UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
PROGRAMA DE PÓS-GRADUAÇÃO PROFISSIONALIZANTE EM PATRIMÔNIO CULTURAL

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA ESTRATÉGIA PARA GARANTIR A PROTEÇÃO E A INTEGRIDADE DAS INFORMAÇÕES ARQUIVÍSTICAS NO DEPARTAMENTO DE ARQUIVO GERAL DA UFSM

DISSERTAÇÃO DE MESTRADO

Josiane Ayres Sfreddo

Santa Maria, RS, Brasil
2012

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:

UMA ESTRATÉGIA PARA GARANTIR A PROTEÇÃO E A INTEGRIDADE DAS INFORMAÇÕES ARQUIVÍSTICAS NO DEPARTAMENTO DE ARQUIVO GERAL DA UFSM

Josiane Ayres Sfreddo

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-Graduação Profissionalizante em Patrimônio Cultural, Área de Concentração em História e Patrimônio Cultural da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de

Mestre em Patrimônio Cultural

Orientador: Profº. Dr. Andre Z. Cordenonsi

Santa Maria, RS, Brasil

2012

Ficha catalográfica elaborada através do Programa de Geração Automática da Biblioteca Central da UFSM, com os dados fornecidos pelo(a) autor(a).

Sfreddo, Josiane Ayres
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA ESTRATÉGIA PARA GARANTIR A PROTEÇÃO E A INTEGRIDADE DAS INFORMAÇÕES ARQUIVÍSTICAS NO DEPARTAMENTO DE ARQUIVO GERAL DA UFSM / Josiane Ayres Sfreddo.-2012.
206 p.; 30cm

Orientador: Andre Zanki Cordenonsi
Dissertação (mestrado) - Universidade Federal de Santa Maria, Centro de Ciências Sociais e Humanas, Programa de Pós-Graduação Profissionalizante em Patrimônio Cultural, RS, 2012

1. Política de Segurança da Informação 2. Segurança da Informação 3. Informação Arquivística não digital 4. Arquivística 5. Patrimônio Documental I. Cordenonsi, Andre Zanki II. Título.

Universidade Federal de Santa Maria
Centro de Ciências Sociais e Humanas
Programa de Pós-Graduação Profissionalizante
em Patrimônio Cultural

A Comissão Examinadora, abaixo assinada,
aprova a Dissertação de Mestrado

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA ESTRATÉGIA PARA GARANTIR A PROTEÇÃO E A INTEGRIDADE DAS INFORMAÇÕES ARQUIVÍSTICAS NO DEPARTAMENTO DE ARQUIVO GERAL DA UFSM

elaborada por
Josiane Ayres Sfreddo

como requisito parcial para obtenção do grau de
Mestre em Patrimônio Cultural

COMISSÃO EXAMINADORA:

Andre Zanki Cordenonsi, Dr.
(Presidente/Orientador)

Daniel Flores, Dr. (UFSM)

Glaucia Vieira Ramos Konrad, Dra. (UFSM)

Santa Maria, 06 de dezembro de 2012.

DEDICATÓRIA

Aos meus pais, por terem me ensinado os maiores valores da vida, além de terem acreditado e incentivado a realização deste sonho.

AGRADECIMENTOS

Agradeço, em primeiro lugar, ao Divino Pai Eterno pela saúde e pela força que me concedeu, para que conseguisse chegar até aqui.

Ao Professor Andre Zanki Cordenonsi, meu orientador, pela competência científica e acompanhamento do trabalho, pela disponibilidade e generosidade reveladas, assim como pelas críticas, correções e sugestões relevantes feitas durante a orientação.

À Professora Glaucia Vieira Ramos Konrad e ao Professor Daniel Flores, componentes da banca examinadora, pelas orientações desde o exame de qualificação, buscando garantir que esta pesquisa alcançasse o seu objetivo.

Ao Programa de Pós-Graduação Profissionalizante em Patrimônio Cultural da Universidade Federal de Santa Maria (UFSM) e todos seus professores, por oportunizar a realização de meu aperfeiçoamento profissional.

A direção e funcionários do Departamento de Arquivo Geral da UFSM pela ajuda no acesso às informações e contribuição para a realização desta pesquisa.

Aos meus pais, Hermes e Rosane pela educação, base para minha vida, por todo o amor, dedicação, paciência e confiança.

À minha avó Anna Edy, pelos seus conselhos, incentivos e suas lições de vida.

Ao meu noivo Pablo, pela colaboração e compreensão e por ser um verdadeiro amigo e companheiro em todos os momentos que passamos juntos.

À amiga e colega de mestrado Priscila Linassi pela atenção e auxílio dados no desenvolvimento deste trabalho.

Enfim, a todas as pessoas que contribuíram direta ou indiretamente, para a concretização desta dissertação.

EPÍGRAFE

Existe uma antiga piada, contada mais ou menos assim:

Um guarda de segurança que trabalha no turno da noite em uma fábrica vê um homem baixinho sair do prédio, empurrando um carrinho de mão vazio. O guarda, com uma suspeita repentina, pára o homem, que pergunta por que está sendo parado. “Apenas quero ter certeza de que você não está roubando nada”, diz o guarda de forma grosseira. “Confira tudo o que quiser”, responde o homem, e o guarda procura, mas não encontra nada suspeito e permite que o homem vá embora. Na noite seguinte, acontece à mesma coisa. Isso se repete por algumas semanas e então o baixinho não aparece mais no portão.
Passam vinte anos e o guarda, já aposentado, está sentado em um bar, quando o baixinho entra. Reconhecendo-o, o guarda aposentado se aproxima, explica quem é e oferece pagar uma bebida, se o baixinho responder a uma pergunta. O homem concorda e o guarda diz: “Tenho certeza de que você estava levando algo, mas nunca consegui descobrir o que você estava roubando”. O baixinho pegou a bebida e, enquanto levava o copo à boca, disse: ”Eu estava roubando carrinhos de mão”.

A ideia dessa piada sugere, é claro, que as medidas de segurança nada representarão se os guardas não souberem o que deverão proteger.

(Marcos Aurelio Pchek Laureano)

RESUMO

Dissertação de Mestrado
Programa de Pós-Graduação Profissionalizante em Patrimônio Cultural
Universidade Federal de Santa Maria

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA ESTRATÉGIA PARA GARANTIR A PROTEÇÃO E A INTEGRIDADE DAS INFORMAÇÕES ARQUIVÍSTICAS NO DEPARTAMENTO DE ARQUIVO GERAL DA UFSM

AUTORA: JOSIANE AYRES SFREDDO
ORIENTADOR: ANDRE ZANKI CORDENONSI
Data e Local da Defesa: Santa Maria/RS, 06 de dezembro de 2012.

Apresenta um estudo sobre a segurança da informação a fim de propor uma Política de Segurança da Informação para o Departamento de Arquivo Geral (DAG) da Universidade Federal de Santa Maria (UFSM), possibilitando a proteção, a disponibilidade e o acesso seguro às informações arquivísticas (não digitais), no contexto universitário. Caracteriza-se como uma pesquisa exploratória com abordagem qualitativa, assumindo a forma de estudo de caso, pois envolve o estudo sobre um determinado assunto permitindo o seu amplo e detalhado conhecimento. Primeiramente foi realizado um estudo mais aprofundado da Norma ABNT NBR ISO/IEC 27002 que é um código de prática para a segurança da informação, apresentando diretrizes para a aplicação de uma Política de Segurança da Informação, baseada em regulamentos de acordo com os propósitos institucionais. O estudo objetivou, em um primeiro momento, adaptar os requisitos e controles presentes nessa norma ao contexto arquivístico, tendo como foco a proteção de informação não digital, caracterizando, deste modo, uma pesquisa na linha do Patrimônio Documental. Assim, a Adaptação da Norma para a arquivologia seguiu a estrutura da Norma original, buscando proporcionar às instituições arquivísticas um instrumento que subsidiasse a elaboração de uma Política de Segurança da Informação, possibilitando a proteção de informações não digitais de uma forma mais segura e confiável. Para a composição dessa Política, foi realizada a coleta de dados por meio de entrevista estruturada com questões sobre a segurança da informação, fundamentada na Norma ABNT NBR ISO/IEC 27002, tendo como base o estudo anterior e a Adaptação da Norma para o contexto arquivístico. Com a análise dos dados coletados junto ao DAG, pode-se verificar que os problemas que causam ameaças à segurança da informação não digital no departamento estão relacionados diretamente à deficiência dos perímetros de segurança e à inexistência de um controle de acesso físico incluindo entradas e saídas. A partir dessas ações de segurança, foi possível, juntamente com a Adaptação da Norma, propor controles a serem aplicados a fim de evitar a ocorrência de novos incidentes. Dessa forma, foi possível estruturar o Documento da Política de Segurança da Informação representando a materialização da Política de Segurança de acordo com as necessidades apresentadas pelo DAG. Esse documento servirá com um instrumento de apoio fundamental para instruir funcionários, usuários e terceiros na realização das atividades institucionais. No entanto, cabe ao departamento aprová-lo e implementá-lo, a fim de prevenir incidentes proporcionando, assim, acesso seguro, confiável e contínuo às informações não digitais por ele custodiadas.

Palavras-chave: Política de Segurança da Informação. Segurança da informação. Informação Arquivística não digital. Patrimônio documental.

ABSTRACT

Dissertation of Master's Degree
Graduate Professionalization Program in Cultural Heritage
Federal University of Santa Maria

INFORMATION SECURITY POLICY: A STRATEGY TO ENSURE THE SECURITY AND INTEGRITY OF THE DEPARTMENT OF ARCHIVAL INFORMATION IN THE GENERAL ARCHIVING DEPARTMENT OF THE UFSM

AUTHORESS: JOSIANE AYRES SFREDDO
ADVISOR: ANDRE ZANKI CORDENONSI
Date and Location of Defense: Santa Maria, December, 06th, 2012.

Presents a study on information security in order to propose an Information Security Policy for the Department of General Archives (DAG), Federal University of Santa Maria (UFSM) as a way of enabling the protection, availability and secure access to archival information (not digital), in the university context. It is characterized as an exploratory qualitative approach, assuming a case study form, because it involves the study of a certain subject allowing its wide and detailed knowledge. It was first conducted a more detailed study of the Standard ISO/IEC 27002 which is a code of practice for information security, providing guidelines for the implementation of an Information Security Policy, based on regulations according to the institutional purposes. The study aimed, at first, to adapt the requirements and controls present in this standard archival context, focusing on the protection of not digital information, a research in the Heritage Documentary line. Thus, the adaptation of the standard for archival followed the structure of the original standard, seeking to provide for the archival institutions a tool to subsidize the development of an Information Security Policy, providing a more secure and reliable protection. In order to compose this policy a data collection was carried out through interviews, structured within questions about security information, based on the standard ISO/IEC 27002, on the previous study and the Adaptation of the Standard for the archival context. With the data collected and analyzed, along with the DAG, it can be verified that the problems causer of threats to the security of not digital archives in the department are directly related to the lack of security to the perimeter and to the absence of a physical control, including entries and exits. These security actions made it possible, together with the adaption of the standard, to propose control in order to prevent further incidents. This way it was possible to structure the Document of the Security Policy representing the materialization of the Security Policy according to the needs presented by DAG. This document will serve as an instrument to support and guide employees, users and third parties in the conduct of institutional activities. However, it is up to the department to approve it and implement it for the purpose of preventing incidents, thereby providing safe reliable and continuous access to not digital information by him guarded.

Keywords: Information Security Policy. Information Security. Archival Information not digital. Documentary Heritage.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT NBR ISO/IEC 27002 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação

CCSC - *Commercial Computer Secury Cente*

CD - *Compact Disc*,

CONARQ - Conselho Nacional de Arquivos

CPAD - Comissão Permanente de Avaliação de Documentos

D.C - Depois de Cristo

DAG - Departamento de Arquivo Geral

DTI - *UK Depertament of Trade and Industry*

DVD - *Digital Versatile Disk*

E-Arq - Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos

FATEC - Fundação de Apoio a Tecnologia e Ciência

GED - Gestão Eletrônica de Documentos

ICMS - *International Committee for Museum Security*

IFES - Instituições Federais Ensino Superior

INMETRO - Instituto Nacional de Metrologia, Normalização e Qualidade Industrial

ISO - *International Organization for Standardization*

ISO 15489 - *Information and Documentation – Records Management*

MAST - Museu de Astronomia e Ciências Afins

MEC - Ministério de Educação

NR - Norma Reguladora

PCO - Plano de Continuidade Operacional

PGC - Plano de Gerenciamento de Crises

PRD - Plano de Recuperação de Desastres

PROINFRA - Pró-Reitoria de Infraestrutura

PSI - Política de Segurança da Informação

QBASI - Questionário Básico de Avaliação da Segurança da Informação

SIE - Sistema de Informações Educacionais

SINAR - Sistema Nacional de Arquivos

TI - Tecnologia da Informação

UCP - Unidade de Coordenação de Programas

UFSM - Universidade federal de Santa Maria

UNICAMP - Universidade Estadual de Campinas

LISTA DE ANEXOS

LISTA DE APÊNDICES

SUMÁRIO

1 INTRODUÇÃO

A segurança é um assunto bastante discutido nos dias de hoje, porém, pouco planejado quando faz referência aos bens de informação. A informação, independente de seu formato, dentro do contexto institucional, pode ser considerada um dos maiores patrimônios do mundo moderno. Considerada fundamental para o desenvolvimento organizacional, ela deve ser gerenciada e protegida. As empresas se preocupam com a segurança dos equipamentos, do prédio e esquecem muitas vezes da segurança das pessoas envolvidas nas atividades de gestão e também na informação que circula em meio institucional.

Dessa forma, os profissionais da informação devem ressaltar a necessidade da aplicação de programas específicos para proteção das informações. Dentro de um contexto arquivístico onde os documentos contêm informações essenciais para o funcionamento institucional, a responsabilidade pela gestão destes documentos deve ser igual à responsabilidade em protegê-los. Ao realizar atividades para a gestão documental, uma instituição não deve preocupar-se somente com a guarda e a preservação das informações contidas nos documentos.

A segurança dos processos de gestão é fundamental para prevenir ameaças advindas do furto, das falsificações documentais e uso inadequado da informação, colocando em risco a confiabilidade das informações que serão acessadas pelos usuários. Além dessas circunstâncias, as instituições estão sujeitas a outras circunstâncias que podem afetar a segurança das informações, pessoas, equipamentos e ambiente institucional, tais como: incêndios, alagamentos, problemas elétricos, entre outros.

Para que o acesso a essas informações se torne confiável e seguro, faz-se necessário o desenvolvimento de ações para a proteção da instituição, evitando, assim, incidentes em segurança da informação. Essas ações referem-se à aplicação de controles ligados a rotina diária dentro da instituição que só serão efetivados se conhecidos e incorporados pelos funcionários e usuários de informação. A responsabilidade não está somente em controlar os processos de gestão, mas também em monitorar a gestão das pessoas envolvidas nas atividades institucionais, seja funcionário, usuários ou terceiros, fazendo com que eles se responsabilizem pela segurança na instituição e contribuam para que ela se efetive.

Portanto, pode-se salientar que embora não exista um modelo de segurança totalmente garantido, torna-se necessário, num primeiro momento, verificar quais são os pontos mais vulneráveis de segurança dentro de uma instituição e, a partir daí, avaliar os riscos que podem provocar incidentes em segurança da informação e, assim, procurar implementar ações a fim de evitá-los. Para que a segurança se efetive é recomendada a elaboração de um programa de segurança de informação e/ou uma política que englobe todas as ações necessárias para minimizar problemas decorrentes da falta de proteção.

A Política de Segurança da Informação (PSI) é composta por um conjunto formal de regras que definem procedimentos de segurança adequados, de acordo com a realidade institucional, realizadas no sentido de garantir a proteção e disponibilidade das informações, proporcionando seu acesso confiável e contínuo. O arquivista, como gestor da informação, assume o papel de proporcionar o acesso seguro aos documentos institucionais. E para que esse objetivo se efetive, ele deve realizar ações a fim de monitorar as atividades desenvolvidas e garantir que a instituição alcance seus objetivos, assegurando a qualidade nos serviços prestados. Assim, a adoção de ações para a segurança da informação em instituições arquivísticas é primordial para proteger e garantir a integridade do patrimônio documental.

Dentro deste contexto, esta pesquisa traz como tema: Política de Segurança da Informação: uma estratégia para garantir a proteção e integridade das informações arquivísticas no Departamento de Arquivo Geral[1] (DAG) da Universidade Federal de Santa Maria (UFSM). A concepção do tema deste projeto de dissertação se deu com a realização da pesquisa para obtenção do grau de especialista em Gestão em Arquivos, defendida em julho de 2010. Cujo tema foi a segurança da informação. Este estudo proporcionou o conhecimento da Norma ABNT NBR ISO/IEC 27002, que é um código de prática para a segurança da informação e apresenta diretrizes para a aplicação de uma Política de Segurança da Informação, baseada em regulamentos e de acordo com os propósitos institucionais.

A questão segurança da informação por si só é muito abrangente e, desta forma, a pesquisa delimita-se em propor uma Política de Segurança da Informação, dentro de um contexto arquivístico universitário, no intuito de garantir a proteção e a integridade das informações arquivísticas (não digitais) do Departamento de Arquivo Geral da UFSM.

[1] Para evitar a repetição do termo completo, será adotada a sua correspondente abreviação DAG.

Para isso, terá como principal referencial os pressupostos teóricos da Norma ABNT NBR ISO/IEC 27002 estando em consonância com a legislação em vigor e diretrizes institucionais que sejam relevantes para a composição desta política.

1.1 Problema

A presente pesquisa tem como proposta a elaboração de uma política de segurança da informação para o DAG objetivando a proteção e a integridade das informações arquivísticas não digitais. Para isso, a questão que norteia esta pesquisa é:

- Que ações podem ser realizadas a fim de evitar a ocorrência de incidentes em segurança da informação, no Departamento de Arquivo Geral da UFSM, em conformidade com a Norma ABNT NBR ISO/IEC 27002?

1.2 Hipótese

A hipótese que orienta esta pesquisa é de que a elaboração de uma Política de Segurança da Informação para o DAG auxiliará na proteção e integridade das informações arquivísticas não digitais (analógicas), prevenindo o acontecimento de incidentes que comprometem a segurança das informações no departamento.

1.3 Objetivos

1.3.1 Objetivo geral

O objetivo geral desta pesquisa é elaborar uma Política de Segurança da Informação para o Departamento de Arquivo Geral da Universidade Federal de Santa Maria, para

contribuir na disponibilidade, integridade e confidencialidade das informações arquivísticas (não digitais) proporcionando, assim, o acesso seguro aos documentos.

1.3.2 Objetivos específicos

- Adaptar os controles de segurança da informação presentes na Norma ABNT NBR ISO/IEC 27002, a fim de reduzir os riscos em segurança da informação em arquivos;

- identificar os problemas que causam ameaças à segurança da informação arquivística no DAG;

- desenvolver o Documento da Política de Segurança da Informação, de acordo com a realidade da instituição, seguindo as diretrizes da Norma ABNT NBR ISO/IEC 27002.

1.4 Justificativa

A questão da segurança da informação passou a ser um assunto muito debatido e planejado nas grandes empresas e instituições cujo objetivo principal é evitar problemas futuros relacionados à falta de proteção. Dessa preocupação com o tratamento e a segurança da informação foram surgindo procedimentos para que as instituições possam adotar controles a fim de reduzir os riscos em segurança da informação.

O Departamento de Arquivo Geral é responsável pela coordenação do sistema de arquivos na UFSM, mantendo sob sua guarda os documentos procedentes das atividades dos órgãos administrativos e das unidades de ensino, pesquisa e extensão. A proposta deste estudo é desenvolver uma Política de Segurança da Informação possibilitando a proteção das informações arquivísticas (não digitais) no contexto universitário do Departamento de Arquivo Geral da UFSM – DAG, utilizando os pressupostos teóricos da Norma ABNT NBR ISO/IEC 27002. A relevância desta pesquisa está em possibilitar a proteção do patrimônio documental da UFSM custodiado pelo DAG, visando o acesso das informações arquivísticas de uma forma confiável e segura.

Para isso objetiva-se, em um primeiro momento, estudar a Norma ABNT NBR ISO/IEC 27002 para compreender os controles referenciados nela a fim de adaptá-los para o contexto arquivístico. A informação não digital, ainda representa a maior quantidade de volume documental nas instituições e a inexistência de uma norma arquivística para a segurança dessa informação também justifica a realização desta pesquisa. Além disso, adaptar os requisitos da Norma para um contexto arquivístico possibilitará verificar e amenizar os riscos que causam incidentes em segurança da informação voltado ao contexto de arquivos universitários. Assim, esta pesquisa servirá de referencial para que outras universidades possam elaborar a sua política de segurança da informação.

É relevante destacar que na maioria das instituições, a falta de recursos acaba por não permitir que se dê a atenção necessária a questões de segurança da informação. Em decorrência desse fato, a falta de conhecimento e conscientização sobre o assunto pode agravar o problema. A bibliografia a respeito da segurança de informação na área arquivística é quase inexistente, dificultando ainda mais a aplicação de ações para a proteção das informações.

Dessa forma, os resultados desta investigação servirão de referencial teórico a respeito da segurança da informação em arquivos, contribuindo para amenizar a carência de material bibliográfico sobre o tema proposto, reforçando assim a relevância da realização desta pesquisa para o contexto arquivístico.

1.5 Estrutura da dissertação

Este trabalho está estruturado da seguinte maneira: o Capítulo um (1) é composto pela introdução da pesquisa trazendo o problema; a hipótese; os objetivos que a norteiam e justificativa de sua execução. Em seguida, o Capítulo dois (2) apresenta-se com o referencial teórico com a fundamentação dos conceitos relacionados aos arquivos e a informação arquivista; arquivos universitários; patrimônio documental; segurança da informação e a Norma ABNT NBR ISO 27002 a fim de melhor esclarecer o tema de pesquisa. Já no Capítulo três (3) são apresentadas algumas colocações sobre o histórico, atividades desenvolvidas e a relevância do DAG para a transparência administrativa e fluxo das atividades na UFSM. No

Capítulo quatro (4) trás a metodologia utilizada para a realização da pesquisa. O Capítulo cinco (5) apresenta a análise e adaptação da Norma ABNT NBR ISO/IEC 27002 para a segurança das informações arquivísticas (não digitais). O Capítulo seis (6) por sua vez, trás a análise e discussão dos resultados coletados junto ao DAG, apresentando a da Política de Segurança da Informação elaborada para o departamento. E por fim, são apresentadas as conclusões de pesquisa e as referências utilizadas para a construção da mesma.

A revisão da bibliografia, apresentada no capítulo dois (2), serve como forma de explicitar o tema proposto através da compilação de teorias, estudos e autores relevantes para a compreensão e desenvolvimento da pesquisa.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 A informação arquivística

A Arquivologia é responsável pela conservação e organização dos documentos como, também, da informação arquivística contida neles e preservada nos arquivos. Brito (2005) salienta que a arquivística faz parte da ciência da informação, sendo considerada como ciência desde que gere conhecimentos que possam ser verificados. O autor relata ainda que, a informação arquivística está sendo considerada um objeto de estudo da arquivologia em substituição aos documentos de arquivos.

Todo arquivo é constituído de informações, portanto, nos documentos encontramos a informação registrada. Santos, Innarelli e Souza (2007) afirmam que esta informação, contida no documento de arquivo, é resultante de uma atividade que o produziu e, por isso, essa informação torna-se vinculada a ela. Neste sentido, as informações de cunho arquivístico desempenham um papel fundamental na construção da história, sendo um alicerce importante para o conhecimento de fatos desconhecidos e fundamentais na organização de uma pesquisa. A informação arquivística pode ainda "comprovar direitos; dar suporte ao ensino e à aprendizagem ou, simplesmente informar" (CASTANHO, GARCIA e SILVA, 2006, p. 10).

No entanto, as informações orgânicas armazenada em arquivos:

> Possuem a competência para produzir conhecimento, mas que só se efetiva a partir de uma ação de comunicação mutuamente consentida entre a fonte (os estoques) e o receptor. Porém, a produção dos estoques de informação não possui um compromisso direto e final com a produção de conhecimento, que permite uma ação de desenvolvimento em diferentes níveis. (BARRETO, 1994, p. 2).

Neste sentido o autor descreve que a disponibilidade desta informação dependerá do acesso concedido a ela, ou seja, "o produtor de informação tem condições de manipular a disponibilidade e o acesso à informação" (BARRETO, 1994, p. 9). A informação só resultará em conhecimento se disponibilizada, se utilizada pelos usuários. O acesso é indispensável para transformar esta informação em algo palpável, assim, esta informação somente contribuirá no desenvolvimento institucional se o acesso a ela for garantido.

O acesso é um direito e disponibilizá-lo é um dever dos gestores da informação, neste caso aos arquivistas, ou seja, um dos serviços que devem ser realizados pelos arquivistas é garantir que as informações permaneçam acessíveis aos usuários. Assim, o acesso à informação contida nos documentos torna-se relevante, pois evidencia também a transparência das atividades. A informação arquivística torna-se um instrumento de apoio à decisão, indispensável para que as instituições realizem as ações de gestão de uma forma mais eficaz possibilitando maior desempenho no desenvolvimento das atividades.

A Legislação Brasileira trás diretrizes que regulamentam o acesso as informações. As principais leis utilizadas que se refere ao acesso a documentos e comumente são aplicadas em instituições arquivísticas são: a Lei brasileira de nº 8.159, de 08 de janeiro de 1991 e a Lei nº 11.111/2005. A primeira dispõe sobre a política nacional de arquivos públicos e privados, considera a gestão de documentos como dever do Poder Público, assim como a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação.

Nesta Lei "considera-se gestão de documentos o conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente" (BRASIL, 1991, Art. 3). Na forma desta lei, a gestão de documentos compreende todas as ações empregadas durante qualquer fase do ciclo de vida dos documentos, seja qual for o suporte em que esteja registrada a informação.

A segunda, Lei nº 11.111/2005, "dispõe sobre a instituição, no âmbito da Casa Civil, de "Comissão de Averiguação e análise de Informações Sigilosas, com a finalidade de decidir sobre a aplicação e ressalva ao acesso dos documentos" (Art. 4º) e ratifica os prazos estabelecidos pela lei 8.159/91" (SANTOS, 2005, p. 86). Ainda referente a legislação arquivística, pode-se citar o decreto Nº 4.553, de 27 de Dezembro de 2002 que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras Providências.

A informação arquivística (como o documento de arquivo) deve ser autêntica e fidedigna garantindo, assim, a segurança na transmissão das informações. Para tanto é relevante não apenas cumprir as determinações legais referentes aos direitos e deveres de

acesso, mas também estar atentos às regras e normas internas adotadas na instituição a fim de proteger e garantir o acesso seguro e continuo aos documentos. A ciência que garante o estudo da estrutura formal dos documentos é a diplomática; ela "estuda as partes que compõem os documentos produzidos por entidades públicas e privadas no desempenho de suas funções, com fins de crítica sobre a autenticidade" (RICHTER, 2004, p. 87).

Vale ressaltar que os profissionais da informação, antes de analisarem os documentos do ponto de vista técnico a fim de conferirem sua autenticidade, devem proporcionar que esta informação tenha condições de se manter autêntica. Dessa forma, a segurança das informações em instituições arquivísticas contribuirá no acesso, mas, principalmente, para garantir a confiabilidade das informações, mantendo-as íntegras, seguras e confiáveis. E, para isso, é fundamental a aplicação de políticas públicas no ambiente arquivístico a fim de proporcionar a padronização dos processos contribuindo para o desenvolvimento das instituições arquivísticas priorizando o acesso e a segurança da informação.

2.1.1 Suportes da informação

Desde as comunidades primitivas o homem sente a necessidade de registrar seus pensamentos e impressões a respeito do mundo. Como exemplo disto, pode-se citar os registros encontrados nas paredes das cavernas com pinturas e desenhos que representavam o cotidiano em que viviam. Esses primeiros registros contribuíram para que o mundo conhecesse a escrita.

Na Idade Antiga, o homem utilizou outros suportes que eram encontrados na natureza e tinham o objetivo de "registrar a visualidade ou sua escrita, como a argila, ossos, conchas, marfim, folhas de palmeiras, bambu, metal, cascas de árvores, madeira, couro, papiro, velino, pergaminho, seda, e finalmente, o papel" (BARATA, 2000, p. 1). Apesar do conhecimento dos diferentes suportes utilizados para a escrita, apenas o papiro e o pergaminho foram os suportes mais utilizados, de cuja evolução culminou na criação do papel.

O papel, foi inventado na antiga China por volta do ano 150 d.C. (depois de Cristo), inicialmente feito a partir de fibras de bambu e da seda. A criação do papel possibilitou a "difusão da escrita que anteriormente era limita a um pequeno grupo monástico, tendo em

vista os custos que eram altos para se ter acesso a suportes como o papiro e o pergaminho" (FARIAS, et. al. 2010, p. 9). Com o passar dos anos, o papel, sofreu modificações a respeito de sua estrutura e produção, chegando ao Brasil somente no ano de 1809.

A invenção das máquinas de produção consecutivas significou um grande estímulo para a indústria do papel. O surgimento da fábrica de papel em bobinas, no início do século XIX, foi o grande marco que alavancou a produção de papel a nível industrial. Mesmo assim, a técnica da produção do papel artesanal, ainda hoje, é difundida e muito realizada no Brasil por profissionais de artes plásticas. (GONÇALVES, 2008).

É importante ressaltar que "há cerca de vinte mil anos o homem exprime o seu pensamento através de meios gráficos, e há mais ou menos seis mil anos que conhece as formas de escrita" (QUEIROZ, 2005, p. 13). Mesmo assim, pode-se dizer que "o papel como suporte para escrita é o material mais usado nos dias de hoje, embora haja ainda a permanência de outros materiais" (REGINATO, 2003, p. 2).

A escrita e seus suportes sofreram diversas modificações no decorrer dos anos que, juntamente com as evoluções tecnológicas, contribuíram para que se modificassem, também, os mecanismos de registros. O mecanismo de registros considerado uma inovação, foi o computador. Desde o século XX, até os dias de hoje, as tecnologias computacionais vem apresentando impressionantes evoluções de velocidade e de memória. Como resultado desse desenvolvimento temos os diferentes "aparelhos, variadas invenções, técnicas, programas operacionais e sistemas que potencializam, facilitam e dinamizam a vida do homem em sua prática política, social, econômica e cultural" (PRADO, 2008, p.1).

Pedro (1996) relata que o papel seria o suporte mais seguro, já que, segundo a autora, é possível identificar o efeito da borracha ou do corretivo, pois uma vez que ao apagar algo no papel, nesse fica gravado as impressões. O mesmo não aconteceria com os suportes magnéticos, sendo difícil identificar uma modificação. No entanto, com a evolução tecnológica e uso de suportes informatizados para escrita, editores de texto e meio digitais, começou-se a pensar não somente na preservação destes suportes, a fim que garantir que as informações permaneçam acessíveis, mas também na segurança e integridade das informações neles armazenada.

Nesse sentido, Rondinelli (2005) afirma que, os documentos em suporte de papel e a informação que contém não podem ser separados, diferentemente dos suportes digitais (os

dispositivo compactos de armazenamento como: CD *(Compact Disc)*, DVD *(Digital Versatile Disk)* e *pen drive)*, onde a parte física é separada do conteúdo. No caso da documentação digital, qualquer perda pode ser considerada catastrófica, pois "o maior problema da preservação dos dados digitais não é a fragilidade dos suportes de armazenamento e sim a rápida mudança de tecnologia" (FUNDAÇÃO OSWALDO CRUZ, 2009, p. 17).

A preservação de documentos digitais requer muito mais do que ações preventivas; necessita de cuidados permanentes. É necessário, também, o uso de um equipamento que possibilite sua leitura e acesso, além disso, deve-se garantir que as informações possam ser recuperadas. A durabilidade do documento em suporte digital está condicionada a obsolescência tecnológica, por isso, a migração periódica de suporte para tecnologias mais atualizadas é fundamental para evitar a perda de informação.

2.1.2 Políticas públicas arquivísticas e o patrimônio documental

> Políticas Públicas podem ser entendidas como o conjunto de planos e programas de ação governamental voltados à intervenção no domínio social, por meio dos quais são traçadas as diretrizes e metas a serem fomentadas pelo Estado, sobretudo na implementação dos objetivos e direitos fundamentais dispostos na Constituição. As políticas públicas funcionam como instrumentos de aglutinação de interesses em torno de objetivos comuns, que passam a estruturar uma coletividade de interesses. Toda política pública é um instrumento de planejamento, racionalização e participação popular. Os elementos das políticas públicas são o fim da ação governamental, as metas nas quais se desdobra esse fim, os meios alocados para a realização das metas e, finalmente, os processos de sua realização. As Políticas Públicas podem ser compreendidas como respostas do Estado aos direitos coletivos da população. (SOUSA, 2006, p.3).

Na Arquivologia, as políticas públicas arquivísticas constituem uma das dimensões das políticas públicas informacionais. No Brasil, a política nacional de arquivos sugere diversas questões à pesquisa em Ciência da Informação. O Conselho Nacional de Arquivos (CONARQ) é um órgão colegiado e vinculado ao Arquivo Nacional da Casa Civil da Presidência da República, criado em 1991 incumbido de definir uma política nacional de arquivos e atuar como órgão central de um Sistema Nacional de Arquivos (SINAR). (JARDIM, 2008).

Desde sua criação, o CONARQ desenvolve diversas ações referentes à gestão documental. No entanto, não existe legalmente uma política nacional de arquivos o que acarreta dificuldades no desenvolvimento de atividades realizadas pelo Estado. Com a criação de uma política pública arquivística, legalmente registrada, seria possível padronizar os processos de gestão documental utilizados em instituições participantes do CONARQ, ampliando os direitos e obrigações dos cidadãos. Uma política de arquivos eficaz é aquela que atende as necessidades institucionais referentes ao acesso, recuperação, conservação e todos os outros processos realizados desde a produção até a destinação final dos documentos.

A ausência de políticas públicas também ocorre na área de preservação do patrimônio cultural, no qual se insere o patrimônio arquivístico provocando, muitas vezes, a destruição de acervos arquivísticos que seriam fundamentais tanto para a produção do conhecimento histórico, como para a construção da identidade local e exercício da cidadania, incluindo o direito de acesso à informação. Nesse contexto, Rodrigues (2000, p. 145) afirma que, "por meio do patrimônio as sociedades criam formas de representação do passado nas quais se justificam valores que fundamentam as relações sociais no presente; ele é um lugar de memória que permite compor imagens que sustentam identidades individuais e coletivas". E assim, "um povo que não guarda suas histórias, suas memórias, seu patrimônio, não sabe quem realmente é" (STANGER, 2009, p. 2).

Para isso, torna-se fundamental a aplicação de iniciativas que contribuam para a proteção do patrimônio. A questão legal de proteção do patrimônio cultural está presente na Constituição Federal, e em seu art. 23, incisos III descreve que é competência comum da União, dos Estados, do Distrito Federal e dos Municípios proteger os documentos, as obras e outros bens de valor histórico, artístico e cultural, os monumentos, as paisagens naturais notáveis e os sítios arqueológicos. (BRASIL, 1988). De acordo com a mesma constituição os documentos foram elevados à categoria de patrimônio cultural brasileiro, determinando ao poder público a sua promoção e proteção. Assim, o patrimônio documental pode ser:

> Um único documento de qualquer tipo ou um grupo de documentos, tais como uma coleção, um acervo ou fundos arquivísticos. Uma coleção é um conjunto de documentos selecionados individualmente. Um fundo é uma coleção ou série de coleções que obram em poder de uma instituição ou uma pessoa, ou um fundo ou conjunto de documentos, ou uma série de documentos que obra em poder de um arquivo. Estas instituições podem ser bibliotecas, arquivos, organizações de tipo educativo, religioso e histórico, museus, organismos oficiais e centros culturais. (BRASIL, 2002, p. 12).

Conforme Pereira, et. al. (2010) pode-se perceber que, o patrimônio documental é da mesma forma um patrimônio cultural devendo ser protegido possibilitando a identificação da cultura de um povo e a herança do passado para as gerações que virão. Por isso, faz-se necessário a aplicação de iniciativas que possibilitem a preservação do patrimônio documental a fim de possibilitar às gerações futuras o acesso continuo a essas memórias.

Sendo assim, uma iniciativa que contribuiria para a preservação de acervos documentais seria priorizar pela conservação dos documentos originais, pois conforme Brasil (2002. p. 16) "os documentos originais possuem, frequentemente, um valor intrínseco que uma cópia jamais terá". Assim, quando se conserva um documento original e protege-se sua integridade, nenhuma informação será perdida, possibilitando a preservação futura e acesso contínuo aos documentos.

