da informação. 5. Nenhuma das organizações possuem procedimentos para análise crítica dos logs a intervalos regulares.	
Tema: Uso de recursos criptográficos	**Nº de controles propostos: 6**

Tabela 3.4 – Consolidação dos resultados – Implementação dos Controles

Relevância verificada: 5 controles foram considerados relevantes, se houver recursos. 1 controle foi considerado "muito relevante".
Comentário: 1. Nenhuma das organizações possuem uma política formal sobre o uso de controles criptográficos para a proteção da informação. 2. Nenhuma das organizações possuem uma política formal sobre o uso, proteção e tempo de vida das chaves criptográficas ao longo de todo o seu ciclo de vida. 3. 42% das organizações produz, armazena ou transmite informação classificada, em qualquer grau de sigilo, por meio eletrônico. Entretanto: a. Nenhuma das organizações utilizam exclusivamente recurso criptográfico baseado em algoritmo de Estado em conformidade com os parâmetros e padrões mínimos estabelecidos na Norma Complementar nº 09/IN01/DSIC/GSIPR para as informações classificadas em qualquer grau de sigilo. b. Nenhuma das organizações utilizam VPN com recurso criptográfico baseado em algoritmo de Estado. c. 14% das organizações cifram e decifram as informações sigilosas não classificadas utilizando recurso criptográfico, no mínimo, baseado em algoritmo registrado.
Tema: Inventário dos ativos — **Nº de controles propostos: 1**
Relevância verificada: o controle proposto *"Sua organização possui um processo formal de inventário e monitoramento de ativos de informação?"* foi considerado "relevante, se houver recursos".
Comentário: 1. Somente 28% das organizações possuem o controle implementado.
Tema: Conformidade e auditoria — **Nº de controles propostos: 2**
Relevância verificada: um controle foi considerado "muito relevante" e o outro controle foi considerado "relevante, se houver recursos".
Comentário: 1. Somente 14% das organizações possuem uma política de avaliação ou auditoria interna da conformidade em SI. 2. 72% das organizações não possuem um programa de auditoria externa, a intervalos planejados nos sistemas de informação, para verificação da conformidade com as normas e políticas de segurança da informação da organização.
Tema: Dispositivos móveis — **Nº de controles propostos: 4**
Relevância verificada: Os 4 controles foram considerados "relevante, se houver recursos".
Comentário: 1. 42 % das organizações possuem política de uso das redes sem fio. 2. 71 % das organizações possuem procedimentos de controle e concessão de acesso a visitantes que durante a permanência em suas instalações, necessitem conectar seus dispositivos móveis a sua rede. 3. Somente 14 % das organizações possuem política de uso de dispositivos móveis corporativos. 4. Nenhuma das organizações possuem uma política para uso de informações classificadas em dispositivos móveis removíveis de armazenamento?
Tema: Gestão de Mudanças — **Nº de controles propostos: 2**
Relevância verificada: Os 2 controles foram considerados "muito relevantes".
Comentário: 1. 72% das organizações não possuem o controle *"processo formal de gestão de mudanças que avalie os potenciais impactos à segurança da informação e comunicações que possam ocorrer durante a*

Tabela 3.4 – Consolidação dos resultados – Implementação dos Controles

implementação da mudança" implementado. 2. 86% das organizações não possuem processo que verifica se o andamento e o resultado das mudanças viabilizam e asseguram a disponibilidade, integridade, confidencialidade e autenticidade da informação.
Tema: Redes Sociais — **Nº de controles propostos: 1**
Relevância verificada: o controle proposto *"Sua organização possui norma interna de segurança da informação relacionada ao uso de redes sociais no ambiente corporativo? "* foi considerado "relevante, se houver recursos".
Comentário: 1. 72% das organizações não possuem o controle implementado.
Tema: Desenvolvimento e aquisição de Software Seguro — **Nº de controles propostos: 10**
Relevância verificada: 1 controle foi considerado "relevante, se houver recursos". 9 controles foram considerados "muito relevante".
Comentário: 1. 86% das organizações não possuem controles da qualidade no desenvolvimento/aquisição de software ou procedimentos com a finalidade de verificar o atendimento dos requisitos de segurança do software. 2. 86% das organizações não possuem procedimentos para configurar adequadamente o software desenvolvido/adquirido quando este passar para o ambiente de produção. 3. Nenhuma das organizações possuem procedimento formal para que a segurança da informação seja integrada nos métodos de gerenciamento de projeto da organização, e para assegurar que os riscos de segurança da informação estejam identificados e considerados como parte de um projeto.
Tema: Atuação e adequações para profissionais de SIC — **Nº de controles propostos: 8**
Relevância verificada: Os 8 controles foram considerados "muito relevantes".
Comentário: 1. 14% das organizações promovem a capacitação dos profissionais de SI, em âmbito interno e externo, preferencialmente alinhada às certificações profissionais presente no mercado de TI. 2. 14% das organizações possuem uma política de conscientização dos controles e da Política de Segurança da Informação. 3. Nenhuma das organizações possuem um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação. 4. Nenhuma das organizações possuem procedimento formal para verificar que as responsabilidades e obrigações pela segurança da informação permaneçam válidas após um encerramento ou mudança da contratação, e que estas responsabilidades sejam definidas, comunicadas aos funcionários ou partes externas e cumpridas
Tema: Classificação da informação — **Nº de controles propostos: 2**
Relevância verificada: Os 2 controles foram considerados "muito relevantes".
Comentário: 1. No controle sobre informações classificadas ou sigilosas, somente 28% das organizações tem o controle implementado de coleta, orientação, produção, armazenamento, disponibilização de informações **classificadas** ou **sigilosas** nos termos da Lei 12.527/2011 ou de outras legislações específicas, inclusive informações pessoais. 2. No controle sobre impressoras e copiadoras e informação de acesso restrito, **nenhuma** das organizações tem esse controle implementado.

3.4. Conjunto mínimo de controles de Segurança da Informação

Após a realização da pesquisa e da consolidação dos resultados, chegamos a dois conjuntos de diretrizes e boas práticas em SI:

(1) 59 controles foram considerados como "muito relevante" pela pesquisa; e

(2) 28 controles considerados "relevantes, se houver recursos".

Tais conjuntos ajudarão aos gestores e a própria administração pública a terem uma orientação segura sobre quais são os controles mínimos que devem implementados, respeitadas as peculiaridades, visão, missão e valores de cada organização pública. Esses conjuntos de controles também serão úteis para as atividades de auditoria realizada pela própria organização (auditoria interna) e pelos órgãos de controle (auditoria externa).

Tabela 3.5 – 59 Controles de SI selecionados como "muito relevantes" na pesquisa

Políticas de Segurança da Informação	1. Sua organização possui uma política de segurança da informação (POSIC) definida, aprovada pela direção, publicada e comunicada para todos os funcionários e partes externas relevantes? 2. Sua POSIC e os instrumentos normativos gerados a partir dela, são revisados sempre que se fizer necessário, não excedendo o período máximo de 03(três) anos?
	Sua POSIC instituiu ou sua organização possui: 3. uma estrutura para a Gestão da Segurança da Informação e Comunicações? 4. um Gestor de Segurança da Informação e Comunicações? 5. um Comitê de Segurança da Informação e Comunicações do órgão ou entidade? 6. uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR?
Organização da Segurança da Informação	7. Sua organização possui um processo de Gestão de Riscos de Segurança da Informação?
Gestão de incidentes de Segurança da Informação	8. Havendo indícios de ilícitos criminais, a ETIR possui procedimentos para acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários?
Gestão da continuidade da Segurança da Informação	9. Sua organização possui procedimentos de continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre? 10. Os controles de continuidade da segurança da informação são verificados a intervalos regulares, para garantir que eles sejam válidos e eficazes em situações adversas? 11. Sua organização possui procedimentos e recursos para que o processamento da informação seja implementado com **redundância** suficiente para atender aos requisitos de disponibilidade?

Tabela 3.5 – 59 Controles de SI selecionados como "muito relevantes" na pesquisa

Controles de Acesso	Em relação à política de criação e administração de **contas de acesso** aos ativos de informação e a rede corporativa, sua organização: 12. Possui **procedimento** que verifique se os **direitos de acesso** às informações e aos recursos de processamento da informação de todos os funcionários e partes externas **são retirados** logo após o **encerramento** de suas atividades, contratos ou acordos, ou ajustados após a mudança destas atividades? 13. Utiliza o princípio do menor privilégio (direitos de acesso privilegiado, restritos e controlados) para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação? 14. O sistema de senhas assegura a criação de senhas de qualidade?
	15. Sua organização faz o registro/logs dos acessos à rede corporativa de computadores e dos serviços utilizados, inclusive acesso remoto, de forma a permitir a rastreabilidade e a identificação dos usuários? 16. Sua organização possui procedimentos de Segurança da Informação para o trabalho remoto?
	17. Sua organização possui controles contra **acesso não autorizado** a sua rede e serviços, em especial controles estabelecidos para proteção da **confidencialidade** e **integridade** dos dados que trafegam sobre redes públicas/redes sem fio (wireless) e dos sistemas e aplicações a elas conectadas?
Controles de Acesso	Sua organização possui implementado: 18. controles de detecção, prevenção e recuperação para proteção contra malware? 19. uma política de geração de cópias de segurança (cópias de segurança das informações, dos softwares e das imagens do sistema)? 20. uma política de registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação? 21. procedimentos para controlar a instalação de software em sistemas? 22. Em relação às vulnerabilidades técnicas dos sistemas de informação em uso, sua organização possui procedimentos para verificar as vulnerabilidades em tempo hábil e tomar as medidas apropriadas para lidar com os riscos associados? 23. Sua organização possui procedimento para que os registros estejam protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio? 24. Quanto à arquitetura de redes, existe **segregação de redes entre grupos** (serviços de informação, usuários e sistemas de informação)? 25. Sua organização possui uma política de uso da Internet, do correio eletrônico e de mensagens instantâneas?
	Sua organização possui uma política de acesso as suas **áreas e instalações físicas**: 26. com barreiras físicas de segurança, controle de entrada e saída para as áreas e instalações consideradas críticas ou para os ativos de informação? 27. com área de recepção com regras claras para a entrada e saída de pessoas, equipamentos e materiais, pontos de entrega e carregamento de material com acesso exclusivo ao pessoal credenciado? 28. possui sistemas de detecção de intrusos nas áreas e instalações de sua organização?