2.2 Arquivos Públicos em Universidades Federais

> As Instituições Federais Ensino Superior (IFES) são constituídas sob a forma de autarquia federal, vinculadas ao Ministério da Educação. Por princípio constitucional, são públicas e gratuitas em todos os cursos ofertados e, como tais, são obrigadas a cumprir a legislação federal a elas aplicada, pois são regidas pelos princípios publicistas previstos na Constituição Federal, no Decreto-lei nº 200/67, na Lei 8.666/93, que institui normas para licitações e contratos com a administração pública, no Decreto nº 93.872/86 e outras. A realização da receita e despesa da União, disciplinada pelo Ministério da Fazenda, deve ter seu produto recolhido à conta do Tesouro Nacional em conta única no Banco do Brasil (Decreto-lei 1.755/79, art. 1º.). As IFES podem, segundo a legislação, contratar por prazo determinado Fundações de Apoio para contribuir nos seus projetos de pesquisas, ensino, extensão e desenvolvimento institucional, sendo elas de direito privado, sem fins lucrativos e regidas pelo Código Civil Brasileiro, em especial a fiscalização pelo Ministério Público. (TAFFAREL, 2009, p. 1).

As IFES são instituições públicas cujas atividades fim são o ensino, a pesquisa, a extensão e a cultura. Dessa forma, seus objetivos, funções e estruturas administrativas encontram-se presentes em seus estatutos e regimentos. A sua manutenção depende dos recursos provenientes do governo federal, complementados com recursos de prestação de serviços, convênios e também de projetos.

Deste modo, pode-se dizer que as IFES possuem características próprias em relação a outras instituições, em função de sua constituição, finalidades e área de atuação. Para isto suas

atividades devem ser organizadas e planejadas para que seus recursos sejam usados para cumprimento de suas atividades de ensino a pesquisa e extensão da melhor forma possível. (SERVILHA, 1995). Neste sentido, Stallivieri (2008) afirma ainda que somente as universidades e os centros universitários possuem autonomia para criar e implantar novos cursos e programas de mestrado e doutorado. Já as faculdades, faculdades integradas, escolas ou institutos superiores a implantação de cursos de pós-graduação está sujeita à autorização do Ministério de Educação (MEC).

Para tanto, a "abrangência nacional das IFES constitui-se em importante fator de redistribuição da riqueza nacional, por permitir a formação de profissionais altamente qualificados em todo o território nacional, além de desenvolver atividades de pós-graduação, pesquisa e de extensão locais" (BRASIL, 2008, p. 14). Além disso, as instituições públicas de ensino superior mostram-se importante para o desenvolvimento econômico e social no Brasil, já que são responsáveis pela maioria da produção científica do País.

O surgimento dos arquivos se deu devido à "necessidade que o homem tinha de registrar e difundir informações relacionadas ao seu tempo, a gerações futuras, organizando-as de acordo com as técnicas possíveis ou existentes em sua época" (HORA, SATURNINO E SANTOS, 2010, p. 1). A preocupação em guardar e preservar os registros do estado e os documentos produzidos como prova de direitos ou obrigações foi aumentando com o passar dos anos.

No entanto, somente "a partir do século XIX o Arquivo, como instituição ganhou espaço. Tal fato ocorreu quando este passou a ser considerado como base de pesquisa histórica, levando os Estados a mantê-los acessíveis a todos os cidadãos" (Silva, et. al., 2009, p. 2). Essa visão foi modificada após a Segunda Guerra Mundial, pois para Silva, et. al. (2009, p. 2) apud Ohira (2000?) com a "inclusão do direito à informação na Declaração dos Direitos Humanos de 1948", o acesso aos documentos torna-se um direito público e não somente base para pesquisa histórica.

Em decorrência deste processo surgem os arquivos públicos, cujos direitos são regidos pela Lei do Arquivo nº 8.159 de 08 de janeiro de 1991, sendo definidos como "um conjunto de documentos produzidos e recebidos, no exercício de suas atividades, por órgãos públicos de âmbito federal, estadual, do Distrito Federal e municipal em decorrência de suas funções administrativas, legislativas e judiciárias". Entre os arquivos públicos a nível federal, é

necessário enfatizar a importância e necessidade de implementação de arquivos universitários não somente para a difusão dos conhecimentos, mas também para a preservação da memória coletiva. Por isso, torna-se fundamental elaborar medidas que possibilitem a preservação e o acesso às informações universitárias. Assim, o arquivo universitário realiza um papel muito importante como fonte de pesquisa e de preservação do patrimônio documental das universidades, cabendo aos profissionais da informação possibilitar o acesso e a preservação continua a estes documentos.

Vale lembrar que a responsabilidade pela organização de arquivos universitários no Brasil só foi despertada na comunidade arquivística "a partir da realização em 1991, do 1º Seminário Nacional de Arquivos Universitários, promovido pela Coordenadoria do Sistema de Arquivos da Universidade Estadual de Campinas – UNICAMP" (OHIRA, 2004, p. 2). A realização deste evento despertou na comunidade arquivística uma nova visão dos arquivos universitários, dando-lhes a importância de um arquivo especializado, como guardião da memória e difusor de conhecimentos.

A Universidade deve ter por meta a busca, difusão e preservação do conhecimento através do ensino, da pesquisa e da extensão. Assim, a preservação do Arquivo Universitário torna-se relevante tanto para docentes e discentes quanto para a sociedade em geral. A universidade deve ser vista como uma coletividade de pessoas buscando o avanço do saber para o bem da comunidade universitária e sociedade envolvida no meio universitário. (ZUBEN, 2006). Dessa forma Belloto (1989, p. 23-24), complementa que o papel fundamental dos arquivos universitários são:

> 1- reunir, processar, divulgar e conservar todos os documentos relativos à administração, histórica e ao funcionamento/desenvolvimento da universidade;
> 2- avaliar e descrever estes documentos tornando possível seu acesso, segundo as políticas e procedimentos elaborados especificamente para estes fins;
> 3- supervisionar eliminação, ter o controle da aplicação das tabelas de temporalidade, a fim de que nenhum documento de valor permanente seja destruído.
> Disto tudo depreende-se seu segundo grande papel que é o de:
> 1- fornecer aos administradores as informações requeridas ao menor prazo possível;
> 2- fazer as demandas de informação e de pesquisa requer-se do serviço de arquivos universitários que proponha e coordene a uniformização de métodos de classificação de documentos dentro das unidades universitárias com afinidade de recuperação acelerada dos documentos necessários aos administradores.

E, para que esses papéis sejam cumpridos é imprescindível que a universidade tenha conhecimento e consciência das necessidades destas funções para o funcionamento institucional. E, para isso, faz-se necessário a implementação de um sistema de gestão documental, que respeite o ciclo vital dos documentos (desde a criação do documento até a eliminação ou guarda permanente), as restrições legais e procedimentos estabelecidos pela instituição, sendo aplicado em todos os setores da mesma. (BOSO, 2007).

Para implantar um sistema de gestão documental seja em ambiente universitário (público) ou em ambiente privado, é necessário ter o apoio e o conhecimento da instituição, pois a gestão contribuirá no desempenho de suas atividades. Um sistema de gestão facilita o processo documental, pois, por meio da avaliação, evitará o acúmulo de documentos ou eliminação não criteriosa que acarretaria na perda de informações importantes para o desenvolvimento institucional. O processo de gestão envolve todas as ações desde a produção até a destinação final dos documentos, buscando a racionalização e acesso facilitado às informações.

Indolfo (1995) enfatiza que a atividade da gestão documental torna-se importante não somente para a instituição que a realiza, mas também para o funcionamento do país, pois além de controlar o fluxo informacional, define a destinação e a preservação dos documentos públicos e privados. Segundo o Arquivo Nacional (2004, slide 11) "a realidade arquivística brasileira aponta, cada vez mais, para a necessidade de sistematização dos processos de tratamento, controle, guarda e acesso aos documentos". Entretanto, para implantar atividades de gestão documental, é necessário contar com o apoio e consentimento da instituição, que irá sistematizá-las.

Por fim, para preservar a memória presente em arquivos sejam eles universitários, ou quaisquer outros, se faz necessário à aplicação de sistemas de gestão documental e informacional. Além disso, é imprescindível a cooperação e auxílio "de todos os agentes geradores, utilizadores e gestores dessa informação, até que as decisões estejam tomadas e o conteúdo informativo da documentação adquira, se for caso disso, valor permanente como fonte de investigação e cultura" (LIMA, 2004, p. 81).

2.3 Segurança da informação

Antes de elaborar medidas que garantam a segurança da informação, é necessário que a instituição elabore uma política de gestão de documentos e, dentro dessa, um dos objetivos deve ser tornar acessível os documentos aos usuários. É necessário salientar que "a segurança da informação evoca a proteção dos ativos da informação, sistemas, recursos e serviços contra desastres, erros, uso indevido, roubos, manipulação não autorizada, visando minimizar os danos ao negócio e maximar o retorno dos investimentos e das oportunidades de negócio" (CAPEMISA, 2008, p. 2).

Os problemas de segurança da informação acontecem quando há quebra nos princípios que norteiam as atividades realizadas nas organizações. Essa quebra é denominada, na área da segurança da informação, como um incidente de segurança da informação. Um sistema de segurança da informação eficiente se baseia em princípios ou características que norteiam seus processos. Segundo a Norma ABNT NBR ISO/IEC 27002 os princípios seriam: confidencialidade, integridade e disponibilidade.

- Confidencialidade: Garantir que as informações sejam acessíveis somente a pessoas que possuam permissão para acesso na instituição;

- Integridade*:* Proporcionar a proteção das informações contra modificações, adulterações ou fraudes;

- Disponibilidade*:* Assegurar que os usuários autorizados tenham acesso às informações quando requisitadas, e estas, se mantenham protegidas e não se tornem indisponíveis.

Aliadas a estes princípios podem estar, ainda, a autenticidade, responsabilidade, não repúdio e confiabilidade. As instituições devem ter a responsabilidade e o interesse pelo tratamento das informações, conscientes que esses princípios que norteiam suas ações para a segurança ajudam a proteger as informações institucionais.

Quando o assunto é segurança, seja a pesquisa realizada em fontes como revistas, livros ou artigos que abordem o assunto, o termo *ativo* é sempre relacionado. Para compreender melhor o que seriam os ativos de segurança é relevante fazer sua relação a um bem material ou imaterial que pertençam à instituição. Nesse sentido, seguindo Campos (2007) o ativo pode ser definido como um bem patrimonial em função do seu valor, e da

mesma forma a informação e tudo aquilo que a suporta e/ou a utiliza são considerados ativos de informação. Campos (2007) afirma, ainda, que os ativos de informação podem ser classificados em tecnologias, processos, pessoas e ambientes cujas fraquezas, podem resultar em incidentes em segurança da informação.

Os ativos, quando dispersos em ambiente institucional, estão sujeitos a diversos problemas que podem colocar em risco a sua segurança. Esses problemas estão "divididos em três categorias: ameaças, vulnerabilidades e incidentes, os quais compõem e caracterizam os riscos" (MARCIANO, 2006, p. 47). E para evitá-los é necessário reconhecer no ambiente institucional as ameaças e vulnerabilidades para que, assim, se possam criar ações a fim de combatê-las.

> A ameaça pode ser definida como qualquer ação, acontecimento ou entidade que possa agir sobre um ativo, processo ou pessoa, através de uma vulnerabilidade e conseqüentemente gerando um determinado impacto. As ameaças apenas existem se houverem vulnerabilidades, sozinhas pouco fazem. (LAUREANO, 2005, p. 15).

Para Campos (2007, p. 25) "a ameaça é um agente externo ao ativo de informação, que se aproveitando de suas vulnerabilidades poderá quebrar a confidencialidade, integridade ou disponibilidade da informação suportada ou utilizada por esse ativo". Deste modo, as ameaças estão diretamente relacionadas à perda dos princípios de segurança da informação.

2.3.1 Segurança da informação arquivística

A informação arquivística pode ser armazenada em diversas formas. Ela pode estar em papéis, documentos impressos, eletronicamente em banco de dados, em imagens ou em vídeos. Independente do meio através do qual a informação é registrada ou difundida, é recomendado que ela seja adequadamente protegida. Entretanto, muitas vezes, a importância da informação só é reconhecida "quando é destruída, perdida ou até roubada" (ESPÍRITO SANTO, 2010, p. 2).

Para evitar que essas situações aconteçam principalmente em arquivos onde a gama de informações é significativa, devendo ser preservada e difundida, as instituições devem realizar

ações a fim de possibilitar o cuidado e a segurança das informações, sejam elas digitais ou não digitais. Mesmo assim, o mais comum em instituições arquivísticas ou não arquivísticas são os cuidados referentes à segurança das informações eletrônicas/digitais (ou em meio eletrônico/digital), cujos incidentes em segurança da informação são mais frequentes do que com documentos em suporte papel (não digitais).

Mesmo assim, no Brasil, a Gestão Eletrônica de Documentos (GED) é menos comum do que nos países mais desenvolvidos, devido aos custos com equipamentos informáticos, ou até mesmo pela falta de interesse por parte do governo de investir em tecnologia. A Arquivística reconhecida atualmente como parte da ciência da informação lida com a metodologia e teorias para o tratamento não somente dos documentos, mas sim, com a informação contida neles.

A bibliografia a respeito da segurança da informação é muito escassa quando se refere à segurança da informação na área arquivística. Uma contribuição importante para a área veio do Museu de Astronomia e Ciências Afins (MAST), que publicou um caderno com diretrizes de políticas de âmbito nacional, podendo ser adotadas por qualquer instituição encarregada da preservação de acervos culturais. Esse caderno pode servir como referência para a implantação de ações a fim de elaborar uma política de segurança em arquivos, bibliotecas e museus.

A realização deste caderno surgiu através de uma pesquisa baseada em documentos do Comitê Internacional para Segurança em Museus (*International Committee for Museum Security – ICMS)*, na "Política de Preservação de Acervos Institucionais", e no "Manual Básico de Segurança em Museus". A segurança do acervo é referenciada no capítulo 5 da publicação. O texto de apresentação do caderno deixa claro que cada instituição deve utilizar as diretrizes que acharem necessárias, de acordo com sua realidade. (BRASIL, 2006).

Sfreddo (2008) corrobora que para a segurança de informações arquivística, o controle de acesso é um dos fatores que contribuem para monitorar as ações realizadas na instituição e assim proteger as informações. O controle de acesso também é citado em normas arquivísticas de gestão de documentos como e-Arq e a ISO 15489, que fazem referência a esse requisito esclarecendo que se adotado de forma eficaz e cuidadosa pode evitar vários danos à massa documental e à própria instituição.

O controle de acesso são regras das quais "as organizações têm de poder controlar quem está autorizado a aceder aos documentos de arquivo e em que circunstâncias o acesso é permitido, dado que os documentos podem conter informação pessoal, comercial ou operacionalmente sensível" [2]. Assim, nas instituições arquivísticas, o controle de acesso tem como finalidade controlar o acesso de modo a proteger a informação, os sistemas, o equipamento e o ambiente institucional do acesso não autorizado de usuários e/ou funcionários.

Para a Câmara Técnica de Documentos Eletrônicos (2006), o controle do acesso é uma medida que deve ser realizada a fim de monitorar o acervo documental possibilitando a proteção e segurança das informações contidas nos documentos. O controle pode ser feito por meio do cadastro dos usuários (identificador de usuário), crachá de identificação (credenciais de autenticação), ou até mesmo pela restrição do espaço do acervo a uso exclusivo dos funcionários autorizados (autorização de acesso).

Outro ponto relevante no que tange o controle de acesso é a classificação da informação quanto ao grau de sigilo e restrição de acesso à informação. Essa medida pode evitar que as informações sensíveis sejam acessadas. A respeito disso, a Norma ISO 15489-1, relata que as instituições devem criar normas ou regras formalizadas que direcionem as restrições, permissões e condições de acesso às informações. As restrições de acesso devem ser aplicadas tanto aos funcionários quanto a usuários externos e necessitam ser revisadas periodicamente, pois podem variar ao longo do tempo.

Para os sistemas informatizados o uso e a manutenção de senhas é uma medida que deve ser adotada e cuidadosamente planejada nas instituições, possibilitando acesso seguro aos documentos. As senhas devem ser individuais, a fim de identificar quem teve acesso às informações. Além do uso de senhas, as instituições podem - e devem - adotar medidas como as cópias de segurança, a criptografia e a assinatura digital (para informações eletrônicas/digitais), de modo a preservar a autenticidade das informações que serão controladas e protegidas.

A proteção da instituição arquivo também é muito relevante quando se refere a segurança da informação. Para a completa proteção de uma instituição é relevante a instalação de um sistema de segurança patrimonial, contemplando o uso de câmeras de segurança e

[2] INSTITUTO DOS ARQUIVOS NACIONAIS/TORRE DO TOMBO, 2002, p. 40

sistemas de alarmes, para evitar roubos e controlar a movimentação no arquivo. Para proteção do acervo, “durante o período de fechamento das instituições, a melhor proteção é feita com alarmes e detectores internos” (Cassares, 2000, p. 23). Essa medida, se adotada pelas instituições, evitará possíveis problemas e controlar a movimentação da instituição principalmente à noite.

2.3.2 Política de segurança da informação

Para que o gerenciamento das informações se torne eficaz e seguro, faz-se necessário o planejamento de medidas de segurança adotadas como forma de evitar o acesso não autorizado e garantir a confiabilidade das informações que circulam no meio institucional. De acordo com Baldissera (2007, p. 56) a implantação de uma Política de Segurança da Informação “surge da necessidade de declaração de regras para: o acesso à informação; o uso da tecnologia da organização; e o tratamento, manuseio e proteção de dados e sistemas informacionais”.

A Política de Segurança da Informação para ser aplicada deve seguir algumas orientações de Spanceski (2004, p. 38) fazendo referência a NBR ISO 17799 afirmando ser:

> Definição de segurança da informação, resumo das metas e escopo e a importância da segurança como um mecanismo que habilita o compartilhamento da informação.
> Declaração do comprometimento da alta direção, apoiando as metas e princípios da segurança da informação.
> Breve explanação das políticas, princípios, padrões e requisitos de conformidade de importância específica para a organização, por exemplo:
> Definição das responsabilidades gerais e especificas na gestão de segurança da informação, incluindo o registro dos incidentes de segurança.
> Referência à documentação que possam apoiar a política, por exemplo, políticas, normas e procedimentos de segurança mais detalhados de sistemas, áreas específicas, ou regras de segurança que os usuários devem seguir.

A política de segurança da informação varia de instituição para instituição de acordo com os objetivos e metas de cada organização. O interesse em evitar problemas com a segurança das informações deve partir da própria instituição, seguindo as medidas que melhor atendam as necessidades de segurança, em consonância com a legislação vigente, regulamentos e normas internas estabelecidas pela própria instituição.

De uma forma geral, a política de segurança é um documento contendo diretrizes a serem seguidas pela organização a fim de proteger as pessoas, o acervo e a própria instituição. E para isso ela "deve ser descrita de forma clara e objetiva e ser amplamente divulgada em todas as suas unidades. É a maneira como a instituição se posiciona perante as questões de segurança" (BRASIL, 2006, p. 98).

Para Nakamura (2007) os fatores que podem ser considerados importantes para possibilitar a eficácia da Política de Segurança são:

- **Vigilância**: os membros da instituição devem compreender a importância da segurança para a mesma, monitorando constantemente os sistemas e a rede;

- **Atitude**: os funcionários da organização devem compreender da importância da Política de Segurança da Informação para instituição e realizar ações para sua aplicação;

- **Estratégia**: definir planos de defesa em caso de riscos em segurança da informação;

- **Tecnologia**: a solução tecnológica deve ser adaptativa e flexível, a fim de suprir as necessidades estratégicas da organização.

A política de Segurança da Informação foi estabelecida em lei pelo Decreto 3.505, de 13 de junho de 2000. Este decreto institui a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal. Vale ressaltar que este decreto refere-se exclusivamente a informações digitais. O que pode ser verificado no artigo 3º que define os objetivos da política de segurança da informação:

> I - dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;
>
> II - eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;
>
> III - promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;
>
> IV - estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação;
>
> V - promover as ações necessárias à implementação e manutenção da segurança da informação;
>
> VI - promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação;

> VII - promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação; e
>
> VIII - assegurar a interoperabilidade entre os sistemas de segurança da informação.

Mesmo assim, ressalta-se a importância em proteger e preservar as informações contidas em documentos de formato analógico possibilitando, de uma forma confiável, a sua conversão para o formato digital.

2.4 ABNT NBR ISO/IEC 27002 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação

Esta norma é a versão atual da Norma NBR ISO/IEC 17799, elaborada em 2005, que foi atualizada em julho de 2007 para numeração NBR ISO/IEC 27002. Conforme Baldissera (2007, p. 40) define que a origem da NBR ISO/IEC 17799:

> Remonta de 1987, quando o departamento de comércio e Indústria do Reino Unido (*UK Depertament of Trade and Industry – DTI)*, com a necessidade de criar um plano para proteção das informações do Reino Unido, criou o Centro de Segurança de Computação Comercial *(Commercial Computer Secury Center – CCSC)*. Este centro tinha como uma de suas finalidades, a criação de uma norma de segurança das informações para empresas britânicas. Em 1989 o CCSC criou um guia de segurança para usuários, o PD0003 - um Código de Práticas para Gerenciamento de Segurança da Informação *(a Code of Practice for Information Security Management)*. Após ter sido disponibilizado para consulta pública, foi desenvolvido pelo Padrão Britânico *(British Standard)* em 1995, uma versão final deste documento, a BS 7799:1995.

A Norma Britânica sofreu algumas modificações pela Organização Internacional para Normalizações, conhecida como ISO, tornando-se, assim, um padrão internacional. No Brasil a mesma norma passou a ser denominada ISO/IEC[3] 17799:200. A Associação Brasileira de Normas Técnicas (ABNT) aceitou a norma como sendo padrão nacional. No ano de 2005 surge o Código de Práticas para Gestão da Segurança da Informação conhecida como: NBR ISO/IEC 17799:2005.

[3] *International Engineering Consortium*

O objetivo da norma não é criar um modelo para a segurança da informação, mas apenas orientar as ações empregadas para garantir a segurança institucional e documental. Ela disponibiliza diretrizes que ajudam na elaboração de uma política de segurança da informação. O uso dessa norma é mais comum em instituições que prezam pela segurança da informação e foi elaborada para aplicação na área de sistemas da informação. Na arquivologia sua aplicabilidade poderá ser útil ao sistema de gestão documental, já que ela é nada mais que um código de prática que auxilia na segurança da informação e o objetivo da arquivística é realizar o tratamento documental e informacional, priorizando pela segurança e confiabilidade que será passada aos usuários.

É uma norma bastante extensa e trata de questões sobre a segurança da informação em todos os níveis em uma instituição, apresenta requisitos que abordam desde a parte física do acervo até a segurança das pessoas que trabalham nele. Nas primeiras páginas da norma, são apresentados conceitos a respeito da segurança da informação. A primeira parte da norma define os conceitos e regras iniciais, apresenta, ainda, a avaliação dos riscos (advindos das falhas de pessoas ou sistêmicas); a seleção dos controles de segurança da informação; fatores críticos e, finalizando, ressalta a necessidade das instituições criarem suas próprias diretrizes para a segurança da informação.

Esta norma possui em seus capítulos (ou seções) informações como: controle, diretrizes para implementação e informações adicionais. Com a leitura e análise da ABNT NBR ISO/IEC 27002, buscou-se compreender seus requisitos a partir do estudo de seus capítulos. Deve-se lembrar de que esta norma não é uma norma própria para arquivos e o enfoque desta pesquisa é a informação não digital.

Desta forma, buscou-se adaptar o estudo e os pressupostos teóricos a fim de relacionalos a arquivos e, consequentemente, à informação não digital. Assim, foi realizado um relato sintético de seus capítulos para relatar um conhecimento geral de suas especificações e ações permitindo, conhecer a norma para, posteriormente, desenvolvê-la e aplicá-la.

Mesmo não sendo uma norma arquivística, a ABNT NBR ISO/IEC 27002 traz inicialmente o objetivo de sua aplicação, termos e definições que auxiliam os usuários na compreensão de seu conteúdo, como nas normas arquivísticas. A norma é estruturada em onze seções e cada uma delas contém um número de categorias principais da segurança da informação. Essas categorias contêm um objetivo de controle para definir o que deve ser

alcançado e, ainda, um ou mais controles que podem ser aliados a esse para alcançar os objetivos propostos.

Antes de apresentar as seções da segurança da informação, propriamente ditas, a norma aborda, no capítulo quatro, a análise/avaliação e tratamento de riscos. Este capítulo salienta a importância da instituição realizar periodicamente a avaliação dos riscos decorrentes dos problemas que causam ameaças à segurança institucional. Como resultado da Análise de Risco, a organização recebe "o controle sobre seu próprio destino – através do relatório final, podem-se identificar quais controles devem ser implementados em curto, médio e longo prazo" (LAUREANO, 2005, p. 78).

Para tratar os riscos advindos de falhas na segurança faz-se necessário que as instituições apliquem controles para reduzi-los. Para isso é necessário que elas conheçam e aceitem estes riscos, verificando se eles atendem a política da organização e aos critérios para sua aceitação. Pode-se, também, evitar os riscos não permitindo ações que possam provocá-los e ainda, transferir a ocorrência deste risco a outras partes como uma seguradora, por exemplo.

A primeira seção que aborda requisitos para a segurança da informação corresponde ao capítulo cinco da Norma. Neste é apresentada a Política de Segurança da Informação. Para Spanceski (2004) é fundamental que as instituições elaborem uma política de segurança da informação, pois só através de uma metodologia específica, de normas e responsabilidades definidas será possível garantir o controle e a segurança das informações institucionais. O objetivo da política de segurança da informação é dar uma orientação à administração da instituição, baseada em regulamentos e de acordo com os propósitos institucionais.

Esse capítulo aborda ainda, o documento da política de segurança da informação que nada mais é que a elaboração de um documento aprovado pela instituição comprometendo-se e relatando seu enfoque para gerenciar a segurança das informações. O capítulo cinco traz ainda a análise crítica da política de segurança da informação, que tem como controle o dever da instituição de analisar periodicamente as mudanças que ocorrerem na política implantada para, só assim, assegurar sua eficácia.

Para compreender melhor, deve ser estabelecida a política de segurança da informação dentro da instituição, o capítulo seis da ABNT NBR ISO/IEC 27002 é denominado: Organizando a segurança da informação. A primeira subdivisão desse capítulo fala sobre a

infraestrutura da segurança da informação, relatando que a direção deve aprovar a política de segurança da informação e atribuir às funções da segurança.

A próxima subdivisão comenta sobre o Comprometimento da direção com a segurança da informação, relatando que esta deve apoiar a segurança da informação dentro da organização, demonstrando o seu comprometimento, definindo atribuições de forma clara e conhecendo as responsabilidades pela segurança da informação. A implementação dessa política deve ser coordenada por representantes de diferentes partes da instituição e com funções e papéis relevantes, pois a participação deve envolver desde administradores até usuários. Esse assunto é abordado no subcapítulo denominado coordenação da segurança da informação. As diretrizes sobre as responsabilidades pela segurança da informação são comentadas no subcapítulo: Atribuição de responsabilidades para a segurança da informação. Após, a norma ainda traz outra subdivisão que compreende o Processo de autorização para os recursos de processamento da informação.

No capítulo seis apresenta-se os requisitos para o contato com autoridade e o contato com grupos especiais. O primeiro refere-se aos incidentes em segurança da informação que podem ocorrer e que tipo de autoridade pode ser contatada para cada tipo de serviço. O segundo faz referência a contatos mantidos com grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais. A Análise crítica independente de segurança da informação é o requisito que propõe que seja realizada uma avaliação dos riscos para identificar quaisquer requisitos de controles específicos, onde existir uma necessidade que permita o acesso de uma parte externa aos recursos de processamento da informação ou às informações na instituição.

Muitas vezes a instituição arquivística, além de prestar serviços externos, necessita da prestação de serviços terceirizados em suas dependências. Os riscos decorrentes das manutenções de mais trabalhos realizados por partes externas a instituição podem causar incidentes de segurança da informação. Pensando nisso, ao tratar às políticas de segurança da informação, as instituições devem prever e atribuir requisitos para possíveis implicações e danos à segurança quando se trabalha com partes externas. As partes externas, como preocupação de quem trabalha na segurança da informação, também está presente nos requisitos do capítulo da norma abordando a Identificação dos riscos relacionados com partes externas; Identificando a segurança da informação, quando tratando com os clientes; e Identificando segurança da informação nos acordos com terceiros.

O Capítulo sete, Gestão de ativos, trata da responsabilidade pelos ativos, ou seja, indicando que, dentro da instituição, devem existir responsáveis pela proteção desses ativos. Para isso, convém que todos os ativos sejam identificados e documentados em um inventário dos ativos, permitindo recuperar em caso de desastre, incluindo o tipo de ativo, forma, localização, informação sobre cópias de segurança, informações sobre licenças e a importância dele para a instituição. Nesse sentido, Fontes (2008, p. 225) afirma que "para possibilitar a proteção adequada da informação é necessário que se tenha a identificação dos ativos (recursos) de informação, seus responsáveis, sua forma de sua classificação em termos de sigilo".

Dentro desse processo, torna-se fundamental que todas as informações e ativos aliados aos recursos de processamento de informação possuam um proprietário[4]. Outro requisito tratado dentro da gestão dos ativos é a Classificação da informação, que tem como objetivo assegurar que a informação receba um nível adequado de proteção indicando, a necessidade e a prioridade para seu tratamento. Em geral, a classificação dada à informação é uma forma de determinar seu tratamento e proteção dentro da instituição. A última subdivisão desse capítulo relata sobre os rótulos e o tratamento da informação dando diretivas a fim de proporcionar que as informações recebam rótulos apropriados de acordo com sua classificação. A rotulação e o tratamento seguro da classificação da informação é um requisito fundamental para os procedimentos de compartilhamento da informação.

No capítulo oito, Segurança em recursos humanos, "são abordados a inclusão de responsabilidades relativas à segurança na descrição dos cargos, a forma de contratação e o treinamento em assuntos relacionados à segurança. (BALDISSERA, 2007, p. 43). Esses requisitos proporcionam aos funcionários contratados (sejam temporários ou por longa duração) o conhecimento de suas responsabilidades dentro da instituição reduzindo, assim, o risco de roubos, fraudes e mau uso de recursos. Em caso de término ou mudança da contratação, convém a devolução dos ativos da organização e a retirada de todos os direitos de acesso que estejam em posse dos funcionários, fornecedores e terceiros após o encerramento de suas atividades na instituição. Neste sentido pode-se afirmar que "a pessoa humana é o elemento da cadeia e segurança que faz acontecer a proteção da informação" (FONTES, 2008, p. 122).

[4] Pessoa ou organismo responsável e autorizado para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos.

O capítulo nove aborda a Segurança física e do ambiente para proporcionar áreas seguras prevenindo o acesso físico não autorizado, danos e interferências com as instalações e informações da instituição. Para isso, é relevante o uso de perímetros de segurança, que podem ser as paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas para proteger e evitar o acesso livre as áreas que contenham as informações e instalações de processamento da informação. Nessas áreas só podem ter acesso às pessoas que possuírem autorização.

As áreas devem ser projetadas e aplicadas com proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem. Nesta perspectiva a aplicação de ações para a "segurança dos equipamentos se atenta a impedir perdas, danos, roubo, comprometimento de ativos e interrupção das atividades da organização" (ANDRADE, 2011, p, 34). A proteção dos equipamentos é necessária, também, para reduzir o risco de acesso não autorizado às informações e para proteger contra perdas ou danos. Os equipamentos têm que ser protegidos contra falta de energia elétrica e a manutenção deve ser apropriada para assegurar a disponibilidade e integridade dos equipamentos.

O capítulo dez, gerenciamento das operações e comunicações, certamente é o mais extenso da ABNT NBR ISO/IEC 27002 e para compreender melhor sua abordagem segue-se Baldissera (2007, p. 43) ao relatar que essa seção:

> Aborda as principais áreas que devem ser objeto de especial atenção e segurança. Dentre estas áreas destacam-se as questões relativas a procedimentos operacionais e respectivas responsabilidades, homologação e implantação de sistemas, gerência de redes, controle e prevenção de vírus, controle de mudanças, execução e guarda de backup, controle de documentação, segurança de correio eletrônico, entre outras.

Esse capítulo faz referência às cópias de segurança, cujo objetivo é manter a integridade e disponibilidade à informação e são recursos de processamento de informação.

No capítulo onze são apresentadas diretrizes para a implementação do Controle de acesso. Esse capítulo abrange basicamente as normas e regras para garantir manter seguras as informações dentro de uma instituição. Expõem, também, a relevância do estabelecimento de uma política de controle de acesso com base nos requisitos de acesso e na segurança da informação. Relata o gerenciamento de acesso de usuários e suas responsabilidades. Comenta sobre o controle de acesso à rede e o controle ao sistema operacional. As últimas abordagens

desse capítulo referem-se ao controle de acesso às aplicações e à informação, e também faz referência à computação móvel e o trabalho remoto.

A questão da Aquisição, desenvolvimento e manutenção de sistemas de informação, abordando requisitos para garantir a segurança da informação é referenciada no capítulo doze na ABNT NBR ISO/IEC 27002. Esse capítulo, além disso, faz menção aos controles criptográficos objetivando proteger a confidencialidade, a autenticidade ou a integridade das informações.

No capítulo treze são discutidos assuntos referentes à Gestão de incidentes de segurança. O primeiro ponto abordado são as notificações de fragilidades, cujo propósito é assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam notificados, permitindo a tomada de ação corretiva em tempo hábil. O capítulo trata ainda da gestão de incidentes de segurança da informação e melhorias, expondo o estabelecimento de responsabilidades e procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.

O penúltimo capítulo da norma, capítulo quatorze, correspondendo à seção dez do conjunto de assuntos sobre a segurança da informação, traz a Gestão da Continuidade do negócio. Relata a relevância em não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres, e assegurar a sua retomada em tempo hábil. Para Fontes (2008, p. 73) as instituições necessitam "elaborar um plano de continuidade que deve ser efetivo e possibilitar que a organização funcione em um nível aceitável para a sua sobrevivência e absorva possíveis impactos financeiros, operacionais e de imagem". As instituições devem estar cientes de que "a gestão da continuidade dos negócios não é um projeto e sim um programa evolutivo contínuo, pois não é uma atividade feita apenas uma vez" (GUINDANI, 2008, p. 62).

A conformidade é abordada no capítulo quinze, correspondendo a última seção do conjunto de assuntos sobre segurança da informação presente na norma. Comenta a necessidade de observar os requisitos estatutários, regulamentares e contratuais relevantes, e o enfoque da organização. De acordo com esses requisitos os registros importantes têm que ser protegidos contra perda, destruição e falsificação. A instituição deve estar atenta também aos controles de criptografia para que sejam usados em conformidade com todas as leis, acordos e

regulamentações relevantes. Essas ações devem garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.

O capítulo três (3) traz um relato sobre a história, estrutura e atividades desenvolvidas pelo departamento, objeto desta pesquisa.

3 DEPARTAMENTO DE ARQUIVO GERAL DA UFSM - DAG[5]

Em 1988, a Administração Superior da Universidade designou, por meio da portaria n. 21941, uma equipe de profissionais arquivistas, com o objetivo de diagnosticar a situação dos arquivos, visando a estabelecer políticas arquivísticas para a instituição. A partir do diagnóstico, observou-se que a estrutura organizacional da UFSM não contemplava o arquivo. O trabalho proposto pela equipe firmou-se em um conjunto de recomendações técnico-científicas que representaram uma mudança de mentalidade com relação a concepção de arquivo, despertando o compromisso da comunidade universitária com a preservação do patrimônio documental da UFSM.

Assim, em 17 de janeiro de 1990, na 438ª sessão do Conselho Universitário, foi aprovado o projeto de implantação do sistema de arquivos na UFSM, o qual cria a Divisão de Arquivo Geral, como órgão executivo da Administração Superior, vinculada à Pró-Reitoria de Administração, por meio da Resolução n. 0006/90 e alterada em seu item I pela Resolução n. 0007/90. Os objetivos do sistema constituem-se em suprir a instituição de todas as informações necessárias para o processo de análise e tomada de decisão; racionalizar a produção documental; garantir a implementação de uma política de avaliação de documentos e preservar o Fundo Documental da UFSM como parte integrante dos Fundos da Administração Federal.

Em março de 2006, a equipe técnica elaborou o Projeto de Reestruturação da Divisão de Arquivo Geral, visando à maior autonomia nas decisões arquivísticas, à execução de novas estratégias para a consolidação da Rede de Arquivos Setoriais e melhor gerenciamento das atividades concernentes às áreas de protocolo, arquivos setoriais, arquivo permanente e reprografia.

A proposta de reestruturação foi aprovada em 22 de dezembro de 2006, na 663ª sessão do Conselho Universitário, parecer n. 114/06 da Comissão de Legislação e Regimento. Dessa forma, a Divisão de Arquivo Geral passou a denominar-se Departamento de Arquivo Geral (DAG), constituindo-se na estrutura organizacional da UFSM como órgão suplementar central, legitimado na **Resolução n. 016/2006**, de 26 de dezembro de 2006.

[5] Informações retiradas do site: <http://w3.ufsm.br/dag/>.

O Departamento de Arquivo Geral - DAG - tem a finalidade de coordenar o sistema de arquivos e desenvolver a política de gestão arquivística da Universidade, mantendo sob custódia, documentos de caráter permanente, oriundos das atividades dos órgãos administrativos e das unidades de ensino, pesquisa e extensão que compõem a Universidade.

Figura 1 - Prédio do Departamento de Arquivo Geral da UFSM

Fonte: Departamento de Arquivo Geral da UFSM

3.1 Sistema de arquivos da UFSM

O sistema de arquivos da UFSM constitui-se da integração das unidades:

- **Departamento de Arquivo Geral -** órgão central do Sistema de Arquivos, subordinado a Pró-Reitoria de Administração responsável pela gestão arquivística na UFSM. Sua estrutura organizacional: Divisão de protocolo, Divisão de Apoio Técnico aos Arquivos Setoriais, Divisão de Arquivo Permanente e Laboratório de Reprografia.

- **Comissão Permanente de Avaliação de Documentos/CPAD –** comissão criada pela Resolução n.018/98-Reitor, de 04/11/1998 e responsável pela orientação e realização do processo de análise, avaliação e seleção da documentação produzida e acumulada no âmbito institucional.

- **Arquivos Setoriais** – unidade arquivística setorial, constituído da seguinte forma:

*** Administração Superior**, formado pelos arquivos setoriais dos órgãos colegiados, do Gabinete do Reitor e Vice-Reitor, dos órgãos de direção e assessoria, dos órgãos executivos, dos órgãos suplementares centrais e da Coordenadoria de Educação Básica, Técnica e Tecnológica.

*** Unidades Universitárias,** formado pelos arquivos setoriais do Centro de Artes e Letras, do Centro de Ciências Naturais e Exatas, do Centro de Ciências Rurais, do Centro de Ciências da Saúde, do Centro de Ciências Sociais e Humanas, do Centro de Educação, do Centro de Educação Física e Desportos, do Centro de Tecnologia, do Centro de Educação Superior Norte-RS e da Unidade Descentralizada de Educação Superior de Silveira Martins-RS.

*** Unidades de Ensino Médio e Tecnológico,** formado pelos arquivos setoriais do Colégio Técnico Industrial de Santa Maria, do Colégio Politécnico da Universidade Federal de Santa Maria e do Colégio Agrícola de Frederico Westphalen.

Os arquivos setoriais estão sendo implementados gradativamente nas unidades universitárias

3.2 Competências do DAG

O Departamento de Arquivo Geral, órgão suplementar central, subordinado diretamente ao Reitor, sob a supervisão administrativa da Pró-Reitoria de Administração, tem por finalidade implementar e coordenar o sistema de arquivos na UFSM, mais especificamente:

- desenvolver e estabelecer a política de gestão documental;
- constituir e preservar o patrimônio documental da UFSM;
- coordenar as atividades de protocolo, arquivos setoriais, arquivo permanente, microfilmagem e outros métodos reprográficos;
- integrar e uniformizar as atividades arquivísticas nas diferentes fases do ciclo vital dos documentos;
- promover a difusão e o acesso às informações custodiadas pela Divisão de Arquivo Permanente;

- elaborar diretrizes, normas e métodos de trabalho relativos as atividades do departamento;
- promover o aperfeiçoamento e a qualificação dos servidores técnico-administrativos;

3.3 Estrutura Organizacional

O Departamento de Arquivo Geral tem sua estrutura presente em seu organograma (Anexo A), cujas atribuições são:

I - DIREÇÃO

A direção tem a responsabilidade de coordenar e supervisionar a gestão documental da Universidade.

a) Secretaria de Apoio Administrativo

A Secretaria tem a finalidade de auxiliar nas atividades administrativas, redigir e emitir documentos, organizar e manter os arquivos do Departamento, controlar frequência e férias dos servidores, providenciar a aquisição de materiais de consumo e permanente da unidade, secretariar reuniões e outras atividades pertinente ao serviço.

II - DIVISÃO DE PROTOCOLO

A Divisão de Protocolo tem como finalidade a coordenação e supervisão das atividades de recebimento, seleção, registro, distribuição e expedição de correspondências e demais documentos institucionais.

a) Seção de Registro e Controle

Proceder a autuação de processos que requeiram análise e decisões das diversas unidades/subunidades da Universidade;

- controlar a tramitação de processos e documentos em geral;
- atender aos usuários internos e externos quanto à consulta e tramitações de processos e documentos;
- realizar a juntada, o desentranhamento, o desmembramento de processos quando solicitado pelas unidades;
- prestar informações relativas ao registro e controle de processos/documentos;
- elaborar normas e manuais de serviço, de acordo com a legislação vigente;
- executar outras atividades inerentes a sua área de atuação.

b) Seção de Movimentação

- Receber, conferir, separar, registrar e distribruir as correspondências e demais documentos;
- coletar e entregar documentos, encomendas, volumes e outros, interna e externamente;
- controlar os serviços de correio e malotes;
- executar outras atividades inerentes a sua área de atuação.

III - DIVISÃO DE APOIO TÉCNICO AOS ARQUIVOS SETORIAIS

A Divisão de Apoio Técnico aos Arquivos Setoriais tem como finalidade a coordenação e supervisão de atividades nos Arquivos Setoriais e mais especificamente:

- orientar e acompanhar a organização dos arquivos correntes e inetrmediários das unidades/subuniades da universidade, de forma a padronizar os procedimentos técnicos;
- orientar o levantamento da produção documental com vistas a eleboração dos instrumentos de gestao, os planos de classificação e tabelas de temporalidade de documentos;
- elaborar normas operacionais para os arquivos setoriais, atendendo as peculiaridades de cada arquivo;
- promover a capacitação dos responsáveis pela execução das atividades nos arquivos setoriais;
- prestar apoio técnico à Comissão Permanente de Avaliação de Documentos no processo de avaliação documental;

- atender aos usuários do sistema de arquivos.

Aos Arquivos Setoriais compete:

- aplicar a gestão documental nas suas respectivas unidades/subunidades;
- cumprir e fazer cumprir as normas emanadas pelo órgão central do sistema de arquivos;
- propor e implementar a classificação dos documentos em seu âmbito de atuação, após aprovação do órgão central;
- prestar orientação técnica as unidades/subunidades;
- participar do processo de avaliação e destinação de documentos, procedendo aos descartes necessários e transferindo a documentação de acordo com a Tabela de Temporalidade de Documentos e planos de destinação estabelecidos;
- controlar as consultas e empréstimo de documentos sob sua custódia;
- elaborar rotinas de trabalho, em conformidade com as diretrizes e normas emanadas do Departamento de Arquivo Geral e da Comissão Permanente de Avaliação de Documentos;
- manter atualizado o cadastro das unidades pertencentes às suas estruturas organizacionais, acompanhando as com´posições funcionais e as relações hieràrquicas;
- zelar pelas condições de conservação do acervo documental produzido e acumulado, enquanto estiver sob sua custódia.

Os arquivos setoriais são responsáveis pelas atividades dos arquivos correntes e intermediários da cada unidade/subunidade (cursos, departamentos, gabinetes, etc) a ele vinculado, com orientação técnica da Divisão de Apoio Técnico aos Arquivos Setoriais do DAG. Cada arquivo setorial obedece a estrutura organizacional da UFSM e está subordinado tecnicamente ao Departamento de Arquivo Geral, órgão central do sistema, e administrativamente às unidades a que pertencem.

IV - DIVISÃO DE ARQUIVO PERMANENTE

À Divisão de Arquivo Permanente tem como finalidade a custódia, a preservação e divulgação dos documentos de valor histórico, probatório e informativo da universidade.

a) Seção de Processamento Técnico

À Seção de Processamento Técnico compete:

- Recolher a documentação proveniente dos arquivos setoriais;
- acondicionar e armazenar os documentos;
- organizar os documentos de acordo com a política de arranjo e descrição estabelecidas para os fundos documentais da UFSM;
- elaborar os instrumentos de pesquisa como inventários, guias, catálogos e outros;
- manter a custódia, a conservação e a preservação do acervo documental.

b) Seção de Estudos e Pesquisas

À Seção de Estudos e Pesquisas compete:

- Atender aos usuários, estabelecendo critérios no que diz respeito ao acesso às informações de acordo com a legislação vigente;
- promover atividades de divulgação do acervo arquivístico;
- controlar a consulta e o empréstimo de documentos;
- orientar e acompanhar pesquisas e estudos na documentação custodiada pela Divisão de Arquivo Permanente.

V - LABORATÓRIO DE REPROGRAFIA

Ao Laboratório de Reprografia compete:

- Desenvolver atividades reprográficas, por meio de serviços de microfilmagem e/ou digitalização;
- garantir segurança, preservação e durabilidade das informações armazenadas em meios reprográficos, respeitando a legislação vigente;
- cumprir as normas e padrões de qualidade a serem seguidos nas diversas operações de microfilmagem e digitalização;
- manter efetivo controle do arquivo de segurança, no que se refere à manutenção dos padrões de controle ambiental de temperatura e umidade;

- elaborar os instrumentos necessários ao acesso às informações;
- promover a capacitação de servidores quanto ao uso adequado das técnicas microfilmagem e digitalização;
- executar outras atividades inerentes a sua área de atuação.

A identificação do Departamento de Arquivo Geral, bem como, os dados de localização, horário de atendimento e telefone de contato podem ser verificados no Quadro 1:

Departamento de Arquivo Geral
Prédio da Reitoria - Térreo - Salas nº 130 e 127 Universidade Federal de Santa Maria Av. Roraima nº 1.000 - Cidade Universitária - Bairro Camobi CEP 97105-900 - Santa Maria – RS Fones: (0xx55) 3220 8212, 3220 8233/Fax: (0xx55) 3220 8130 Horário de Atendimento: de segunda a sexta-feira, das 8h às 11h30min, e das 14h às 17h30min

Quadro 1 - Identificação do Departamento de Arquivo Geral da UFSM

No capítulo quatro (4), serão apresentados os passos metodológicos que possibilitaram a realização desta pesquisa.

4 METODOLOGIA

A pesquisa científica "é um conjunto de ações, propostas para encontrar a solução para um problema, que têm por base procedimentos racionais e sistemáticos" (SILVA e MENEZES, 2001, p. 20). Sua realização decorre da falta de informações suficientes para solucioná-la. Para que se considere um conhecimento científico "torna-se necessário identificar as operações mentais e técnicas que possibilitam a sua verificação" (GIL, 1999, p. 26).

A presente pesquisa tem como foco um estudo sobre a Segurança da Informação seguindo os requisitos metodológicos e teóricos da Norma ABNT NBR ISO/IEC 27002. De acordo com determinações desta Norma, a segurança da informação pode ser materializada através da composição de uma Política de Segurança da Informação. Assim, esta pesquisa objetivou a elaboração de uma Política de Segurança da Informação para o Departamento de Arquivo Geral da UFSM - DAG como forma de possibilitar a proteção, disponibilidade e acesso seguro às informações arquivísticas no contexto universitário.

Do ponto de vista da forma de abordagem, a pesquisa classifica-se como qualitativa. Nesse sentido a pesquisa qualitativa "considera a existência de uma relação dinâmica entre mundo real e sujeito" (SANCHEZ, 2009, p. 7). Assim, a característica da investigação define-se como exploratória, já que visa proporcionar maior familiaridade com o problema tornando-o explícito. Nesse caso, assume a forma de estudo de caso, pois envolve o estudo sobre um determinado assunto permitindo o seu amplo e detalhado conhecimento. Assim, o estudo de caso é "um tipo de pesquisa cujo objeto é uma unidade que se analisa profundamente, e visa o exame detalhado de uma situação" (FLORES, 2000, p. 47 apud GODOY, 1999, p.25).

Primeiramente foi realizada a revisão da literatura, compreendendo a literatura arquivística, arquivos universitários, segurança da informação e a Norma ABNT NBR ISO/IEC 27002, buscando, assim, o conhecimento e reflexão em relação ao que os autores têm produzido sobre esses temas. A revisão bibliográfica foi realizada durante todo o desenvolvimento da pesquisa, sendo embasada em teorias que subsidiem a realização da mesma.

A adaptação da Norma para a arquivologia seguiu a estrutura da norma original, buscando proporcionar as instituições arquivísticas um material que subsidie a elaboração de sistemas de segurança da informação mais seguros para a informação arquivística não digital que representa a maioria do volume documental das instituições. Para isso foi realizado um estudo mais aprofundado da Norma ABNT NBR ISO/IEC 27002 através da leitura minuciosa de suas seções possibilitando a análise de sua estrutura completa a fim de conhecer e verificar cada ponto descrito nela. Após optou-se por não considerar os requisitos que referenciavam a Tecnologia da Informação (TI), ou seja, que fizessem menção a procedimentos relativos à rede de computadores e questões digitais, já que o foco da pesquisa seria a informação não digital. A versão adaptada da Norma ABNT NBR ISO/IEC 27002 para o contexto arquivístico serviu como material de referência para a elaboração da Política de Segurança da Informação no DAG.

O estudo de caso foi no Departamento de Arquivo Geral (DAG), cuja documentação corresponde a informações arquivísticas universitárias. Dessa forma, o público alvo desta pesquisa foram as pessoas que serão beneficiadas com a sua realização, sendo os funcionários do departamento, usuários do arquivo e comunidade acadêmica em geral. Para a realização do estudo de caso, foi organizado um roteiro para entrevista estruturada (Apêndice A) a ser aplicado no DAG, com questões sobre a segurança da informação, fundamentado na Norma ABNT NBR ISO/IEC 27002, tendo como base o estudo anterior e a adaptação da Norma para o contexto arquivístico.

Esse roteiro teve como referência, também, o Questionário Básico de Avaliação da Segurança da Informação (QBASI) elaborado por Edson Fontes, a partir da Norma NBR ISO/IEC 27002, publicado no livro Praticando a Segurança da Informação, do ano de 2008, páginas 233 a 244. Em um primeiro momento, foi mantido contato com a pessoa responsável no departamento e realizada uma visita para conhecer o setor e suas atividades e posteriormente marcado a entrevista estruturada. Também foi entregue uma carta de apresentação (Apêndice B).

A entrevista foi realizada, apenas, com a pessoa responsável no DAG, sendo o encarregado pelo desenvolvimento e coordenação das atividades de gestão. A análise dos dados coletados na entrevista possibilitou a identificação de problemas que causam ameaças à segurança da informação e falhas de segurança no departamento. Assim foi possível elaborar a política de segurança da informação adaptada à realidade e às necessidades do

departamento, contribuindo para a proteção das informações arquivísticas custodiadas pelo no departamento.

Uma vez conhecidos as falhas em segurança da informação foi possível, juntamente com o estudo da ABNT NBR ISO/IEC 27002, determinar os controles adequados para reforçar e garantir a segurança da informação no departamento. Os controles foram definidos de acordo com os capítulos da adaptação da Norma que abordam os seguintes assuntos: Política de segurança da informação, Gestão de ativos; Segurança em recursos humanos; Segurança física e do ambiente; Gerenciamento das operações e comunicações; Controle de acessos; Gestão de incidentes de segurança da informação; Gestão da continuidade do negócio e Conformidade. Por fim, a elaboração do documento da Política de Segurança da Informação contém ações, regras e determinações no intuito de possibilitar a proteção e integridade das informações arquivísticas não digitais do DAG.

No capítulo cinco (5), se apresentará a adaptação da Norma ABNT NBR ISO/IEC 27002 para a segurança das informações arquivísticas (não digitais), servindo de subsídio para a elaboração de Políticas de Segurança da Informação e, contribuindo para a proteção dos ativos de informação.

5 ADAPTAÇÃO DA NORMA ABNT NBR ISO/IEC 27002 PARA A SEGURANÇA DAS INFORMAÇÕES ARQUIVÍSTICAS NÃO DIGITAIS

Neste capítulo e no capítulo seguinte (capítulo 6) serão apresentados os resultados da pesquisa expondo as ações que foram realizadas com o propósito de contribuir para a composição da Política de Segurança da Informação (não digital) elaborada para o DAG. Portanto, serão retomados os objetivos desta investigação, com o intuito de responder à pergunta proposta. A principal finalidade desta pesquisa é propor uma Política de Segurança da Informação para o DAG da UFSM, para contribuir com a disponibilidade, a integridade e a confidencialidade das informações arquivísticas (não digitais) proporcionando, assim, o acesso seguro aos documentos.

Para a realização deste objetivo, primeiramente, foram realizados uma análise e um estudo detalhado da Norma ABNT NBR ISO/IEC 27002, a fim de definir e de selecionar apenas os requisitos que pudessem ser aplicados à segurança das informações não digitais. Como essa Norma será adaptada somente ao contexto arquivístico, ou seja, para a proteção de informações não digitais, todos os itens, referentes à informação digital foram automaticamente excluídos.

Vale ressaltar que a Norma ABNT NBR ISO/IEC 27002 foi elaborada para aplicação na área de sistemas da informação, por isso muitos termos e definições referem-se mais especificamente à Tecnologia da Informação (TI). Assim, alguns termos foram modificados na sua Adaptação, a fim de, relacioná-los melhor ao contexto arquivístico e à segurança da informação não digital, foco da pesquisa. Por isso, o primeiro termo substituído foi organização por instituição. Esse fato se deu devido ao conceito de arquivo constar no Dicionário Brasileiro de Terminologia Arquivística (2005, p 27) como "instituição ou serviço que tem por finalidade a custódia, o processamento técnico, a conservação e o acesso a documentos".

A Adaptação da Norma à arquivologia seguiu a estrutura da Norma atual. O primeiro capítulo apresentado é o capítulo numerado como zero (0). Na Norma original, esse capítulo apresenta oito pontos em forma de questionamentos, explicando alguns conceitos de segurança da informação numerados do 01 até 08. Para essa Adaptação, optou-se por numerar

o capítulo da introdução como um (1) já que representava o primeiro capítulo da Adaptação. Assim, esta apresenta, do mesmo modo que a Norma original, os conceitos brevemente explanados na introdução.

Na introdução da Adaptação, foram deixados os oito pontos presentes na introdução da Norma original. No quadro abaixo (Quadro 2), é possível visualizar os itens presentes na Norma original e os itens modificados para a sua Adaptação, como também um comentário sobre suas especificações.

NORMA	ADAPTAÇÃO	O QUE MUDOU?
0 Introdução	1 Introdução	- os itens foram renumerados;
0.1 O que é segurança da informação?	1.1 O que é segurança da informação não digital?	- a segurança de informações digitais limitou-se apenas à segurança de informações não digitais, com ênfase no suporte papel;
0.2 Por que a segurança da informação é necessária?	1.2 Por que a segurança da informação é necessária em instituições arquivísticas?	- a resposta refere-se apenas à proteção e à integridade de informações não digitais;
0.3 Como estabelecer requisitos de segurança da informação	1.3 Como estabelecer requisitos de segurança da informação	- das três (3) fontes principais de requisitos de segurança da informação, na Adaptação, aparecem apenas duas (2); - a fonte que referenciava informação digital foi retirada;
0.4 Analisando/avaliando os riscos de segurança da informação	1.4 Analisando/avaliando os riscos de segurança da informação	- os requisitos permaneceram iguais na Norma e na Adaptação;
0.5 Seleção de controles	1.5 Seleção de controles	- nas duas Normas foi ressaltado que a definição dos controles deve acontecer de acordo com a realidade institucional;
0.6 Ponto de partida para a segurança da informação	1.6 Ponto de partida para a segurança da informação	- os requisitos permaneceram iguais, sendo citados exemplos de controles considerados essenciais para uma instituição;
0.7 Fatores críticos de sucesso	1.7 Fatores críticos de sucesso	- apresentados os fatores críticos para a implementação da segurança da informação (requisitos iguais nas duas Normas);
0.8 Desenvolvendo suas próprias diretrizes	1.8 Desenvolvendo suas próprias diretrizes	- foi ressaltado o uso de requisitos para a segurança da informação não digital em arquivos.

Quadro 2 - Comparativo da Norma ABNT NBR ISO/IEC 27002 e sua Adaptação

Ao observar o quadro, pode-se verificar que os dois primeiros itens apareciam em forma de questionamento na Norma original e foi mantido na sua Adaptação, porém a finalidade modificou-se, levando em conta o objetivo desta pesquisa que se refere exclusivamente à segurança de informações (não digitais) para a aplicação em arquivos. Os demais itens continuaram os mesmos, porém seus argumentos foram ao encontro dos objetivos desta pesquisa. Isso pode ser verificado na versão final da Adaptação da Norma (Apêndice C).

No entanto, como a numeração do capítulo 1 iniciava nos objetivos na Norma original e nesta Adaptação iniciou na introdução, consequentemente, o capítulo dois (2) será composto pelos objetivos que agora passará a ser denominado: objetivos e aplicação da Adaptação da Norma. Outra modificação realizada foi que, na Norma modelo, o capítulo dois que correspondia aos termos e às definições foi sucumbido da Adaptação da Norma e será substituído pelo glossário no final. O capítulo 3 segue com a mesma numeração, correspondendo à estrutura da Adaptação. Sua estrutura original sofreu algumas modificações, como foi esclarecido no início deste capítulo.

É necessário salientar que, como os requisitos para a segurança da informação não digital foram excluídos da Norma e os capítulos (seções) renumerados, a seção/capítulo doze (12) - Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação- foi também excluída da Adaptação. Esse fato se deu por este capítulo abranger diretrizes específicas para sistemas de informação, ou seja, referir-se diretamente à informação digital. Outra modificação se deu na seção/capítulo seis (6) - Organizando a segurança da informação- que, da mesma forma que o capítulo anterior, aparecerá na Adaptação. Entretanto, ela não foi suprimida como a seção doze (12), mas alguns requisitos presentes nela foram recolocados em outras seções, de acordo com a finalidade, a fim de facilitar a compreensão.

As seções que fazem parte da Adaptação da Norma são:

1 - Política de Segurança da Informação;

2 - Gestão de Ativos;

3 - Segurança em Recursos Humanos;

4 - Segurança Física e do Ambiente;

5 - Gerenciamento das Operações e Comunicações;

6 - Controle de Acesso;

7- Gestão de Incidentes de Segurança da Informação;

8 - Gestão da Continuidade do Negócio;

9 - Conformidade.

As seções contém um número de categorias principais de segurança da informação. A Norma adaptada será composta por nove (9) seções ao invés das onze (11) seções (ou capítulos) apresentadas na Norma original, que juntas totalizam dezesseis (16) categorias ao invés das trinta e nove (39) apresentadas na original. Essa diminuição do número de categorias é devido à abordagem da Adaptação que se refere apenas à segurança da informação não digital em arquivos. Em relação ao uso de Normalização em arquivos, Beyea (2007, p. 34) ressalta que os "arquivistas devem ser instruídos sobre o objetivo e os detalhes de uma Norma. Eles devem ser encorajados a apoiar e a implementar as Normas. Normas devem ser mantidas e revisadas". Essa afirmação reforça a necessidade e a importância da Adaptação da Norma ABNT NBR ISO/IEC 27002 para as seguranças de informações arquivísticas não digitais, visto que não existem Normas com esse enfoque em arquivos.

O capítulo seguinte, capítulo três (3) (Estrutura da Adaptação da Norma), apresenta as principais categorias de segurança da informação demonstrando como se organiza os requisitos ao longo da Norma e por isso não sofreu alteração na sua Adaptação. Assim, a categoria principal é apresentada contendo um "objetivo de controle", que define o que deve ser alcançado, e um ou mais "controles", que podem ser aplicados para se alcançar o "objetivo do controle". Portanto, a Norma se estrutura apresentando o controle específico para atender ao objetivo do controle, às diretrizes para a implementação desse controle e, quando necessário, às informações adicionais que podem ser considerações legais e referências a outras Normas.

O capítulo quatro (4) que corresponde à análise/avaliação e ao tratamento de risco permaneceu igual na Adaptação, porém foram retiradas as informações que referenciavam informação digital. Assim, permite que as instituições arquivísticas realizem apenas a análise e o tratamento de riscos que envolvam informações (não digitais).

É necessário ressaltar que, muitas vezes, o resultado da aplicação da Política de Segurança da Informação se dá a partir da análise e do tratamento de riscos, considerados o ponto de partida para verificar os problemas que estão causando incidentes em segurança da informação e traçar objetivos a fim de evitá-los. Essa afirmação vai ao encontro de Laureano (2005, p. 78) quando afirma que "o resultado da Análise de Risco dá à organização o controle sobre seu próprio destino – através do relatório final, pode-se identificar quais controles devem ser implementados em curto, médio e longo prazo".

Os próximos capítulos podem ser considerados a Norma propriamente dita, contemplando os requisitos para a elaboração de uma Política de Segurança da Informação. Na Adaptação, tanto quanto na Norma original, a seção um (1) corresponde à Política de Segurança da Informação seguida das outras seções que compõem essa política. Na Adaptação, essa seção assume a numeração de capítulo cinco (5) (seguindo a ordem dos capítulos da Norma), mas como se refere à primeira seção dos requisitos de segurança da informação é numerada como seção um (1).

Logo, os demais capítulos são apresentados na Adaptação da Norma seguindo essa numeração. Assim, juntamente com a análise dos capítulos/seções será referenciada a numeração dos itens possibilitando ao leitor identificá-los na Adaptação da Norma, compreendendo melhor como foi realizada a adaptação dos controles da Norma original para a Norma adaptada.

5.1 Política de Segurança da Informação - Seção 1, Capítulo 5

A Política de Segurança da Informação, propriamente dita, inicia com o capítulo cinco (5) da Adaptação da Norma, sendo correspondente à primeira seção dos requisitos de segurança da informação. De uma forma geral, a política de segurança é um documento contendo diretrizes a serem seguidas pela organização, a fim de proteger as pessoas, o acervo e a própria instituição. E, para isso, ela "deve ser descrita de forma clara e objetiva e ser amplamente divulgada em todas as suas unidades. É a maneira como a instituição se posiciona perante as questões de segurança" (BRASIL, 2006, p. 98).

Como já foi dito, cada seção possui suas categorias principais e secundárias. As categorias principais trazem o objetivo de controle e um ou mais controles que podem ser aplicados para se alcançar esse objetivo. Assim, a seção um (1), na Norma original apresentava apenas uma categoria principal, mas sua Adaptação apresentará duas categorias principais, conforme é possível verificar:

- 5.1 Política de Segurança da Informação: primeira categoria apresentada abordando diretrizes para composição do Documento da Política de Segurança da Informação e a realização da análise crítica da Política de Segurança da Informação (possibilita assegurar a permanência e eficácia da política).

- 5.2 Controlando a segurança da informação: segunda categoria principal apresentada. Esses requisitos apareciam no capítulo seis (6) da Norma original, mas como fazem parte da composição da Política de Segurança da Informação foram colocados junto com a seção um (1). Assim, este subcapítulo apresenta o comprometimento da direção com a segurança da informação; a coordenação da segurança da informação; as atribuições de responsabilidades para a segurança da informação; e o contato com autoridades.

Essa união dos requisitos se deu a partir da afirmação exposta por Spanceski (2004, p. 38) quando salienta que o documento da Política de Segurança da Informação deve conter a "declaração do comprometimento da alta direção, apoiando as metas e os princípios da segurança da informação". Em função disso, a direção deve, primeiramente, compreender a Política de Segurança da Informação para, assim, poder se comprometer em cumprir suas atribuições e responsabilidades, a fim de possibilitar a proteção e integridade das informações institucionais, garantindo o resultado positivo na aplicação dessa política.

Para garantir a efetividade da Política de Segurança da Informação, além do comprometimento da instituição, é necessário o controle e a gestão dos processos de segurança. Dessa maneira, é necessário relatar que a responsabilidade pela gestão da Política de Segurança da Informação, em instituições arquivísticas, ficará a cargo do arquivista. Nesse sentido, Andrade e Almeida (2011, p. 53) relatam que "o arquivista é um gestor, pois é responsável pela organização, classificação etc., dos documentos de uma dada instituição, seja essa pública, privada ou um centro de informação". Dessa forma, ele adquire a função de gestor da informação no processo de segurança dentro das instituições. Esse dado foi

acrescentado nas informações adicionais do controle denominado atribuição de responsabilidades para a segurança da informação (5.2.3), na Adaptação da Norma.

5.2 Gestão de ativos - Seção 2, Capítulo 6

A primeira diretriz desse capítulo, na Norma original, referia-se à elaboração de um inventário contendo todos os ativos institucionais, cujo objetivo de controle é alcançar e manter a proteção adequada dos ativos de informação. Como o foco desta pesquisa é garantir a segurança das informações arquivísticas, Sfreddo e Flores (2012, p. 162) ressaltam que "a Arquivística reconhecida atualmente como parte da ciência da informação lida com a metodologia e teorias para o tratamento não somente dos documentos, mas sim, com a informação contida neles". Dessa forma, na Adaptação da Norma, ao invés de compor um inventário de ativos, contendo uma lista de documentos arquivísticos (ativos de informação), sugeriu-se que os ativos estejam presentes no plano de classificação de documentos da instituição, conforme a metodologia arquivística.

Por esse motivo, ao invés da elaboração do inventário de ativos, a primeira subdivisão do capítulo seis (6) - Gestão de ativos - aborda recomendações para a classificação dos ativos de informação (6.1), ao invés do requisito inventário de ativos, como na Norma original. É necessário retomar a definição de ativo que, conforme Campos (2007), pode ser um bem patrimonial em função do seu valor e, da mesma forma, a informação e tudo aquilo que a suporta e/ou a utiliza são considerados ativos. De acordo com a Norma ABNT NBR ISO/IEC 27002, existem seis (6) tipos de ativos que podem ser: ativos de informação; ativos de software; ativos físicos; serviços; pessoas e suas qualificações, habilidades e experiências, e ativos intangíveis, tais como a reputação e a imagem da organização.

Considerando essa lista de ativos e centrando a pesquisa em seu foco, que é o estudo da segurança da informação, serão considerados apenas como ativos, para Adaptação da Norma, os ativos de informação (não digitais). Nesse sentido a importância de elaborar ações para possibilitar a proteção e integridade desses ativos é relatada por Castanho, Garcia e Silva (2006, p. 10) quando afirmam que a informação arquivística pode "comprovar direitos; dar suporte ao ensino e à aprendizagem ou, simplesmente informar".

Definido o tipo de ativo que será protegido, ou seja, os ativos de informação, a Adaptação apresenta a segunda subdivisão do capítulo seis (6) denominado plano de classificação e código de classificação. Para construção desses requisitos, foram seguidos os requisitos teóricos presentes na Norma e-ARQ Brasil (Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos) da Câmara Técnica de Documentos Eletrônicos, versão de 2011. Certamente foi utilizado o referencial teórico da e-ARQ por "além de orientar tecnicamente na prática de ações para gestão de documentos, [...] orienta teoricamente os seus usuários nos processos arquivísticos que poderão ser realizados" (SFREDDO E FLORES, 2012, p. 162).

A próxima subdivisão (Rótulos e tratamento da informação) existente na Norma original foi retirada da Adaptação, pois continha requisitos para tratamento de informações digitais.

5.3 Segurança em recursos humanos - Seção 3, Capítulo 7

No capítulo oito, Segurança em recursos humanos, da Norma original que corresponde ao capítulo sete (7) da Adaptação, "são abordados a inclusão de responsabilidades relativas à segurança na descrição dos cargos, a forma de contratação e o treinamento em assuntos relacionados à segurança" (BALDISSERA, 2007, p. 43). Seguindo a ideia do autor, a Adaptação da Norma permaneceu com os mesmos requisitos presentes na Norma original. A única modificação realizada foi referente ao número de categorias. Na Norma original havia três (3) categorias principais: Antes da contratação; Durante a contratação e Encerramento de atividades. Para facilitar o entendimento, como se tratavam de requisitos complementares, a categoria antes e durante da contratação aparecem como uma só categoria. Assim, a primeira categoria da Adaptação da Norma refere-se a requisitos referentes a antes e durante a contratação.

É necessário deixar claro que a palavra contratação, para efeitos da Norma ABNT NBR ISO/IEC 27002, pode se referir à "contratação de pessoas (temporárias ou por longa duração), nomeação de funções, mudança de funções, atribuições de contratos e encerramento

de quaisquer destas situações" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p. 25).

No decorrer das categorias, é apresentado o objetivo de controle e os controles a serem seguidos para atingir o objetivo principal. O objetivo principal desta seção é assegurar que todas as pessoas que trabalham ou acessam o arquivo tenham consciência de suas responsabilidades relativas à segurança da informação. Por isso, devem estar preparados para apoiar a Política de Segurança da Informação da instituição durante os seus trabalhos normais, a fim de reduzir o risco de erro humano.

A primeira subdivisão desta seção denomina-se papéis e responsabilidades (7.1.1). Essa subdivisão tem como requisito que os papéis e as responsabilidades pela segurança da informação sejam definidos e documentados de acordo com a Política de Segurança da Informação para todas as pessoas que fazem parte da instituição. Portanto, a Norma original traz como recursos humanos funcionários, fornecedores e terceiros. No entanto, na sua Adaptação, além desses, foram acrescentados, em alguns casos, os usuários do arquivo.

Nesse sentido, Fontes (2008, p. 122) ressalta que "a pessoa humana é o elemento da cadeia e segurança que faz acontecer a proteção da informação". Em função disso, o processo de seleção dentro de uma instituição arquivística, seja ela pública ou privada, deve ser cuidadosamente planejado, evitando a contratação de pessoas que não cumpram seu papel e sua responsabilidade.

A segunda subdivisão da categoria principal - Antes e durante a contratação- trata especificamente da seleção (7.1.2). É necessário salientar que, mesmo sendo distintas as maneiras para seleção de pessoal nos setores público e privado, os requisitos presentes na Norma original continuaram iguais na Adaptação. Entretanto, apenas foi sugerido que cada instituição defina os controles de acordo com a sua realidade para o processo de seleção dos funcionários, fornecedores, terceiros e usuários de arquivo.

A próxima subdivisão apresentada na Adaptação refere-se aos Termos e condições de contratação (7.1.3), tendo como medida principal no ato de contratação que funcionários, fornecedores e terceiros assinem termos declarando suas responsabilidades para a segurança da informação. Na sequência, são apresentadas as Responsabilidades da direção; (7.1.4) os requisitos apresentados estabelecem como função principal da direção o monitoramente e cumprimento da Política de Segurança da Informação. "As pessoas são o elemento central de

um sistema de segurança da informação" (CAMPOS, 2007, p. 162). É nesse sentido que se salienta que tanto funcionários quanto direção devem estar cientes de suas responsabilidades dentro do processo de segurança da informação; é necessário trabalhar conceitos, estratégia, esclarecendo a Política de Segurança da Informação para que possa ser cumprida, da uma forma eficaz, por todos.

Assim, o próximo requisito abordado refere-se à Conscientização, educação e treinamento em segurança da informação (7.1.5). Ele é fundamental para que funcionários, fornecedores, terceiros e usuários possam contribuir no processo de segurança da informação dentro da instituição, cumprindo suas responsabilidades. Fontes (2008) salienta que a pessoa é quem realiza e faz cumprir as determinações de segurança da informação dentro das organizações e, por isso, é indispensável conscientizá-la e treiná-la para que utilize a informação de acordo com sua realidade organizacional.

Se, mesmo assim, após a conscientização e o treinamento acontecer uma violação das regras e Normas que regem a Política de Segurança da Informação, a instituição pode realizar um processo disciplinar formal para aqueles que tenham cometido essa infração. O processo disciplinar (7.1.6) aparece como última subdivisão apresentada na categoria: antes e durante a contratação (7.1). Para a Associação Brasileira de Normas Técnicas (2005), esse processo deve conceder um tratamento justo ao funcionário ou suspeito de cometer violação de segurança da informação, podendo ser usado para evitar que funcionários, fornecedores e terceiros violem os procedimentos e a Política de Segurança da Informação institucional. Na opinião de Campos (2007), o uso de mecanismos formais pode ser utilizado para disciplinar os casos de violação da segurança, devendo estar de acordo com a legislação vigente, e também com regras, norma e regulamento institucionais.

A próxima categoria apresentada refere-se ao encerramento ou à mudança da contratação (7.2). Os requisitos apresentados nessa categoria devem ser realizados para que a saída de funcionários, fornecedores e terceiros da organização seja feita de modo controlado e que a devolução de todos os equipamentos e a retirada de todos os direitos de acesso seja concluída. A primeira subdivisão dessa categoria refere-se ao encerramento de atividades (7.2.1), cujo controle determina que as responsabilidades para realizar o encerramento ou a mudança de um trabalho sejam claramente definidas e atribuídas.

Com o conhecimento das responsabilidades e do encerramento das atividades, a próxima subdivisão aborda o passo seguinte a ser realizado: devolução de ativos de informação (7.2.2). Esse item traz como diretriz principal que todos os funcionários, fornecedores e terceiros devolvam todos os ativos de informação da instituição que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.

A última subdivisão dessa categoria é retirada de direitos de acesso (7.2.3). Desse item foram extraídos todos os requisitos que referenciavam sistemas de informação, pois o foco da pesquisa é a segurança da informação não digital. Em relação ao direito de acesso, a Associação Brasileira de Normas Técnicas (2005) enfatiza que após o encerramento das atividades, dos contratos ou acordos é indispensável que sejam retirados os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações, à instituição e suas dependências. Por isso, "os desligamentos devem ser comunicados a todas as áreas relevantes da organização" (CAMPOS, 2007, p. 165).

5.4 Segurança física e do ambiente - Seção 4, Capítulo 8

O próximo capítulo ou seção abordado refere-se à segurança física e do ambiente. Nesta seção foram realizadas algumas modificações a fim de adaptar os termos à questão da segurança de informações (não digitais) em arquivos. A primeira categoria apresentada é áreas seguras (8.1). Seu objetivo de controle é prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da instituição. Vale ressaltar que para a composição dos requisitos dessa categoria foram retiradas todas as informações que referenciavam instalações de processamento da informação, o restante dos requisitos continuaram iguais.