Tabela 3.5 – 59 Controles de SI selecionados como "muito relevantes" na pesquisa

	29. Sua organização possui procedimentos ou requisitos de segurança da informação com a finalidade mitigar os riscos associados com o acesso dos fornecedores aos ativos ou aos componentes de infraestrutura de TI da organização?
	Em relação aos equipamentos relacionados à informação e à segurança da informação: 30. encontram-se protegidos e colocados em locais para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado? 31. estão protegidos contra falta de energia elétrica e outras interrupções causadas por eventos externo? 32. o cabeamento de energia e de telecomunicações que transporta dado ou dá suporte aos serviços de informações está protegido contra interceptação, interferência ou danos?
	33. possuem manutenção correta para assegurar a sua contínua integridade e disponibilidade? 34. Existem medidas de segurança para ativos que operam fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da sua organização?
	35. Sua organização classificou os ativos de informação em níveis de criticidade, considerando o tipo de ativo de informação, o provável impacto no caso de quebra de segurança, tomando como base a gestão de risco e a gestão de continuidade de negócios relativa aos aspectos da segurança da informação e comunicações?
	36. Sua organização realiza testes periódicos de restauração das informações contidas nas cópias de segurança, a fim de garantir o seu uso na ocorrência de incidentes quando houver comprometimento das informações?
Uso de recursos criptográficos	37. Sua organização produz, armazena ou transmite informação classificada, em qualquer grau de sigilo, por meio eletrônico?
Conformidade e auditoria	38. Sua organização possui uma política de avaliação ou auditoria interna da conformidade em Segurança da Informação? (Verificação se os controles da segurança da informação estão em conformidade aos requisitos legais, estatutários, regulamentares, contratuais relacionados à segurança da informação).
Gestão de Mudanças	39. Sua organização possui um processo formal de gestão de mudanças que avalie os potenciais impactos à Segurança da Informação que possam ocorrer durante a implementação de mudanças? 40. Esse processo verifica se o andamento e o resultado da mudança viabilizam e asseguram a disponibilidade, integridade, confidencialidade e autenticidade da informação?
	Em relação ao desenvolvimento e aquisição de software seguro por sua organização: 41. constrói o software de forma que suas mensagens de erro não revelem detalhes da sua estrutura interna? 42. possui controles da qualidade no desenvolvimento/aquisição de software ou procedimentos (p. ex.: análise estática e/ou análise dinâmica do software) com a finalidade de verificar o atendimento dos requisitos de segurança do software?

Tabela 3.5 – 59 Controles de SI selecionados como "muito relevantes" na pesquisa

Desenvolvimento e aquisição de Software Seguro	43. possui procedimentos para configurar adequadamente o software desenvolvido/adquirido quando este passar para o ambiente de produção? (São exemplos: todo código de teste, de "backups" ou arquivos desnecessários, de informações sigilosas nos comentários de código e das contas criadas para teste devem ser removidos). 44. existe procedimento formal para que a segurança da informação seja integrada nos métodos de gerenciamento de projeto da organização, e para assegurar que os riscos de segurança da informação estejam identificados e considerados como parte de um projeto? 45. estabelece definições sobre a custódia de código-fonte e manutenção do software em caso de falha da empresa contratada? 46. define regras e procedimentos operacionais para a contratada quanto à liberação de acesso aos recursos tecnológicos e ao ambiente físico ou lógico de sua organização, caso seja necessário? 47. define as regras para transferência do conhecimento sobre o software desenvolvido/adquirido de modo a permitir a sua manutenção, de forma independente, por sua organização? 48. estão previstos no instrumento contratual correspondente os procedimentos de segurança, como os descritos acima? 49. os ambientes de desenvolvimento, teste e produção são separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção?
Atuação e adequações para profissionais de SIC	Quanto ao treinamento e certificações dos profissionais de SI, sua organização: 50. promove ou participa de ciclo de palestras, seminários, cursos, reuniões e outros eventos nos áreas da SIC? 51. mantém contato formal com fóruns, associações ou grupos especiais para conhecimento sobre as melhores práticas, receber previamente advertências de alertas, aconselhamentos e correções relativos a ataques e vulnerabilidades, trocar informações sobre novas tecnologias, produtos, ameaças ou vulnerabilidades? 52. promove a capacitação dos profissionais de SIC, em âmbito interno e externo, preferencialmente alinhada às certificações profissionais presente no mercado de TI? 53. A direção de sua organização solicita a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização? 54. Sua organização possui uma política de conscientização dos controles e da POSIC – Política de Segurança da Informação? 55. Sua organização possui um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação? 56. Sua organização possui procedimento formal para verificar que as responsabilidades e obrigações pela segurança da informação permaneçam válidas após um encerramento ou mudança da contratação, e que estas responsabilidades sejam definidas, comunicadas aos funcionários ou partes externas e cumpridas?

Tabela 3.5 – 59 Controles de SI selecionados como "muito relevantes" na pesquisa

	57. Sua organização possui regras para devolução dos ativos que estejam em posse de funcionários, após o encerramento de suas atividades, do contrato ou acordo.
Classificação da informação	58. Sua organização possui política ou procedimentos (relacionados à segurança da informação) de coleta, orientação, produção, armazenamento, disponibilização de informações classificadas ou sigilosas nos termos da Lei 12.527/2011 ou de outras legislações específicas, inclusive informações pessoais? 59. Sua organização possui regulamentação do uso de impressoras e copiadoras, definindo as diretrizes para a impressão/cópia de documentos que contenham informação de acesso restrito (conforme definido pela sua organização ou pela legislação)?

Tabela 3.6 – 28 Controles de SI selecionados como "relevantes" na pesquisa

Gestão de incidentes de segurança da informação	A Equipe de Tratamento e Resposta a Incidentes – ETIR de sua organização: 1. monitora e analisa tecnicamente os incidentes de segurança em redes de computadores emitindo alertas? 2. comunica a ocorrência de incidentes de segurança da informação ao Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR Gov ou realiza a elaboração de relatório de comunicação do incidente para público interno e/ou externo?
	Em relação aos Incidentes de Segurança em Redes Computacionais: 3. Sua organização possui procedimento formal de coleta e preservação de evidências na ocorrência de um incidente de Segurança da informação e comunicações – SIC? 4. faz a sincronização da data, hora e fuso horário do relógio interno dos ativos de informação com a "Hora Legal Brasileira do Observatório Nacional (ON)?
	5. Os servidores de hospedagem de página eletrônica de sua organização estão configurados para armazenar registros históricos de eventos (*logs*) em formato que permita a completa identificação dos fluxos de dados?
Controles de Acesso	Sua organização: 6. utiliza autenticação de multifatores para o controle de acesso lógico, a fim de verificar a identidade de um usuário e vinculá-lo a uma conta de acesso a ativos de informação? 7. mecanismos apropriados de registro e monitoração para gravação e detecção de ações que possam afetar, ou ser relevante para a segurança da informação?
	Sua organização possui implementado: 8. um programa de conscientização do usuário contra malware? 9. análise critica dos logs a intervalos regulares? 10. um mapa das áreas e instalações consideradas críticas, como ativos de informação de acordo com o valor, a criticidade, o tipo de ativo de informação e o grau de sigilo das informações que podem ser tratadas em tais áreas?
	11. Sua organização possui implementado normas específicas para o armazenamento, a veiculação de imagem, vídeo ou áudio, registrados em perímetros de segurança?

Tabela 3.6 – 28 Controles de SI selecionados como "relevantes" na pesquisa

Controles de Acesso	12. Existem procedimentos formais para que todos os equipamentos com mídias de armazenamento de dados sejam examinados antes da reutilização, para assegurar que todos os dados sensíveis e *software* licenciados tenham sido removidos ou sobregravados com segurança? 13. Sua organização estabeleceu distância mínima de segurança para manutenção das mídias contendo as cópias de segurança (backups)? 14. Sua organização possui procedimentos para o gerenciamento de mídias removíveis, incluindo descarte e proteção contra acesso não autorizado, de acordo com o esquema de classificação adotado pela organização? 15. Sua organização adota uma política de mesa limpa para papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação?
Uso de recursos criptográficos	Sua organização possui uma política formal: 16. sobre o uso de controles criptográficos para a proteção da informação? 17. sobre o uso, proteção e tempo de vida das chaves criptográficas ao longo de todo o seu ciclo de vida?
	18. Sua organização utiliza exclusivamente recurso criptográfico baseado em algoritmo de Estado em conformidade com os parâmetros e padrões mínimos estabelecidos na Norma Complementar nº 09/IN01/DSIC/GSIPR para as informações classificadas em qualquer grau de sigilo? 19. Sua organização utiliza VPN com recurso criptográfico baseado em algoritmo de Estado? 20. A cifração e decifração das informações sigilosas não classificadas utiliza recurso criptográfico, no mínimo, baseado em algoritmo registrado?
Inventário e monitoramento de ativos de SI	21. Sua organização possui um processo formal de inventário e monitoramento de ativos de informação? (Por exemplo: identificação e classificação de ativos de informação, responsáveis, proprietários e custodiantes de cada ativo de informação; caracterização dos contêineres dos ativos de informação; valor do ativo de informação; identificação de potenciais ameaças e vulnerabilidades e avaliação de riscos definição dos requisitos de segurança da informação e comunicações).
Conformidade e auditoria	22. Existe previsão de programa de auditoria externa em sua organização, a intervalos planejados nos sistemas de informação, para verificação da conformidade com as normas e políticas de segurança da informação da organização?
Dispositivos móveis	23. Sua organização possui política de uso das redes sem fio? 24. Sua organização possui procedimentos de controle e concessão de acesso a visitantes que durante a permanência em suas instalações, necessitem conectar seus dispositivos móveis a sua rede? 25. Sua organização possui política de uso de dispositivos móveis corporativos?
	26. Sua organização possui uma política para uso de informações classificadas em dispositivos móveis removíveis de armazenamento?

Tabela 3.6 – 28 Controles de SI selecionados como "relevantes" na pesquisa

Redes Sociais	27. Sua organização possui norma interna de segurança da informação relacionada ao uso de redes sociais no ambiente corporativo?
Desenvolvimento e aquisição de Software Seguro	28. Em relação ao desenvolvimento e aquisição de software seguro por sua organização estão previstos formalmente pela sua organização requisitos relacionados à segurança da informação?

4. CONCLUSÕES

Hoje a legislação e os normativos que tratam de Segurança da Informação (SI) são cada vez mais complexos. Existem mais de 400 princípios, diretrizes e recomendações de SI nas normas elaboradas pelo Gabinete de Segurança Institucional. A NBR ISO/IEC 27002, dividida em 14 seções, prevê ainda outros 114 controles sobre boas práticas de SI para as organizações.