Assim, a próxima subdivisão, como na Norma original, denomina-se perímetro de segurança física (8.1.1). É necessária a utilização de perímetros de segurança ou "(barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p. 32). Esses controles devem ser cuidadosamente planejados e seguidos pelas instituições que pretendem evitar incidentes em segurança da informação. A questão da segurança física exerce um papel muito relevante nas

instituições, pois é a base para a proteção das informações e representa um dos maiores fatores de investimentos (FERREIRA e ARAÚJO, 2006).

Ainda em relação às barreiras de segurança, a Adaptação da Norma traz como controle o uso de alarmes. E para que a proteção seja efetiva é necessário que esses cubram todas as portas, janelas e áreas não ocupadas, devendo funcionar em tempo integral. Essa afirmação está em consonância com Cassares (2000, p.23) quando relata que "a melhor proteção é feita com alarmes e detectores internos". Assim, o uso desse requisito em instituições arquivísticas poderá contribuir para a proteção e o monitoramento do acervo, evitando incidentes em segurança da informação que colocam em risco a integridade, confidencialidade e disponibilidade da informação.

As próximas subdivisões referem-se ainda à categoria áreas seguras (8.1), apresentando requisitos para determinadas situações, direcionando diretrizes para sua implementação. A primeira refere-se aos controles de entrada física (8.1.2), para assegurar que somente pessoas autorizadas tenham acesso às instalações da instituição. Em resumo, as diretrizes apresentadas na categoria resumem-se ao registro das visitas e à identificação de todos os funcionários, fornecedores, terceiros e usuários, a fim de evitar a entrada de pessoas não autorizadas. Nesse sentido, a Câmara Técnica de Documentos Eletrônicos (2006) afirma que o controle do acesso é uma medida que deve ser realizada a fim de monitorar o acervo documental, possibilitando a proteção e segurança das informações contidas nos documentos. As diretrizes específicas de controle de acesso serão apresentadas no capítulo dez (10) da Adaptação.

O próximo item que aparece na Adaptação refere-se à segurança em escritórios, salas e instalações (8.1.3). E, segundo a Adaptação da Norma, para garantir a proteção desses ambientes, as instituições devem ter como diretrizes principais cumprir os regulamentos e normas de saúde e segurança, evitar o acesso às instalações principais e o uso de letreiros evidentes fora ou dentro do edifício. Na sequência, o próximo item presente da Adaptação refere-se à proteção contra ameaças externas e do meio ambiente (8.1.4). A fim de prevenir a ocorrência de problemas externos ou ambientais, é conveniente que as instituições apliquem proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem.

Além da proteção física, convém que sejam projetadas e aplicadas diretrizes para o trabalho em áreas seguras. Por isso, o penúltimo assunto da categoria áreas seguras (8.1) denomina-se trabalhando em áreas seguras (8.1.5). O controle de acesso deve ser redobrado em áreas seguras, por isso os "ambientes considerados seguros não devem ser identificados, a fim de dificultar sua localização por quem não é autorizado para estar lá" (FONTES, FONSECA e PEREIRA, 2006, p. 43).

O acesso por pessoas não autorizadas também deve ser impedido nos pontos de acesso à instituição como nas áreas de entrega e de carregamento. Assim, as diretrizes de acesso do público, áreas de entrega e de carregamento (8.1.6) aparece como último item da primeira categoria principal citada na Adaptação da Norma. Sobre a aplicação desse item, Fontes, Fonseca e Pereira (2006, p. 44) afirmam que:

> É comum que a área de carga e descarga de materiais esteja localizada próximo às áreas seguras e o acesso e controle destas áreas não seja tão eficaz como o aplicado às áreas seguras. A Norma é bem clara quanto ao cuidado especial que deve ser feito a este tipo de acesso às instalações. O acesso das pessoas que estão levando o material deve ser feito em local protegido do acesso a área interna da organização e o material deve ser inspecionado, verificado e autorizado antes do mesmo ter sua entrada permitida. Em especial, recomenda-se que esta área seja distante das áreas consideradas seguras.

Ainda em relação à segurança física e do ambiente (capítulo 8), a segunda categoria principal presente na Adaptação refere-se à segurança de equipamentos nos locais de guarda da documentação (8.2). Vale salientar que essa categoria denominava-se, na Norma original, apenas segurança de equipamentos. Entretanto, a mudança na denominação da categoria se dá devido à Adaptação objetivar a segurança de informações (não digitais) em instituições arquivísticas. Portanto, o cuidado com os equipamentos deve ser realizado principalmente nos locais de guarda da documentação. Nessa perspectiva, a aplicação de ações para a "segurança dos equipamentos se atenta a impedir perdas, danos, roubo, comprometimento de ativos e interrupção das atividades da organização" (ANDRADE, 2011, p, 34).

A primeira subdivisão presente nessa categoria refere-se à instalação e proteção do equipamento (8.2.1), cujo objetivo de controle é a proteção dos equipamentos para reduzir os riscos de ameaças e perigos do meio ambiente evitando, também, o acesso não autorizado. E, por fim, o último requisito presente na Adaptação da Norma é utilidades (8.2.2). Os requisitos

abordados nesse item são de grande importância para evitar incidentes em segurança da informação, cujas diretrizes definem a proteção de equipamentos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.

Vale ressaltar que as subdivisões da categoria segurança de equipamentos nos locais de guarda da documentação (8.2) citadas anteriormente só permaneceram na Adaptação, pois ao proteger os equipamentos indiretamente se protege também as informações (não digitais) presentes no mesmo local ou próximo a eles. Para tanto, quando os equipamentos estiverem na sala de guarda da documentação deve-se redobrar os cuidados com manutenção e quedas de energia evitando incêndios e outros incidentes que coloquem em risco a segurança das informações. Nesse sentido, Campos (2007) recomenda a aplicação de um programa para manutenção preventiva para esses equipamentos, a fim de mantê-los sempre em boas condições para o uso.

Os demais requisitos não serão citados na Adaptação, pois fazem, na sua maioria, referência mais especificamente à documentação digital e aos sistemas de informação. Os itens suprimidos na Adaptação da Norma (conforme numeração da Norma ANBT NBR ISO/IEC 27002) foram:

- 9.2.3 - Segurança do cabeamento;
- 9.2.4 - Manutenção dos equipamentos;
- 9.2.5 - Segurança de equipamentos fora das dependências da instituição;
- 9.2.6 - Reutilização e alienação segura de equipamentos;
- 9.2.7 - Remoção de propriedade.

Mesmo assim, caso as instituições achem necessário abordar esses requisitos na sua Política de Segurança da Informação, podem acessar a Norma original em sites de busca, procurando por: ABNT NBR ISO/IEC 17799. O *download* da Norma é rápido e o conteúdo é idêntico ao da Norma ABNT NBR ISO/IEC 27002.

5.5 Gerenciamento das operações e comunicações - Seção 5, Capítulo 9

Este capítulo abrange muitos requisitos para a aplicação da segurança em sistemas de informação, propriamente para a segurança em tecnologia da informação. Esse fato pode ser verificado quando Campos (2007, p. 173) denomina na Norma original essa seção como "gestão das operações em TI". Em decorrência disso, a primeira categoria da Norma modelo refere-se aos procedimentos e às responsabilidades operacionais, cujo objetivo é garantir a operação segura e correta dos recursos de processamento da informação. No entanto, como a Adaptação não aborda informação digital, essa categoria e as demais que referenciavam informação digital foram retiradas da Adaptação.

Em função disso, o único item ou categoria que permaneceu refere-se ao gerenciamento de serviços terceirizados (9.1). Essa categoria continua na Adaptação devido aos arquivos, muitas vezes, terceirizarem os serviços de limpeza, digitalização, entre outros. É necessário ressaltar que, quando outras pessoas realizam serviços dentro de uma instituição ou ficam responsáveis pelos ativos de informação fora dela, é necessário que cumpram as determinações e políticas determinadas pela mesma. Portanto, "os contratos precisam garantir a segurança das informações, inclusive com cláusulas de indenização, bem como de incidentes de segurança causados por esses prestadores de serviços" (CAMPOS, 2007, p. 155). Só assim será possível que a aplicação de controles para serviços terceirizados reflita diretamente na eficácia da segurança das informações (não digitais) custodiadas pelas instituições.

A primeira subdivisão deste capítulo ou seção apresentado refere-se à entrega de serviços (9.1.1). Para implementar seu controle, convém que o terceiro[6] implemente, execute e mantenha os controles de segurança, as definições de serviço e os níveis de entrega incluídos no acordo de entrega de serviços terceirizados. Logo depois aparece o controle denominado monitoramento e análise crítica de serviços terceirizados (9.1.2). Neste, salienta-se a necessidade da monitoração e análise crítica dos serviços terceirizados, a fim de garantir a aderência entre os termos de segurança de informação e as condições dos acordos, e que problemas e incidentes de segurança da informação sejam gerenciados adequadamente. De acordo com a Associação Brasileira de Normas Técnicas (2005), quando o assunto é

[6] Definição presente no glossário da Adaptação da Norma.

terceirização a instituição precisa estar ciente de que a responsabilidade final pelos ativos de informação permanece com ela.

Ainda na Adaptação da Norma, com o fim de instruir as instituições para a realização de serviços terceirizados, citou-se, nas informações adicionais, como referência, a publicação Recomendações para digitalização de documentos arquivísticos permanentes do Conselho Nacional de Arquivos (CONARQ), publicada em 2010. Por fim, o último item presente neste capítulo refere-se ao gerenciamento de mudanças para serviços terceirizados (9.1.3). Neste, convém que mudanças no provisionamento dos serviços, incluindo manutenção e melhoria da Política de Segurança da Informação, procedimentos e controles existentes, sejam gerenciadas. Desse modo, esses serviços são necessários, a fim de "garantir a execução do que foi estabelecido; e é muito importante que toda a equipe esteja integrada ao processo e que a importância do mesmo esteja clara para todos" (COSTA e ALMEIDA, 2010, p. 18).

5.6 Controle de acessos - Seção 6, Capítulo 10

O próximo capítulo apresentado na Adaptação da Norma referencia o controle de acessos. Vale destacar que os requisitos e controles deste capítulo são fundamentais para o desenvolvimento das atividades arquivísticas. Isso se dá a partir da ideia de que acesso é um direito e disponibilizá-lo é um dever dos gestores da informação. Essa ideia está em conformidade com o código de ética dos arquivistas ao afirmar que um dos serviços que devem ser realizados pelos arquivistas é facilitar o acesso aos arquivos (INTERNATIONAL COUNCIL ON ARCHIVES, 1996).

O controle apresentado a seguir refere-se aos requisitos de negócio para controle de acesso (10.1), cujo objetivo é controlar/monitorar o acesso à informação. Como o controle de acesso é um assunto muito amplo e abrange toda a instituição, o próximo item faz referência a uma política de controle de acesso (10.1.1). Sobre esse assunto, Rossato (2001, p. 34) assegura que "as políticas de acesso aos documentos também constituem meios de difusão em arquivos, porque é possibilitando a consulta aos documentos que se promove o acesso". Portanto, não basta apenas adotar políticas de acesso, as instituições devem estar capacitadas para controlá-las.

Nesse sentido, a disponibilidade dessa informação dependerá do acesso concedido a ela, ou seja, "o produtor de informação tem condições de manipular a disponibilidade e o acesso à informação" (BARRETO, 1994, p. 9). A informação só resultará em conhecimento se disponibilizada e utilizada pelos usuários. O acesso é indispensável para transformar essa informação em algo palpável, portanto, ela só contribuirá no desenvolvimento institucional se o acesso a ela for garantido.

Assim, o próximo controle apresentado refere-se ao Gerenciamento de acesso do usuário de arquivo (10.2). Esses requisitos tiveram alterações na Adaptação devido ao foco de estudo ser a segurança da informação arquivística. Desse modo, o objetivo de controle passou a ser assegurar acesso de usuário autorizado e prevenir acesso não autorizado aos locais de guarda da documentação. Para isso, convém que os procedimentos formais sejam implementados para controlar o acesso e direitos de acessos aos locais de guarda da documentação. E que eles também garantam todas "as fases do ciclo de vida de acesso do usuário, ou seja, desde o cadastro inicial até o cancelamento final do registro de usuários que já não requerem acesso" ao arquivo (se for o caso) (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, P. 66).

Assim sendo, o próximo assunto tratado aborda o registro de usuário (10.2.1). E referente a esse assunto, a Câmara Técnica de Documentos Eletrônicos (2006) enfatiza que uma das medidas mais empregadas para proteger as informações, contidas nos documentos, é por meio do cadastro dos usuários (identificador de usuário). O identificador de usuários, nesse caso, já que não se refere a sistemas informatizados, pode ser um número de cadastro (único) a fim de identificá-lo.

Os demais controles da primeira categoria (Requisitos de negócio para controle de acesso - 10.1) tiveram muitas modificações devido ao controle de acesso, na Norma original, referir-se também ao acesso a sistemas informatizados e uso de computadores, rede, etc. Os controles que foram retirados da Adaptação (conforme numeração da Norma ANBT NBR ISO/IEC 27002) são:

- 11.2.2 - Gerenciamento de privilégios;
- 11.2.3 - Gerenciamento de senha do usuário;
- 11.2.4 - Análise crítica dos direitos de acesso de usuário.

Vale relembrar que as numerações da Adaptação e da Norma diferenciam-se devido à Adaptação conter dois (2) capítulos ou seções a menos que a Norma original. As demais categorias presentes na Norma modelo juntamente com seus controles foram excluídas da Adaptação. As categorias que não estarão presentes na Adaptação e o objetivo que explica sua eliminação são:

- 11.3 - Responsabilidades dos usuários: o objetivo é prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação.

- 11.4 - Controle de acesso à rede: o objetivo é prevenir acesso não autorizado aos serviços de rede.

- 11.5 - Controle de acesso ao sistema operacional: o objetivo é prevenir o acesso não autorizado aos sistemas operacionais;

- 11.7 - Computação móvel e trabalho remoto: o objetivo é garantir a segurança da informação quando se utilizam a computação móvel e os recursos de trabalho remoto.

Os requisitos retirados da Adaptação da Norma objetivam evitar o acesso não autorizado aos sistemas de informação e não proporcionam controles para o acesso às informações não digitais, foco da pesquisa. Faz-se necessário relembrar que o controle de acesso em instituições é regra que determina quem está autorizado ou não a acessar determinados conjuntos documentais e em que ocasião isso é consentido (INSTITUTO DOS ARQUIVOS NACIONAIS/TORRE DO TOMBO, 2002). Vale ressaltar que o acesso não autorizado pode ser evitado por meio do cadastro dos usuários do arquivo, do monitoramento do acesso físico e do ambiente e, também, com o comprometimento dos usuários e funcionários para gerenciar a segurança das informações institucionais.

A última categoria que aparece na Adaptação chama-se controle de acesso à informação (10.3), lembrando que na Norma original denominava-se controle de acesso à aplicação e à informação (11.6). O objetivo do controle dessa categoria é evitar o acesso não autorizado à informação arquivística que esteja sob a guarda da instituição. E, para isso, o acesso só pode ser concedido para usuários autorizados. Nesse sentido, a Câmara Técnica de Documentos Eletrônicos (2006) afirma que, para uma gestão arquivística ser eficaz, deve-se

adotar o controle de acesso e outros procedimentos que garantam a segurança dos documentos, definindo os tipos de usuários e tipos documentais que podem ser acessados.

A próxima divisão de categoria, e última na Adaptação da Norma, refere-se à restrição de acesso à informação (10.3.1). Para atingir seu controle, é necessário que o acesso à informação seja restrito de acordo com a política de controle de acesso, definida pela instituição. Entretanto, essa política deve estar em consonância com a política de acesso da instituição.

Na área arquivística, destaca-se o autor José Maria Jardim, cujos estudos resultam em ações a fim de incentivar a promoção e elaboração de Políticas Públicas. Essas políticas podem ser consideradas como "um instrumento de planejamento, racionalização e participação popular [...] podem ser compreendidas como respostas do Estado aos direitos coletivos da população" (SOUSA, 2006, p.3). Assim, a aplicação de Políticas Públicas contribui diretamente nas questões referentes ao acesso à informação e demais ações que envolvem a gestão de documentos em arquivos públicos ou privados.

5.7 Gestão de incidentes em segurança da informação - Seção 7, Capítulo 11

Como a Norma é voltada para sistemas de informação, a maioria dos requisitos apresentados neste capítulo é voltada para gestão de incidentes em sistemas informatizados. Por isso, alguns controles foram excluídos na Adaptação. Mesmo assim, esse assunto pode ser considerado relevante para a implementação em arquivos. Nesse sentido, a maioria dos termos utilizados na Adaptação permaneceu igual aos da Norma original, a fim de manter a fidelidade aos requisitos de segurança da informação. Apesar de não tratar de termos arquivísticos, a sua compreensão é simples e indispensável para a aplicação dos requisitos de gerenciamento dos incidentes em segurança da informação.

Para tanto, a primeira categoria que aparece na Adaptação da Norma refere-se à notificação de fragilidades e eventos de segurança da informação (11.1). O objetivo de controle dessa categoria é assegurar que fragilidades e eventos de segurança da informação relacionados com os ativos de informação (não digitais) sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil. Nesse sentido, Campos (2007, p. 204) alega que

“mesmo que não tenha ocorrido eventos suspeitos, mas se um colaborador identifica uma eventual fragilidade no sistema de segurança da informação, provavelmente em um de seus controles essa fragilidade também precisa ser comunicada imediatamente”. Esse procedimento é necessário para evitar qualquer possibilidade de ocorrência de incidente.

Desse modo, a primeira subdivisão dessa categoria é notificação de eventos de segurança da informação (11.1.1). Para a aplicação desse controle, é necessário que os eventos de segurança da informação sejam relatados à direção o mais rápido possível, evitando perdas desnecessárias. Assim, “todos os colaboradores devem estar envolvidos de forma a contribuir com a redução de incidentes de segurança” (ANDRADE, 2011, p. 68).

As informações adicionais que aparecem nessa subdivisão citam exemplos de incidentes de segurança da informação que envolvem informações digitais e não digitais, na Norma original. No entanto, na Adaptação da Norma, foram citados apenas exemplos de incidentes de segurança da informação a serem aplicados para informações não digitais. Assim, os incidentes mais comuns são:

a) roubo ou extravio de informação;

b) acesso não autorizado (violação de acesso);

c) erros humanos;

d) não conformidade com políticas ou diretrizes;

e) violações de procedimentos de segurança física;

f) desastres naturais que danificaram a informação (documentação arquivística);

h) divulgação de informações sigilosas.

Após o conhecimento dos incidentes em segurança da informação que envolva informações não digitais, é necessário que funcionários, fornecedores, terceiros e usuários tenham ciência da sua responsabilidade em relatar a ocorrência de um evento em segurança da informação. Assim, a próxima subdivisão da categoria é notificando fragilidades de segurança da informação (11.1.2). Para aplicação desse controle, convém que funcionários, fornecedores, terceiros e usuários do arquivo sejam instruídos a registrar e notificar qualquer observação ou suspeita em relação à segurança da informação.

Dessa forma, torna-se fundamental a existência de “um procedimento formal de notificação, prevendo o uso de uma linha de comunicação, tal como um ramal telefônico, um endereço eletrônico, um sistema de informação na Intranet ou mesmo um formulário em papel” (CAMPOS, 2007, p. 204).

A segunda categoria principal apresentada no capítulo 11 (onze) refere-se à gestão de incidentes de segurança da informação e melhorias (11.2). Seu objetivo é assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação. Nesse sentido, a responsabilidade da instituição faz-se indispensável no desenvolvimento das atividades e controle delas.

Na primeira divisão dessa categoria, aparecem, então, as responsabilidades e os procedimentos (11.2.1). Nela é conveniente que os objetivos da gestão de incidentes de segurança da informação estejam em concordância com a direção. Por isso, as responsabilidades de tratamento dos incidentes devem ser claramente definidas. Mesmo assim, é necessário saber quem são os responsáveis pelos tipos de incidentes. Dessa forma, esses procedimentos devem ser registrados facilitando sua divulgação entre todos que realizam essas ações dentro da instituição (CAMPOS, 2007).

O próximo controle ou subdivisão apresentado denomina-se aprendendo com os incidentes de segurança da informação (11.2.2). O primeiro passo é a realização de análises de incidentes de segurança da informação e o resultado desse processo pode “indicar a necessidade de melhorias ou controles adicionais para limitar a frequência, danos e custos de ocorrências futuras [...]” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p. 101). Nesse sentido, Campos (2007, p. 201) salienta que mesmo com a aplicação dos controles, a fim de “prevenir e evitar incidentes de segurança da informação, estes ainda poderão acontecer. Isto pode ser indicação de que alguns dos controles não estão sendo eficazes e é um bom motivo para reavaliar o referido controle”.

Por fim, o último controle ou subdivisão apresentado é a coleta de evidências (11.2.3). Após a realização de um incidente, pode ser aberta uma ação legal (civil ou criminal), a fim de realizar a coleta de evidências para casos de ação de acompanhamento contra uma pessoa ou instituição. Todos os procedimentos devem ser realizados em conformidade com a legislação em vigor.

5.8 Gestão da continuidade do negócio - Seção 8, Capítulo 12

Quando há a ocorrência de um incidente em segurança da informação, é necessário que a instituição esteja preparada para a não interrupção de suas atividades contínuas. Por isso, o capítulo doze (12) da Adaptação da Norma apresenta a gestão da continuidade do negócio. O primeiro controle desse capítulo refere-se aos aspectos da gestão da continuidade do negócio, relativos à segurança da informação (12.1).

O controle apresentado nessa categoria é comunmente utilizado por organizações que visam ao lucro e dependem dele para sua sobrevivência, assim não podem permitir a interrupção de suas atividades. Dessa forma, o objetivo dessa delimita-se a não permitir a interrupção das atividades institucionais para proteger os processos críticos contra desastres, a fim de assegurar a sua retomada em tempo hábil. Os planos de continuidade de negócio podem ser considerados "conjuntos de procedimentos emergenciais a serem adotados na eventualidade da ocorrência de um determinado incidente de segurança da informação" (CAMPOS, 2007, p. 209).

Em instituições arquivísticas, a gestão da continuidade do negócio pode parecer algo inovador ou até mesmo desnecessário. Porém, deve-se salientar que como benefício da aplicação da gestão da continuidade do negócio, a instituição arquivo terá subsídios para proceder em casos de incidentes em segurança da informação evitando, assim, a interrupção das atividades institucionais. Para Fontes (2008, p. 73), as instituições necessitam "elaborar um plano de continuidade que deve ser efetivo e possibilitar que a organização funcione em um nível aceitável para a sua sobrevivência e absorva possíveis impactos financeiros, operacionais e de imagem". Além disso, é relevante que as instituições tenham a consciência de que "a gestão da continuidade dos negócios não é um projeto e sim um programa evolutivo contínuo, pois não é uma atividade feita apenas uma vez" (GUINDANI, 2008, p. 62).

Por isso, na primeira subdivisão dessa categoria, aparece o controle denominado incluindo segurança da informação no processo de gestão da continuidade de negócio (12.1.1). Para o cumprimento desse controle, convém que os processos de gestão sejam desenvolvidos e mantidos com o objetivo de assegurar a continuidade do negócio (não interrupção das atividades) por toda a instituição, contemplando os requisitos de segurança da informação necessários para a continuidade do negócio na mesma.

Em primeiro lugar, para a realização da gestão da continuidade de negócio, é imprescindível a avaliação dos riscos que correm as instituições quando o assunto é segurança da informação. Assim, a próxima subdivisão denomina-se continuidade de negócios e análise/avaliação de riscos (12.1.2). O controle apresentado aqui tem o objetivo de identificar possíveis eventos que possam causar interrupções nos processos de negócio.

> Avaliar os riscos não traz em si a garantia de proteção e sim oferece uma possibilidade de se analisar vulnerabilidades e de tomar medidas que permitam reduzir as probabilidades de ocorrência e minimizar seus possíveis impactos, fazendo com que a empresa continue a trabalhar, mesmo com pequena redução no desempenho de seus processos de negócio (GUINDANI, 2008, p. 57).

Logo depois, aparece, na Adaptação da Norma, a subdivisão denominada desenvolvimento e implementação de planos de continuidade relativos à segurança da informação (12.1.3). Os planos devem ser desenvolvidos para assegurar a disponibilidade da informação no momento e tempo requeridos. Vale ressaltar que o Plano de Continuidade de Negócios "é um conjunto de três outros planos: o Plano de Gerenciamento de Crises (PGC), o Plano de Continuidade Operacional (PCO) e o Plano de Recuperação de Desastres (PRD)". (SILVA et al. 2005, p. 3). No entanto, para que esse plano seja eficiente, é necessário manter uma estrutura principal para esses planos de continuidade do negócio. Por isso, o assunto abordado na próxima subdivisão da categoria é estrutura do plano de continuidade do negócio (12.1.4), cujo controle deve contemplar os requisitos de segurança da informação possibilitando a identificação de prioridades para a realização de testes e manutenção, se necessário.

Por fim, é apresentado o controle denominado testes, manutenção e reavaliação dos planos de continuidade do negócio (12.1.5). A atualização dos planos é imprescindível para o cumprimento e a realização das ações de continuidade de negócio. Por isso, a realização de testes também se faz necessária, a fim de garantir a efetividade dos mesmos. De acordo com Guindani (2008, p. 16), os testes podem ser realizados de várias formas, dentre elas:

> - Teste de Mesa: em que os participantes ensaiam a execução do plano, geralmente na mesa de reunião;
> - Teste Modular: focado em um único processo de negócio ou recurso;
> - Teste Funcional: integrado de vários processos de negócio, esse teste é mais realista por envolver vários grupos, múltiplas interfaces e considerar as interdependências existentes.

> A freqüência com que os testes serão realizados varia de acordo com a instituição, tipo de teste, quantidade de alterações sofridas nos planos ou alterações significativas nos processos de negócio.

5.9 Conformidade - Seção 9, Capítulo 13

Para a aplicação da Política de Segurança da Informação e qualquer outra política ou ação realizada dentro da instituição, seja ela pública ou privada, os requisitos aplicados devem estar em consonância com a legislação vigente. Assim, o último capítulo da Adaptação da Norma traz os controles referentes à conformidade. Vale destacar que, na Norma original, aparecem diversos requisitos e controles que são aplicados apenas para sistemas de informação e, por isso, foram suprimidos da Adaptação. A conformidade apresentada, na Adaptação da Norma, será somente referente aos requisitos legais que envolvam informações não digitais.

Desse modo, a primeira categoria apresentada denomina-se conformidade com requisitos legais (13.1). Seu objetivo de controle é evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação. Por isso, o primeiro controle ou subdivisão dentro dessa categoria refere-se à identificação da legislação vigente (13.1.1). Primeiramente, é necessário que todos identifiquem as leis, os regulamentos, os estatutos e demais normas e/ou regras escritas que devem ser conhecidas e seguidas dentro da instituição. Nesse sentido, convém que os requisitos estatutários, regulamentares e contratuais e o enfoque da instituição para atender a esses requisitos, sejam explicitamente definidos, documentados e mantidos, sobretudo atualizados.

Para a aplicação desses controles, é necessário que as instituições arquivísticas mantenham-se atentas à legislação vigente. E, com esse fim, o CONARQ disponibiliza a legislação arquivística brasileira, atualizada anualmente, em seu *site*[7]. Para a aplicação dessa Adaptação, é relevante o conhecimento da Lei nº 11.111/2005 e da Lei brasileira nº 8.159, de 08 de janeiro de 1991. Esta lei dispõe sobre a política nacional de arquivos públicos e privados, considerando a gestão de documentos como dever do Poder Público. Vale salientar que a gestão de documentos é um fator que contribuirá para a efetividade da Adaptação da

[7] <http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm>

Norma, em instituições arquivísticas. Para tanto, o conhecimento da legislação vigente é imprescindível.

O próximo controle presente na Adaptação refere-se aos direitos de propriedade intelectual (13.1.2). Alguns requisitos foram retirados, pois faziam referência ao uso de *software* e direitos de propriedade relativa ao uso de sistemas de informação. Para a Adaptação, serão consideradas as seguintes diretrizes para proteger qualquer material que possa ser considerado como propriedade intelectual:

a) divulgar uma política de conformidade com os direitos de propriedade intelectual que defina o uso legal de informação;

b) manter conscientização das políticas para proteger os direitos de propriedade intelectual e notificar a intenção de tomar ações disciplinares contra pessoas que violarem essas políticas;

c) manter de forma adequada os registros de ativos (plano de classificação de documentos) e identificar todos os ativos com requisitos para proteger os direitos de propriedade intelectual;

d) não copiar, no todo ou em partes, livros, artigos, relatórios ou outros documentos, além daqueles permitidos pela lei de direito autoral.

A informação arquivística, como o documento de arquivo, deve ser autêntica e fidedigna, garantindo, assim, a segurança na transmissão das informações. Assim, o próximo assunto apresentado refere-se à proteção de registros institucionais (13.1.3). Seu controle estabelece que os registros importantes sejam protegidos contra perda, destruição e falsificação, de acordo com os regulamentos, estatutos, contratos e demais documentos institucionais. Nessa subdivisão na Norma original, foi abordada a questão dos suportes eletrônicos. Campos (2007) ressalta que o problema de armazenamento e mídias eletrônicas está em manter acesso contínuo ao longo dos anos.

Nesse sentido e tendo em vista o foco da pesquisa, que é a segurança de informações não digitais, optou-se por citar apenas requisitos para a proteção de registros institucionais em suporte não digital. E, de acordo com Reginato (2003), o papel pode ser considerado um dos suportes mais utilizados atualmente para a escrita. Essa afirmação vai ao encontro de Pedro (1996) quando afirma que o papel seria o suporte mais seguro, já que não deixa apagar os

vestígios, sendo possível identificar o efeito da borracha ou do corretivo. O mesmo não se aplica aos suportes magnéticos, pois é difícil identificar uma modificação.

A última subdivisão da categoria conformidade com requisitos legais (13.1) é denominada proteção de dados e privacidade de informações pessoais (13.1.4). Para a aplicação desse controle, é conveniente que "a privacidade e proteção de dados sejam asseguradas conforme exigido nas legislações relevantes, regulamentações e, se aplicável, nas cláusulas contratuais" (ASSOCIAÇÃO BRASILEIRA DE NORMA TÉCNICAS, 2005, p. 110). Como as demais subdivisões dessa categoria referenciavam informação digital, foram suprimidas da Adaptação. Assim, os controles que foram retirados da Adaptação (conforme numeração da Norma ANBT NBR ISO/IEC 27002) são:

- 15.1.5 Prevenção de mau uso de recursos de processamento da informação;
- 15.1.6 Regulamentação de controles de criptografia.

E, por fim, a segunda categoria principal do capítulo treze (13) refere-se à conformidade com Normas e políticas de segurança da informação (13.2). Vale destacar que essa categoria, na Norma original, também abrangia a questão da conformidade técnica, que foi retirada para Adaptação, pois referenciava apenas sistemas de informação. O objetivo dessa categoria é garantir conformidade com as políticas e normas institucionais de segurança da informação. Na sequência, o próximo controle apresentado nessa categoria refere-se diretamente à conformidade com as políticas e normas de segurança da informação (13.2.1). A responsabilidade com a Política de Segurança da Informação, o cumprimento da legislação, estatutos e demais diretrizes institucionais cabe ao gestor da informação. Nesse caso, o arquivista (em instituições arquivísticas) deve cumprir esse papel de analisar a conformidade com a legislação vigente.

As demais subdivisões dessa categoria referenciavam informação digital e foram suprimidas da Adaptação. Os controles que foram retirados na Adaptação (conforme numeração da Norma ANBT NBR ISO/IEC 27002) são:

- 15.2.2 Verificação da conformidade técnica;
- 15.3 Considerações quanto à auditoria de sistemas de informação;
- 15.3.1 Controles de auditoria de sistemas de informação;

- 15.3.2 Proteção de ferramentas de auditoria de sistemas de informação.

E, por fim, a Adaptação da Norma traz um glossário com termos referenciados na Norma ABNT NBR ISO/IEC 27002 e também um conjunto de termos arquivísticos relevantes para a compreensão da mesma. Vale ressaltar que, na Norma modelo, ao invés de um glossário no final da mesma, o capítulo dois (2) apresentava uma relação de termos e definições. Estes, por sua vez, referenciavam apenas sistemas de informação. Foi devido a esse fato que se optou pela elaboração do glossário, para abranger, também, termos referentes à segurança de informações arquivísticas (não digitais), foco da pesquisa.

Dessa forma, pode-se afirmar que os resultados obtidos nesse capítulo culminaram para a construção da Adaptação da Norma brasileira ABNT NBR ISO/IEC 27002 para a segurança das informações arquivísticas não digitais (Apêndice C). Com essa Adaptação, será possível estimular as instituições arquivísticas para a elaboração de Políticas de Segurança da Informação, contribuindo para reduzir os riscos decorrentes da falta de segurança em arquivos. Entretanto, todos os controles apresentados ao longo da Adaptação da Norma devem ser implementados de acordo com a realidade de cada instituição.

Por conseguinte, com a Adaptação concluída, é possível partir para a segunda etapa da pesquisa que é a composição da Política de Segurança da Informação para o DAG. Assim, o capítulo seis abordará a análise dos dados coletados junto ao departamento, estabelecendo relações entre os dados obtidos e os objetivos propostos nesta investigação.

6 A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA O DEPARTAMENTO DE ARQUIVO GERAL DA UFSM

Neste capítulo será apresentada a análise dos dados coletados junto ao DAG. Para isso, serão discutidos, novamente, os objetivos desta investigação, com a finalidade de responder a pergunta de pesquisa proposta. A principal finalidade deste capítulo é expor a realidade em que se encontra o DAG em relação à segurança da informação não digital. Assim, em um primeiro momento, serão relatados os problemas que causam ameaças à segurança da informação arquivística no departamento. Com essa análise, será possível definir os requisitos (ações, medidas) a serem implementados para a segurança das informações (não digitais) no local e assim expor a composição do Documento da Política de Segurança da Informação para o mesmo.

6.1 A segurança da informação arquivística não digital no DAG

Quando o assunto é a segurança dos ativos de informação, é necessário ressaltar que esses são diariamente expostos a diversas vulnerabilidades ou fraquezas. Conforme Campos (2007), as vulnerabilidades podem ser as tecnologias, os processos, as pessoas e os ambientes. Entretanto, as vulnerabilidades presentes no DAG se restringem às pessoas e aos ambientes. Esse fato deve-se à pesquisa referir-se somente à segurança da informação não digital excluindo, assim, os processos e as tecnologias que estariam interligadas. Essa explicação é necessária, pois, antes de conhecer as ameaças à segurança no DAG, é relevante saber suas vulnerabilidades, partindo do princípio de que "a ameaça é um agente externo ao ativo de informação, que se aproveitando de suas vulnerabilidades poderá quebrar a confidencialidade, integridade ou disponibilidade da informação suportada ou utilizada por esse ativo" (CAMPOS, 2007, p. 25)

Dessa forma, a análise dos dados coletados no DAG seguirá o embasamento teórico conforme proposto na fundamentação teórica de pesquisa e, também, da adaptação da Norma ABNT NBR ISO/IEC 27002 para a segurança das informações arquivísticas não digitais (Apêndice B). Por isso, a fim de identificar as ameaças à segurança das informações no DAG

e propor os controles necessários para amenizar seus efeitos, serão retomadas as questões que foram levantadas na entrevista estruturada aplicada junto ao departamento. A seguir será discutido cada assunto, conforme o instrumento de coleta de dados (Apêndice A) e controles presentes na Adaptação da Norma.

6.1.1 Política de Segurança da Informação – PSI

A Universidade deve ter por meta a busca, difusão e preservação do conhecimento através do ensino, da pesquisa e da extensão. Por isso, ela pode ser definida por uma coletividade de pessoas buscando o avanço do saber para o bem da comunidade e sociedade envolvida no meio universitário. Nesse sentido, a preservação do arquivo universitário torna-se relevante tanto para docentes e discentes quanto para a sociedade em geral (ZUBEN, 2006). É nessa perspectiva que surge a Política de Segurança da Informação no contexto de arquivos universitários, a fim de possibilitar a proteção da instituição arquivo e das informações custodiadas por ele. Dessa forma a política de segurança da informação é composta por um conjunto de princípios de segurança importantes para o desenvolvimento das atividades institucionais.

Vale ressaltar que os controles aplicados em uma política de segurança por si só não garantem a eficácia da mesma. Para alcançar um nível de segurança desejável, as instituições necessitam, primeiramente, planejar suas ações e coordená-las de forma a garantir o cumprimento dos controles de segurança. Por isso, a função do gestor da informação no processo de segurança é fundamental, pois, além de coordenar a política na instituição, "ele organiza as medidas a serem implantadas na corporação para que a empresa possa estar em segurança" (ESPÍRITO SANTO, 2010, p.6).

Desse modo, o primeiro questionamento objetivou verificar quem assumia a função de gestor da informação no departamento e se essa função era conhecida por todos. Pode-se constatar que o diretor (a) do departamento assume o papel de gestor. Mesmo assim, como o departamento é responsável pelo sistema de arquivos da UFSM, realizando diversas funções, sugere-se que em cada setor tenha uma pessoa responsável pela gestão da segurança da informação. Tal medida facilitaria o controle e a responsabilidade pela política.

É nessa perspectiva que Espírito Santo (2010) afirma que a ação do gestor de segurança da informação faz-se necessária para a aplicação da política de segurança nas instituições, e seu monitoramento é essencial para o sucesso do processo de segurança da informação. O conhecimento do gestor da informação no DAG, aparentemente, é reconhecido por todos, porém o departamento não possui uma Política de Segurança da Informação instituída. Por isso, o termo "gestor da informação" ainda não se aplica ao mesmo. Após a elaboração da Política de Segurança da Informação e sua aprovação, é necessário que sejam definidos formalmente os gestores da informação no departamento de acordo com os cargos e as funções que desempenham.

6.1.2 Gestão de ativos

Uma vez definida a responsabilidade dos gestores da informação, é necessário que a instituição preocupe-se com o gerenciamento dos ativos de informação. Para isso, é preciso salientar que a pesquisa estudará apenas a segurança de ativos de informação (não digitais) no DAG. A adaptação da norma é específica para a segurança de informações arquivísticas não digitais, cujo objetivo é a proteção de ativos de informação, nesse caso, os documentos arquivísticos. Vale lembrar que todo arquivo é constituído de informação, portanto, nos documentos encontramos a informação registrada. Santos, Innarelli e Souza (2007) afirmam que essa informação, contida no documento de arquivo, é resultante de uma atividade que o produziu e, por isso, essa informação torna-se vinculada a ela.

O DAG tem sob sua custódia documentos de caráter permanente, procedentes de órgãos administrativos e das unidades de ensino, pesquisa e extensão da UFSM. Dentre as funções designadas pelo departamento está a de proporcionar acesso contínuo aos documentos. Entretanto, o acesso deve ser controlado, a fim de garantir a efetividade das ações de segurança no departamento. Por isso, a consulta aos documentos no local só pode ser feita mediante solicitação, sendo realizada tanto pelos servidores técnico-administrativos, docente e alunos, como pela comunidade em geral. Mesmo assim, a maioria dos usuários do arquivo no DAG pertence à comunidade universitária. Na opinião de Fontes (2008, p. 124),

> O usuário é o fator crítico de sucesso em um processo de proteção da informação. Devem existir regras e normas rígidas, mesmo aquelas que não são simpáticas aos usuários, porém todo o processo de proteção deve contar com o comprometimento do usuário em proteger um dos bens mais importantes da organização: a informação.

Vale ressaltar que um dos pontos mais relevantes dentro da PSI é a questão da conscientização e responsabilidade pelo gerenciamento da informação. O usuário deve ter a plena consciência de seu papel como instrumento no processo de segurança da informação dentro da instituição. Por isso, Fontes (2008) utiliza-se da argumentação de que de nada adiantaria uma grande estrutura de segurança se as pessoas dentro da organização não compreenderem os conceitos e não agirem a fim de aplicá-los.

Evidentemente que, para a aplicação da segurança da informação, no DAG, além dos usuários do arquivo, os funcionários exercem papel fundamental no tratamento e na conscientização em segurança da informação. Do comprometimento delas dependerá a efetividade do processo de segurança no departamento. Assim, um dos questionamentos da entrevista foi em relação ao número de funcionários que trabalhavam no local. Foi possível averiguar que o departamento possui vinte e dois (22) servidores efetivos e dois (2) contratados. Esses exercem suas funções de acordo com a estrutura organizacional do DAG (Anexo A) distribuídos em: divisão de protocolo, divisão de arquivo permanente, divisão de arquivos setoriais e laboratório de reprografia.

6.1.3 Segurança em recursos humanos

Na Adaptação da Norma, os controles abordados na seção sete (7) segurança em recursos humanos trazem questões referentes a todo o processo de contratação de pessoal nas instituições. As pessoas são consideradas uma parte vulnerável no processo de segurança da informação, pois são elas as responsáveis pela execução dos processos no meio institucional. Do ponto de vista de Fontes (2008, p. 129), “para desenvolver pessoas em segurança da informação é necessário conscientizar e treinar os usuários de uma maneira sob medida para cada organização”.

Primeiramente, é necessário afirmar que, como não existe a Política de Segurança da Informação no DAG, também não há um programa para conscientização e treinamento dos usuários, funcionários e terceiros em segurança da informação. Entretanto, segundo o entrevistado, a maioria dos funcionários conhece as suas responsabilidades no que tange à segurança informacional. Mesmo assim, sugere-se que seja realizado o treinamento e a conscientização em segurança da informação antes de aplicar a política no departamento. Para Ferreira e Araújo (2008), o treinamento pode ser realizado através de palestras de conscientização, elaboração de cartazes, avisos entre outros. Ao investir nessas ações, a instituição tem mais chance de alcançar sucesso no processo de segurança.

Outro ponto abordado na Adaptação da Norma é referente à devolução de ativo e retiradas de permissão de acesso, quando ocorre encerramento ou mudança de contratação do funcionário. Em conformidade com os controles da adaptação, no DAG, quando o servidor é aposentado ou afastado, ele perde o acesso aos sistemas informatizados, aos equipamentos e documentos institucionais. Esse procedimento é fundamental para impedir que os funcionários levem consigo informações ou documentos que possam comprometer a instituição. A fim de evitar esses inconvenientes, "os desligamentos devem ser comunicados a todas as áreas relevantes da organização" (CAMPOS, 2007, p. 165).

Enfim, para a efetividade da Política de Segurança da Informação, é necessário que os funcionários no momento da contratação compreendam suas responsabilidades, quanto à segurança, e as punições, caso haja descumprimento da mesma. Por isso, "convém que exista um processo disciplinar formal para os funcionários que tenham cometido uma violação da segurança da informação" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p.28). Desse modo, é aconselhável que o DAG elabore um Termo de Compromisso com o objetivo de comprometer formalmente funcionários, usuários e terceiros a seguir a política de segurança. O termo deve ser firmado no momento de contratação, para funcionários, ou a partir da aprovação da política, para todos.

6.1.4 Segurança física e do ambiente

Para Campos (2007, p. 24), "os ambientes são suscetíveis a incêndios, enchentes, terremotos e outras catástrofes". Por isso, em relação à segurança da informação, o ambiente

apresenta-se como uma das partes vulneráveis. A fim de possibilitar a segurança dos ativos de informação, convém, principalmente, que os locais de guarda da documentação sejam protegidos por perímetros de segurança, com barreiras e controles de acesso. Os perímetros de segurança podem ser "barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p. 32).

No DAG, um dos perímetros de segurança existentes corresponde ao serviço de portaria e abrange apenas a entrada do prédio da administração central, ou seja, esse controle é para todo o prédio e não apenas para o departamento. Dessa forma, não há impedimento que compreenda a entrada indevida de pessoas em suas dependências. Um dos fatores que contribui para esse fato pode ser o livre acesso pela porta de entrada (Figura 2) ao departamento, pois essa geralmente permanece aberta. Assim, faz-se necessário que, nos locais de processamento de informação, as pessoas devem ser orientadas "para que portas e janelas sejam trancadas quando estiverem sem monitoração" (SILVA, 2009, p. 7).

Figura 2 - Porta de entrada para as dependências do DAG

A porta de entrada permanecendo aberta está suscetível ao acesso de pessoas não autorizadas, representando, assim, uma ameaça à segurança das informações no

departamento. Nesse sentido, a Associação Brasileira de Normas Técnicas (2005. p. 32) recomenda que as todas as portas "sejam adequadamente protegidas contra acesso não autorizado por meio de mecanismos de controle, por exemplo, barras, alarmes, fechaduras etc.". Por isso, recomenda-se que a porta permaneça fechada, para que somente pessoas autorizadas possam acessar os ambientes do departamento.

Outro fato preocupante no que tange à segurança física e ao acesso no DAG é a ausência de um registro formal para visitantes. Esse registro é realizado pelo sistema de portaria do prédio, porém não compreende o controle de visitação às dependências e/ou salas do acervo. O Fórum do Patrimônio Documental (2006) salienta que as instituições devem realizar o registro das consultas, para controle da instituição. Esse instrumento deve conter o horário de entrada e saída do pesquisador, e algumas informações pessoais facilitando, se necessário, a identificação de quem e quando utilizou o acervo. Desse modo, pode-se verificar que os problemas que causam ameaças à segurança da informação no DAG, principalmente, estão relacionadas à deficiência nos perímetros de segurança e à inexistência de um controle de acesso físico, incluindo as entradas e saídas das dependências do departamento e do seu acervo.

Ricardo (2009) afirma que uma das formas de minimizar esses problemas de segurança pode ser através da aplicação de sistemas de vigilância, porém só serão efetivos se complementados por outras ações de controle. No prédio do DAG (prédio da administração central), existe o monitoramento por câmeras de segurança. Esse controle é realizado pelo serviço de vigilância da UFSM e serve apenas para monitorar a entrada principal do prédio, não cobrindo as dependências do departamento.

Nesse sentido, sugere-se como medida de controle para o departamento o monitoramento por câmeras de segurança principalmente cobrindo a área correspondente à entrada do acervo documental (Figura 3), que se localiza no subsolo do prédio. Essa porta permanece trancada com chave, porém todos os funcionários da divisão permanente e pessoal terceirizado (limpeza) possuem permissão de acesso ao local. O uso de câmeras de segurança possibilitará o controle da movimentação no arquivo, facilitando a identificação em casos de incidentes de segurança da informação.

Figura 3 - Entrada do acervo documental do DAG

A próxima sequência de questionamentos buscou verificar a situação de prevenção contra ameaças ambientais que possam causar riscos à segurança da informação não digital no departamento. Primeiramente foi questionada a realização da análise e avaliação, contemplando as principais ameaças ambientais: incêndio, roubo, enchente e vazamento de água. Desse questionamento, pode-se verificar que no DAG a responsabilidade pela segurança física e manutenção é delegada a Pró-Reitoria de Infraestrutura[8].

Por esse motivo, no departamento não se obteve muitas informações a respeito do assunto. Mesmo assim, buscou-se saber se, em caso de incidentes, havia uma ação realizada a fim de corrigir e evitar riscos provocados por causas naturais. Conforme o entrevistado, são realizadas vistorias anuais correspondendo à manutenção e adequação de extintores de incêndio. Salienta-se que as demais ações para evitar outros tipos de incidentes ambientais (como vazamento de água) não foram mencionadas. Entretanto, essa situação está em consonância com Ohira (2008, p. 9) quando relata que geralmente em arquivos são aplicadas apenas medidas básicas para roubos e incêndios.

[8] Em 27/03/2009 o Conselho Universitário, na sua 691ª Sessão, aprova a transformação da Prefeitura da Cidade Universitária em Pró-Reitoria de Infraestrutura- PROINFRA, Res. Nº. 001/2009 do Gabinete do Reitor em 30/03/2009 com a Estrutura Organizacional compatível com suas necessidades.

Assim, pode-se notar que são realizadas ações para prevenção de incêndio no local, constatadas pela presença de extintores de incêndio (Figura 4) espalhados nos ambientes e corredores do departamento e por toda a área de guarda da documentação. E, conforme informações da Pró-Reitoria de Infraestrutura, estão de acordo com as normas e os regulamentos legais e são vistoriados uma vez por ano.

Figura 4 - Sinalização de extintor de incêndio

A proteção contra incêndios é regida pela Norma Reguladora – NR 23. Conforme essa Norma, só podem ser utilizados extintores de incêndio que satisfaçam às normas brasileiras ou os regulamentos técnicos do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial - INMETRO. Para o estudo no DAG, como já foi dito, as Normas, aparentemente, estão de acordo com os requisitos legais e são exercidas pela Pró-Reitoria de Infraestrutura da UFSM.

Entretanto, foi possível verificar que algumas medidas de prevenção de incêndio não estão sendo periodicamente revisadas. As portas e paredes do acervo documental do DAG deveriam ser resistentes ao fogo, conforme a normalização. Da mesma forma que os alarmes de incêndio (Figura 5) do acervo documental deveriam estar funcionando.

Figura 5 - Alarme de incêndio desativado

As instituições, muitas vezes, reagem ao incidente depois que ele acontece. Nesse sentido, Silva (2009, p. 4) salienta que um "programa de segurança física é o passo inicial para a segurança da corporação no sentido de proteger as suas informações contra acessos indevidos". Tendo isso em vista, recomenda-se que, em primeiro lugar, seja revisada a questão da segurança física no departamento e posteriormente seja elaborado um projeto. Esse deve ser estruturado com a parceria da Pró-Reitoria de Infraestrutura, contemplando apenas a questão física e ambiental, a fim de possibilitar maior proteção para o acervo e também para as pessoas envolvidas nas atividades institucionais.

6.1.5 Gerenciamento das operações e comunicações

Vale lembrar que este assunto é referenciado no capítulo nove (9) da Adaptação da Norma. Nesse capítulo permaneceram apenas controles referentes a serviços terceirizados, sendo retirados os demais controles que referenciavam informação digital. Nesse sentido, no DAG objetivou-se verificar se os serviços realizados por terceiros eram monitorados, a fim de evitar a ocorrência de problemas de segurança que envolvesse os mesmos. De acordo com Campos (2007), os prestadores de serviços podem ter dois tipos de acessos às informações

institucionais. O primeiro através do acesso físico, durante a realização de suas atividades, e o segundo através do acesso lógico, envolvendo acesso aos sistemas de informação.

No DAG apenas o serviço de limpeza é terceirizado e ocorre durante o horário de expediente da instituição. Esse tipo de serviço é realizado permanentemente e o acesso é inevitável para que cumpram suas atividades. Assim, os prestadores de serviço possuem acesso livre às salas do departamento. A falta de um controle de acesso físico no local possibilita a ocorrência de incidentes em segurança da informação. Devido a fatos como esse, os contratos com terceiros "precisam garantir a segurança das informações, inclusive a cláusula e indenização em caso de incidentes de segurança causados por esses prestadores de serviços" (CAMPOS, 2007, p. 155).

A segurança dos ativos de informação deve, também, ser de responsabilidade daqueles que realizam serviços terceirizados. Acidentes podem ser evitados. Por isso, prestadores de serviço devem estar cientes de sua responsabilidade pela segurança da informação no departamento. Como no DAG o objeto de trabalho é a informação, os cuidados com ela são fundamentais para possibilitar seu acesso contínuo. Por isso, a fim de proteger e evitar a perda dessas informações, existem recomendações especiais para a higienização em arquivos.

Um exemplo disso é o uso de produtos químicos, que pode acelerar a deterioração dos documentos, afetando assim um dos princípios de segurança da informação: a disponibilidade. Desse modo, a forma mais apropriada para a limpeza do chão, nas áreas de guarda de documentos, seria com o uso do aspirador de pó. Nesses locais deve ser evitado o uso de cera, de produtos de limpeza e até de água (CASSARES, 2000). Para a realização de procedimentos de preservação do acervo, o DAG conta com um Manual de Preservação de Documentos elaborado pela Arquivista Débora Flores.

Entretanto, o DAG não possui uma Política de Segurança das Informações e não realiza ações a fim de aplicá-la. Apenas, pode-se verificar que, no departamento, são aplicadas medidas para a preservação do acervo. Essas ações contribuirão para a Política de Segurança da Informação, já que colaboram com a segurança física dos documentos. Esse fato pode ser resultante das ações que são realizadas no departamento para a gestão de documentos. De acordo com Valentim (2008), a Gestão de Documentos deve ter como finalidade, além do gerenciamento, a manutenção e a preservação de documentos, a fim de apoiar as funções e atividades institucionais.

6.1.6 Controle de acessos

Em um primeiro momento, pode-se verificar que no DAG tanto as chefias quanto os servidores da divisão de arquivo permanente possuem permissão para acesso aos documentos. Da mesma forma aos usuários do arquivo é permitido o acesso. Vale lembrar que os usuários, nesse caso, correspondem aos servidores de outras unidades da UFSM, cujos documentos estão sob custódia do departamento.

Nessa perspectiva, a Câmara Técnica de Documentos Eletrônicos (2006) salienta que o controle do acesso é uma medida que deve ser realizada com o propósito de monitorar o acervo documental, possibilitando a proteção e segurança das informações contidas nos documentos. Para controlar o acesso, podem ser implementadas ações como cadastro dos usuários do arquivo, crachás de identificação ou, até mesmo, a restrição do espaço do acervo a uso exclusivo dos funcionários autorizados.

Em conformidade com o autor, o uso do crachá para identificação dos funcionários é obrigatório, de acordo com determinações da instituição (UFSM). Como a maioria dos usuários também é funcionário da instituição, o uso de crachá facilitaria muito a identificação dos mesmos, possibilitando, assim, um controle mais efetivo. Entretanto, esta regra nem sempre é cumprida, segundo relatado pelo entrevistado. Nesse caso, salienta-se que um dos elementos vulneráveis dentro do departamento são as pessoas, pois, de acordo com Fontes (2008), são elas que fazem acontecer a proteção da informação.

Outra questão relevante no que tange ao controle de acesso é o cadastro de usuários, também, como forma de identificar quem consulta os documentos proporcionando mais segurança para o arquivo. No DAG não existe um registro específico para usuários, porém há um controle interno por meio de um "guia de controle de pesquisa", cujo acesso se dá por sistema eletrônico. De acordo com a Universidade Federal de Campinas (2002, p. 1), esse sistema é denomina-se SIE (Sistema de Informações Educacionais) e,

> seu desenvolvimento está fundamentado nas especificações fornecidas pela Unidade de Coordenação de Programas (UCP) do Ministério da Fazenda e da Comissão de Informática da Fundação de Apoio a Tecnologia e Ciência (FATEC) da UFSM e Ministério da Educação e Cultura (MEC) e visa adequar o sistema às necessidades das instituições de ensino superior do Brasil.

Assim, no DAG o protocolo e controle de processos são realizados por meio desse sistema (Figura 6).

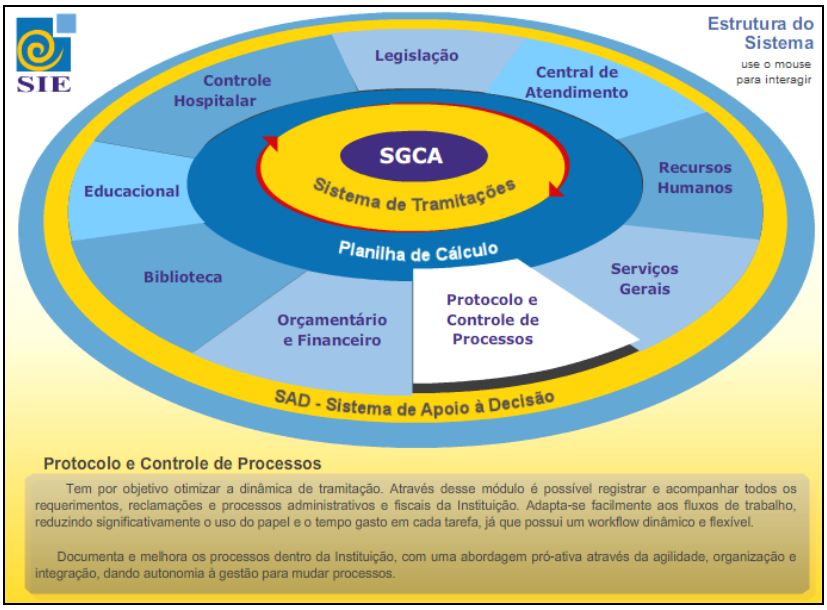


Figura 6 - Estrutura do SIE – Protocolo e Controle de Processos

Fonte: <http://w3.ufsm.br/programati/articles.php?id=5&page=4#>.

Vale ressaltar que, mesmo esse sistema sendo em meio eletrônico, ele contribui para a realização das atividades no departamento, proporcionando o maior controle dos processos. Além desse sistema, o DAG conta, também, com um Manual impresso de Normas e Procedimentos Gerais para Controle de Processos. Este visa a orientar as unidades e subunidades da UFSM a respeito da gestão dos processos, facilitando, assim, seu controle. Entretanto, alguns procedimentos podem ser alterados conforme o SIE. A respeito desse assunto, Campos (2007, p. 183) salienta que "o controle de acesso à informação deve ser controlado em algum nível, sempre de acordo com os requisitos de segurança e contribuindo de alguma forma com o negócio da organização". Em conformidade com esse autor, pode-se afirmar que o SIE e o Manual de Normas determinam alguns procedimentos de controle de acesso às informações no DAG possibilitando, mesmo que indiretamente, a segurança das mesmas.

6.1.7 Gestão de incidentes em segurança da informação

Primeiramente, é necessário lembrar que a Norma ABNT NBR ISO/IEC 27002 é voltada para sistemas de informação e, dessa forma, muitos controles foram retirados na Adaptação da mesma. O termo incidente pode ser considerado novo no que tange à segurança da informação em arquivos, porém a sua gestão é fundamental para evitar danos ou perda do patrimônio documental custodiado pelas instituições.

No DAG e em outras instituições, o primeiro procedimento que deve ser realizado, a fim de evitar a ocorrência de um problema de segurança, é a notificação. Esse procedimento possibilita a tomada de ação corretiva a tempo de evitar um desastre. Esse controle aparece, na Adaptação da Norma, na categoria denominada notificação de fragilidades e eventos de segurança da informação (11.1). De acordo com o entrevistado, os funcionários, usuários e terceiros estão cientes da responsabilidade em notificar a ocorrência de eventos em segurança no departamento. Mesmo assim, pode-se verificar que já ocorreram incidentes envolvendo a informação não digital. Os incidentes citados foram extravio de documentos e desastres naturais que danificaram a informação.

No dizer de Sêmola (2005, p. 15), as ameaças só "existem quando houver uma circunstância, potencialidade, ação ou evento que poderia romper a segurança e causar o dano". Assim, pode-se dizer que, no DAG, as vulnerabilidades compostas pelas pessoas e pelos ambientes acarretaram os incidentes. Esse efeito pode ter se agravado principalmente pela ação do primeiro grupo. Nesse sentido, afirma-se que "um dos principais problemas envolvendo a segurança do ambiente corporativo é o fator humano. Grande parte dos incidentes ocorre devido a pouca preocupação com a interação dos usuários com os diversos ambientes e sistemas da empresa" (MENEZES e TEIXEIRA, 2005, p.9).

Assim, após a identificação das vulnerabilidades que podem ter contribuído para a ocorrência dos incidentes no departamento, é necessário verificar como é realizada a identificação de incidentes no mesmo. Vale ressaltar que um dos controles para prevenir incidentes, de acordo com a Adaptação da Norma, se dá por meio da notificação de eventos de segurança da informação para a direção da instituição. O DAG encontra-se em conformidade com esse requisito da Adaptação, pois quando acontecem incidentes o fato é imediatamente comunicado ao dirigente do órgão competente.

Salienta-se que, mesmo sendo responsabilidade do DAG a notificação da ocorrência de incidentes da informação, há a necessidade de um documento formal (Termo de compromisso) com diretrizes específicas para instruir a realização de atividades de segurança da informação não digital no departamento, como já foi comentado anteriormente. Pois não basta apenas conhecer, identificar e notificar a possível ocorrência de incidentes. Devem-se, também, criar ações a fim de evitá-las. Nesse sentido, Sêmola (2005, p.2) esclarece que "qualquer processo de segurança estará tão seguro quanto à segurança oferecida pelo ativo humano que o compõe". Dessa forma, o documento da Política de Segurança da Informação será essencial para contribuir no desenvolvimento das atividades do departamento amenizando os riscos.

6.1.8 Gestão da continuidade do negócio

Nos dias atuais, é fundamental que as instituições estejam preparadas para dar continuidade às suas atividades, caso ocorra um incidente em segurança da informação, seja simples ou grave. Para isso, é necessária a aplicação de projetos para a gestão de continuidade do negócio a fim de reduzir o impacto sobre a instituição; e assim possibilitar a recuperação de "perdas de ativos da informação (que pode ser resultante de, por exemplo, desastres naturais, acidentes, falhas de equipamentos e ações intencionais) a um nível aceitável através da combinação de ações de prevenção e recuperação" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p. 103)

No caso do DAG, verificou-se no departamento que existe um plano para continuidade das atividades, porém não foi citado. Entretanto, salienta-se que esse plano contemple ações para serem realizadas em casos de incidentes com informações não digitais. Por isso, os planos de continuidade do negócio devem ser constantemente testados e revisados, a fim de garantir a eficácia da sua ação. Dessa forma, "o Plano de Continuidade deve ser estruturado para responder a determinados desastres." (SILVA et al, 2005, p. 10).

Pode-se verificar que no DAG, em casos de perda ou extravio de processo, é realizada a reconstituição do mesmo. Procedimento esse realizado a fim de manter disponível esse processo evitando que ele se perca. Esse procedimento contribui para disponibilidade das

informações, porém não se aplica a todo o acervo. Portanto, devem ser aplicadas outras ações a fim de possibilitar acesso contínuo a todo o acervo não digital custodiado pelo DAG.

6.1.9 Conformidade

A conformidade legal apresenta-se como um dos aspectos indispensáveis "para uma adequada gestão da segurança da informação, sem a qual as organizações ficam vulneráveis a incidentes de segurança" (MENEZES e TEIXEIRA, 2005, p. 16). A conformidade (seção 13) aparece como último assunto referenciado na Adaptação da Norma para a segurança de informações não digitais em arquivos.

No estudo do DAG, esse assunto foi abordado a fim de verificar se as pessoas envolvidas nas atividades (funcionário, usuários e terceiros) conhecem suas responsabilidades e obrigações legais. Assim, pode-se constatar que no departamento todos devem conhecer os estatutos, as leis contratuais e demais determinações, necessárias para o cumprimento de suas funções. Mesmo assim, já ocorreu descumprimento de algumas regras. Um exemplo disso é o uso de crachá de identificação; como o uso não é obrigatório e não existe punição ou medida disciplinar para quem não a exerce, acaba sendo descumprida.

Vale ressaltar que como não foi instituída a Política de Segurança da Informação no DAG não existem, também, normas específicas para a segurança para informações não digitais no local. Entretanto, são utilizadas algumas normas para controle de processos e para a preservação do Acervo que, indiretamente contribuem na segurança das informações no departamento. Como já foi dito anteriormente, essas normas estão presentes no Manual de Normas e Procedimentos Gerais para Controle de Processos e também no Manual de Preservação de Documentos do DAG.

Por fim, salienta-se novamente que com a aprovação da Política de Segurança da Informação no DAG os funcionários, usuários e terceiros devem concordar e assinar "os termos e condições de sua contratação para o trabalho, os quais devem declarar as suas responsabilidades e a da organização para a segurança da informação" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p. 26). Esse procedimento pode fazer toda a diferença no processo de segurança do departamento. A Política deve ser de responsabilidade

de todos, pois de nada adiantará elaborar ações a fim de proteger as informações se não há cumprimento das normas existentes para esse fim.

6.2 O Documento da Política de Segurança da Informação

A Adaptação da Norma ABNT NBR ISO/IEC 27002 para a segurança de informações arquivísticas não digitais foi um instrumento fundamental na construção da Política de Segurança da Informação para o DAG. Para elaborar o Documento da política de Segurança da Informação (Apêndice D), primeiramente, foi preciso conhecer as ameaças à segurança não digital presentes no DAG para, a partir delas, propor ações a fim de reduzir os riscos e dificultar a ocorrência de incidentes.

Pode-se verificar, assim, que os problemas que causam ameaças à segurança da informação não digital no departamento estão relacionados diretamente à deficiência dos perímetros de segurança e à inexistência de um controle de acesso físico incluindo as entradas e saídas. Salienta-se que os controles apresentados no Documento da Política de Segurança da Informação estão de acordo com as necessidades apresentadas pelo DAG no que tange à segurança de informações não digitais. Dessa forma, esse documento representa a materialização da Política de Segurança relatando o comprometimento do departamento para gerenciar a segurança das informações, objetivando sua proteção e integridade.

O primeiro item presente no documento refere-se à introdução. Em conformidade com a Adaptação da Norma, a introdução apresenta o enfoque do departamento para com a segurança de informações não digitais e a necessidade do cumprimento da política para a proteção dos ativos de informação. Na sequência, aparece o objetivo da política desenvolvida para o DAG, que é designar as ações a serem realizadas no departamento para a segurança das informações não digitais. Para cumprir esse objetivo, é necessário que todas as pessoas envolvidas nas atividades do departamento tenham claro suas responsabilidades no que se refere à questão de segurança.

Assim, no próximo item aparecem as responsabilidades. Como sugerido na análise, será designado um gestor para cada divisão/setor do departamento, conforme a estrutura organizacional. Assim a departamento contará com cinco (5) gestores correspondendo à

Direção, Divisão de Protocolo, Divisão de Apoio Técnico aos Arquivos Setoriais, Divisão de Arquivo Permanente e Laboratório de Reprografia. Vale ressaltar que cabe à direção o papel principal entre os gestores. O Documento determina, também, as responsabilidades dos funcionários técnico-administrativos do DAG, dos usuários do arquivo, que em sua maioria é representada por funcionários da UFSM. E, ainda, define as responsabilidades para serviços terceirizados que, no caso do departamento, correspondem ao serviço de limpeza.

As normas, regras e ações a serem aplicadas para a segurança de informações não digitais no departamento aparecem como próximo item do Documento. O Termo de Compromisso foi elaborado para servir de instrumento para que funcionários, usuários e terceiros se comprometam formalmente a cumprir a Política de Segurança da Informação. Esse procedimento reduz o risco de incidentes em segurança decorrentes do fator humano. Na opinião da Associação Brasileira de Normas Técnicas (2005, p. 28), as "pessoas motivadas têm uma maior probabilidade de serem mais confiáveis e de causar menos incidentes de segurança da informação." Por isso que, concomitantemente com o termo de compromisso, devem ser realizadas, no departamento, ações para conscientização e treinamento dos funcionários, usuários e terceiros. Esse processo deve ser realizado em conjunto com a direção e os gestores da informação.

A princípio não foram definidos controles específicos para a segurança física e do ambiente no DAG. Foi sugerido apenas que essa questão seja revisada pela direção e pelos gestores de segurança da informação do DAG. E seja, também, elaborado um projeto específico em parceria com a Pró-Reitoria de Infraestrutura, contemplando a segurança física e ambiental, além de amenizar os riscos de segurança, poderá prevenir a ocorrência de incidentes mais graves. Contudo, a elaboração e implementação de um projeto como este pode demorar.

Em seguida, o Documento da Política de Segurança da Informação apresenta controles para monitoramento do acesso físico e do acesso à informação. Esses controles tem o objetivo de minimizar o problema de perímetro de segurança e principalmente definir a questão do controle de acesso, que não existia no departamento. Os controles são compostos por regras e ações cotidianas, a fim de evitar o acesso de pessoas não autorizadas. Foram definidos conforme a adaptação da norma e a análise das necessidades principais do DAG.

A questão dos incidentes de segurança da informação não poderia faltar na política de segurança. Assim, o Documento da política apresenta controles para serem atingidos quando houver, inicialmente, a suspeita da ocorrência de eventos de segurança no departamento, com a finalidade de evitar o acontecimento do incidente. Logo após, apresenta, também, uma lista com exemplos dos principais incidentes (conforme adaptação da norma), que podem acontecer envolvendo informações não digitais. Para que os funcionários, usuários e terceiros reconheçam esses incidentes a fim de evitá-los, o documento ainda apresentou a questão dos Planos de Continuidade do Negócio, evitando a interrupção das atividades em caso de incidentes de segurança. Para a eficácia desses planos, eles devem ser revisados e testados periodicamente. Após esses requisitos, aparece a conformidade. Seu controle define que, para o cumprimento da Política de Segurança, ela deve ser desenvolvida em conjunto com as regras, normas, leis e demais diretrizes institucionais.

O penúltimo item abordado nas diretrizes de segurança refere-se à medida disciplinar. É necessário enfatizar que funcionários, usuários e terceiros podem se sujeitar ao cumprimento da medida disciplinar, em caso de violação ou descumprimento de algum controle da Política de Segurança da Informação do DAG. Em caso de transgressão, o funcionário, usuário ou terceiro receberá uma advertência por escrito e em casos mais graves está sujeito a determinações legais. As revisões, a vigência e validade aparecem como último item do Documento, determinando que a política primeiro deve ser revisada pela direção e gestores da informação, para se aprovada, publicada e desenvolvida no departamento.

Dessa forma, o Documento da Política de Segurança da Informação será um instrumento que contribuirá para direcionar as ações de segurança, a fim de proteger as informações (não digitais) custodiadas pelo DAG. Entretanto, cabe ao departamento aprovar e implementar esse instrumento como forma de evitar incidentes proporcionando, assim, acesso seguro, confiável e continuo às informações não digitais por ele custodiadas. Esse documento poderá servir de subsídio, juntamente com a adaptação da norma para que outros arquivos universitários elaborem a sua Política de Segurança da Informação, reduzindo os riscos da falta de proteção. Por fim, vale ressaltar que a quebra dos princípios de segurança da informação (confidencialidade, integridade ou disponibilidade) pode ser inevitável. Entretanto, o que diferencia uma instituição da outra é a maneira como se preparam para reagir a essas situações (SÊMOLA, 2005).

CONCLUSÕES

As conclusões apresentadas procuram, além de responder à pergunta proposta na pesquisa, retomar e salientar os objetivos que nortearam o trabalho. Primeiramente, é importante ressaltar que a adoção de ações para a segurança da informação em instituições arquivísticas é primordial para proteger e garantir a integridade do patrimônio documental. Durante os procedimentos metodológicos, buscou-se atingir o objetivo geral de pesquisa que consistiu na elaboração de uma Política de Segurança da Informação não digital para o Departamento de Arquivo Geral da UFSM.

Primeiramente foi preciso adaptar os controles da Norma ABNT NBR ISO/IEC 27002 para a segurança das informações não digitais em arquivos. O estudo minucioso dos capítulos da Norma resultou na exclusão dos controles que faziam referência às informações digitais. Essa etapa foi necessária para compor a Adaptação da Norma, voltada para as seguranças de informações arquivísticas não digitais. Para isso, foi necessária a exclusão de dois (2) capítulos da Norma original. O capítulo doze (12) foi excluído totalmente da Adaptação, pois correspondia à Aquisição, ao Desenvolvimento e à Manutenção de Sistemas de Informação, referenciando apenas a segurança das informações digitais. Esse capítulo não poderia ser aplicado a arquivos já que o foco da pesquisa era apenas a segurança de informações não digitais.

Já o capítulo seis (6) da Adaptação, que se denominava Organizando a Segurança da Informação, também foi excluído, porém teve alguns controles vinculados ao capítulo cinco (5) da Adaptação (Política de segurança da informação). Isso foi necessário para compactar a Adaptação e estruturá-la segundo o seu foco de estudo: a segurança de informação não digital em arquivos. Dessa forma, o número de capítulos e categorias presentes na Norma original e na Adaptação são diferentes. Os capítulos ou as seções da Norma foram reduzidos, passando de onze (11) para nove (9) na Adaptação. As categorias também foram reduzidas de trinta e nove (39) da Norma original para dezesseis (16) na Adaptação.

Os requisitos correspondentes aos controles de segurança aparecem na Adaptação da norma a partir do capítulo cinco (5), como na Norma original. Vale ressaltar que o conjunto desses controles possibilita a elaboração de uma Política de Segurança da Informação. Para

compor um instrumento que permitisse a elaboração de Políticas de Segurança em arquivos, foi necessário realizar uma alteração nos controles apresentados no capítulo seis (6) da Adaptação (Gestão de ativos). Assim, ao invés de compor um inventário de ativos, contendo uma lista de documentos arquivísticos (ativos de informação), conforme a Norma original, sugeriu-se que os ativos fizessem parte do plano de classificação de documentos da instituição, conforme metodologia arquivística. Esse procedimento foi necessário para adequar a Adaptação da norma ao contexto arquivístico.

Através dos aspectos apresentados, essa Adaptação pode estimular as instituições arquivísticas para a elaboração de Políticas de Segurança da Informação, contribuindo para reduzir os riscos decorrentes da falta de segurança em arquivos. Entretanto, salienta-se que todos os controles apresentados ao longo da Adaptação da norma devem ser implementados de acordo com a realidade de cada instituição. Nesse sentido, a versão adaptada da Norma ABNT NBR ISO/IEC 27002 para o contexto arquivístico serviu como material de referência para a elaboração da Política de Segurança da Informação no DAG.

Assim, na segunda etapa da pesquisa, que correspondeu ao estudo de caso no departamento, foram verificados, primeiramente, os problemas que causam ameaças à segurança da informação arquivística no local, por meio da análise da entrevista estruturada e da realidade institucional. Portanto, pode-se constatar que os problemas que causam ameaças à segurança da informação no DAG estão relacionados à deficiência nos perímetros de segurança e à inexistência de um controle de acesso físico incluindo as entradas e saídas das dependências do departamento e do seu acervo. Esse resultado pode ser evidenciado devido à ocorrência de incidentes em segurança da informação no departamento envolvendo a informação não digital. Os incidentes de segurança da informação que ocorreram no departamento incluem a perda de informações e os desastres naturais que danificaram a informação. As causas desses incidentes estão relacionadas, principalmente, aos problemas citados anteriormente.