Este estudo teve como objetivo delimitar um conjunto mínimo de controles, diretrizes e boas práticas em Segurança da Informação, tendo por base as 21 Normas Complementares (NC) à IN nº 01 GSI/PR/2008, do Gabinete de Segurança Institucional, e os 114 controles contidos na NBR ISO/IEC 27002:2013 (Apêndice 1).

Foram revisados os conceitos necessários ao entendimento do tema proposto: auditoria e tipos de auditorias; legislação e normas de Segurança da Informação.

Utilizou-se neste trabalho uma metodologia quali-quantitativa, transversal, com a aplicação de questionário aos gestores de TI de organizações públicas, que foram selecionadas conforme seu destaque nas suas áreas finalísticas de atuação. Aplicou-se então um questionário de 87 itens de verificação, agregados em 14 temas de Segurança da Informação.

Após consolidação e análise das respostas, foram delimitados dois conjuntos de controles para a Segurança da Informação, conforme a percepção dos gestores quanto à relevância dos controles: 59 controles foram considerados "muito relevantes"; e 28, considerados "relevantes", se a organização possuir recursos necessários para a sua implementação. Verificou-se ainda que muitos dos controles considerados como "muito relevantes" não estão implementados nas organizações públicas.

Esse conjunto de dois conjuntos de controles serão uma ferramenta útil:

(1) nas auditorias de Segurança da Informação realizadas pela própria organização (auditoria interna) e pelos órgãos de controle (auditoria externa) na elaboração das questões de auditoria;

(2) no auxílio para o planejamento e execução de projetos pelo gestor de TI; e

(3) na racionalização dos custos de implementação da Segurança da Informação nas organizações públicas.

Com o aperfeiçoamento dos controles de SI, as organizações públicas estarão melhor preparadas e equipadas para suportar os ataques provenientes de falhas na Segurança da Informação. Não é possível eliminar todas as vulnerabilidades, mas é possível mitigar os riscos inerentes à Tecnologia da Informação.

Entende-se que para o atingimento das suas missões institucionais as organizações públicas precisam dispender recursos e energia na melhoria da Segurança da Informação. Isso ocorrerá com auditorias de qualidade da Segurança da Informação.

4.1. TRABALHOS FUTUROS

Como proposta de trabalhos futuros, entende-se que novos estudos podem ser realizados, sendo que alguns pontos poderão ser aperfeiçoados:

(1) incremento da abordagem quantitativa/estatística das amostras;

(2) elaboração de indicadores e artefatos que auxiliem o gestor na tarefa de implementação dos controles sugeridos;

(3) verificação da eficiência, eficácia e efetividade dos controles propostos neste trabalho.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT. NBR ISO/IEC 17799:2005. Brasília, 2016.

_____. NBR ISO/IEC 17000:2005 – Avaliação de conformidade.

_____. NBR ISO/IEC 27000:2015. *Information technology – Security techniques – Information security management systems — Overview and vocabular.*

_____. NBR ISO/IEC 27001:2013. Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação — Requisitos. Brasília, 2016.

_____. NBR ISO/IEC 27002:2013. Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Brasília, 2016.

_____. NBR ISO/IEC 31000:2009. Gestão de riscos – Princípios e diretrizes. Brasília, 2016.

AVALIAÇÃO DE PROGRAMAS DE GOVERNO. TCU.2016. Disponível em < http://portal.tcu.gov.br/comunidades/avaliacao-de-programas-de-governo/ciclo-de-anop/>. Acesso em 01.04.2016.

BARDIN, L. Análise de Conteúdo. Trad. Luis Antero Reto e Augusto Pinheiro. Lisboa: Edições 70. 2002.

BASTOS, Alberto e CAUBIT, Rosângela. ISO 27001 e 27001. Gestão da Segurança da Informação – Uma Visão prática. 2009. Módulo Educaton Center. Editora Zouk.

BRASIL (2000). 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.

BRASIL (2017), CTIR, Centro de Tratamento de Incidentes de Redes do Governo (2017). Disponível em < http://www.ctir.gov.br/>. Acesso em 28.06.2017.

BRASIL (2017). SERPRO. Sistemas estruturantes. Disponível em < https://intra.serpro.Gov .br/noticias/noticias-2015/voce-sabe-o-que-sao-sistemas-estruturantes>. Acesso em 28.06.2017.

BRASIL (2017). SISP. Legislação de Seguranca da Informacao. Disponível em < https://www.governoeletronico.gov.br/eixos-de-atuacao/governo/sistema-de-administracao-dos-recursos-de-tecnologia-da-informacao-sisp/seguranca-da-informacao/legislacao>. Acesso em 28.06.2017.

CONTROLADORIA-GERAL DA UNIÃO. Instrução Normativa n.º 01, de 06 de abril de 2001. Disponível em <http://www.cgu.gov.br/sobre/legislacao/arquivos/instrucoes-normativas/in-01-06042001.pdf >. Acesso em 28.06.2017.

CICCO, Francesco de, 2006. AUDITORIA BASEADA EM RISCOS: mudando o paradigma das auditorias internas. Disponível em http://www.qsp.org.br/auditoria_risco.shtml>. Acesso em 28.06.2017.

DIAS, Claudia. Segurança e Auditoria da Tecnologia da Informação. São Paulo: Axcel Books, 2000. 222 p. ISBN: 8573231319

DIEHL, Astor Antônio; TATIM, Denise Carvalho. Pesquisa em ciências sociais aplicadas. São Paulo: Prentice Hall, 2004. 168 p. ISBN: 858791894X.

FERREIRA, RF, Calvoso, GG, Gonzales, CBL. Caminhos da pesquisa e a contemporaneidade. Psicologia: Reflexão e Crítica. Porto Alegre, vol.15 nº 2, p. 243-250. 2002.

GABINTE DE SEGURANÇA INSTITUCIONAL – GSI. Normas complementares à IN nº 01 GSI/PR/2008. Disponível em < http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares >. Acesso em 28.06.2017.

_____. Guia de Referência para a Segurança das Infraestruturas Críticas da Informação. 2010. Disponível em < http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf>.Acesso em 28.06.2017.

_____. Instrução Normativa GSI nº 2, de 5 de fevereiro de 2013. Disponível em <http://dsic.planalto.gov.br/documentos/instrucao_normativa_nr2.pdf>. Acesso em 28.06 .2017.

_____. Instrução Normativa GSI Nº 3, de 6 de março de 2013. Disponível em < http://dsic.planalto.gov.br/documentos/instrucao_normativa_nr3.pdf >. Acesso em 28.06.2017.

_____. Norma complementar à IN nº 02 GSI/PR/2013. Disponível em < http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/432-normas-complementares-2>. Acesso em 28.06.2017.

GLOSSÁRIO DE TERMOS DO CONTROLE EXTERNO. TCU. 2012. Disponível em < http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A14DB4AFB3014DBAC9E2994CFD>. Acesso em 01.04.2016.

KOSUTIC, Dejan. Visão geral do Anexo A da ISO 27001:2013. 2017. Disponível em < https://advisera.com/27001academy/pt-br/knowledgebase/visao-geral-do-anexo-a-da-iso-270012013/ >. Acesso em 28.06.2017.

ISSAI 200, Normas Internacionais das Entidades Fiscalizadoras Superiores, 2001. Disponível em < http://portal.tcu.gov.br/fiscalizacao-e-controle/auditoria/normas-internacionais/>. Acesso em 28.06.2017.

NORMAS DE AUDITORIA GOVERNAMENTAL: aplicáveis ao controle Externo Brasileiro. 2010. Disponível em < http://www.tc.df.gov.br/c/document_library/get_file?uuid=e8add8c6-3daa-49c3-8390-5e407af89dc7&groupId=20402 > Acesso em 28.06.2017.

NBC TA 200. Objetivos Gerais do Auditor Independente e a Condução da Auditoria em Conformidade com Normas de Auditoria. 2013. Disponível em < http://portalcfc.org.br/wordpress/wp-content/uploads/2013/01/NBC_TA_AUDITORIA.pdf>.Acesso em 28.06.2017.

NBC T 11 – Normas de Auditoria Independente das Demonstrações Contábeis, 2009. Disponível em <http://www.portaldecontabilidade.com.br/nbc/t11.htm >. Acesso em 28.06.2017.

PALMA, Fernando. 45 normas da família ISO/IEC 27000 - Gestão da Segurança da Informação . 2014. Disponível em <https://www.portalgsti.com.br/2013/12/as-normas-da-familia-iso-27000.html >. Acesso em 28.06.2017.

PORTAL REALPROTEC. As maiores ameaças de segurança em 2016. Disponível em <http://realprotect.net/blog/as-maiores-ameacas-de-seguranca-em-2016//>. Acesso em 15.05.2016.

PIRES, Wagner Salazar. Normas de segurança da informação aplicada a um órgão público. 2016. Disponível em < http://www.conteudojuridico.com.br/pdf/cj055537.pdf >. Acesso em 28.06.2017.

TCU. Manual de auditoria operacional. 2010. Disponível em < http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A14DB4AFB3014DBAC9EC7B5EF9>. Acesso em 28.06.2017.

_____. Boas práticas em Segurança da Informação. 2012. 4ª Edição. Disponível em <http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf>. Acesso em 28.06.2017.

VIEIRA, Tatiana Malta; FRAGA, Josemar Andrade. 2014. Quadro da legislação relacionada à segurança da informação e comunicações. Disponível em: < http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm>. Acesso em:28.06.2017.

APÊNDICE 1 - CONTROLES DA 27002

A.5 Política de segurança		
A.5.1 Política de segurança da informação		
A.5.1 .1	Documento da política de segurança da informação	Controle Um documento da política de segurança da informação deve ser aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.
A.5.1 .2	Análise crítica da política de segurança da informação	Controle A política de segurança da informação deve ser analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.
A.6 Organizando a segurança da informação		
A.6.1 Infra-estrutura da segurança da informação		
A.6.1 .1	Comprometimento da direção com a segurança da informação	Controle A Direção deve apoiar ativamente a segurança da informação dentro da organização, por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e conhecendo as responsabilidades pela segurança da informação.
A.6.1 .2	Coordenação da segurança da informação	Controle As atividades de segurança da informação devem ser coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes.
A.6.1 .3	Atribuição de responsabilidades para a segurança da informação	Controle Todas as responsabilidades pela segurança da informação devem estar claramente definidas.
A.6.1 .4	Processo de autorização para os recursos de processamento da informação	Controle Deve ser definido e implementado um processo de gestão de autorização para novos recursos de processamento da informação.