A partir da definição dessas ações de segurança, foi possível, juntamente com a Adaptação da norma, estabelecer, como produto final desta dissertação, o Documento da Política de Segurança da Informação com o intuito de evitar a ocorrência de novos incidentes no departamento. Salienta-se que os controles apresentados nesse documento estão de acordo com as necessidades apresentadas pelo DAG no que tange à segurança de informações não digitais. Nesse sentido, o documento representa a materialização da Política de Segurança

relatando o comprometimento do departamento para gerenciar a segurança das informações, objetivando sua proteção e integridade.

Por isso, a organização da Política de Segurança da Informação deve ser realizada pelos gestores da informação no departamento. Conforme definido no Documento da Política de Segurança, são cinco (5) gestores da informação, que correspondem à Direção, Divisão de Protocolo, Divisão de Apoio Técnico aos Arquivos Setoriais, Divisão de Arquivo Permanente e Laboratório de Reprografia. Essas pessoas têm a responsabilidade de coordenar a política para que o departamento possa estar em segurança.

As etapas apresentadas anteriormente foram essenciais na definição das diretrizes para a segurança das informações não digitais no DAG que se encontram no Documento da Política de Segurança da Informação do mesmo. E, assim, foi possível responder ao questionamento proposto na pesquisa. Portanto, as ações ou os controles aplicados no departamento, conforme a Adaptação da norma ABNT NBR ISO/IEC 27002, para a segurança das informações arquivísticas não digitais são:

- Termo de compromisso: é um instrumento formal elaborado com a finalidade de comprometer formalmente os funcionários, usuários e terceiros a cumprir a Política de Segurança da Informação no departamento. Esse instrumento objetiva reduzir o risco de incidentes em segurança decorrentes do fator humano.

- Segurança física e do ambiente: um dos problemas de segurança da informação encontrado no departamento é devido a fatores ambientais. Por esse motivo, a questão da segurança física e ambiental deve ser revista no DAG. Deve, também, ser revisada a questão de prevenção de incêndio, como também realizado um planejamento para compra de equipamento de segurança, incluindo câmeras de monitoração, que controlem as entradas e saídas das dependências do departamento. Um projeto específico compreendendo estas e outras ações para a segurança física, além de amenizar os riscos de segurança, previne a ocorrência de incidentes mais graves.

- Controle de acesso físico e à informação não digital: como se pode verificar, no departamento não existia um controle de acesso, tanto referente à entrada e saída quanto ao acesso à documentação. Esse fator pode ter resultado nos incidentes de segurança da informação relatados no decorrer da pesquisa. Por isso, foi necessário incorporar no documento da Política de Segurança das Informações ações/controles a serem realizados a fim

de prevenir o acesso indevido às dependências do departamento e à sala de guarda da documentação. Esses controles objetivam minimizar o problema dos perímetros de segurança e principalmente definir a questão do controle de acesso, que não existia no departamento.

- Gestão de incidentes em segurança da informação: o primeiro procedimento que deve ser realizado, a fim de evitar a ocorrência de um problema de segurança é a notificação. Esse procedimento possibilita a tomada de ação corretiva a tempo de evitar um desastre. Assim o Documento da política apresenta, nesse item, controles para serem atingidos quando houver, inicialmente, a suspeita da ocorrência de eventos de segurança no departamento.

- Gestão da continuidade do negócio: a elaboração ou manutenção de um Plano de continuidade do negócio evita a interrupção das atividades quando há a ocorrência de um incidente em segurança da informação. Por isso, foi sugerido ao DAG que revise e teste periodicamente o seu Plano de continuidade do negócio principalmente envolvendo a proteção das informações não digitais.

- Conformidade: a conformidade legal é essencial para o cumprimento da Política de Segurança da Informação. Por isso, todas as ações aplicadas no departamento para segurança da informação não digital devem estar em conformidade com regulamentos, estatutos e legislação vigente.

Assim, foram atingidos certamente os objetivos propostos na pesquisa. É relevante destacar que o Documento da Política de Segurança da Informação será um instrumento que contribuirá para direcionar as ações de segurança, a fim de proteger as informações (não digitais) no DAG. Entretanto, cabe ao departamento implementar esse instrumento como forma de evitar incidentes proporcionando, assim, acesso seguro e contínuo às informações não digitais sob sua custódia.

Por fim, conclui-se que os resultados desta investigação poderão servir de subsídio para que outros arquivos universitários e, da mesma forma, outras instituições arquivísticas, possam elaborar a sua Política de Segurança da Informação. Para isso, recomenda-se que sejam realizados estudos, pesquisas e análises compreendendo a questão da segurança da informação e da adaptação da Norma ABNT NBR ISO/IEC 27002, possibilitando a sua revisão e complementação, pois somente assim será possível contribuir, cada vez mais, para a proteção do patrimônio documental custodiado pelas instituições arquivísticas.

REFERÊNCIAS

ANDRADE, Andresa Léia de; ALMEIDA, Daniela Pereira dos Reis de. Capacitação em serviço de arquivo: o arquivista frente aos desafios das tecnologias da informação e comunicação. **Revista EDICIC**. v.1, n.3, p.52-58, Jul./Sep. 2011. Disponível em: <http://www.edicic.org/revista/>. Acesso em 16 ago. 2012.

ANDRADE, Alex Sales. **Segurança da informação com foco em infraestrutura:** um estudo de caso em uma empresa do setor de tecnologia da informação. Lavras. Minas gerais, 2011. Disponível em: <http://www.bcc.ufla.br/monografias/2011/alexsa.pdf>. Acesso em 05 mar. 2012.

ARQUIVO NACIONAL. **Gestão de Documentos:** recurso estratégico na modernização dos serviços arquivísticos governamentais. Rio de Janeiro, março de 2004. Disponível em: <www.cinform.ufba.br/v_anais/palestras/gestao_de_documentos_ap.ppt>. Acesso em 14 abr. 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC27002** - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação (Conteúdo técnico idêntico ao da ABNT NBR ISO/IEC 17799), 2005.

BALDISSERA, Thiago André. **Gestão da Segurança da Informação em Colégio**: uma análise da utilização da Norma NBR/IEC 17799. 2007. Dissertação (Mestrado em Engenharia da Produção). Universidade Federal de Santa Maria, Santa Maria, 2007.

BARATA, Dulce Fernandes. **Os suportes da História Escrita do Homem**. Matéria publicada em 01/03/2000 - Edição Número 7. Campinas, São Paulo. Disponível em: <http://kplus.cosmo.com.br/materia.asp?co=42&rv=Literatura>. Acesso em 08 dez. 2011.

BARRETO, Aldo de Albuquerque. **A questão da informação.** Pesquisador Titular do MCT/IBICT. (Publicado na Revista São Paulo em Perspectiva, Fundação Seade, v 8, n 4, 1994). Disponível em: <http://www.e-iasi.org/DOWNLOAD/aquestao.pdf>. Acesso em 05 out. 2011.

BELLOTO. Heloísa Liberalli. **Universidade e arquivo:** perfil, história e convergência. Transinformação. V.1, n. 3, set/dez, 1989. p. 15-28.

BEYEA, Marion et. al. A Favor de Normas para a Prática Arquivística**. Acervo:** revista do Arquivo Nacional. Rio de Janeiro: Arquivo Nacional, v. 20 n. 1-2, p. 31-38, jan/dez 2007.

BOSO, Augiza Karla et al. Importância do Arquivo Universitário. **Revista ACB**: Biblioteconomia em Santa Catarina, V. 12, n. 1, 2007, p.123-131. Disponível em <http://www.acbsc.org.br/revista/ojs/viewissue.php?id=20>. Acesso em 20 dez. 2011.

BRASIL. Arquivo Nacional. **Dicionário brasileiro de terminologia arquivística.** Rio de Janeiro: Arquivo Nacional, 2005. Disponível em: <http://www.portalan.arquivonacional.gov.br/Media/Dicion%20Term%20Arquiv.pdf>. Acesso em 28 mar. 2007.

BRASIL. Conselho Nacional de Arquivos. **Lei n. 8.159, de 8 de janeiro de 1991.** Dispõe sobre a política nacional de arquivo público e privados e dá outras providências. Diário Oficial. Brasília, n. 6, p. 455, 9 de janeiro de 1999, seção 1.

BRASIL. **Constituição da República Federativa do Brasil**. Presidência da República, Casa Civil, Subchefia para assuntos jurídicos. Brasília, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm>. Acesso em 4 jun. 2007.

BRASIL. Ministério da Ciência e Tecnologia. **Política de Segurança para Arquivos, Bibliotecas e Museus.** Museu de Astronomia e Ciências Afins - MAST. Rio de Janeiro – RJ, 2006.

BRASIL. Ministério da Justiça. **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. Publicado no DOU de 14.6.2000. Disponível em: <http://www.jf.jus.br/cjf/tecnologia-da-informacao/gestao-documental/seguranca-da-informacao/gsi-pr/Dec3505-13junho2000_Institui%20a%20PSI%20na%20APF.pdf/view>. Acesso em 25 out. 2011.

BRASIL. Ministério da Justiça. **Memória do Mundo.** Diretrizes para a salvaguarda do patrimônio documental. Edição revisada, 2002. Divisão da Sociedade da Informação Organização das Nações Unidas para Educação, Ciência e Cultura. Disponível em: <http://www.portalan.arquivonacional.gov.br/Media/Diretrizes%20para%20a%20salvaguarda%20do%20patrim%C3%B4nio%20documental.pdf>. Acesso em 10 out. 2011.

BRASIL. Tribunal de Contas da União. **I Fórum sobre as Instituições Federais de Ensino Superior.** Brasília, 2008. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2056834.PDF>. Acesso em 03 ago. 2011.

BRITO, Djalma Mandu de. **A informação arquivística na arquivologia pós-custodial.** Arquivística.net - www.arquivistica.net. Rio de Janeiro, v.1, n.1, p. 31- 50 jan/jun. 2005.

CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS. **Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos:** e-ARQ. Conarq, 2006. Disponível em: <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/earqbrasilv1.pdf>. Acesso em 09 out. 2007.

CAMPOS, André. **Sistema de Segurança da Informação:** controlando os riscos. 2. ed. Florianópolis: Visual Books, 2007.

CAPEMISA. **Diretrizes e Políticas de Segurança da Informação.** Conselho de Administração, 2008. Disponível em: <http://www.capemisa.com.br/SegurancadaInformacao.pdf>. Acesso em 14 mai. 2010.

CASSARES, Norma Cianflone. c**omo fazer conservação preventiva em arquivos e bibliotecas**. São Paulo: Arquivo do Estado: Imprensa Oficial, 2000.

CASTANHO, Denise Molon; GARCIA, Olga Maria Correa; SILVA, Rosani Beatriz Pivetta. **Arranjo e descrição de documentos arquivísticos.** Santa Maria: Universidade Federal de Santa Maria, 2006.

CONSELHO NACIONAL DE ARQUIVOS - CONARQ. Câmara Técnica de Documentos Eletrônicos. **E-ARQ BRASIL**: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos. 2006.

COSTA, Regivaldo Gomes; ALMEIDA, Henrique Andrade de. **Terceirização de Serviços de TI:** Aspectos de Segurança. Programa de Pós-Graduação Latu Sensu – Universidade Católica de Brasília, 2010. Brasília – DF. Disponível em: <http://rclabs.com.br/docs/papers/Terceirizacao_de_Servicos_de_TI-Aspectos_de_Seguranca.pdf>. Acesso em 15 jun. 2012.

ESPÍRITO SANTO, Adrielle Fernanda Silva do. **Segurança da Informação**. Departamento de Ciência da Computação - Instituto Cuiabano de Educação (ICE). Cuiabá – MT – Brasil, 2010. Disponível em: <http://www.ice.edu.br/TNX/storage/webdisco/2011/03/11/outros/2bc3b892c73868cf712dcf084ed96b8a.pdf>. Acesso em 14 mai. 2011.

FARIAS, Karla Meneses et al. **A história dos registros do conhecimento.** Universidade Federal da Paraíba. Encontro Nacional de Estudantes de Biblioteconomia, Documentação, Gestão e Ciência da Informação, de 18 a 24 de julho de 2010. João Pessoa, 2010. Disponível em: <http://dci.ccsa.ufpb.br/enebd/index.php/enebd/article/viewFile/104/111>. Acesso em 20 fev. 2012.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Marcio Tadeu. **Política de segurança da informação:** Guia prático para embalagem e implementação. Rio de Janeiro: Ciência Moderna, 2006.

FLORES, Daniel. **Análise do Programa de Legislação Educacional Integrada - ProLEI:** uma abordagem arquivística na Gestão Eletrônica de Documentos – GED. 2000. Dissertação (Mestrado em Engenharia de Produção) – Universidade Federal de Santa Maria, Santa Maria, 2000.

FONTES, Edson Luiz Gonçalves. **Praticando a segurança da informação.** Rio de Janeiro: Brasport, 2008.

FONTES, Edison; FONSECA, Fernando Sérgio Santos; PEREIRA, Sérgio Toscano Dias. **Entendendo e implementando a norma NBR ISO/IEC 17799.** Aspectos teóricos e práticos da Norma NBR ISO/IEC 17799. Módulo 2. Academia Latino-Americana de Segurança da Informação, 2006. Disponível em: <http://pt.scribd.com/doc/65705046/20/%E 2%80%93-TRABALHANDO-EM-AREAS-SEGURAS>. Acesso em 20 mai. 2012.

FÓRUM DO PATRIMÔNIO DOCUMENTAL. **Grupo de trabalho de controle de acesso e circulação de acervo.** Documento final. Rio de janeiro, julho 2006. Disponível em <www.aab.org.br/download/GT_acervo25jul.pdf> Acesso em 1 abr. 2008.

FUNDAÇÃO OSWALDO CRUZ – FIOCRUZ. **Preservação Suporte Digital.** Rio de Janeiro, 2009. Disponível em: <http://bvsfiocruz.fiocruz.br/local/temp/Treinamento2009_1/Treinamento2009-1ApreConservacao.pdf>. Acesso em 18 dez. 2011.

GIL, Antonio C. **Métodos e Técnicas de Pesquisa Social**. 5 ed. São Paulo: Atlas, 1999.

GONÇALVES, Edmar Moraes. **Estudo das estruturas das encadernações de livros do século XIX na coleção Rui Barbosa:** uma contribuição para a conservação-restauração de livros raros no Brasil. 2008. Dissertação (Mestrado em Artes). Escola de Belas Artes da Universidade Federal de Minas Gerais - UFMG. Belo Horizonte, 2008. Disponível em: <http://www.bibliotecadigital. ufmg.br/dspace/bitstream/1843/JSSS-7U5K6G/1/disserta__o_edmar_moraes_gon_alves.pdf>. Acesso em 12 jan. 2012.

GUINDANI, Alexandre. **Gestão da Continuidade dos Negócios.** Integração, V. 1, 2008. Disponível em: <http://system7.upis.br/posgraduacao/revista_integracao/gestao_continuidade.pdf>.Acesso em 26 jan. 2012.

HORA, Sergio Ricardo Almeida da; SATURNINO, Luyz Paullo Targino; SANTOS, Eliete Correia dos. **A evolução do arquivo e da arquivologia na perspectiva da história.** Universidade Estadual da Paraíba – UEPB, 2010. Disponível em: <http://www.webartigos.com/artigos/a-evolucao-do-arquivo-e-da-arquivologia-na-perspectiva-da-historia/33326/>. Acesso em 20 dez. 2011.

INDOLFO, Ana Celeste et al. **Gestão de documentos:** conceitos e procedimentos básicos. Rio de Janeiro: Arquivo Nacional, 1993.

INSTITUTO DOS ARQUIVOS NACIONAIS/TORRE DO TOMBO. **Caderno de Recomendações para gestão de documentos de arquivo electrónicos:** Modelo de requisitos para gestão de arquivos electrónicos – MoReq. Lisboa, 2002. Disponível em: <http://www.iantt.pt>. Acesso em 21 nov. 2007.

INTERNATIONAL COUNCIL ON ARCHIVES. **ICA Code of Ethics (Portuguese).** Comitê Executivo do Conselho Internacional de Arquivos. Beijing, China, 1996. Disponível em: <http://www.ica.org/5555/reference-documents/ica-code-of-ethics.html>. Acesso em 12 jan. 2012.

ISO 15489-1: 2001 - Information and documentation – Records management - Part 1: General.

JARDIM, José Maria. **Políticas públicas de informação:** a (não) construção da política nacional de arquivos públicos e privados (1994-2006). Comunicação oral apresentada ao GT-5 - Política e Economia da Informação. IX ENANCIB – Diversidade Cultural e Políticas de Informação. São Paulo, USP, 2008. Disponível em: <http://www.contagem.mg.gov.br/arquivos/downloads/jardim_-_politicas_publicas_de_informacao.pdf>. Acesso em 22 nov. 2011.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação.** Apostila, 2005. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf >. Acesso em 20 Nov. 2011.

LIMA, Maria João Pires de**. Avaliar para preservar o património arquivístico.** Biblioteca Digital. Conferência sobre arquivos universitários, 2004. Faculdade de Letras da Universidade do Porto. Disponível em: <http://ler.letras.up.pt/uploads/ficheiros/artigo5471.pdf>. Acesso em 18 dez. 2011.

MARCIANO, João Luiz Pereira. **Segurança da Informação** - uma abordagem social. Tese (Doutorado em Ciência da Informação) Brasília, 2006. Disponível em: <http://www.enancib.ppgci.ufba.br/premio/UnB_ Marciano.pdf>. Acesso em 28 jun. 2011.

MENEZES, Regina S.; TEIXEIRA, Francisco. **Gestão da segurança da informação:** práticas de segurança da informação implementadas em das organizações que atuam no estado da Bahia. Universidade Federal da Bahia, 2005. Disponível em: <http://www.rp-bahia.com.br/biblioteca/pdf/ReginaS%E1Menezes.pdf>. Acesso em 10 ago. 2012.

NAKAMURA, Emílio Tissato; GEUS, Paulo Licio de. Segurança de Redes em Ambientes Cooperativo – Novatec, 2007.

OHIRA, Maria Lourdes Blatt et al. Gestão de documentos em arquivos universitários: estudo de caso no arquivo central da FAED-UDESC. In: **CONGRESSO NACIONAL DE ARQUIVOLOGIA,** 1, Brasília, 2004. Disponível em: <http://www.udesc.br/arquivos/id_submenu/619/faed_congresso.pdf>. Acesso em 18 dez. 2011.

_____. **Arquivos públicos do Brasil:** da realidade à virtualidade. Universidade do Estado de Santa Catarina – UDESC. Florianópolis, Santa Catarina, 2008. Disponível em: <http://www.udesc.br/arquivos/id_submenu/619/artigo_arquivo_ publico.pdf>. Acesso em 12 fev. 2012.

PEDRO, José Maria. **A evolução dos suportes de informação.** In: Semanário Económico nº 492, 14 de Junho de 1996. Disponível em: <http://www.knowkapital.com/index.php?option=com_content&view=article&id=69%3A-a-evolucao-dos-suportes-de-informacao-in-qsemanario-economicoq-no-492-14-de-junho-de-1996&catid=12%3Asemanario-economico&Itemid=73&lang=pt>. Acesso em 10 jan. 2011.

PEREIRA, Carminda de Aguiar et al. **Preservação do Patrimônio Documental e resgate da memória:** um estudo de caso da Coleção "Monumento aos Bandeirantes". Encontro Nacional de Estudantes de Biblioteconomia, Documentação, Gestão e Ciência da Informação, 18 a 24 de julho de 2010. UNIVERSIDADE FEDERAL DA PARAÍBA. Disponível em: <http://dci.ccsa.ufpb.br/enebd/index.php/enebd/article/view/170/115>. Acesso em 30 nov. 2011.

PRADO, André Pires. **Relações sociais e internet:** algumas observações. Anais do XI Encontro Regional da Associação Nacional de História – ANPUH/PR. "Patrimônio Histórico no Século XXI". Jacarezinho, dos dias 21 a 24 de Maio de 2008. ISSN: 978-85-61646-01-1. Disponível em: < http://cj.uenp.edu.br/ch/anpuh/textos/017.pdf>. Acesso em 24 jan. 2011.

QUEIROZ, Rita de Cássia Ribeiro de. **A informação escrita:** do manuscrito ao texto virtual. Universidade Estadual de Feira de Santana, 2005. Disponível em: <http://www.cinform.ufba.br/vi_anais/docs/RitaQueiroz.pdf>. Acesso em 12 jan. 2012.

REGINATO, Virginia Prux. **Papel artesanal reciclado e papel artesanal de fibras naturais:** suporte de preservação ecológica. Arte e história dos suportes. Universidade do Vale do Rio dos Sinos – UNISINOS. São Leopoldo, junho de 2003. Disponível em: <http://www.sebrae.com.br/setor/artesanato/sobre-artesanato/tipologias-e-ategorias/utilitarias-e-decorativas/papel%20artesanal.pdf>. Acesso em 10 jan. 2012.

RICARDO, Carolina de Mattos. **Câmeras:** problema ou solução? Jornal da PUC (Pontifícia Universidade Católica) de Campinas, Ano V, Número 95, de 26/10 a 08/11 de 2009. Campinas, São Paulo. Disponível em: <http://www2.forumseguranca.org.br/node/23052>. Acesso em 23 nov. 2011.

RICHTER, Eneida Izabel Schirmer. **Introdução à Arquivologia.** 2. ed – Santa Maria: FACOS-UFSM, 2004.

RODRIGUES, Marly. **Imagens do Passado:** a instituição do patrimônio em São Paulo, 1969-1987. São Paulo: Ed. UNESP, Imprensa Oficial, CONDEPHAAT, 2000.

RONDINELLI, Rosely Curi. **Gerenciamento arquivístico de documentos eletrônicos:** uma abordagem teórica da diplomática arquivística contemporânea. Rio de Janeiro: Editora FGV, 2005.

ROSSATO, Carlos Alessio. **O Arquivo Público do Rio Grande do Sul na percepção de usuários***:* um ambiente a ser descoberto. 2001. 85f. Dissertação (Mestrado em administração) – Universidade Federal de Santa Catarina, Florianópolis, 2001.

SANCHEZ, Sandra. **Instrumentos da Pesquisa Qualitativa.** Disponível em: <http://www.ia.ufrrj.br/ppgea/conteudo/T2-5SF/Sandra/Instrumentos%20da%20Pesquisa%20Qualitativa.ppt#260,7,Slide 7> Acesso em 16 jun. 2009.

SANTOS, Vanderlei Batista dos. **Gestão de documentos eletrônicos:** uma visão arquivística. Brasília: ABARQ, 2005.

SANTOS, Vanderlei Batista dos; INNARELLI, Humberto Celeste; SOUZA, Renato Tarciso Barbosa. **Arquivística**: Temas contemporâneos – classificação, preservação digital, gestão do conhecimento. Distrito Federal: SENAC, 2007.

SÊMOLA, Marcos. **Gestão da Segurança da Informação – Uma visão Executiva**. Rio de Janeiro: Campus, 2003.

SERVILHA, Valdemar. (Coord.). **Planejamento estratégico em Instituições Federais de Ensino Superior:** proposta de processo participativo. Comissão de Planejamento - FORPLAD - Fórum Nacional de Pró-Reitores de Planejamento e Administração. Brasília, 1995. Disponível em: <http://www.uel.br/pei/download/FORPLAD.pdf>. Acesso em 20 jan. 2012

SFREDDO, Josiane Ayres. **O controle de acesso na percepção dos profissionais de arquivo:** uma questão de segurança das informações institucionais. Trabalho de Conclusão de Curso (Graduação em Arquivologia). Universidade Federal de Santa Maria, 2008.

_____; FLORES, Daniel. **Segurança da informação arquivística:** o controle de acesso em arquivos públicos estaduais. Perspectivas em Ciência da Informação, v.17, n.2, p.158-178, abr./jun. 2012. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/1290/1034>. Acesso em 19 de mai. 2012.

SILVA, Edna Lúcia da; MENEZES, Estera Muszkat. **Metodologia da Pesquisa e Elaboração de Dissertação.** 3 ed. rev. e atual. Florianópolis: Laboratório de Ensino a Distância da UFSC, 2001, 121p.

SILVA, Glayson Keler de Paula. **Segurança física e de ambientes.** Trabalho apresentado à disciplina de Segurança da Informação (ASI 308) como proposta de reescrever o capítulo 6 da apostila corrente. Universidade Federal de Lavras, 2009. Disponível em: <http://www.biblioteca.sebrae.com.br/bds/bds.nsf/97cc241db9bd939e03257170004bcd72/0a95ed63c5294cf283257649006607be/$FILE/Seguran%C3%A7a%20Fisica%20e%20de%20Ambientes%20por%20Glayson%20Keler.pdf>. Acesso em 19 jul. 2012.

SILVA, Maria Amélia Teixeira da et. al. A importância dos arquivos públicos na construção da memória da sociedade. **Biblionline**, João Pessoa, v. 5, n. 1-2, 2009. Disponível em: <http://periodicos.ufpb.br/ojs2/index.php/biblio/article/view/3951/3114> Acesso em 08 mar. 2010.

SILVA, Ronaldo et al. **Plano de continuidade de negócios** - planejamento. Universidade Católica de Brasília (UCB). Brasília DF – Brasil, 2005. Disponível em: <http://www.lyfreitas.com/ant/artigos_mba/artpcn.pdf>. Acesso em 13 jul. 2012.

SOUSA, Renato Tarciso Barbosa de. **O arquivista e as políticas públicas de arquivo.** Texto apresentado originalmente no II Congresso Nacional de Arquivologia, Porto Alegre - RS, julho de 2006. Disponível em: <http://repositorio.bce.unb.br/bitstream/10482/1026/1/EVENTO_ArquivistaPoliticaPublicaArquivo.pdf>. Acesso em 22 nov. 2011.

SPANCESKI, Francini Reitz. **Política de Segurança da Informação** - Desenvolvimento de um modelo de segurança da informação voltado para instituições de ensino. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação). Instituto Superior Tupy. Joinville, 2004. Disponível em: <http://www.mlaureano.org/aulas_material/orientacoes 2/ist_2004_francini_politicas.pdf>. Acesso em 20 abr. 2010.

STALLIVIERI, Luciane. **O sistema de ensino superior do Brasil:** características, tendências e perspectivas. Universidade de Caxias do Sul. Caxias do Sul, 2008. Disponível em: <http://www.ucs.br/ucs/tplCooperacaoCapa/cooperacao/assessoria/artigos/sistema_ensino_superior.pdf>. Acesso em 20 jan. 2012.

STANGER, Monica Zanellato. **Memória, Patrimônio e História:** uma abordagem prática. Centro Universitário Católico do Sudoeste do Paraná – UNICS, Paraná, 2009. Disponível em: <http://www.diaadiaeducacao.pr.gov.br/portals/pde/arquivos/2513-8.pdf>. Acesso em 23 nov. 2011.

TAFFAREL, Celi Zulke. **Sobre as instituições federais de ensino superior e as fundações de apoio:** o que fazer? Universidade Federal da Bahia - UFBA, 2009. Disponível em: <http://www.faced.ufba.br/rascunho_digital/textos/906.htm>. Acesso em 20 fev. 2012.

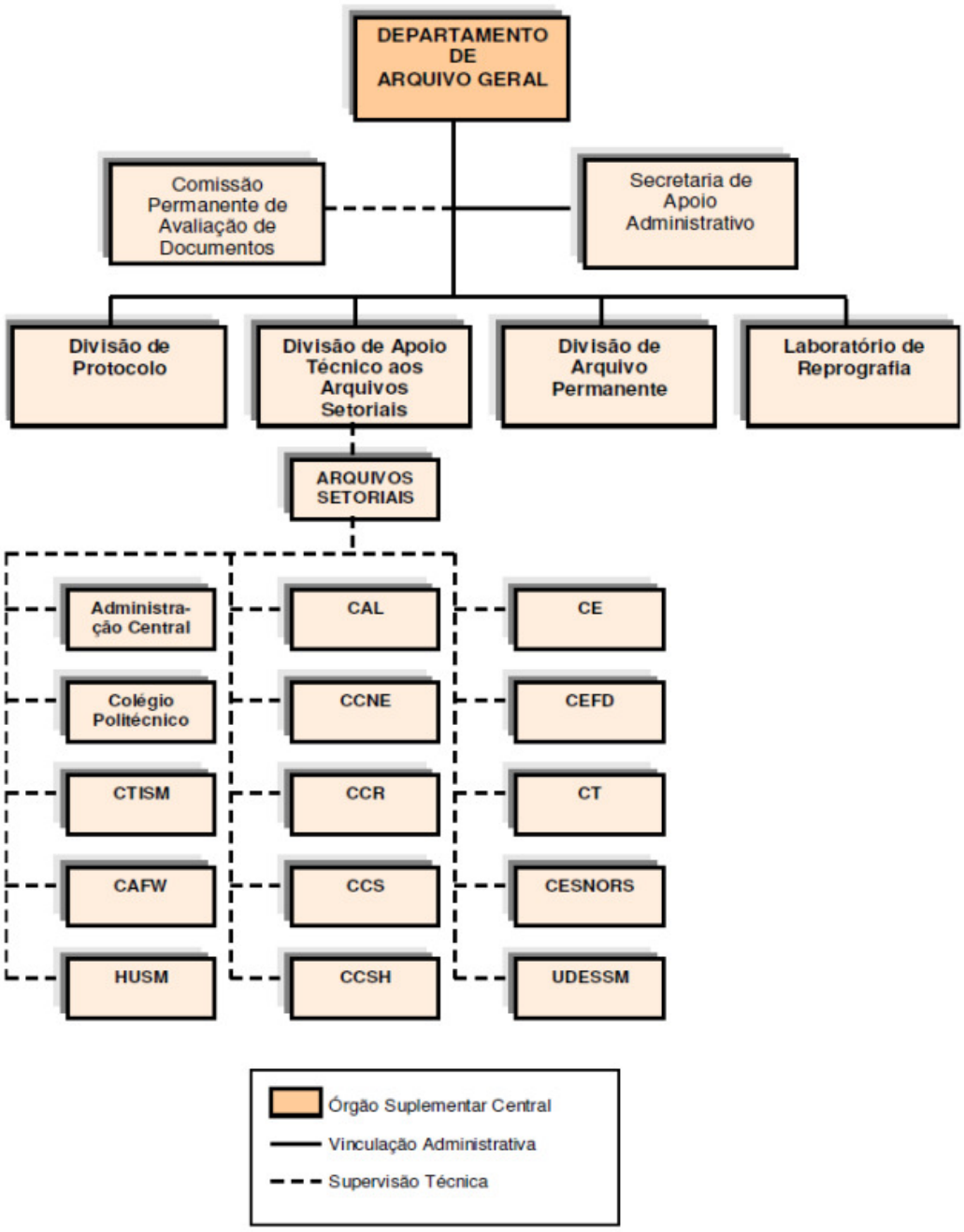
UNIVERSIDADE FEDERAL DE CAMPINAS. **Projeto Santa Maria** – Implantação do SIE na UNICAMP. Universidade Federal de Campinas- UNICAMP, São Paulo, 2002. Disponível em: <http://www.unicamp.br/cgi/zope/database/pdf/SantaMariaResumo.pdf>. Acesso em 15 mar. 2012.

VALENTIM, Marta. **Gestão Documental.** Universidade Estadual Paulista. Marília, 2008. Disponível em: <www.valentim.pro.br/Slides/Arquivos/**Gestao**_Documental. ppt>. Acesso em 29 mai. 2010.

ZUBEN, Newton Aquiles von. **A Relevância da Iniciação à Pesquisa Científica na Universidade.** UNIVERSIDADE ESTADUAL DE CAMPINAS. Disponível em: <http://www.fae.unicamp.br/vonzuben/pesquisa.html>. Acesso em 22 out. 2006.

ANEXOS

Anexo A – Organograma do Departamento de Arquivo Geral da UFSM


DEPARTAMENTO DE ARQUIVO GERAL
Comissão Permanente de Avaliação de Documentos
Secretaria de Apoio Administrativo
Divisão de Protocolo
Divisão de Apoio Técnico aos Arquivos Setoriais
Divisão de Arquivo Permanente
Laboratório de Reprografia
ARQUIVOS SETORIAIS
Administração Central
Colégio Politécnico
CTISM
CAFW
HUSM
CAL
CCNE
CCR
CCS
CCSH
CE
CEFD
CT
CESNORS
UDESSM
Órgão Suplementar Central
Vinculação Administrativa
Supervisão Técnica

APÊNDICES

Apêndice A – Roteiro para entrevista

UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
PROGRAMA DE PÓS-GRADUAÇÃO PROFISSIONALIZANTE EM PATRIMÔNIO CULTURAL

"POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA ESTRATÉGIA PARA GARANTIR A PROTEÇÃO E A INTEGRIDADE DAS INFORMAÇÕES ARQUIVÍSTICAS NO DEPARTAMENTO DE ARQUIVO GERAL DA UFSM"

por : *Josiane Ayres Sfreddo, Mestranda do Curso Profissionalizante em Patrimônio Cultural da UFSM*

Orientador: *André Z. Cordenonsi*

Instituição: *Universidade Federal de Santa Maria*
Departamento: *Departamento de Arquivo Geral- DAG*
Nome do Entrevistado: _____
Cargo/função que exerce: _____
e-mail: _____
Data da Entrevista: ___/___/_____
Hora: _____

ROTEIRO PARA ENTREVISTA

1 Política de segurança da informação

1.1 Quem assume a função de gestor da informação (pessoa responsável por autorizar o acesso à informação) no departamento?

1.1.1 A existência e responsabilidade do gestor da informação são conhecidas por todas as pessoas (funcionário e usuários) do departamento?

2 Gestão de Ativos

2.1 Quem são os usuários do arquivo no DAG?

2.2 Quantos funcionários tem no departamento e que funções desempenham?

3 Segurança em Recursos Humanos

3.1 Existe um processo para conscientização e treinamento de usuários e funcionários em segurança da informação?

3.1.1 Como funciona?

3.2 Os funcionários e usuários estão cientes de suas responsabilidades pela segurança da informação dentro do departamento?

3.3 Quando o funcionário se aposenta ou é afastado de sua função no departamento, ele perde os direitos de acesso e devolve os equipamentos e/ou documentos institucionais que estejam em sua posse? Como é realizado esse controle?

4 Segurança Física e do Ambiente

4.1 No departamento existem os serviços de portaria e de monitoramento de imagens e gravação (uso de câmeras de segurança) nos principais pontos de acesso ao ambiente físico, do departamento? Explique:

4.1.1 Existe pontos de vigilância que cobrem todo o ambiente físico do departamento?

4.2 Como é controlado o acesso as áreas do departamento impedindo que pessoas não autorizadas acessem ambientes em que não estão autorizadas?

4.2.1 Cada pessoa tem autorização de acesso apenas aos ambientes que necessita para desempenhar suas funções profissionais no departamento?

4.2.2 Os visitantes são identificados individualmente e tem registrada sua entrada e saída dos ambientes?

4.3 Já foram feita análise de risco contemplando as principais ameaças: incêndio, roubo, enchente, vazamento de água?

4.3.1 Que medidas preventivas e corretivas são realizadas para evitá-las?

4.4 Nos locais de guarda da documentação:

4.1.1 As portas possuem fechamento contra acesso não autorizado? Que tipo (fechadura, tranca)?

4.1.2 As portas são resistentes ao fogo?

4.1.3 As janelas possuem proteção? Qual?

4.1.4 As paredes são resistentes ao fogo?

5 Gerenciamento das Operações e Comunicações;

Gerenciamento de serviços terceirizados

5.1 Os serviços prestados por terceiros são monitorados? Como é realizado este controle? Explique:

6 Controle de Acessos

6.1 Quem possui permissão de acesso aos documentos?

6.1.1 Funcionários, quais?

6.1.2 Usuários, quais?

6.2 Como é realizado o cadastro dos usuários de arquivo?

6.3 Os usuários e/ou funcionários usam crachá de identificação ou alguma outra forma individual para identificação?

6.4 Existem Normas internas de acesso aos documentos? Quais?

7 Gestão de Incidentes de Segurança da Informação;

7.1 Os funcionários, usuários e terceiros estão cientes da sua responsabilidade em notificar a ocorrência de qualquer evento de segurança da informação, que coloque em risco a segurança das informações no departamento?

7.2 Já teve algum caso de incidente em segurança da informação no departamento?

7.2.1 Que tipo:

- Roubo ou extravio de informações;

- Acesso não autorizado (violação de acesso);

- Divulgação de informações sigilosas;

- Desastres naturais que danificaram a informação (documentação arquivística);

- Acidentes de trabalho resultando na perda de informação (não digitais):

- Outro. Qual?

7.3 Como é realizada a análise e a identificação de um incidente?

7.4 Existe um planejamento e implementação de ações corretivas para prevenir a repetição de um incidente?

8 Gestão da Continuidade do Negócio;

8.1 O departamento possui algum plano para continuidade dos negócios quando ocorre algum incidente em segurança da informação, a fim de não permitir a interrupção das atividades institucionais?

8.2 Há registro de procedimentos de emergência que descrevam as ações a serem tomadas após a ocorrência de um incidente que coloque em risco o desenvolvimento das atividades insitucionais?

8.3 Que ações são desenvolvidas para assegurar a disponibilidade da informação e seu acesso seguro, após a ocorrência de incidente?

9 Conformidade.

Conformidade com requisitos legais

9.1 Que normas são utilizadas para a segurança da informação no departamento?

9.2 Os funcionários conhecem os estatutos, leis contratuais e demais determinações legais necessárias para o cumprimento de suas atividades?

Apêndice B - Carta de apresentação

UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
PROGRAMA DE PÓS-GRADUAÇÃO PROFISSIONALIZANTE
EM PATRIMÔNIO CULTURAL

Santa Maria, 17 de maio de 2011.

Senhora diretora:

Pelo intermédio deste apresento-lhe JOSIANE AYRES SFREDDO, acadêmica do Curso de Mestrado do Programa de Pós-Graduação Profissionalizante em Patrimônio Cultural pela Universidade Federal de Santa Maria, a fim de desenvolver sua pesquisa junto a este departamento.

Para tanto, solicito a sua colaboração no sentido de que a acadêmica realize a coleta de dados e demais etapas da pesquisa, intitulada: **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA ESTRATÉGIA PARA GARANTIR A PROTEÇÃO E A INTEGRIDADE DAS INFORMAÇÕES ARQUIVÍSTICAS NO DEPARTAMENTO DE ARQUIVO GERAL DA UFSM.**

Atenciosamente.

Prof. Dr. Andre Z. Cordenonsi
Orientador

Illma. Srª
DIONE CALIL GOMES
Diretora do Departamento de Arquivo Geral da UFSM
Avenida Roraima, nº 1000. Cidade Universitária
Santa Maria, RS

Apêndice C - Adaptação da Norma ABNT NBR ISO/IEC 27002 para a segurança das informações arquivísticas não digitais

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA NÃO DIGITAL

Adaptação da Norma brasileira

ABNT NBR ISO/IEC 27002

para a segurança das informações arquivísticas não digitais

2012

SUMÁRIO

1 INTRODUÇÃO

1.1 O que é segurança da informação não digital?

A documentação em suporte papel ainda representa a maioria do volume documental produzido e armazenado nas instituições. Nesse sentido a segurança da informação é a proteção das informações não digitais (em suporte papel) de vários tipos de ameaças para garantir a continuidade das atividades de gestão, minimizando o risco da ocorrência de incidentes em segurança da informação.

A segurança da informação (não-digital) em arquivos é obtida a partir da aplicação de um conjunto de controles adequados (regras, normas e ações). Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, para garantir que os objetivos institucionais e de segurança informação sejam atendidos. Convém que isto seja realizado em conjunto com os outros processos de gestão. Por isso recomenda-se que, antes de elaborar ações para a segurança em arquivos é necessário que as instituições implementem um programa de gestão de documentos.

1.2 Por que a segurança da informação é necessária em instituições arquivísticas?

A segurança da informação pode ser alcançada por meio de ações, medidas e regras presentes em uma Política de Segurança da Informação que deve ser apoiada por uma gestão e por procedimentos apropriados. A identificação de controles a serem implantados requer um planejamento cuidadoso e muita atenção aos detalhes. A gestão da segurança da informação requer pelo menos a participação de todos os funcionários da instituição.

Ao desenvolver atividades de gestão documental, a instituição arquivística não se preocupa somente com a guarda e preservação das informações contidas nos documentos. O controle dos processos de gestão, como um todo, previne as ameaças advindas do furto, das falsificações documentais e outros procedimentos que coloquem em risco a confiabilidade das informações que serão recebidas pelos usuários. O sucesso da segurança da informação em instituições arquivísticas dependerá do comprometimento e conscientização tanto dos funcionários e estagiários como, também, dos usuários do arquivo. Como resultado disto a instituição, em contraponto, garantirá não somente a segurança física do arquivo como, também, a proteção e integridade das informações que circulam no meio institucional.

1.3 Como estabelecer requisitos de segurança da informação?

É essencial que as instituições, primeiramente, identifiquem os seus requisitos de segurança da informação. Para ajudá-los existem duas fontes principais de requisitos de segurança da informação.

Elas podem ser obtidas a partir:

- da análise/avaliação de riscos para a instituição, levando-se em conta os objetivos, metas, atividades meio e fim da instituição. Com a análise/avaliação de riscos, é possível identificar as ameaças aos ativos de informação e as vulnerabilidades destes evitando assim, a ocorrência de incidentes em segurança da informação.

- da legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a instituição, seus parceiros comerciais e contratados têm que atender, além do seu ambiente sociocultural.

1.4 Analisando/avaliando os riscos de segurança da informação

Os requisitos de segurança da informação são identificados por meio de uma análise/avaliação sistemática dos riscos (tudo que possa causar incidentes) de segurança da informação. Os gastos com os controles precisam ser balanceados de acordo com os danos causados pelas falhas na segurança da informação.

Os resultados da análise/avaliação de riscos ajudarão a direcionar e a determinar as ações gerenciais apropriadas e as prioridades para o gerenciamento dos riscos da segurança da informação, e para a implementação dos controles selecionados para a proteção contra estes riscos. Convém que a análise/avaliação de riscos seja repetida periodicamente para contemplar quaisquer mudanças que possam influenciar os resultados desta análise/avaliação.

1.5 Seleção de controles

Uma vez que os requisitos de segurança da informação e os riscos tenham sido identificados e as decisões para o tratamento dos riscos tenham sido tomadas, convém que controles apropriados sejam selecionados e implementados para assegurar que os riscos sejam reduzidos a um nível aceitável. Os controles podem ser selecionados a partir desta adaptação da Norma ABNT NBR ISO/IEC 27002, ou de outros conjuntos de controles, a fim de atender às necessidades específicas, conforme apropriado.

A seleção de controles de segurança da informação depende das decisões da instituição, baseadas nos critérios para aceitação de risco, nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado à instituição, e convém que também esteja sujeito a todas as legislações e regulamentações nacionais e internacionais, relevantes.

1.6 Ponto de partida para a segurança da informação

De acordo com a Norma ABNT NBR ISO/IEC 27002 o ponto de partida para a implementação da segurança da informação pode ser a aplicação de um determinado número de controles. Estes

controles são baseados tanto em requisitos legais como nas melhores práticas de segurança da informação normalmente usadas. Nesta adaptação:

Os controles considerados essenciais para uma instituição, sob o ponto de vista legal, incluem, dependendo da legislação aplicável:

a) proteção de dados e privacidade de informações pessoais (ver 13.1.4);

b) proteção de registros institucionais (ver 13.1.3);

c) direitos de propriedade intelectual (ver 13.1.2).

Os controles considerados práticas para a segurança da informação incluem:

a) documento da política de segurança da informação (ver 5.1.1);

b) atribuição de responsabilidades para a segurança da informação (ver 5.2.3);

c) conscientização, educação e treinamento em segurança da informação (ver 7.1.5);

d) gestão da continuidade do negócio (ver seção 12);

e) gestão de incidentes de segurança da informação e melhorias (ver 11.2).

Esses controles se aplicam para a maioria das instituições e na maioria dos ambientes.

Convém observar que, embora todos os controles nesta adaptação sejam importantes e devam ser considerados, a relevância de qualquer controle deve ser determinada segundo os riscos específicos a que uma instituição arquivística está exposta. Por isto, embora o enfoque acima seja considerado um bom ponto de partida, ele não substitui a seleção de controles, baseado na análise/avaliação de riscos de acordo com a realidade que se encontra cada instituição.

1.7 Fatores críticos de sucesso

A experiência tem mostrado que os seguintes fatores são geralmente críticos para o sucesso da implementação da segurança da informação dentro de uma instituição:

a) política de segurança da informação, objetivos e atividades, que reflitam os objetivos do negócio;

b) uma abordagem e uma estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação que seja consistente com a cultura organizacional;

c) comprometimento e apoio visível de todos os níveis gerenciais;

d) um bom entendimento dos requisitos de segurança da informação, da análise/avaliação de riscos e da gestão de risco;

e) divulgação eficiente da segurança da informação para todos os gerentes, funcionários e outras partes envolvidas para se alcançar a conscientização;

f) distribuição de diretrizes e normas sobre a política de segurança da informação para todos os gerentes, funcionários e outras partes envolvidas;

g) provisão de recursos financeiros para as atividades da gestão de segurança da informação;

h) provisão de conscientização, treinamento e educação adequados;

i) estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação;

j) implementação de um sistema de medição, que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria.

1.8 Desenvolvendo suas próprias diretrizes

Esta adaptação da Norma ABNT NBR ISO/IEC 27002 para a segurança das informações não digitais pode ser considerada como um ponto de partida para o desenvolvimento de diretrizes específicas para as instituições arquivísticas. Esta adaptação foi realizada com o intuito de possibilitar que a maioria dos controles e diretrizes contidas nela pudesse ser aplicada para a segurança da informação não digital em arquivos.

Entretanto, os controles adicionais e recomendações não incluídas nesta adaptação podem ser necessários. Quando os documentos são desenvolvidos contendo controles ou recomendações adicionais, pode ser útil realizar uma referência cruzada para as seções desta Norma, onde aplicável, para facilitar a verificação da conformidade pelos responsáveis na instituição.

Convém observar que, embora todos os controles nesta adaptação sejam importantes, sua aplicação para a segurança das informações não digitais deve ser determinada segundo a realidade e necessidade de cada instituição arquivística.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA NÃO DIGITAL – Adaptação da Norma ABNT NBR ISO/IEC 27002 para a segurança das informações arquivísticas não digitais.

2 OBJETIVOS E APLICAÇÃO DA ADAPTAÇÃO DA NORMA

Esta é a adaptação da Norma ABNT NBR ISO/IEC 27002. A sua finalidade é possibilitar que instituições arquivística elaborem uma política de segurança da informação de acordo com as diretrizes que estão sendo adaptadas. Seu foco de estudo é a proteção das informações não digitais. A adaptação estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma instituição.

Os objetivos definidos nesta Norma proveem diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação. Os objetivos de controle e os controles desta Norma têm como finalidade ser implementados para atender aos requisitos identificados por meio da análise/avaliação de riscos. Esta Norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da instituição e as eficientes práticas de gestão da segurança, e para ajudar a criar confiança nas atividades interinstitucionais.

Desde que a instituição estabeleça um programa ou sistema de gestão arquivística de documentos, a adaptação da Norma ABNT NBR ISO/IEC 27002 para a segurança das informações arquivísticas não digitais, é aplicável às instituições dos setores público e privado e em qualquer esfera e âmbito de atuação, contribuindo para a proteção e integridade de documentos arquivísticos não digitais.

3 ESTRUTURA DA ADAPTAÇÃO DA NORMA

Esta Norma contém 9 seções de controles de segurança da informação, que juntas totalizam 16 categorias principais de segurança e uma seção introdutória que aborda a análise/avaliação e o tratamento de riscos.

3.1 Seções

Cada seção contém um número de categorias principais de segurança da informação. As 9 seções (acompanhadas com o respectivo número de categorias) são:

1 - Política de Segurança da Informação (2)

2 - Gestão de Ativos (1);

3 - Segurança em Recursos Humanos (2);

4 - Segurança Física e do Ambiente (2);

5 - Gerenciamento das Operações e Comunicações (1);

6 - Controle de Acesso (3);

7 - Gestão de Incidentes de Segurança da Informação (2);

8 - Gestão da Continuidade do Negócio (1);

9 - Conformidade (2).

Nota: A ordem das seções nesta adaptação da Norma ABNT NBR ISO/IEC 27002 não significa o seu grau de importância. Dependendo das circunstâncias, todas as seções podem ser importantes. Entretanto, cada instituição arquivística que utilize esta adaptação deve identificar quais as seções aplicáveis, quão importantes elas são e a sua aplicação na instituição. Todas as alíneas nesta adaptação também não estão ordenadas por prioridade, a menos que explicitado.

3.2 Principais categorias de segurança da informação

Cada categoria principal (exemplo: gestão de ativos) de segurança da informação contém:

a) um **objetivo de controle** que define o que deve ser alcançado; e

b) um ou mais **controles** que podem ser aplicados para se alcançar o **objetivo do controle**.

As descrições dos controles estão estruturadas da seguinte forma:

Controle

Define qual o controle específico para atender ao objetivo do controle.

Diretrizes para a implementação

Contém informações mais detalhadas para apoiar a implementação do controle e atender ao objetivo de controle. Algumas destas diretrizes podem não ser adequadas em todos os casos e assim outras formas de implementação do controle podem ser mais apropriadas.

Informações adicionais

Contém informações adicionais que podem ser consideradas, como, por exemplo, considerações legais e referências a outras normas.

4 ANÁLISE/AVALIAÇÃO E TRATAMENTO DE RISCOS

4.1 Analisando/avaliando os riscos de segurança da informação

Convém que as análises/avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base em critérios para aceitação dos riscos e dos objetivos relevantes para a instituição.

Convém que os resultados orientem e determinem as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de segurança da informação, e para a implementação dos controles selecionados, de maneira a proteger contra estes riscos. O processo de avaliar os riscos e selecionar os controles pode ser realizado várias vezes, de forma a cobrir diferentes partes da instituição ou de sistemas de informação específicos.

Convém que a análise/avaliação de riscos inclua um enfoque sistemático de estimar a magnitude do risco (análise de riscos) e o processo de comparar os riscos estimados contra os critérios de risco para determinar a significância do risco (avaliação do risco).

Convém que as análises/avaliações de riscos também sejam realizadas periodicamente, para contemplar as mudanças nos requisitos de segurança da informação e na situação de risco, ou seja, nos ativos, ameaças, vulnerabilidades, impactos, avaliação do risco e quando uma mudança significativa ocorrer. Essas análises/avaliações de riscos devem ser realizadas de forma metódica, capaz de gerar resultados comparáveis e reproduzíveis.

Convém que a análise/avaliação de riscos de segurança da informação tenha um escopo claramente definido para ser eficaz e inclua os relacionamentos com as análises/avaliações de riscos em outras áreas, se necessário. O escopo de uma análise/avaliação de riscos pode tanto ser em toda a instituição, partes da instituição, em um sistema de informação específico, em componentes de um sistema específico ou em serviços onde isto seja praticável, realístico e útil. Exemplos de metodologias de análise/avaliação de riscos são discutidas no ISO/IEC TR 13335-3 (*Guidelines for the management of IT security: Techniques for the management of ITSecurity*).

4.2 Tratando os riscos de segurança da informação

Convém que, antes de considerar o tratamento de um risco, a instituição defina os critérios para determinar se os riscos podem ser ou não aceitos. Riscos podem ser aceitos se, por exemplo, for avaliado que o risco é baixo ou que o custo do tratamento não é economicamente viável para a instituição. Convém que tais decisões sejam registradas.

Para cada um dos riscos identificados, seguindo a análise/avaliação de riscos, uma decisão sobre o tratamento do risco precisa ser tomada. Possíveis opções para o tratamento do riscoincluem:

a) aplicar controles apropriados para reduzir os riscos;

b) conhecer e objetivamente aceitar os riscos, sabendo que eles atendem claramente à política da instituição e aos critérios para a aceitação de risco;

c) evitar riscos, não permitindo ações que poderiam causar a ocorrência de riscos;

d) transferir os riscos associados para outras partes, por exemplo, seguradoras ou fornecedores.

Convém que, para aqueles riscos onde a decisão de tratamento do risco seja a de aplicar os controles apropriados, esses controles sejam selecionados e implementados para atender aos requisitos identificados pela análise/avaliação de riscos. Convém que os controles assegurem que os riscos sejam reduzidos a um nível aceitável, levando-se em conta:

a) os requisitos e restrições de legislações e regulamentações nacionais e internacionais;

b) os objetivos institucionais;

c) os requisitos e restrições operacionais;

d) custo de implementação e a operação em relação aos riscos que estão sendo reduzidos e que permanecem proporcionais às restrições e requisitos da instituição;

e) a necessidade de balancear o investimento na implementação e operação de controles contra a probabilidade de danos que resultem em falhas de segurança da informação.

Os controles podem ser selecionados desta adaptação ou de outros conjuntos de controles, ou novos controles podem ser considerados para atender às necessidades específicas da instituição. É importante reconhecer que alguns controles podem não ser praticáveis em todas as instituições arquivísticas. Assim, os controles devem ser definidos de acordo com a realidade de cada instituição.

Convém que seja lembrado que nenhum conjunto de controles pode conseguir a segurança completa, e que uma ação gerencial adicional deve ser implementada para monitorar, avaliar e melhorar a eficiência e eficácia dos controles de segurança da informação, para apoiar as metas da instituição.

5 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

5.1 Política de segurança da informação

Objetivo: Prover uma orientação e apoio da direção para a segurança da informação não digital de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Convém que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a instituição.

5.1.1 Documento da política de segurança da informação

Controle:

Convém que um documento da política de segurança da informação seja aprovado pela direção, publicado e comunicado para todos os funcionários e usuários da instituição.

Diretrizes para implementação:

Convém que o documento da política de segurança da informação declare o comprometimento da direção e estabeleça o enfoque da instituição para gerenciar a segurança da informação. Convém que o documento da política contenha declarações relativas a:

a) uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação (ver introdução);

b) uma declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhada com os objetivos e estratégias do negócio;

c) breve explanação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a instituição, incluindo:

1) conformidade com a legislação e com requisitos regulamentares e contratuais;

2) requisitos de conscientização, treinamento e educação em segurança da informação;

3) gestão da continuidade do negócio;

4) consequências das violações na política de segurança da informação.

d) definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança da informação;

Convém que esta política de segurança da informação seja comunicada através de toda a instituição para os usuários de forma que seja relevante, acessível e compreensível para o leitor em foco.

Informações adicionais:

A política de segurança da informação pode ser uma parte de um documento da política geral. Se a política de segurança da informação for distribuída fora da instituição, convém que sejam tomados cuidados para não revelar informações sensíveis. Informações adicionais podem ser encontradas na ISO/IEC 13335-1:2004.

5.1.2 Análise crítica da política de segurança da informação

Controle:

Convém que a política de segurança da informação seja analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Diretrizes para implementação:

Convém que a política de segurança da informação tenha um gestor que tenha aprovado a responsabilidade pelo desenvolvimento, análise crítica e avaliação da política de segurança da informação.

Convém que a análise crítica inclua a avaliação de oportunidades para melhoria da política de segurança da informação da instituição e tenha um enfoque para gerenciar a segurança da informação em resposta às mudanças ao ambiente organizacional, às circunstâncias do negócio, às condições legais, ou ao ambiente técnico.

5.2 Controlando a segurança da informação

Objetivo: Gerenciar a segurança da informação dentro da instituição.

Convém que a direção aprove a política de segurança da informação, atribua as funções da segurança, coordene e analise criticamente a implementação da segurança da informação por toda a instituição.

5.2.1 Comprometimento da direção com a segurança da informação

Controle:

Convém que a direção apoie ativamente a segurança da informação dentro da instituição, por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e conhecendo as responsabilidades pela segurança da informação.

Diretrizes para implementação:

Convém que a direção:

a) assegure que as metas de segurança da informação estão identificadas, atendem aos requisitos da instituição e estão integradas nos processos relevantes;

b) formule, analise criticamente e aprove a política de segurança da informação;

c) analise criticamente a eficácia da implementação da política de segurança da informação;

d) forneça um claro direcionamento e apoio para as iniciativas de segurança da informação;

e) forneça os recursos necessários para a segurança da informação;

f) aprove as atribuições de tarefas e responsabilidades específicas para a segurança da informação por toda a instituição;

g) inicie planos e programas para manter a conscientização da segurança da informação;

5.2.2 Coordenação da segurança da informação

Controle:

Convém que as atividades de segurança da informação sejam coordenadas por representantes de diferentes partes da instituição, com funções e papéis relevantes.

Diretrizes para implementação:

Convém que a coordenação da segurança da informação envolva a cooperação e colaboração de gerentes, usuários, administradores, desenvolvedores, auditores, pessoal de segurança e especialistas (se necessário) com habilidades em diferentes áreas.

5.2.3 Atribuição de responsabilidades para a segurança da informação

Controle:

Convém que todas as responsabilidades pela segurança da informação estejam claramente definidas.

Diretrizes para implementação:

Convém que a atribuição das responsabilidades pela segurança da informação seja feita em conformidade com a política de segurança da informação.

Convém que sejam claramente definidas as responsabilidades em cada local, dentro da instituição, para a proteção dos ativos de informação.

Informações adicionais:

Em instituições arquivísticas, o arquivista será o responsável por coordenar a Política de Segurança da Informação e apoiar a identificação de controles. Mesmo assim, essa função poderá ser exercida por mais pessoas (para instituições de médio a grande porte), sendo que poderá ter um responsável pela gestão da segurança da informação em cada setor e/ou departamento de acordo com o organograma e distribuição das responsabilidades de chefia em cada instituição.

5.2.4 Contato com autoridades

Controle:

Convém que contatos apropriados com autoridades relevantes sejam mantidos.

Diretrizes para implementação:

Convém que as instituições tenham procedimentos em funcionamento que especifiquem quando e por quais autoridades (por exemplo, obrigações legais, corpo de bombeiros, autoridades fiscalizadoras) devem ser contatadas e como os incidentes de segurança da informação identificados devem ser notificados em tempo hábil, no caso de suspeita de que a lei foi violada.

6 GESTÃO DE ATIVOS

6.1 Responsabilidade pelos ativos de informação

Objetivo: Alcançar e manter a proteção adequada dos ativos de informação.

Convém que todos os ativos de informação estejam presentes no plano de classificação de documentos da instituição.

Convém que os proprietários[9] dos ativos sejam identificados e a eles seja atribuída a responsabilidade pela manutenção apropriada dos controles. A implementação de controles específicos pode ser delegada pelo proprietário, conforme apropriado, porém o proprietário permanece responsável pela proteção adequada dos ativos.

6.1.1 Recomendações para classificação dos ativos de informação

Controle:

Convém que a Classificação seja o ato ou efeito de analisar e identificar o conteúdo dos documentos arquivísticos e de selecionar a classe sob a qual serão recuperados.

Convém que essa classificação seja feita a partir de um plano de classificação elaborado pelo órgão ou entidade que poderá incluir, ou não, a atribuição de um código aos documentos.

Convém que as informações sejam classificadas com o objetivo de:

a) estabelecer a relação orgânica dos documentos arquivísticos;

b) assegurar que os documentos sejam identificados de forma consistente ao longo do tempo;

c) auxiliar a recuperação de todos os documentos arquivísticos relacionados a uma determinada função ou atividade;

d) possibilitar a avaliação de um grupo de documentos de forma que os documentos associados sejam transferidos, recolhidos ou eliminados em conjunto.

[9] O “proprietário” do ativo é aquele que esteja com a posse do documento (usuário, funcionário, etc.), permanecendo responsável pela proteção adequada dos ativos de informação até sua devolução. Entretanto, o termo “proprietário” apenas identifica a pessoa autorizada a 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 ao ativo.

e) a classificação deve se basear no plano de classificação e envolve os seguintes passos:

1) identificar a ação que o documento registra;

2) localizar a ação ou atividade no plano de classificação;

3) comparar a atividade com a estrutura organizacional para verificar se é apropriada à unidade que gerou o documento;

4) aplicar a classificação ao documento.

Informações adicionais

Para esta adaptação da Norma ABNT NBR ISO/IEC 27002 para a segurança das informações arquivísticas não-digitais será considerado apenas como ativos:

a) ativos de informação: documentos arquivísticos (não-digitais).

6.1.2 Plano de Classificação e Código de Classificação

Controle:

Convém que todos os ativos de informação sejam claramente identificados e façam parte do plano de classificação de documentos da instituição, devendo ser atualizado periodicamente e mantido.

Diretrizes para implementação

Convém que:

a) o plano de classificação seja um esquema de distribuição de documentos em classes, de acordo com métodos de arquivamento específicos, elaborado a partir do estudo das estruturas e funções de uma instituição e da análise do arquivo por ela produzido.

b) a estruturação do plano de classificação pode ser facilitada pela utilização de códigos (numéricos ou alfanuméricos) para designar as classes, constituindo um código de classificação.

c) o Código de Classificação de Documentos é um instrumento de trabalho utilizado para classificar todo e qualquer documento produzido ou recebido por um órgão ou entidade no exercício de suas funções e atividades.

d) a classificação é utilizada para agrupar os documentos a fim de contextualizá-los, agilizar sua recuperação e facilitar tanto as tarefas de destinação (eliminação ou recolhimento dos documentos) como de acesso.

e) o número de níveis de classificação modifique de acordo com o órgão ou entidade e envolve os seguintes fatores:

1) natureza das atividades desenvolvidas;

2) tamanho do órgão ou entidade;

3) complexidade da estrutura organizacional;

4) tecnologia utilizada.

Informações adicionais

As definições utilizadas foram retiradas da e-ARQ Brasil: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos/Câmara Técnica de Documentos Eletrônicos. 1.1. versão. - Rio de Janeiro : Arquivo Nacional, 2011.

7 SEGURANÇA EM RECURSOS HUMANOS

7.1 Antes e durante a contratação[10]

Objetivo: Assegurar que os funcionários, fornecedores, terceiros e usuários entendam suas responsabilidades e fiquem conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estejam preparados para apoiar a política de segurança da informação da instituição durante os seus trabalhos normais, a fim de reduzir o risco de erro humano.

Convém que as responsabilidades pela segurança da informação sejam atribuídas de forma adequada, nas descrições de cargos e nos termos e condições de contratação.

Convém que todos os funcionários, fornecedores, terceiros e usuários de arquivo, (se a instituição achar necessário) assinem acordos sobre seus papéis e responsabilidades pela segurança da informação.

Convém que as responsabilidades pela direção sejam definidas para garantir que a segurança da informação é aplicada em todo trabalho individual dentro da instituição.

Convém que um nível adequado de conscientização, educação e treinamento nos procedimentos de segurança da seja fornecido para todos os funcionários, fornecedores, terceiros e usuários, para minimizar possíveis riscos de segurança da informação.

Convém que um processo disciplinar formal para tratar das violações de segurança da informação seja estabelecido.

7.1.1 Papéis e responsabilidades

Controle:

Convém que papéis e responsabilidades pela segurança da informação de funcionários, fornecedores, terceiros e usuários sejam definidos e documentados de acordo com a política de segurança da informação da instituição.

[10] 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.

Diretrizes para implementação:

Convém que os papéis e responsabilidades pela segurança da informação incluam requisitos para:

a) implementar e agir de acordo com a política de segurança da informação da instituição;

b) proteger ativos de informação contra acesso não autorizado, divulgação, modificação ou destruição;

c) executar processos ou atividades particulares de segurança da informação;

d) assegurar que a responsabilidade é atribuída à pessoa para tomada de ações;

e) relatar eventos potenciais ou reais de segurança da informação ou outros riscos de segurança para a instituição.

Convém que papéis e responsabilidades de segurança da informação sejam definidos e claramente comunicados aos candidatos a cargos, durante o processo de pré-contratação.

Informações adicionais:

Descrições de cargos podem ser usadas para documentar responsabilidades e papéis pela segurança da informação. Convém que papéis e responsabilidades pela segurança da informação para pessoas que não estão engajadas por meio do processo de contratação da instituição, como, por exemplo, através de uma instituição terceirizada, sejam claramente definidos e comunicados.

7.1.2 Seleção

Controle:

Convém que verificações de controle de todos os candidatos a emprego, fornecedores, terceiros e usuários do arquivo sejam realizadas de acordo com as leis relevantes, regulamentações, éticas, metas e objetivos institucionais, proporcional à classificação das informações a serem acessadas e aos riscos percebidos.

Diretrizes para implementação:

Convém que as verificações de controle levem em consideração todos os aspectos relevantes relacionados com a privacidade, legislação baseada na contratação e/ou proteção de dados pessoais e, *onde permitido*, incluam os seguintes itens:

a) disponibilidade de referências de caráter satisfatórias, por exemplo, uma profissional e uma pessoal;

b) uma verificação (da exatidão e inteireza) das informações do *curriculum vitae* do candidato;

c) confirmação das qualificações acadêmicas e profissionais;

d) verificação independente da identidade (passaporte ou documento similar);

e) verificações mais detalhadas, tais como verificações financeiras (de crédito) ou verificações de registros criminais**.**

Convém que a instituição também faça verificações mais detalhadas, onde um trabalho envolver pessoas, tanto por contratação como por promoção, que tenham acesso a informações sensíveis, tais como informações financeiras ou informações altamente confidenciais.

Convém que os procedimentos definam critérios e limitações para as verificações de controle, por exemplo, quem está qualificado para selecionar as pessoas, e como, quando e por que as verificações de controle são realizadas.

Convém que um processo de seleção também seja feito para fornecedores e terceiros. Quando essas pessoas vêm por meio de uma agência, convém que o contrato especifique claramente as responsabilidades da agência pela seleção e os procedimentos de notificação que devem ser seguidos se a seleção não for devidamente concluída ou quando os resultados obtidos forem motivos de dúvidas ou preocupações.

Convém que informações sobre todos os candidatos que estão sendo considerados para certas posições dentro da instituição sejam levantadas e tratadas de acordo com qualquer legislação apropriada existente na jurisdição pertinente. Dependendo da legislação aplicável, convém que os candidatos sejam previamente informados sobre as atividades de seleção.

Informações adicionais

O processo de seleção dos funcionários, fornecedores, terceiros e usuários do arquivo devem proceder de acordo com a realidade e interesse de cada instituição.

7.1.3 Termos e condições de contratação

Controle:

Como parte das suas obrigações contratuais, convém que os funcionários, fornecedores e terceiros concordem e assinem os termos e condições de sua contratação para o trabalho, os quais devem declarar as suas responsabilidades e a da instituição para a segurança da informação.

Diretrizes para implementação:

Convém que os termos e condições de trabalho reflitam a política de segurança da instituição, esclarecendo e declarando:

a) que todos os funcionários, fornecedores e terceiros que tenham acesso a informações sensíveis assinem um termo de confidencialidade ou de não divulgação da informação;

b) as responsabilidades legais e direitos dos funcionários, fornecedores e quaisquer outros usuários, por exemplo, com relação às leis de direitos autorais ou à legislação de proteção de dados;

c) as responsabilidades para a segurança da informação e pelos dos ativos da instituição associados com os serviços conduzidos pelos funcionários, fornecedores, terceiros ou usuários (ver 5.2.3 e 6.1);

d) as responsabilidades dos funcionários, fornecedores e terceiros pelo tratamento da informação recebida de outras companhias ou de partes externas;

e) responsabilidades da instituição pelo tratamento das informações pessoais, incluindo informações pessoais criadas como resultado de, ou em decorrência da contratação com a instituição (ver 13.1.4);

f) responsabilidades que se estendem para fora das dependências da instituição e fora dos horários normais de trabalho.

g) ações a serem tomadas no caso de o funcionário, fornecedor ou terceiro desrespeitar os requisitos de segurança da informação da instituição (ver 7.1.6).

Convém que a instituição assegure que os funcionários, fornecedores e terceiros concordam com os termos e condições relativas à segurança da informação adequados à natureza e extensão do acesso que eles terão aos ativos da instituição associados com os sistemas e serviços de informação.

Convém que as responsabilidades contidas nos termos e condições de contratação continuem por um período de tempo definido, após o término da contratação (ver 7.2), onde apropriado.

Informações adicionais:

Um código de conduta pode ser usado para contemplar as responsabilidades dos funcionários, fornecedores ou terceiros, em relação à confidencialidade, proteção de dados, éticas, uso apropriado dos recursos e dos equipamentos da instituição, bem como práticas de boa conduta esperada pela instituição. O fornecedor ou o terceiro pode estar associado com uma instituição

externa que possa, por sua vez, ser solicitada a participar de acordos contratuais, em nome do contratado.

A instituição pode definir que os usuários do arquivo devem concordar e assinar termos e condições para seu acesso e consulta ao acervo, declarando as suas responsabilidades para a segurança da informação dentro da instituição.

7.1.4 Responsabilidades da direção

Controle:

Convém que a direção solicite aos funcionários, fornecedores e terceiros que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da instituição.

Diretrizes para implementação:

Convém que as responsabilidades da direção assegurem que os funcionários, fornecedores, terceiros e usuários:

a) estão adequadamente instruídos sobre as suas responsabilidades e papéis pela segurança da informação antes de obter acesso às informações sensíveis;

b) recebam diretrizes que definam quais as expectativas sobre a segurança da informação de suas atividades dentro da instituição;

c) estão motivados para cumprir com as políticas de segurança da informação da instituição;

d) atinjam um nível de conscientização sobre segurança da informação que seja relevante para os seus papéis e responsabilidades dentro da instituição (ver 7.1.5);

e) atendam aos termos e condições de contratação, que incluam a política de segurança da informação da instituição e métodos apropriados de trabalho;

f) tenham as habilidades e qualificações apropriadas.

Informações adicionais:

Se os funcionários, fornecedores, terceiros e usuários não forem conscientizados das suas responsabilidades, eles podem causar consideráveis danos para a instituição. Pessoas motivadas têm uma maior probabilidade de serem mais confiáveis e de causar menos incidentes de segurança da informação.

Uma má gestão pode causar às pessoas o sentimento de subvalorizarão, resultando em um impacto de segurança da informação negativo para a instituição. Por exemplo, uma má gestão pode

levar a segurança da informação a ser negligenciada ou a um potencial mau uso dos ativos da instituição.

7.1.5 Conscientização, educação e treinamento em segurança da informação

Controle:

Convém que todos os funcionários da instituição e, onde pertinente, fornecedores, terceiros e usuários recebam treinamento apropriados em conscientização e atualizações regulares nas políticas e procedimentos institucionais, relevantes para as suas funções.

Diretrizes para implementação:

Convém que o treinamento em conscientização comece com um processo formal de indução concebido para introduzir as políticas e expectativas de segurança da informação da instituição, antes que seja dado o acesso às informações ou serviços.

Convém que os treinamentos em curso incluam requisitos de segurança da informação, responsabilidades legais e demais procedimentos relevantes para o desenvolvimento institucional.

Informações adicionais:

Convém que a conscientização, educação e treinamento nas atividades de segurança da informação sejam adequados e relevantes para os papéis, responsabilidades e habilidades da pessoa, e que incluam informações sobre conhecimento de ameaças, quem deve ser contatado para orientações sobre segurança da informação e os canais adequados para relatar os incidentes de segurança da informação (ver 11.1.1).

O treinamento para aumentar a conscientização visa permitir que as pessoas reconheçam os problemas e incidentes de segurança da informação, e respondam de acordo com as necessidades do seu trabalho.

7.1.6 Processo disciplinar

Controle:

Convém que exista um processo disciplinar formal para os funcionários que tenham cometido uma violação da segurança da informação.

Diretrizes para implementação

Convém que o processo disciplinar não inicie sem uma verificação prévia de que a violação da segurança da informação realmente ocorreu (ver 11.2.3 em coleta de evidências).

Convém que o processo disciplinar formal assegure um tratamento justo e correto aos funcionários que são suspeitos de cometer violações de segurança da informação. O processo disciplinar formal deve dar uma resposta de forma gradual, que leve em consideração fatores como a natureza e a gravidade da violação e o seu impacto, se este é ou não o primeiro delito, se o infrator foi ou não adequadamente treinado, as legislações relevantes, os e outros fatores conforme requerido. Em casos sérios de má conduta, convém que o processo permita, por um certo período, a remoção das responsabilidades, dos direitos de acesso e privilégios e, dependendo da situação, solicitar à pessoa, a saída imediata das dependências da instituição, escoltando-a.

Informações adicionais:

Convém que o processo disciplinar também seja usado como uma forma de dissuasão, para evitar que os funcionários, fornecedores, terceiros e usuários violem os procedimentos e as políticas de segurança da informação da instituição, e quaisquer outras violações na segurança.

7.2 Encerramento ou mudança da contratação

Objetivo: Assegurar que funcionários, fornecedores e terceiros deixem a instituição ou mudem de trabalho (setor e/ou departamento) de forma ordenada.

Convém que responsabilidades sejam definidas para assegurar que a saída de funcionários, fornecedores e terceiros da instituição seja feita de modo controlado e que a devolução de todos os equipamentos e a retirada de todos os direitos de acesso estão concluídas.

7.2.1 Encerramento de atividades

Controle:

Convém que responsabilidades para realizar o encerramento ou a mudança de um trabalho sejam claramente definidas e atribuídas.

Diretrizes para implementação:

Convém que a comunicação de encerramento de atividades inclua requisitos de segurança e responsabilidades legais existentes e, onde apropriado, responsabilidades contidas em quaisquer acordos de confidencialidade e os termos e condições de trabalho (ver 7.1.3) que continuem por um período definido após o fim do trabalho do funcionário, do fornecedor ou do terceiro.

Convém que as responsabilidades e obrigações contidas nos contratos dos funcionários, fornecedores ou terceiros permaneçam válidas após o encerramento das atividades.

Convém que as mudanças de responsabilidades ou do trabalho sejam gerenciadas quando do encerramento da respectiva responsabilidade ou do trabalho, e que novas responsabilidades ou trabalho sejam controlados conforme descrito em 7.1.

Informações adicionais:

A função de Recursos Humanos é geralmente responsável pelo processo global de encerramento e trabalha em conjunto com o gestor responsável pela pessoa que está saindo, para gerenciar os aspectos de segurança da informação dos procedimentos pertinentes. No caso de um fornecedor, o processo de encerramento de atividades pode ser realizado por uma agência responsável pelo fornecedor e, no caso de outro usuário, isto pode ser tratado pela sua instituição. Pode ser necessário informar aos funcionários, usuários, fornecedores ou terceiros sobre as mudanças de pessoal e procedimentos operacionais.