A.6.1 .5	Acordos de confidencialidade	Controle Os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação devem ser identificados e analisados criticamente, de forma regular.
A.6.1 .6	Contato com autoridades	Controle Contatos apropriados com autoridades relevantes devem ser mantidos.
A.6.1 .7	Contato com grupos especiais	Controle Contatos apropriados com grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais devem ser mantidos.
A.6.1 .8	Análise crítica independente de segurança da informação	Controle O enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, controles, objetivo dos controles, políticas, processos e procedimentos para a segurança da informação) deve ser analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas relativas à implementação da segurança da informação.
A.6.2 Partes externas Objetivo: Manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas.		

A.6.2.1	Identificação dos riscos relacionados com partes externas	Controle 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 devem ser identificados e controles apropriados devem ser implementados antes de se conceder o acesso.
A.6.2.2	Identificando a segurança da ir	Controle Todos os requisitos de segurança da informação identificados devem ser considerados antes de conceder aos clientes o acesso aos ativos ou às informações da organização.
A.6.2.3	Identificando segurança da informação nos acordos com terceiros	Controle Os acordos com terceiros envolvendo o acesso, processamento, comunicação ou gerenciamento dos recursos de processamento da informação ou da informação da organização, ou o acréscimo de produtos ou serviços aos recursos de processamento da informação devem cobrir todos os requisitos de segurança da informação relevantes.
A.7 Gestão de ativos		
A.7.1 Responsabilidade pelos ativos Objetivo: Alcançar e manter a proteção adequada dos ativos da organização.		
A.7.1 .1	Inventário dos ativos	Controle Todos os ativos devem ser claramente identificados e um inventário de todos os ativos importantes deve ser estruturado e mantido.

A.7.1 .2	Proprietário dos ativos	Controle Todas as informações e ativos associados com os recursos de processamento da informação devem ter um "proprietário"[3] designado por uma parte definida da organização.
A.7.1 .3	Uso aceitável dos ativos	Controle Devem ser identificadas, documentadas e implementadas regras para que seja permitido o uso de informações e de ativos associados aos recursos de processamento da informação.
A.7.2 Classificação da informação Objetivo: Assegurar que a informação receba um nível adequado de proteção.		
A.7.2.1	Recomendações para classificação	Controle A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.
A.7.2.2	Rótulos e tratamento da informação	Controle Um conjunto apropriado de procedimentos para rotular e tratar a informação deve ser definido e implementado de acordo com o esquema de classificação adotado pela organização.
A.8 Segurança em recursos humanos		
A.8.1 Antes da contratação[4]) Objetivo: Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades, e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso de recursos.		
A.8.1 .1	Papéis e responsabilidades	Controle Os papéis e responsabilidades pela segurança da informação de funcionários, fornecedores e terceiros devem ser definidos e documentados de acordo com a política de segurança da informação da organização.

A.8.1 .2	Seleção	Controle Verificações de controle de todos os candidatos a emprego, fornecedores e terceiros devem ser realizadas de acordo com as leis relevantes, regulamentações e éticas, e proporcionalmente aos requisitos do negócio, à classificação das informações a serem acessadas e aos riscos percebidos.
A.8.1 .3	Termos e condições de contratação	Controle Como parte das suas obrigações contratuais, os funcionários, fornecedores e terceiros devem concordar e assinar os termos e condições de sua contratação para o trabalho, os quais devem declarar as suas responsabilidade e da organização para a segurança da informação.
A.8.2 Durante a contratação Objetivo: Assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.		
A.8.2.1	Responsabilidades da direção	Controle A direção deve solicitar aos funcionários, fornecedores e terceiros que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.
A.8.2.2	Conscientização, educação e t	Controle Todos os funcionários da organização e, onde pertinente, fornecedores e terceiros devem receber treinamento apropriado em conscientização, e atualizações regulares nas políticas e procedimentos organizacionais relevantes para as suas funções.

A.8.2.3	Processo disciplinar	Controle Deve existir um processo disciplinar formal para os funcionários que tenham cometido uma violação da segurança da informação.
A.8.3 Encerramento ou mudança da contratação Objetivo: Assegurar que funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada.		
A.8.3.1	Encerramento de atividades	Controle As responsabilidades para realizar o encerramento ou a mudança de um trabalho devem ser claramente definidas e atribuídas.
A.8.3.2	Devolução de ativos	Controle Todos os funcionários, fornecedores e terceiros devem devolver todos os ativos da organização que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo.
A.8.3.3	Retirada de direitos de acesso	Controle Os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou devem ser ajustados após a mudança destas atividades.
A.9 Segurança física e do ambiente		
A.9.1 Áreas seguras Objetivo: Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.		

A.9.1 .1	Perímetro de segurança física	Controle Devem ser utilizados perímetros de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e recursos de processamento da informação.
A.9.1 .2	Controles de entrada física	Controle As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.
A.9.1 .3	Segurança em escritórios salas e instalações	Controle Deve ser projetada e aplicada segurança física para escritórios, salas e instalações.
A.9.1 .4	Proteção contra ameaças externas e do meio ambiente	Controle Deve ser projetada e aplicada proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem.
A.9.1 .5	Trabalhando em áreas seguras	Controle Deve ser projetada e aplicada proteção física, bem como diretrizes para o trabalho em áreas seguras.
A.9.1 .6	Acesso do público, áreas de entrega e de carregamento	Controle Pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, devem ser controlados e, se possível, isolados dos recursos de processamento da informação, para evitar o acesso não autorizado.

A.9.2 Segurança de equipamentos Objetivo: Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.		
A.9.2.1	Instalação e proteção do equipamento	Controle Os equipamentos devem ser colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.
A.9.2.2	Utilidades	Controle Os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.
A.9.2.3	Segurança do cabeamento	Controle O cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação ou danos.
A.9.2.4	Manutenção dos equipamentos	Controle Os equipamentos devem ter manutenção correta, para assegurar sua disponibilidade e integridade permanente.
A.9.2.5	Segurança de equipamentos fora das dependências da organização	Controle Devem ser tomadas medidas de segurança para equipamentos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.

A.9.2.6	Reutilização e alienação segura de equipamentos	Controle Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.
A.9.2.7	Remoção de propriedade	Controle Equipamentos, informações ou software não devem ser retirados do local sem autorização prévia.
A.10 Gerenciamento das operações e comunicações		
A. 10.1 Procedimentos e responsabilidades operacionais Objetivo: Garantir a operação segura e correta dos recursos de processamento da informação.		
A. 10.1.1	Documentação dos procedimentos de operação	Controle Os procedimentos de operação devem ser documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem.
A. 10.1.2	Gestão de mudanças	Controle Modificações nos recursos de processamento da informação e sistemas devem ser controladas.
A.10.1.3	Segregação de funções	Controle Funções e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos ativos da organização.
A. 10.1.4	Separação dos recursos de de	Controle Recursos de desenvolvimento, teste e produção devem ser separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais.

A.10.2 Gerenciamento de serviços terceirizados Objetivo: Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados.		
A.10.2.1	Entrega de serviços	Controle Deve ser garantido que os controles de segurança, as definições de serviço e os níveis de entrega incluídos no acordo de entrega de serviços terceirizados sejam implementados, executados e mantidos pelo terceiro.
A. 10.2.2	Monitoramento e análise crítica de serviços terceirizados	Controle Os serviços, relatórios e registros fornecidos por terceiro devem ser regularmente monitorados e analisados criticamente, e auditorias devem ser executadas regularmente.
A.10.2.3	Gerenciamento de mudanças para serviços terceirizados	Controle Mudanças no provisionamento dos serviços, incluindo manutenção e melhoria da política de segurança da informação, dos procedimentos e controles existentes, devem ser gerenciadas levando-se em conta a criticidade dos sistemas e processos de negócio envolvidos e a reanálise/reavaliação de riscos.
A.10.3 Planejamento e aceitação dos sistemas Objetivo: Minimizar o risco de falhas nos sistemas.		
A.10.3.1	Gestão de capacidade	Controle A utilização dos recursos deve ser monitorada e sincronizada e as projeções devem ser feitas para necessidades de capacidade futura, para garantir o desempenho requerido do sistema.

A.10.3.2	Aceitação de sistemas	Controle Devem ser estabelecidos critérios de aceitação para novos sistemas, atualizações e novas versões e que sejam efetuados testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação.
A.10.4 Proteção contra códigos maliciosos e códigos móveis Objetivo: Proteger a integridade do software e da informação.		
A.10.4.1	Controle contra códigos maliciosos	Controle Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.
A.10.4.2	Controles contra códigos móveis	Controle Onde o uso de códigos móveis é autorizado, a configuração deve garantir que o código móvel autorizado opere de acordo com uma política de segurança da informação claramente definida e que códigos móveis não autorizados tenham sua execução impedida.
A.10.5 Cópias de segurança Objetivo: Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.		
A.10.5.1	Cópias de segurança das informações	Controle Cópias de segurança das informações e dos softwares devem ser efetuadas e testadas regularmente, conforme a política de geração de cópias de segurança definida.
A.10.6 Gerenciamento da segurança em redes Objetivo: Garantir a proteção das informações em redes e a proteção da infra-estrutura de suporte.		

A.10.6.1	Controles de redes	Controle Redes devem ser adequadamente gerenciadas e controladas, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes, incluindo a informação em trânsito.
A.10.6.2	Segurança dos serviços de rede	Controle Características de segurança, níveis de serviço e requisitos de gerenciamento dos serviços de rede devem ser identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados.
A.10.7 Manuseio de mídias Objetivo: Prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos e interrupções das atividades do negócio.		
A.10.7.1	Gerenciamento de mídias removíveis	Controle Devem existir procedimentos implementados para o gerenciamento de mídias removíveis.
A.10.7.2	Descarte de mídias	Controle As mídias devem ser descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais.
A. 10.7.3	Procedimentos para tratamento de informação	Controle Devem ser estabelecidos procedimentos para o tratamento e o armazenamento de informações, para proteger tais informações contra a divulgação não autorizada ou uso indevido.
A .1 0.7 .4	Segurança da documentação dos sistemas	Controle A documentação dos sistemas deve ser protegida contra acessos não autorizados.

A. 10.8 Troca de informações Objetivo: Manter a segurança na troca de informações e softwares internamente à organização e com quaisquer entidades externas.		
A.10.8.1	Políticas e procedimentos para troca de informações	Controle Políticas, procedimentos e controles devem ser estabelecidos e formalizados para proteger a troca de informações em todos os tipos de recursos de comunicação.
A. 10.8.2	Acordos para a troca de informações	Controle Devem ser estabelecidos acordos para a troca de informações e softwares entre a organização e entidades externas.
A.10.8.3	Mídias em trânsito	Controle Mídias contendo informações devem ser protegidas contra acesso não autorizado, uso impróprio ou alteração indevida durante o transporte externo aos limites físicos da organização.
A.10.8.4	Mensagens eletrônicas	Controle As informações que trafegam em mensagens eletrônicas devem ser adequadamente protegidas.
A.10.8.5	Sistemas de informações do negócio	Controle Políticas e procedimentos devem ser desenvolvidos e implementados para proteger as informações associadas com a interconexão de sistemas de informações do negócio.
A.10.9 Serviços de comércio eletrônico Objetivo: Garantir a segurança de serviços de comércio eletrônico e sua utilização segura.		

A.10.9.1	Comércio eletrônico	Controle As informações envolvidas em comércio eletrônico transitando sobre redes públicas devem ser protegidas de atividades fraudulentas, disputas contratuais, divulgação e modificações não autorizadas.
A.10.9.2	Transações on-line	Controle Informações envolvidas em transações on-line devem ser protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.
A.10.9.3	Informações publicamente disponíveis	Controle A integridade das informações disponibilizadas em sistemas publicamente acessíveis deve ser protegida, para prevenir modificações não autorizadas.
A. 10.10 Monitoramento Objetivo: Detectar atividades não autorizadas de processamento da informação.		
A.10.10.1	Registros de auditoria	Controle Registros (log) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação devem ser produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.
A.10.10.2	Monitoramento do uso do sistema	Controle Devem ser estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento devem ser analisados criticamente, de forma regular.

A .10.10.3	Proteção das informações dos registros (logs)	Controle Os recursos e informações de registros (log) devem ser protegidos contra falsificação e acesso não autorizado.
A.10.10.4	Registros (log) de administrador e operador	Controle As atividades dos administradores e operadores do sistema devem ser registradas.
A.10.10.5	Registros (logs) de falhas	Controle As falhas ocorridas devem ser registradas e analisadas, e devem ser adotadas as ações apropriadas.
A.10.10.6	Sincronização dos relógios	Controle Os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, devem ser sincronizados de acordo com uma hora oficial.
A.11 Controle de acessos		
A.11.1 Requisitos de negócio para controle de acesso Objetivo: Controlar o acesso à informação.		
A. 11.1.1	Política de controle de acesso	Controle A política de controle de acesso deve ser estabelecida, documentada e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e da segurança da informação.
A.11.2 Gerenciamento de acesso do usuário Objetivo: Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.		
A. 11.2.1	Registro de usuário	Controle Deve existir um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços.

A.1 1.2.2	Gerenciamento de privilégios	Controle A concessão e o uso de privilégios devem ser restritos e controlados.
A. 11.2.3	Gerenciamento de senha do usuário	Controle A concessão de senhas deve ser controlada por meio de um processo de gerenciamento formal.
A. 11.2.4	Análise crítica dos direitos de acesso de usuário	Controle O gestor deve conduzir a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal.
A.11.3 Responsabilidades dos usuários Objetivo: Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação.		
A. 11.3.1	Uso de senhas	Controle Os usuários devem ser orientados a seguir boas práticas de segurança da informação na seleção e uso de senhas.
A. 11.3.2	Equipamento de usuário sem monitoração	Controle Os usuários devem assegurar que os equipamentos não monitorados tenham proteção adequada.
A. 11.3.3	Política de mesa limpa e tela limpa	Controle Deve ser adotada uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.
A.11.4 Controle de acesso à rede Objetivo: Prevenir acesso não autorizado aos serviços de rede.		

A. 11.4.1	Política de uso dos serviços de rede	Controle Os usuários devem receber acesso somente aos serviços que tenham sido especificamente autorizados a usar.
A. 11.4.2	Autenticação para conexão externa do usuário	Controle Métodos apropriados de autenticação devem ser usados para controlar o acesso de usuários remotos.
A. 11.4.3	Identificação de equipamento em redes	Controle Devem ser consideradas as identificações automáticas de equipamentos como um meio de autenticar conexões vindas de localizações e equipamentos específicos.
A. 11.4.4	Proteção e configuração de portas de diagnóstico remotas	Controle Deve ser controlado o acesso físico e lógico para diagnosticar e configurar portas.
A. 11.4.5	Segregação de redes	Controle Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes.
A. 11.4.6	Controle de conexão de rede	Controle Para redes compartilhadas, especialmente as que se estendem pelos limites da organização, a capacidade de usuários para conectar-se à rede deve ser restrita, de acordo com a política de controle de acesso e os requisitos das aplicações do negócio (ver 11.1).
A.1 1.4.7	Controle de roteamento de redes	Controle Deve ser implementado controle de roteamento na rede para assegurar que as conexões de computador e fluxos de informação não violem a política de controle de acesso das aplicações do negócio.
A.11.5 Controle de acesso ao sistema operacional Objetivo: Prevenir acesso não autorizado aos sistemas operacionais.		

A. 11.5.1	Procedimentos seguros de entrada no sistema (log-on)	Controle O acesso aos sistemas operacionais deve ser controlado por um procedimento seguro de entrada no sistema (log-on).
A.11.5.2	Identificação e autenticação de usuário	Controle Todos os usuários devem ter um identificador único (ID de usuário), para uso pessoal e exclusivo, e uma técnica adequada de autenticação deve ser escolhida para validar a identidade alegada por um usuário.
A. 11.5.3	Sistema de gerenciamento de senha	Controle Sistemas para gerenciamento de senhas devem ser interativos e assegurar senhas de qualidade.
A. 11.5.4	Uso de utilitários de sistema	Controle O uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações deve ser restrito e estritamente controlado.
A. 11.5.5	Desconexão de terminal por inatividade	Controle Terminais inativos devem ser desconectados após um período definido de inatividade.
A. 11.5.6	Limitação de horário de conexão	Controle Restrições nos horários de conexão devem ser utilizadas para proporcionar segurança adicional para aplicações de alto risco.
A. 11.6 Controle de acesso à aplicação e à informação Objetivo: Prevenir acesso não autorizado à informação contida nos sistemas de aplicação.		
A. 11.6.1	Restrição de acesso à informação	Controle O acesso à informação e às funções dos sistemas de aplicações por usuários e pessoal de suporte deve ser restrito de acordo com o definido na política de controle de acesso.

A. 11.6.2	Isolamento de sistemas sensíveis	Controle Sistemas sensíveis devem ter um ambiente computacional dedicado (isolado).
A.11.7 Computação móvel e trabalho remoto Objetivo: Garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto.		
A. 11.7.1	Computação e comunicação móvel	Controle Uma política formal deve ser estabelecida e medidas de segurança apropriadas devem ser adotadas para a proteção contra os riscos do uso de recursos de computação e comunicação móveis.
A.1 1.7.2	Trabalho remoto	Controle Uma política, planos operacionais e procedimentos devem ser desenvolvidos e implementados para atividades de trabalho remoto.
A.12 Aquisição, desenvolvimento e manutenção de sistemas de informação		
A.12.1 Requisitos de segurança de sistemas de informação Objetivo: Garantir que segurança é parte integrante de sistemas de informação.		
A. 12.1.1	Análise e especificação dos requisitos de segurança	Controle Devem ser especificados os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhorias em sistemas existentes.
A. 12.2 Processamento correto de aplicações Objetivo: Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.		
A .12.2.1	Validação dos dados de entrada	Controle Os dados de entrada de aplicações devem ser validados para garantir que são corretos e apropriados.

A.12.2.2	Controle do processamento interno	Controle Devem ser incorporadas, nas aplicações, checagens de validação com o objetivo de detectar qualquer corrupção de informações, por erros ou por ações deliberadas.
A.12.2.3	Integridade de mensagens	Controle Requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações devem ser identificados e os controles apropriados devem ser identificados e implementados.
A.12.2.4	Validação de dados de saída	Controle Os dados de saída das aplicações devem ser validados para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias.
A.12.3 Controles criptográficos Objetivo: Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos.		
A.12.3.1	Política para o uso de controles criptográficos	Controle Deve ser desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.
A.12.3.2	Gerenciamento de chaves	Controle Um processo de gerenciamento de chaves deve ser implantado para apoiar o uso de técnicas criptográficas pela organização.
A.12.4 Segurança dos arquivos do sistema Objetivo: Garantir a segurança de arquivos de sistema.		
A.12.4.1	Controle de software operacional	Controle Procedimentos para controlar a instalação de software em sistemas operacionais devem ser implementados.
A .12.4 .2	Proteção dos dados para teste de sistema	Controle Os dados de teste devem ser selecionados com cuidado, protegidos e controlados.

A.12.4.3	Controle de acesso ao código-fonte de programa	Controle O acesso ao código-fonte de programa deve ser restrito.
A. 12.5 Segurança em processos de desenvolvimento e de suporte Objetivo: Manter a segurança de sistemas aplicativos e da informação.		
A.12.5.1	Procedimentos para controle de mudanças	Controle A implementação de mudanças deve ser controlada utilizando procedimentos formais de controle de mudanças.
A.12.5.2	Análise crítica técnica das apli	Controle Aplicações críticas de negócios devem ser analisadas criticamente e testadas quando sistemas operacionais são mudados, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança.
A.12.5.3	Restrições sobre mudanças em pacotes de software	Controle Modificações em pacotes de software não devem ser incentivadas e devem estar limitadas às mudanças necessárias, e todas as mudanças devem ser estritamente controladas.
A.12.5.4	Vazamento de informações	Controle Oportunidades para vazamento de informações devem ser prevenidas.
A.12.5.5	Desenvolvimento terceirizado de software	Controle A organização deve supervisionar e monitorar o desenvolvimento terceirizado de software.
A.12.6 Gestão de vulnerabilidades técnicas Objetivo: Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.		

A.12.6.1	Controle de vulnerabilidades técnicas	Controle Deve ser obtida informação em tempo hábil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliada a exposição da organização a estas vulnerabilidades e tomadas as medidas apropriadas para lidar com os riscos associados.
A.13 Gestão de incidentes de segurança da informação		
A. 13.1 Notificação de fragilidades e eventos de segurança da informação Objetivo: Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.		
A.13.1 .1	Notificação de eventos de segurança da informação	Controle Os eventos de segurança da informação devem ser relatados através dos canais apropriados da direção, o mais rapidamente possível.
A. 13.1.2	Notificando fragilidades de segurança da informação	Controle Os funcionários, fornecedores e terceiros de sistemas e serviços de informação devem ser instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade em sistemas ou serviços.
A.13.2 Gestão de incidentes de segurança da informação e melhorias Objetivo: Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.		
A.13.2.1	Responsabilidades e procedimentos	Controle Responsabilidades e procedimentos de gestão devem ser estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.

A.13.2.2	Aprendendo com os incidentes de segurança da informação	Controle Devem ser estabelecidos mecanismos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorados.
A.13.2.3	Coleta de evidências	Controle Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), evidências devem ser coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição ou jurisdições pertinentes.
A.14 Gestão da continuidade do negócio		
A.14.1 Aspectos da gestão da continuidade do negócio, relativos à segurança da informação Objetivo: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.		
A.14.1.1	Incluindo segurança da informação no processo de gestão da continuidade de negócio	Controle Um processo de gestão deve ser desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio da organização.
A.14.1.2	Continuidade de negócios e análise/avaliação de risco	Controle Devem ser identificados os eventos que podem causar interrupções aos processos de negócio, junto à probabilidade e impacto de tais interrupções e as conseqüências para a segurança de informação.

A.14.1.3	Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação	Controle Os planos devem ser desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.
A. 14.1.4	Estrutura do plano de continuidade do negócio	Controle Uma estrutura básica dos planos de continuidade do negócio deve ser mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção.
A.14.1 .5	Testes, manutenção e reavaliação dos planos de continuidade do negócio	Controle Os planos de continuidade do negócio devem ser testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.
A.15 Conformidade		
A.15.1 Conformidade com requisitos legais Objetivo: Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação		
A. 15.1.1	Identificação da legislação vigente	Controle Todos os requisitos estatutários, regulamentares e contratuais relevantes, e o enfoque da organização para atender a estes requisitos devem ser explicitamente definidos, documentados e mantidos atualizados para cada sistema de informação da organização.

A. 15.1.2	Direitos de propriedade intelectual	Controle Procedimentos apropriados devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e sobre o uso de produtos de software proprietários.
A. 15.1.3	Proteção de registros organizacionais	Controle Registros importantes devem ser protegidos contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.
A. 15.1.4	Proteção de dados e privacidade da informação pessoal	Controle A privacidade e a proteção de dados devem ser asseguradas conforme exigido nas legislações relevantes, regulamentações e, se aplicável, nas cláusulas contratuais.
A. 15.1.5	Prevenção de mau uso de recursos de processamento da informação	Controle Os usuários devem ser dissuadidos de usar os recursos de processamento da informação para propósitos não autorizados.
A.15.1 .6	Regulamentação de controles de criptografia	Controle Controles de criptografia devem ser usados em conformidade com leis, acordos e regulamentações relevantes.
A.15.2 Conformidade com normas e políticas de segurança da informação e conformidade técnica Objetivo: Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.		

A.15.2.1	Conformidade com as políticas e normas de segurança da informação	Controle Os gestores devem garantir que todos os procedimentos de segurança dentro da sua área de responsabilidade sejam executados corretamente para atender à conformidade com as normas e políticas de segurança da informação.
A.15.2.2	Verificação da conformidade técnica	Controle Os sistemas de informação devem ser periodicamente verificados quanto à sua conformidade com as normas de segurança da informação implementadas.
A.15.3 Considerações quanto à auditoria de sistemas de informação Objetivo: Maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.		
A.15.3.1	Controles de auditoria de sistemas de informação	Controle Os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais devem ser cuidadosamente planejados e acordados para minimizar os riscos de interrupção dos processos do negócio.
A.15.3.2	Proteção de ferramentas de auditoria de sistemas de informação	Controle O acesso às ferramentas de auditoria de sistema de informação deve ser protegido para prevenir qualquer possibilidade de uso impróprio ou comprometimento.

A.15.3 Considerações quanto à auditoria de sistemas de informação Objetivo: Maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.		
A.15.3.1	Controles de auditoria de sistemas de informação	Controle Os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais devem ser cuidadosamente planejados e acordados para minimizar os riscos de interrupção dos processos do negócio.
A.15.3.2	Proteção de ferramentas de auditoria de sistemas de informação	Controle O acesso às ferramentas de auditoria de sistema de informação deve ser protegido para prevenir qualquer possibilidade de uso impróprio ou comprometimento.

Anexo A
(normativo)

Objetivos de controle e controles

Os objetivos de controle e controles listados na tabela A.1 são derivados diretamente e estão alinhados com aqueles listados na ABNT NBR ISO/IEC 17799:2005 – seções 5 a 15. As listas na tabela A.1 não são exaustivas e uma organização pode considerar que objetivos de controle e controles adicionais são necessários. Os objetivos de controle e controles desta tabela devem ser selecionados como parte do processo de SGSI especificado em 4.2.1.

A ABNT NBR ISO/IEC 17799:2005 - seções 5 a 15 fornece recomendações e um guia de implementação das melhores práticas para apoiar os controles especificados em A.5 a A. 15.

Tabela A.1 — Objetivos de controle e controles

 ©ABNT 2006 - Todos os direitos reservados

©ABNT 2006 - Todos os direitos reservados

Folha3

3)Explicação: O termo "proprietário" identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. O termo "proprietário" não significa que a pessoa realmente tenha qualquer direito de propriedade pelo ativo

4)Explicação: A palavra "contratação", neste contexto, visa cobrir todas as seguintes diferentes situações: contratação de pessoas (temporárias ou por longa duração), nomeação de funções, mudança de funções, atribuições de contratos e encerramento de quaisquer destas situações.

 ©ABNT 2006 - Todos os direitos reservados

Folha4

©ABNT 2006 - Todos os direitos reservados

Folha5

ABNT NBR ISO/IEC 27001:2006

Folha6

ABNT NBR ISO/IEC 27001:2006

Folha7

ABNT NBR ISO/IEC 27001:2006

Folha8

ABNT NBR ISO/IEC 27001:2006

Folha9

ABNT NBR ISO/IEC 27001:2006

Folha10

ABNT NBR ISO/IEC 27001:2006

Folha11

ABNT NBR ISO/IEC 27001:2006

Folha12

ABNT NBR ISO/IEC 27001:2006

Folha13

ABNT NBR ISO/IEC 27001:2006

Folha14

ABNT NBR ISO/IEC 27001:2006

Folha15

ABNT NBR ISO/IEC 27001:2006

Folha16

ABNT NBR ISO/IEC 27001:2006

Folha17

 ©ABNT 2008 - Todos os direitos reservados

APÊNDICE 2 - QUESTIONÁRIO

APÊNDICE 2 - QUESTIONÁRIO

CONTROLE	O Controle está implementado na sua organização?							
	Não se aplica	SIM	NÃO	Em parte	Desconheço	1 - Pouco relevante	2 - relevante se houver recursos	3 - Muito relevante, independente dos recursos necessários
Políticas de segurança da informação								
1) Sua organização possui uma política de segurança da informação (POSIC) definida, aprovada pela direção, publicada e comunicada para todos os funcionários e partes externas relevantes?								
2) Sua **POSIC** e os instrumentos normativos gerados a partir dela, são revisados sempre que se fizer necessário, **não excedendo o período máximo de 03(três) anos?**								
3) Sua POSIC instituiu ou sua organização possui:								
a) uma **estrutura** para a Gestão da Segurança da Informação e Comunicações?								
b) um **Gestor de Segurança da Informação e Comunicações**?								
c) um **Comitê de Segurança da Informação e Comunicações** do órgão ou entidade?								
d) uma **Equipe de Tratamento e Resposta a Incidentes** em Redes Computacionais – **ETIR**?								
Organização da segurança da informação								
4) Sua organização possui um processo de **Gestão de Riscos de Segurança da Informação**?								
Gestão de incidentes de segurança da informação								
5) A **Equipe de Tratamento e Resposta a Incidentes** – ETIR de sua organização:								
a) monitora e analisa tecnicamente os incidentes de segurança em redes de computadores emitindo alertas?								
b) comunica a ocorrência de incidentes de segurança da informação ao Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR Gov ou realiza a elaboração de relatório de comunicação do incidente para público interno e/ou externo?								
Em relação aos Incidentes de Segurança em Redes Computacionais:								
6) Sua organização possui procedimento formal de coleta e preservação de evidências na ocorrência de um incidente de Segurança da informação e comunicações – SIC?								
7) faz a sincronização da data, hora e fuso horário do relógio interno dos ativos de informação com a "Hora Legal Brasileira do Observatório Nacional (ON)?								
8) Os servidores de hospedagem de página eletrônica de sua organização estão configurados para armazenar registros históricos de eventos (*logs*) em formato que permita a completa identificação dos fluxos de dados?								
9) Havendo indícios de ilícitos criminais, a ETIR aciona as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários?								

APÊNDICE 2 - QUESTIONÁRIO

Continuidade da segurança da informação								
10) Sua organização possui procedimentos de continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre?								
11) Os controles de continuidade da segurança da informação são verificados a intervalos regulares, para garantir que eles sejam válidos e eficazes em situações adversas?								
12) Sua organização possui procedimentos e recursos para que o processamento da informação seja implementado com **redundância** suficiente para atender aos requisitos de disponibilidade?								
CONTROLES DE ACESSO								
13) Em relação à política de criação e administração de **contas de acesso** aos ativos de informação e a rede corporativa, sua organização:								
a) Possui **procedimento** que verifique se os **direitos de acesso** às informações e aos recursos de processamento da informação de todos os funcionários e partes externas **são retirados** logo após o **encerramento** de suas atividades, contratos ou acordos, ou ajustados após a mudança destas atividades?								
b) Utiliza o princípio do menor privilégio (direitos de acesso privilegiado, restritos e controlados) para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação?								
c) Utiliza autenticação de multifatores para o controle de acesso lógico, a fim de verificar a identidade de um usuário e vinculá-lo a uma conta de acesso a ativos de informação?								
d) O sistema de senhas assegura a criação de senhas de qualidade?								
14) Sua organização faz o registro/logs dos acessos à rede corporativa de computadores e dos serviços utilizados, inclusive acesso remoto, de forma a permitir a rastreabilidade e a identificação dos usuários?								
15) Sua organização possui procedimentos de segurança da informação para o trabalho remoto?								
16) Sua organização possui controles contra **acesso não autorizado** a sua rede e serviços, em especial:								
a) controles estabelecidos para proteção da **confidencialidade** e **integridade** dos dados que trafegam sobre redes públicas/redes sem fio (wireless) e dos sistemas e aplicações a elas conectadas?								
b) mecanismos apropriados de registro e monitoração para gravação e detecção de ações que possam afetar, ou ser relevante para a segurança da informação?								
17) Sua organização possui implementado:								
a) controles de detecção, prevenção e recuperação para proteção contra malware?								
b) um programa de conscientização do usuário contra malware?								
c) uma política de geração de cópias de segurança (cópias de segurança das informações, dos softwares e das imagens do sistema)?								
d) uma política de registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação?								

e) análise crítica dos logs a intervalos regulares?								
f) procedimentos para controlar a instalação de software em sistemas?								
18) Em relação às vulnerabilidades técnicas dos sistemas de informação em uso, sua organização possui procedimentos para verificar as vulnerabilidades em tempo hábil e tomar as medidas apropriadas para lidar com os riscos associados?								
19) Sua organização possui procedimento para que os registros estejam protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio?								
20) Quanto à arquitetura de redes, existe **segregação de redes entre grupos** (serviços de informação, usuários e sistemas de informação)?								
21) Sua organização possui uma política de uso da Internet, do correio eletrônico e de mensagens instantâneas?								
22) Possui mapa das **áreas e instalações** consideradas críticas, como ativos de informação de acordo com o valor, a criticidade, o tipo de ativo de informação e o grau de sigilo das informações que podem ser tratadas em tais áreas?								
23) Sua organização possui uma política de acesso as suas **áreas e instalações físicas**:								
a) com barreiras físicas de segurança, controle de entrada e saída para as áreas e instalações consideradas críticas ou para os ativos de informação?								
b) com área de recepção com regras claras para a entrada e saída de pessoas, equipamentos e materiais, pontos de entrega e carregamento de material com acesso exclusivo ao pessoal credenciado?								
c) possui sistemas de detecção de intrusos nas áreas e instalações de sua organização?								
d) possui normas específicas para o armazenamento, a veiculação de imagem, vídeo ou áudio, registrados em perímetros de segurança?								
24) Sua organização possui procedimentos ou requisitos de segurança da informação com a finalidade mitigar os riscos associados com o acesso dos fornecedores aos ativos ou aos componentes de infraestrutura de TI da organização?								
25) Em relação aos **equipamentos** relacionados à informação e à segurança da informação:								
a) encontram-se protegidos e colocados em locais para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado?								
b) Estão protegidos contra falta de energia elétrica e outras interrupções causadas por eventos externo?								
c) o cabeamento de energia e de telecomunicações que transporta dado ou dá suporte aos serviços de informações está protegido contra interceptação, interferência ou danos?								
d) possuem manutenção correta para assegurar a sua contínua integridade e disponibilidade?								
e) Existem medidas de segurança para ativos que operam fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da sua organização?								
f) Existem procedimentos formais para que todos os equipamentos com mídias de armazenamento de dados **sejam examinados** antes da reutilização, para assegurar que								

todos os dados sensíveis e *software* licenciados tenham sido removidos ou sobregravados com segurança?								
26) Sua organização classificou os ativos de informação em níveis de criticidade, considerando o tipo de ativo de informação, o provável impacto no caso de quebra de segurança, tomando como base a gestão de risco e a gestão de continuidade de negócios relativa aos aspectos da segurança da informação e comunicações?								
27) Sua organização estabeleceu distância mínima de segurança para manutenção das mídias contendo as cópias de segurança (backups)?								
28) Sua organização realiza testes periódicos de restauração das informações contidas nas cópias de segurança, a fim de garantir o seu uso na ocorrência de incidentes quando houver comprometimento das informações?								
29) Sua organização possui procedimentos para o gerenciamento de mídias removíveis, incluindo descarte e proteção contra acesso não autorizado, de acordo com o esquema de classificação adotado pela organização?								
30) Sua organização adota uma política de mesa limpa para papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação?								
Uso de recursos criptográficos								
31) Sua organização possui uma política formal:								
a) sobre o uso de controles criptográficos para a proteção da informação?								
b) sobre o uso, proteção e tempo de vida das chaves criptográficas ao longo de todo o seu ciclo de vida?								
32) Sua organização produz, armazena ou transmite informação classificada, em qualquer grau de sigilo, por meio eletrônico?								
33) Sua organização utiliza exclusivamente recurso criptográfico baseado em algoritmo de Estado em conformidade com os parâmetros e padrões mínimos estabelecidos na Norma Complementar nº 09/IN01/DSIC/GSIPR para **as informações classificadas em qualquer grau de sigilo**?								
34) Sua organização utiliza VPN com recurso criptográfico baseado em **algoritmo de Estado**?								
35) A cifração e decifração **das informações sigilosas** não classificadas utiliza recurso criptográfico, no mínimo, baseado em **algoritmo registrado**?								
Inventário dos ativos								
36) Sua organização possui um **processo formal de inventário e monitoramento de ativos de informação**? (Por exemplo, identificação e classificação de ativos de informação, responsáveis, proprietários e custodiantes de cada ativo de informação; caracterização dos contêineres dos ativos de informação; valor do ativo de informação; identificação de potenciais ameaças e vulnerabilidades e avaliação de riscos definição dos requisitos de segurança da informação e comunicações)								

Conformidade e auditoria								
37) Sua organização possui uma política de avaliação ou auditoria interna da conformidade em SIC? (Verificação dos controles da segurança da informação se estão em conformidade aos requisitos legais, estatutários, regulamentares, contratuais relacionados à segurança da informação).								
38) Existe previsão de programa de auditoria externa em sua organização, a intervalos planejados nos sistemas de informação, para verificação da conformidade com as normas e políticas de segurança da informação da organização?								
Dispositivos móveis								
39) Sua organização possui política de uso das redes sem fio?								
40) Sua organização possui procedimentos de controle e concessão de acesso a visitantes que durante a permanência em suas instalações, necessitem conectar seus dispositivos móveis a sua rede?								
41) Sua organização possui política de uso de dispositivos móveis corporativos?								
42) Sua organização possui uma política para uso de informações classificadas em dispositivos móveis removíveis de armazenamento?								
Gestão de Mudanças								
43) Sua organização possui um processo formal de **gestão de mudanças** que avalie os potenciais impactos à segurança da informação e comunicações que possam ocorrer durante a implementação da mudança?								
44) Esse processo verifica se o andamento e o resultado da mudança viabilizam e asseguram a disponibilidade, integridade, confidencialidade e autenticidade da informação?								
Redes Sociais								
45) Sua organização possui norma interna de segurança da informação relacionada ao uso de redes sociais no ambiente corporativo?								
Desenvolvimento e aquisição de Software Seguro								
46) Em relação ao **desenvolvimento** e **aquisição** de software seguro por sua organização:								
a) estão previstos formalmente pela sua organização requisitos relacionados à segurança da informação?								
b) constrói o software de forma que suas mensagens de erro não revelem detalhes da sua estrutura interna?								
c) possui controles da qualidade no desenvolvimento/aquisição de software ou procedimentos (p. ex.: análise estática e/ou análise dinâmica do software) com a finalidade de verificar o atendimento dos requisitos de segurança do software?								

d) possui procedimentos para configurar adequadamente o software desenvolvido/adquirido quando este passar para o ambiente de produção? (São exemplos: todo código de teste, de "backups" ou arquivos desnecessários, de informações sigilosas nos comentários de código e das contas criadas para teste devem ser removidos).								
e) existe procedimento formal para que a segurança da informação seja integrada nos métodos de gerenciamento de projeto da organização, e para assegurar que os riscos de segurança da informação estejam identificados e considerados como parte de um projeto?								
f) estabelece definições sobre a custódia de código-fonte e manutenção do software em caso de falha da empresa contratada?								
g) define regras e procedimentos operacionais para a contratada quanto à liberação de acesso aos recursos tecnológicos e ao ambiente físico ou lógico de sua organização, caso seja necessário?								
h) define as regras para transferência do conhecimento sobre o software desenvolvido/adquirido de modo a permitir a sua manutenção, de forma independente, por sua organização?								
i) estão previstos no instrumento contratual correspondente os procedimentos de segurança, como os descritos acima?								
j) os ambientes de desenvolvimento, teste e produção **são separados** para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção?								
Atuação e adequações para profissionais de SIC								
47) Quanto ao treinamento e certificações dos profissionais de SI, sua organização:								
a) promove ou participa de ciclo de palestras, seminários, cursos, reuniões e outros eventos nos áreas da SIC?								
b) mantém contato formal com fóruns, associações ou grupos especiais para conhecimento sobre as melhores práticas, receber previamente advertências de alertas, aconselhamentos e correções relativos a ataques e vulnerabilidades, trocar informações sobre novas tecnologias, produtos, ameaças ou vulnerabilidades?								
c) promove a capacitação dos profissionais de SIC, em âmbito interno e externo, preferencialmente alinhada às certificações profissionais presente no mercado de TI?								
48) A direção de sua organização solicita a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização?								
49) Sua organização possui uma política de conscientização dos controles e da POSIC – Política de Segurança da Informação?								
50) Sua organização possui um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação?								
51) Sua organização possui procedimento formal para verificar que as responsabilidades e obrigações pela segurança da informação permaneçam válidas após um encerramento ou mudança da contratação, e que estas responsabilidades sejam definidas, comunicadas aos								

funcionários ou partes externas e cumpridas?								
52) Sua organização possui regras para devolução dos ativos que estejam em posse de funcionários, após o encerramento de suas atividades, do contrato ou acordo.								
Classificação da informação								
53) Sua organização possui política ou procedimentos (relacionados à segurança da informação) de coleta, orientação, produção, armazenamento, disponibilização de informações **classificadas** ou **sigilosas** nos termos da Lei 12.527/2011 ou de outras legislações específicas, inclusive informações pessoais?								
54) Sua organização possui regulamentação do uso de impressoras e copiadoras, definindo as diretrizes para a impressão/cópia de documentos que contenham informação de **acesso restrito** (conforme definido pela sua organização ou pela legislação)?								

APÊNDICE 3 – CORRESPONDÊNCIA EXPLICATIVA

APÊNDICE 3 – CORRESPONDÊNCIA EXPLICATIVA

Bom dia,

Esta pesquisa faz parte da elaboração do trabalho de conclusão de curso da Especialização em Gestão de Segurança da Informação da Faculdade de Tecnologia da UNB, turma 2016/2017.

A pesquisa tem a finalidade de verificar a percepção dos gestores e usuários avançados de TI, quanto aos controles de segurança da informação implementados e utilizados em sua organização. Não é uma verificação da conformidade da organização com as normas e legislação.

questionário foi elaborado a partir dos 114 controles da NBR ISO 27002:2013 e das 21 normas complementares à IN 01 do Gabinete de Segurança Institucional – GSI, da Presidência da República.

São 54 perguntas sobre vários temas de segurança da informação, com foco de controles que sejam eficazes na melhoria da segurança da informação na administração pública.

Não são abordados no questionário especificações técnicas de protocolos de redes ou da arquitetura **ePING** – Padrões de Interoperabilidade de Governo Eletrônico.

Orientações quanto ao preenchimento:

Escolha uma opção (marque um "X") quanto à implementação do controle em sua organização (Sim; Não; "Em parte implementado", "não se aplica"; e "desconheço se foi implementado") e uma opção quanto à relevância do controle para sua organização ("1 - Pouco relevante "; relevante se houver recursos "; Muito relevante, independente dos recursos necessários ").

Termo de Confidencialidade

O pesquisador do projeto assume o compromisso de:

1. Preservar o sigilo e a privacidade dos sujeitos e organizações cujos dados serão estudados;

2. Assegurar que as informações serão utilizadas, única e exclusivamente, para a execução do projeto em questão;

3. Assegurar que os resultados da pesquisa somente serão divulgados de forma anônima, não sendo usadas iniciais ou quaisquer outras indicações que possam identificar o sujeito da pesquisa.

Conceitos:

Algoritmo de Estado: função matemática utilizada na cifração e na decifração de informações sigilosas, necessariamente as informações classificadas, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, não comercializável.

Algoritmo Registrado: função matemática utilizada na cifração e na decifração de informações não classificadas, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, cujo código fonte e método de processo sejam passíveis de controle e auditoria

.

Análise Dinâmica: tipo de teste de software que verifica seu comportamento externo em busca de anomalias ou vulnerabilidades. A análise dinâmica ocorre por meio de interações com o software em execução.

Análise Estática: tipo de teste de software que verifica sua lógica interna em busca de falhas ou vulnerabilidades. A análise estática ocorre por meio da verificação do código-fonte ou dos binários

.

Ativos de Informação - os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

Contêiner: local onde "vive" o ativo de informação, onde está armazenado, como é transportado ou processado

.

Informação classificada – A LAI prevê que tais informações podem ser classificadas como reservadas, secretas e ultrassecretas, conforme estabelecido no art. 23 da Lei.

Política de mesa limpa e tela limpa se refere a práticas relacionadas a assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos (e.g., notebooks, celulares, tablets, etc.) não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso, ou quando alguém deixa sua área de trabalho, seja por um curto período de tempo ou ao final do dia.

Agradeço desde já

Cláudio Z umpichiatte Miranda
Celular: 98147-9816

APÊNDICE 4 - Normas da família NBR ISO/IEC 27000

APÊNDICE 4 - Normas da família NBR ISO/IEC 27000 (PALMA, 2014)

NBR ISO/IEC 27000:2009	Sistema de Gerenciamento de Segurança - Explicação da série de normas, objetivos e vocabulários
NBR ISO/IEC 27001:2013	Sistema de Gestão de Segurança da Informação – Requisitos
NBR ISO/IEC 27002:2013	Boas práticas para controles de segurança da informação
NBR ISO/IEC 27003:2011	Guia de implantação do Sistema de Gestão de Segurança da Informação
NBR ISO/IEC 27004:2010	Gestão da segurança da informação – Medição
NBR ISO/IEC 27005: 2011	Gestão de risco em segurança da informação
ISO/IEC 27006 (inglês)	Requisitos para empresas de auditoria e certificação de Sistemas de Gestão de Segurança da Informação
NBR ISO/IEC 27007:2012	Diretrizes para auditoria em Sistemas de Gestão de Segurança da Informação
NBR ISO/IEC 27008:2012	Diretrizes para auditores sobre controle de segurança da informação
ISO/IEC 27009 (inglês)	Norma apoia a industrias específicas pretendem trabalhar orientadas às normas ISO 27000.
ISO/IEC 27010	Gestão de segurança da informação para comunicação intersetorial e interorganizacional
NBR ISO/IEC 27011:2009	Diretrizes para gestão de segurança da informação em organizações de telecomunicação com base na ISO/IEC 27002
ISO/IEC 27013	Diretrizes para a implementação integrada da ISO/IEC 27001 e ISO/IEC 20000-1
NBR ISO/IEC 27014:2013	Governança de segurança da informação

Fonte: site: www.abnt.org.br

ISO/IEC TR 27015	Diretrizes para a gestão de segurança da informação em serviços financeiros
ISO/IEC TR 27016	Diretrizes para a gestão de segurança da informação – Empresas de economia
ISO/IEC 27015	Aborda a gestão da segurança da informação para serviços financeiros. Pode ser interpretada como uma norma que fornece controles e diretrizes complementares a ISO 27002 para empresas e departamentos deste segmento.
ISO/IEC 27016	O mesmo raciocínio da 27015, só que para o setor de economia.
ISO/IEC 27017	Controles específicos para cloud computing.
ISO/IEC 27018	Cobre especificamente a privacidade (PII Personally Identifiable Information) para serviços em cloud computing . Como podemos interpretar, é uma norma que complementa a ISO 27017.
ISO 27019	Controles específicos para industria de energia.
ISO 27031	Propõe um guia de princípios/conceitos por trás do papel da segurança da informação para TIC no sentido de garantir a continuidade dos negócios. Inclui diretrizes de mensuração do nível de proteção da organização para a gestão da continuidade na ótica da tecnologia e comunicação.
ISO 27032	Aborda "Cybersecurity". Está em sua definição a preservação da confidencialidade, integridade e disponibilidade da informação em " Cyberspace ".
ISO 27033-1	Esta é uma das 06 partes da norma 27033. O conjunto de normas 27033-1 a 27033-6 são derivadas das 05 partes da norma de segurança em redes 18028. A ISO 27033-1 trata sobre a introdução e conceitos gerais para segurança em redes.
ISO 27033-2	Guia para o planejamento, desenho, implementação e documentação da segurança em redes.
ISO 27033-3	Tem o objetivo de definir os riscos específicos, técnicas de projetos e controles relacionados a segurança em redes.
ISO 27033-4	Propõe uma visão geral e requisitos para identificação e análise de ameaças

	para a segurança da informação relacionadas a gateways de segurança da informação que compõem a arquitetura de segurança em redes.
ISO 27033-5	Protegendo a comunicação entre redes usando Virtual Private Networks (VPNs).
ISO 27033-6	Define riscos, técnicas de projeto e desenho e controles específicos para a segurança da informação em redes sem fio e rádio.
ISO 27034-1	Segurança da informação em aplicações - parte 01. Nesta primeira parte, é definida e abordada uma introdução e conceitos. As partes 02 a 06 encontram-se em desenvolvimento, mas já é possível obter informações sobre elas, conforme descrições a seguir.
ISO 27034-2	Segurança da informação em aplicações - parte 02. A segunda parte trata sobre a organização normativa para segurança em aplicações.
ISO 27034-3	Guia para o processo de gestão da segurança em aplicações.
ISO 27034-4	Validação de requisitos de segurança em aplicações.
ISO 27034-5	Protocolos e estrutura de dados de controle de segurança de aplicativos.
ISO 27034-6	Guia de segurança da informação para aplicações específicas

Nota: as próximas normas especificam em maiores detalhes muitas das seções da norma ISO 27002

ISO 27035	Guia detalhado para a gestão de incidentes de segurança da informação, cobrindo o processo de mapeamento de eventos, incidentes e vulnerabilidades em de segurança.
ISO 27036	Segurança da informação para o relacionamento com fornecedores. Oferece orientações sobre a avaliação e tratamento de riscos de segurança da informação envolvidos na aquisição de informações ou produtos relacionados com as TIC (Tecnologia de Informação e Comunicação) de outras organizações.

Nota: as duas próximas normas (ISO 27037 e ISO 27038) tratam sobre segurança forense, e este tema volta a ser citado nas normas ISO 27041 e ISO 27042 ". Já as ISO 27038 e ISO 27039 tratam sobre ferramentas que automatizam atividades para SI.

ISO 27037	Orientações para a identificação, coleta, aquisição e preservação de evidências forenses digitais. Esta norma está focada na manutenção da integridade destas evidências. Sem dúvidas, uma das normas mais relevantes para profissionais que seguem ou pretendem seguir carreira de perito
ISO 27038	Especificação para redação digital. Uma norma qual considero bem interessante por conta do seu grau de especificidade, pois trata sobre requisitos para a redação e compartilhamento da informação digital de forma adequada, seja ela publicada internamente na organização ou a partes externas.
ISO 27039	Detecção de intrusos. Um guia para seleção, contratação, desenho, operação e administração de sistemas IDS.
ISO 27040	Aspectos de segurança da informação para sistemas e Infraestrutura de storage.
ISO 27041	Regula sobre a conformidade para métodos de investigação de evidências digitais, sendo mais uma norma entre as disponíveis para análise forense computacional/ segurança forense.
ISO 27042	Mais uma entre as normas forenses, sendo que esta prevê diretrizes para a análise e interpretação de evidências digitais. Existem especulações de que todas estas normas forenses sejam reestruturadas, no futuro, em uma norma

APÊNDICE 4 - Normas da família NBR ISO/IEC 27000 (PALMA, 2014)

	com diversas partes assim como está definida a ISO 27034.
ISO 27043	Princípios e processo de investigação de incidentes da segurança da informação. Esta é mais uma norma voltada exclusivamente para gestão de incidentes de segurança, assim como a ISO 27035.
ISO 27044	Diretrizes específicas para o Gerenciamento de Eventos de Segurança da Informação (SIEM).
ISO 27799	Gerenciamento de segurança da informação para a área de saúde.
ISO/IEC 27050	Esta norma ainda está em fase de elaboração (informação atualizada em Novembro de 2016). Versa sobre padrões forenses digitais com objetivo de contribuir para a captura de evidências digitais. Será lançada como uma continuação de outras normas da família que já tratam do tema.

Fonte: (PALMA, 2014) https://www.portalgsti.com.br/2013/12/as-normas-da-familia-iso-27000.html