7.2.2 Devolução de ativos de informação

Controle:

Convém que todos os funcionários, fornecedores e terceiros devolvam todos os ativos de informação da instituição que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.

Diretrizes para implementação:

Convém que o processo de encerramento de atividades seja formalizado para contemplar a devolução de todos os equipamentos e ativos de informação entregues à pessoa. É necessário que sejam devolvidos os demais ativos da instituição como dispositivos de computação móvel, cartões de créditos, cartões de acesso, manuais e informações armazenadas em mídia eletrônica, também precisam ser devolvidos. No caso em que um funcionário, fornecedor ou terceiro compre o equipamento da instituição ou use o seu próprio equipamento pessoal, convém que procedimentos sejam adotados para assegurar que toda a informação relevante seja transferida para a instituição e que seja apagada de forma segura do equipamento.

7.2.3 Retirada de direitos de acesso

Controle:

Convém que os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e a instituição e suas dependências sejam retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança destas atividades.

Diretrizes para implementação:

Convém que os direitos de acesso que sejam retirados ou adaptados incluam o acesso lógico e físico, chaves, cartões de identificação, subscrições e retirada de qualquer documentação que os identifiquem como um membro atual da instituição. Caso o funcionário, fornecedor ou terceiro que esteja saindo tenha conhecimento de senhas de contas que permanecem ativas, convém que estas sejam alteradas após um encerramento das atividades, mudança do trabalho, contrato ou acordo.

8 SEGURANÇA FÍSICA E DO AMBIENTE

8.1 Áreas seguras

Objetivo: Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da instituição.

Convém que os locais de guarda da documentação sejam áreas seguras, protegidas por perímetros de segurança definidos, com barreiras de segurança e controles de acesso apropriados.

Convém que sejam fisicamente protegidas contra o acesso não autorizado, danos e interferências.

Convém que a proteção oferecida seja compatível com os riscos identificados.

8.1.1 Perímetro de segurança física

Controle:

Convém que sejam 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 os ativos de informação.

Diretrizes para a implementação:

Convém que sejam levadas em consideração e implementadas as seguintes diretrizes para perímetros de segurança física, quando apropriado:

a) os perímetros de segurança sejam claramente definidos e que a localização e a capacidade de resistência de cada perímetro dependam dos requisitos de segurança dos ativos existentes no interior do perímetro, e dos resultados da análise/avaliação de riscos;

b) convém que as paredes externas do local sejam de construção robusta e todas as portas externas sejam adequadamente protegidas contra acesso não autorizado por meio de mecanismos de controle, por exemplo, barras, alarmes, fechaduras etc.; convém que as portas e janelas sejam trancadas quando estiverem sem monitoração, e que uma proteção externa para as janelas seja considerada, principalmente para as que estiverem situadas no andar térreo;

c) seja implantada uma área de recepção, ou um outro meio para controlar o acesso físico ao local ou ao edifício; o acesso aos locais ou edifícios deve ficar restrito somente ao pessoal autorizado;

d) sejam construídas barreiras físicas, onde aplicável, para impedir o acesso físico não autorizado e a contaminação do meio ambiente;

e) todas as portas corta-fogo do perímetro de segurança sejam providas de alarme, monitoradas e testadas juntamente com as paredes, para estabelecer o nível de resistência exigido, de acordo com normas regionais, nacionais e internacionais aceitáveis; elas devem funcionar de acordo com os códigos locais de prevenção de incêndios e prevenção de falhas;

f) sistemas adequados de detecção de intrusos, de acordo com normas regionais, nacionais e internacionais, sejam instalados e testados em intervalos regulares, e cubram todas as portas externas e janelas acessíveis; as áreas não ocupadas devem ser protegidas por alarmes o tempo todo.

Informações adicionais:

Pode-se obter proteção física criando uma ou mais barreiras físicas ao redor dos locais de guarda dos ativos de informação da instituição. O uso de barreiras múltiplas proporciona uma proteção adicional, uma vez que neste caso a falha de uma das barreiras não significa que a segurança fique comprometida imediatamente.

Uma área segura pode ser um escritório trancável ou um conjunto de salas rodeado por uma barreira física interna contínua de segurança. Pode haver necessidade de barreiras e perímetros adicionais para o controle do acesso físico, quando existem áreas com requisitos de segurança diferentes dentro do perímetro de segurança. Convém que sejam tomadas precauções especiais para a segurança do acesso físico no caso de edifícios que alojam diversas instituições.

8.1.2 Controles de entrada física

Controle:

Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.

Diretrizes para implementação:

Convém que sejam levadas em consideração as seguintes diretrizes:

a) a data e hora da entrada e saída de visitantes sejam registradas, e todos os visitantes sejam supervisionados, a não ser que o seu acesso tenha sido previamente aprovado; convém que as permissões de acesso sejam concedidas somente para finalidades específicas e autorizadas, e sejam emitidas com instruções sobre os requisitos de segurança da área e os procedimentos de emergência;

b) acesso às áreas em que são processadas ou armazenadas informações sensíveis seja controlado e restrito às pessoas autorizadas; convém que sejam utilizados controles de autenticação, por exemplo, cartão de controle de acesso mais PIN *(personal identification number)*, para autorizar e

validar todos os acessos; deve ser mantido de forma segura um registro de todos os acessos para fins de auditoria;

c) seja exigido que todos os funcionários, fornecedores e terceiros, e todos os visitantes, tenham alguma forma visível de identificação, e eles devem avisar imediatamente o pessoal de segurança caso encontrem visitantes não acompanhados ou qualquer pessoa que não esteja usando uma identificação visível;

d) aos terceiros que realizam serviços de suporte, seja concedido acesso restrito às áreas seguras ou às instalações de guarde de informação sensível (ou confidencial) somente quando necessário. Este acesso deve ser autorizado e monitorado;

e) os direitos de acesso a áreas seguras sejam revistos e atualizados em intervalos regulares, e revogados quando necessário (ver 8.1.5).

8.1.3 Segurança em escritórios, salas e instalações

Controle:

Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações.

Diretrizes para implementação

Convém que sejam levadas em consideração as seguintes diretrizes para proteger escritórios, salas e instalações:

a) sejam levados em conta os regulamentos e normas de saúde e segurança aplicáveis;

b) as instalações-chave sejam localizadas de maneira a evitar o acesso do público;

c) os edifícios sejam discretos e deem a menor indicação possível da sua finalidade, sem letreiros evidentes, fora ou dentro do edifício.

8.1.4 Proteção contra ameaças externas e do meio ambiente

Controle:

Convém que sejam projetadas e aplicadas proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem.

Diretrizes para implementação:

Convém que sejam levadas em consideração todas as ameaças à segurança representadas por instalações vizinhas, por exemplo, um incêndio em um edifício vizinho, vazamento de água do telhado ou em pisos do subsolo ou uma explosão na rua.

Convém que sejam levadas em consideração as seguintes diretrizes para evitar danos causados por incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem:

a) os materiais perigosos ou combustíveis sejam armazenados a uma distância segura da área de segurança. Suprimentos em grande volume, como materiais de papelaria, não devem ser armazenados dentro de uma área segura;

b) os equipamentos apropriados de detecção e combate a incêndios sejam providenciados e posicionados corretamente.

8.1.5 Trabalhando em áreas seguras

Controle:

Convém que seja projetada e aplicada proteção física, bem como diretrizes para o trabalho em áreas seguras.

Diretrizes para implementação:

Convém que sejam levadas em consideração as seguintes diretrizes:

a) pessoal só tenha conhecimento da existência de áreas seguras ou das atividades nelas realizadas, apenas se for necessário;

b) seja evitado o trabalho não supervisionado em áreas seguras, tanto por motivos de segurança como para prevenir as atividades mal intencionadas;

c) as áreas seguras não ocupadas sejam fisicamente trancadas e periodicamente verificadas;

d) não seja permitido o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos móveis, salvo se for autorizado. As normas para o trabalho em áreas seguras incluem o controle dos funcionários, fornecedores e terceiros que trabalham em tais áreas, bem como o controle de outras atividades de terceiros nestas áreas.

8.1.6 Acesso do público, áreas de entrega e de carregamento

Controle:

Convém que os pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, sejam controlados.

Diretrizes para implementação:

Convém que sejam levadas em consideração as seguintes diretrizes:

a) acesso a uma área de entrega e carregamento a partir do exterior do prédio fique restrito ao pessoal identificado e autorizado;

b) as áreas de entrega e carregamento sejam projetadas de tal maneira que seja possível descarregar suprimentos sem que os entregadores tenham acesso a outras partes do edifício;

c) as portas externas de uma área de entrega e carregamento sejam protegidas enquanto as portas internas estiverem abertas;

d) os materiais entregues sejam inspecionados para detectar ameaças potenciais (ver 8.2.1) antes de serem transportados da área de entrega e carregamento para o local de utilização;

e) os materiais entregues sejam registrados por ocasião de sua entrada no local, usando-se procedimentos de gerenciamento de ativos;

f) as remessas entregues sejam segregadas fisicamente das remessas que saem, sempre que possível.

8.2 Segurança de equipamentos nos locais de guarda da documentação

Objetivo: Impedir perdas, danos, furto ou comprometimento dos equipamentos presentes nos locais de guarda dos ativos de informação, colocando em risco a interrupção das atividades da instituição.

Convém que os equipamentos sejam protegidos contra ameaças físicas e do meio ambiente. A proteção dos equipamentos (incluindo aqueles utilizados fora do local, e a retirada de ativos) é necessária para reduzir o risco de acesso não autorizado às informações e para proteger contra perdas ou danos.

Convém que também seja levada em consideração a introdução de equipamentos no local, bem como sua remoção.

8.2.1 Instalação e proteção do equipamento

Controle:

Convém que os equipamentos sejam colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.

Diretrizes para implementação:

Convém que sejam levadas em consideração as seguintes diretrizes para proteger os equipamentos:

a) os equipamentos sejam colocados no local, a fim de minimizar o acesso desnecessário às áreas de trabalho;

b) os itens que exigem proteção especial devem ser isolados para reduzir o nível geral de proteção necessário;

c) sejam adotados controles para minimizar o risco de ameaças físicas potenciais, tais como furto, incêndio, explosivos, fumaça, água (ou falha do suprimento de água), poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo;

d) as condições ambientais, como temperatura e umidade, sejam monitoradas para a detecção de condições que possam causar incidentes em segurança da informação;

e) todos os edifícios sejam dotados de proteção contra raios e todas as linhas de entrada de força e de comunicações tenham filtros de proteção contra raios;

f) para equipamentos em ambientes industriais, o uso de métodos especiais de proteção, tais como membranas para teclados, deve ser considerado.

8.2.2 Utilidades

Controle:

Convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.

Diretrizes para implementação:

Convém que as utilidades, como suprimento de energia elétrica, de água, esgotos, calefação/ventilação e ar-condicionado sejam adequados para os sistemas que eles suportam.

Convém que as utilidades sejam inspecionadas em intervalos regulares e testadas de maneira apropriada para assegurar seu funcionamento correto e reduzir os riscos de defeitos ou interrupções do funcionamento.

Convém que seja providenciado um suprimento adequado de energia elétrica, de acordo com as especificações do fabricante dos equipamentos. Recomenda-se o uso de UPS (Uninterruptible Power Supply – Unidade de Alimentação sem Interrupções – No Break) para suportar as paradas e desligamento dos equipamentos ou para manter o funcionamento contínuo dos equipamentos que suportam operações críticas dos negócios.

Convém que hajam planos de contingência de energia referentes às providências a serem tomadas em caso de falha do UPS. Convém que seja considerado um gerador de emergência caso seja necessário que o processamento continue mesmo se houver uma interrupção prolongada do suprimento de energia.

Convém que os equipamentos UPS e os geradores sejam verificados em intervalos regulares para assegurar que eles tenham capacidade adequada, e sejam testados de acordo com as recomendações do fabricante. Além disto, deve ser considerado o uso de múltiplas fontes de energia ou de uma subestação de força separada, se o local for grande.

Convém que as chaves de emergência para o desligamento da energia fiquem localizadas na proximidade das saídas de emergência das salas de equipamentos, para facilitar o desligamento rápido da energia em caso de uma emergência. Convém que seja providenciada iluminação de emergência para o caso de queda da força.

Convém que o suprimento de água seja estável e adequado para abastecer os equipamentos de arcondicionado e de umidificação, bem como os sistemas de extinção de incêndios (quando usados). Falhas de funcionamento do abastecimento de água podem danificar o sistema ou impedir uma ação eficaz de extinção de incêndios.

Convém que seja analisada a necessidade de sistemas de alarme para detectar falhas de funcionamento das utilidades, instalando os alarmes, se necessário.

Convém que os equipamentos de telecomunicações sejam conectados à rede pública de energia elétrica através de pelo menos duas linhas separadas, para evitar que a falha de uma das conexões interrompa os serviços de voz. Convém que os serviços de voz sejam adequados para atender às exigências legais locais relativas a comunicações de emergência.

Informações adicionais

As opções para assegurar a continuidade do suprimento de energia incluem múltiplas linhas de entrada, para evitar que uma falha em um único ponto comprometa o suprimento de energia.

9 GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

9.1 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.

Convém que a instituição verifique a implementação dos acordos, monitore a conformidade com tais acordos e gerencie as mudanças para garantir que os serviços atendem a todos os requisitos acordados com os terceiros.

9.1.1 Entrega de serviços

Controle:

Convém que seja 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.

Diretrizes para implementação:

Convém que a entrega de serviços por um terceiro inclua os arranjos de segurança acordados, definições de serviço e aspectos de gerenciamento de serviços.

Convém que a instituição garanta que o terceiro mantenha capacidade de serviço suficiente, juntamente com planos viáveis projetados para garantir que os níveis de continuidade de serviços acordados sejam mantidos após falhas de serviços severas ou desastres (ver 12.1).

9.1.2 Monitoramento e análise crítica de serviços terceirizados

Controle:

Convém que os serviços, relatórios e registros fornecidos por terceiro sejam regularmente monitorados e analisados criticamente, e que auditorias sejam executadas regularmente (se necessário).

Diretrizes para implementação:

Convém que a monitoração e análise crítica dos serviços terceirizados garantam a aderência entre os termos de segurança de informação e as condições dos acordos, e que problemas e incidentes de segurança da informação sejam gerenciados adequadamente.

Convém que isto envolva processos e relações de gerenciamento de serviço entre a instituição e o terceiro para:

a) monitorar níveis de desempenho de serviço para verificar aderência aos acordos;

b) analisar criticamente os relatórios de serviços produzidos por terceiros e agendamento de reuniões de progresso conforme requerido pelos acordos;

c) fornecer informações acerca de incidentes de segurança da informação e análise crítica de tais informações tanto pelo terceiro quanto pela instituição, como requerido pelos acordos e por quaisquer procedimentos e diretrizes que os apoiem;

d) analisar criticamente as trilhas de auditoria do terceiro e registros de eventos de segurança, problemas operacionais, falhas, investigação de falhas e interrupções relativas ao serviço entregue;

e) resolver e gerenciar quaisquer problemas identificados.

Convém que a responsabilidade do gerenciamento de relacionamento com o terceiro seja atribuída a um indivíduo designado ou equipe de gerenciamento de serviço. Adicionalmente, convém que a instituição garanta que o terceiro atribua responsabilidades pela verificação de conformidade e reforço aos requisitos dos acordos.

Convém que habilidades técnicas suficientes e recursos sejam disponibilizados para monitorar se os requisitos de segurança da informação estão sendo atendidos.

Convém que ações apropriadas sejam tomadas quando deficiências na entrega dos serviços forem observadas.

Convém que a instituição garanta a retenção da visibilidade nas atividades de segurança como gerenciamento de mudanças, identificação de vulnerabilidades e relatório/resposta de incidentes de segurança da informação através de um processo de notificação, formatação e estruturação claramente definido.

Informações adicionais

Em caso de terceirização, a instituição precisa estar ciente de que a responsabilidade final pelos ativos de informação permanece com ela.

Para serviços terceirizados de digitalização cita-se como referência a publicação: Recomendações para digitalização de documentos arquivísticos permanentes. Conselho Nacional de Arquivos (CONARQ), 2010.

9.1.3 Gerenciamento de mudanças para serviços terceirizados

Controle:

Convém que mudanças no provisionamento dos serviços, incluindo manutenção e melhoria da política de segurança da informação, procedimentos e controles existentes, sejam gerenciadas.

Diretrizes para implementação:

O processo de gerenciamento de mudanças para serviços terceirizados precisa levar em conta:

a) mudanças feitas pela instituição para a implementação de:

1) melhorias dos serviços correntemente oferecidos;

2) desenvolvimento de quaisquer novas aplicações ou sistemas;

3) modificações ou atualizações das políticas e procedimentos da instituição;

4) novos controles para resolver os incidentes de segurança da informação e para melhorar a segurança;

b) mudanças em serviços de terceiros para implementação de:

1) mudanças e melhorias em redes;

2) uso de novas tecnologias;

3) adoção de novos produtos ou novas versões;

4) novas ferramentas e ambientes de desenvolvimento;

5) mudanças de localização física dos recursos de serviços;

6) mudanças de fornecedores.

10 CONTROLE DE ACESSOS

10.1 Requisitos de negócio para controle de acesso

Objetivo: Controlar o acesso à informação.

Convém que o acesso à informação seja controlado com base na segurança da informação e Política de Segurança da Informação aplicada na instituição.

10.1.1 Política de controle de acesso

Controle:

Convém que a política de controle de acesso seja estabelecida documentada e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e segurança da informação.

Diretrizes para implementação:

Convém que as regras de controle de acesso e direitos para cada usuário ou grupos de usuários sejam expressas claramente na política de controle de acesso.

Convém considerar os controles de acesso lógico e físico (ver seção 8) de forma conjunta.

Convém fornecer aos usuários e provedores de serviços uma declaração nítida dos requisitos do negócio a serem atendidos pelos controles de acessos.

Convém que a política leve em consideração os seguintes itens:

a) requisitos de segurança de aplicações de negócios individuais;

b) identificação de todas as informações relacionadas às aplicações de negócios e os riscos a que as informações estão expostas;

c) política para disseminação e autorização da informação, por exemplo, a necessidade de conhecer princípios e níveis de segurança e a classificação dos ativos de informação (ver 6.1.1);

d) legislação pertinente e qualquer obrigação contratual relativa à proteção de acesso (ver 13.1);

e) perfis de acesso de usuário-padrão para trabalhos comuns na instituição;

f) segregação de regras de controle de acesso, por exemplo, pedido de acesso, autorização de acesso, administração de acesso;

g) requisitos para autorização formal de pedidos de acesso ver 10.2.1);

h) requisitos para análise crítica periódica de controles de acesso;

i) remoção de direitos de acesso (ver 7.2.3).

10.2 Gerenciamento de acesso dos usuários de arquivo

Objetivo: Assegurar acesso de usuário autorizado e prevenir acesso não autorizado nos locais de guarda da documentação

Convém que procedimentos formais sejam implementados para controlar o acesso e direitos de acessos aos locais de guarda da documentação.

Convém que os procedimentos cubram todas as fases do ciclo de vida de acesso do usuário, da inscrição inicial como novos usuários até o cancelamento final do registro de usuários que já não requerem acesso ao arquivo.

10.2.1 Registro de usuários

Controle:

Convém que exista um procedimento formal de registro e cancelamento de usuário.

Diretrizes para implementação:

Convém que os procedimentos de controle de acesso para registro e cancelamento de usuários incluam:

a) utilizar identificador de usuário (ID de usuário) único para assegurar a responsabilidade de cada usuário por suas ações; convém que o uso de grupos de ID somente seja permitido onde existe a necessidade para o negócio ou por razões operacionais, e isso seja aprovado e documentado;

b) verificar se o nível de acesso concedido é apropriado ao propósito do negócio (ver 10.1) e é consistente com a política de segurança da instituição.

c) dar para os usuários uma declaração por escrito dos seus direitos de acesso;

d) requerer aos usuários a assinatura de uma declaração indicando que eles entendem as condições de acesso;

e) manter um registro formal de todas as pessoas registradas para usar o serviço;

f) remover imediatamente ou bloquear direitos de acesso de usuários que mudaram de cargos ou funções, ou deixaram a instituição;

g) verificar periodicamente e remover ou bloquear identificadores (ID) e contas de usuário redundantes;

h) assegurar que identificadores de usuário (ID de usuário) redundantes não sejam atribuídos para outros usuários.

Informações adicionais:

Convém que seja considerado estabelecer perfis de acesso do usuário baseados nos requisitos dos negócios que resumam um número de direitos de acessos dentro de um perfil de acesso típico de usuário. Solicitações de acessos e análises críticas (ver 11.2.4) são mais fáceis de gerenciar ao nível de tais perfis do que ao nível de direitos particulares.

Convém que seja considerada a inclusão de cláusulas nos contratos de usuários e de serviços que especifiquem as sanções em caso de tentativa de acesso não autorizado pelos usuários ou por terceiros (7.1.3 e 7.1.6).

10.3 Controle de acesso à informação

Objetivo: Prevenir acesso não autorizado à informação arquivística sob guarda da instituição.

Convém que o acesso à informação seja restrito a usuários autorizados.

10.3.1 Restrição de acesso à informação

Controle:

Convém que o acesso à informação seja restrito de acordo com o definido na política de controle de acesso.

Diretrizes para implementação:

Convém que a política de controle de acesso seja consistente com a política de acesso da instituição. (ver 10.1).

11 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

11.1 Notificação de fragilidades e eventos de segurança da informação

Objetivo: Assegurar que fragilidades e eventos de segurança da informação associados com ativos de informação não digitais sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.

Convém que todos os funcionários, fornecedores, terceiros e usuários de arquivo estejam conscientes sobre os procedimentos para notificação dos diferentes tipos de eventos e fragilidades que possam ter impactos na segurança dos ativos da instituição.

Convém que seja requerido que os eventos de segurança da informação e fragilidades sejam notificados, tão logo quanto possível, ao ponto de contato designado.

11.1.1 Notificação de eventos de segurança da informação

Controle:

Convém que os eventos de segurança da informação sejam relatados através dos canais apropriados da direção, o mais rapidamente possível.

Diretrizes para Implementação:

Convém que um procedimento de notificação formal seja estabelecido para relatar os eventos de segurança da informação, junto com um procedimento de resposta a incidente, estabelecendo a ação a ser tomada ao se receber a notificação de um evento de segurança da informação.

Convém que um ponto de contato seja estabelecido para receber as notificações dos eventos de segurança da informação.

Convém que este ponto de contato seja de conhecimento de toda a instituição e esteja sempre disponível e em condições de assegurar uma resposta adequada e oportuna.

Convém que todos os funcionários, fornecedores, terceiros e usuários sejam alertados sobre sua responsabilidade de notificar qualquer evento de segurança da informação o mais rapidamente possível.

Convém que eles também estejam cientes do procedimento para notificar os eventos de segurança da informação e do ponto de contato designado para este fim.

Convém que os procedimentos incluam:

a) processos adequados de realimentação e feedback para assegurar que os eventos de segurança da informação relatados sejam notificados dos resultados após a questão ter sido conduzida e concluída;

b) formulário para apoiar a ação de notificar um evento de segurança da informação e ajudar as pessoas a lembrar as ações necessárias para a notificação do evento;

c) o comportamento correto a ser tomado no caso de um evento de segurança da informação, como, por exemplo:

1) anotar todos os detalhes importantes imediatamente (por exemplo, tipo de não-conformidade ou violação, comportamento estranho, etc.);

2) não tomar nenhuma ação própria, mas informar imediatamente o evento ao ponto de contato;

d) referência para um processo disciplinar formal estabelecido para lidar com funcionários, fornecedores, terceiros ou usuários que cometam violações de segurança da informação. Em ambientes de alto risco, podem ser fornecidos alarmes de coação[11] através do qual a pessoa que está sendo coagida possa sinalizar o que está ocorrendo.

Convém que os procedimentos para responder a alarmes de coação reflitam o alto risco que a situação exige.

Informações adicionais:

Exemplos de eventos e incidentes de segurança da informação (não digital) são:

a) roubo ou extravio de informação;

b) acesso não autorizado (violação de acesso);

c) erros humanos;

d) não-conformidade com políticas ou diretrizes;

e) violações de procedimentos de segurança física;

f) desastres naturais que danificaram a informação (documentação arquivística);

h) divulgação de informações sigilosas

[11] Alarme de coação é um método usado para indicar, de forma secreta, que uma ação está acontecendo sob coação.

Considerando os cuidados com os aspectos de confidencialidade, os incidentes de segurança da informação podem ser utilizados em treinamento de conscientização (ver 7.1.5) como exemplos do que poderia ocorrer, como responder a tais incidentes e como evitá-los futuramente. Para ser capaz de destinar os eventos e incidentes de segurança da informação adequadamente, pode ser necessário coletar evidências tão logo quanto possível depois da ocorrência (ver 11.2.3). Mais informações sobre notificação de eventos de segurança da informação e gestão de incidentes de segurança da informação podem ser encontradas na ISO/IEC TR 18044.

11.1.2 Notificando fragilidades de segurança da informação

Controle:

Convém que os funcionários, fornecedores, terceiros e usuários do arquivo sejam instruídos a registrar e notificar qualquer observação ou suspeita em relação à segurança da informação.

Diretrizes para implementação:

Convém que os funcionários, fornecedores, terceiros e usuários notifiquem esse assunto o mais rápido possível para sua direção, de forma a prevenir incidentes de segurança da informação. Convém que o mecanismo de notificação seja fácil, acessível e disponível sempre que possível. Convém que os usuários sejam informados que não podem, sob nenhuma circunstância, tentar averiguar fragilidade suspeita.

Informações adicionais

Convém que os funcionários, fornecedores e terceiros sejam alertados para não tentarem averiguar uma fragilidade de segurança da informação suspeita. Testar fragilidades pode causar danos às informação, resultando em responsabilidade legal ao indivíduo que efetuar o teste.

11.2 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.

Convém que responsabilidades e procedimentos estejam definidos para o manuseio efetivo de eventos de segurança da informação e fragilidades, uma vez que estes tenham sido notificados.

Convém que um processo de melhoria contínua seja aplicado às respostas, monitoramento, avaliação e gestão total de incidentes de segurança da informação.

Convém que onde evidências sejam exigidas, estas sejam coletadas para assegurar a conformidade com as exigências legais.

11.2.1 Responsabilidades e procedimentos

Controle:

Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.

Diretrizes para implementação:

Convém que, adicionalmente à notificação de eventos de segurança da informação e fragilidades (ver 11.1), o monitoramento, alertas e vulnerabilidades seja utilizado para a detecção de incidentes de segurança da informação.

Convém que as seguintes diretrizes para procedimentos de gestão de incidentes de segurança da informação sejam consideradas:

a) procedimentos sejam estabelecidos para os diferentes tipos de incidentes de segurança da informação.

b) além dos planos de contingência (ver 12.1.3), convém que os procedimentos também considerem (ver 11.2.2):

1) análise e identificação da causa do incidente;

2) retenção;

3) planejamento e implementação de ação corretiva para prevenir a sua repetição, se necessário;

4) comunicação com aqueles afetados ou envolvidos com a recuperação do incidente;

5) notificação da ação para a autoridade apropriada;

c) convém que trilhas de auditoria e evidências similares sejam coletadas (ver 11.2.3) e protegidas, como apropriado, para:

1) análise de problemas internos;

2) uso como evidência forense para o caso de uma potencial violação de contrato ou de normas reguladoras ou em caso de delitos civis ou criminais, por exemplo relacionados a legislação de proteção dos dados;

Convém que os objetivos da gestão de incidentes de segurança da informação estejam em concordância com a direção e que seja assegurado que os responsáveis pela gestão de incidentes

de segurança da informação entendem as prioridades da instituição no manuseio de incidentes de segurança da informação.

Informações adicionais:

Os incidentes de segurança da informação podem transcender fronteiras institucionais e nacionais. Para responder a estes incidentes, cada vez mais há a necessidade de resposta coordenada e troca de informações sobre eles com instituições externas, quando apropriado.

11.2.2 Aprendendo com os incidentes de segurança da informação

Controle:

Convém que sejam estabelecidos mecanismos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorados.

Diretrizes para implementação:

Convém que a informação resultante da análise de incidentes de segurança da informação seja usada para identificar incidentes recorrentes ou de alto impacto.

Informações adicionais:

A análise de incidentes de segurança da informação pode indicar a necessidade de melhorias ou controles adicionais para limitar a frequência, danos e custos de ocorrências futuras ou para ser levada em conta quando for realizado o processo de análise crítica da política de segurança da informação (ver 5.1.2).

11.2.3 Coleta de evidências

Controle:

Nos casos em que uma ação de acompanhamento contra uma pessoa ou instituição, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), convém que evidências sejam coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição (ões) pertinente(s).

Diretrizes para implementação:

Convém que procedimentos internos sejam elaborados e respeitados para as atividades de coleta e apresentação de evidências com o propósito de ação disciplinar movida em uma instituição.

Em geral, as normas para evidências abrangem:

a) admissibilidade da evidência: se a evidência pode ser ou não utilizada na corte;

b) importância da evidência: qualidade e inteireza da evidência.

Convém que o valor da evidência esteja de acordo com algum requisito aplicável. Para obter o valor da evidência, convém que a qualidade e a inteireza dos controles usados para proteger as evidências de forma correta e consistente (ou seja, o processo de controle de evidências) durante todo o período de armazenamento e processamento da evidência sejam demonstradas por uma trilha forte de evidência.

Em geral, essa trilha forte de evidência pode ser estabelecida sob na seguinte condição:

a) para documentos em papel: o original é mantido de forma segura, com um registro da pessoa que o encontrou, do local e data em que foi encontrado e quem testemunhou a descoberta; convém que qualquer investigação assegure que os originais não foram adulterados;

Convém que qualquer trabalho forense seja somente realizado em cópias do material de evidência. Convém que a integridade de todo material de evidência seja preservada.

Convém que o processo de cópia de todo material de evidência seja supervisionado por pessoas confiáveis e que as informações sobre a data, local, pessoas, ferramentas e programas envolvidos no processo de cópia sejam registradas.

Informações adicionais:

Quando um evento de segurança da informação é detectado, pode não ser óbvio que ele resultará num possível processo jurídico. Entretanto, existe o perigo de que a evidência seja destruída intencional ou acidentalmente antes que seja percebida a seriedade do incidente. É conveniente envolver um advogado ou a polícia tão logo seja constatada a possibilidade de processo jurídico e obter consultoria sobre as evidências necessárias.

As evidências podem ultrapassar limites institucionais e/ou de jurisdições. Nesses casos, convém assegurar que a instituição seja devidamente autorizada para coletar as informações requeridas como evidências.

Convém que os requisitos de diferentes jurisdições sejam também considerados para maximizar as possibilidades de admissão da evidência em todas as jurisdições relevantes.

12 GESTÃO DA CONTINUIDADE DO NEGÓCIO

12.1 Aspectos da gestão da continuidade do negócio, relativos à segurança da informação

Objetivo: Não permitir a interrupção das atividades institucionais e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se necessário.

Convém que o processo de gestão da continuidade do negócio seja implementado para minimizar um impacto sobre a instituição e recuperar perdas de ativos da informação (que pode ser resultante de, por exemplo, desastres naturais, acidentes, falhas de equipamentos e ações intencionais) a um nível aceitável através da combinação de ações de prevenção e recuperação.

Convém que este processo identifique os processos críticos e integre a gestão da segurança da informação com as exigências da gestão da continuidade do negócio com outros requisitos de continuidade relativo a tais aspectos como operações, funcionários, materiais, transporte e instalações.

Convém que as consequências de desastres, falhas de segurança estejam sujeitas a uma análise de impacto nos negócios. Convém que os planos de continuidade do negócio sejam desenvolvidos e implementados para assegurar que as atividades sejam recuperadas dentro da requerida escala de tempo. Convém que a segurança da informação seja uma parte integrante do processo global de continuidade de negócios e a gestão de outros processos dentro da instituição.

Convém que a gestão da continuidade do negócio inclua controles para identificar e reduzir riscos, em complementação ao processo de análise/avaliação de riscos global, limite as consequências aos danos do incidente e garanta que as informações requeridas para os processos do negócio estejam prontamente disponíveis.

12.1.1 Incluindo segurança da informação no processo de gestão da continuidade de negócio

Controle:

Convém que um processo de gestão seja desenvolvido e mantido para assegurar a continuidade do negócio por toda a instituição e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio (das atividades) na instituição.

Diretrizes para implementação:

Convém que este processo agregue os seguintes elementos-chave da gestão da continuidade do negócio:

a) entendimento dos riscos a que a instituição está exposta, no que diz respeito à sua probabilidade e impacto no tempo, incluindo a identificação e priorização dos processos críticos do negócio (ver 12.1.2);

b) identificação de todos os ativos de informação envolvidos em processos críticos de negócio (ver 6.1.2);

c) entendimento do impacto que incidentes de segurança da informação provavelmente terão sobre os negócios (é importante que as soluções encontradas possam tratar tanto os pequenos incidentes, como os mais sérios, que poderiam colocar em risco a continuidade da instituição) e estabelecimento dos objetivos do negócio;

d) consideração de contratação de seguro compatível que possa ser parte integrante do processo de continuidade do negócio, bem como a parte de gestão de risco operacional;

e) identificação e consideração da implementação de controles preventivos e de mitigação;

f) identificação de recursos financeiros, institucionais, técnicos e ambientais suficientes para identificar os requisitos de segurança da informação;

g) garantia da segurança de pessoal e proteção das informações e bens institucionais;

h) detalhamento e documentação de planos de continuidade de negócio que contemplem os requisitos de segurança da informação alinhados com a estratégia da continuidade do negócio estabelecida (ver 12.1.3);

i) testes e atualizações regulares dos planos e processos implantados (ver 12.1.5);

j) garantia de que a gestão da continuidade do negócio esteja incorporada aos processos e estrutura da instituição.

Convém que a responsabilidade pela coordenação do processo de gestão de continuidade de negócios seja atribuída a um nível adequado dentro da instituição.

12.1.2 Continuidade de negócios e análise/avaliação de riscos

Controle:

Convém identificar os eventos que podem causar interrupções aos processos de negócio, junto a probabilidade e impacto de tais interrupções e as consequências para a segurança de informação.

Diretrizes para implementação:

Convém que os aspectos da continuidade do negócios relativos à segurança da informação sejam baseados na identificação de eventos (ou sucessão de eventos) que possam causar interrupções aos processos de negócios das instituições, por exemplo erros humanos, roubo, incêndio, desastres naturais e atos terroristas.

Em seguida, convém que seja feita uma análise/avaliação de riscos para a determinação da probabilidade e impacto de tais interrupções, tanto em termos de escala de dano quanto em relação ao período de recuperação.

Convém que as análises/avaliações de riscos da continuidade do negócio sejam realizadas com total envolvimento dos responsáveis pelos processos e recursos do negócio.

Convém que a análise/avaliação considere todos os processos do negócio e não esteja limitada aos recursos de processamento das informações, mas inclua os resultados específicos da segurança da informação. É importante a junção de aspectos de riscos diferentes, para obter um quadro completo dos requisitos de continuidade de negócios da instituição.

Convém que a análise/avaliação identifique, quantifique e priorize os critérios baseados nos riscos e os objetivos pertinentes à instituição.

Em função dos resultados da análise/avaliação de riscos, convém que um plano estratégico seja desenvolvido para se determinar a abordagem mais abrangente a ser adotada para a continuidade dos negócios.

Uma vez criada a estratégia, convém que ela seja validada pela direção e que um plano seja elaborado e validado para implementar tal estratégia.

12.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação

Controle:

Convém que os planos sejam desenvolvidos e implementados para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida.

Diretrizes para implementação:

Convém que o processo de planejamento da continuidade de negócios considere os seguintes itens:

a) identificação e concordância de todas as responsabilidades e procedimentos da continuidade do negócio;

b) identificação da perda aceitável de informações;

c) implementação dos procedimentos que permitam a recuperação e restauração das operações do negócio e da disponibilidade da informação nos prazos necessários; atenção especial precisa ser dada à avaliação de dependências externas ao negócio e de contratos existentes;

d) procedimentos operacionais que permitam a conclusão de restauração e recuperação que estejam pendentes;

e) documentação dos processos e procedimentos acordados;

f) educação adequada de pessoas nos procedimentos e processos definidos, incluindo o gerenciamento de crise;

g) teste e atualização dos planos.

Convém que o processo de planejamento foque os objetivos requeridos do negócio, por exemplo recuperação de determinados serviços específicos para os usuários, em um período de tempo aceitável.

Convém que o plano de continuidade do negócio trate as vulnerabilidades da instituição, que pode conter informações sensíveis e que necessitem de proteção adequada.

Convém que cópias do plano de continuidade do negócio sejam guardadas em um ambiente remoto, a uma distância suficiente para escapar de qualquer dano de um desastre no local principal.

Convém que o gestor garanta que as cópias dos planos de continuidade do negócio estejam atualizadas e protegidas no mesmo nível de segurança como aplicado no ambiente principal.

Convém que outros materiais necessários para a execução do plano de continuidade do negócio também sejam armazenados em local afastado.

Convém que, se os ambientes alternativos temporários forem usados, o nível de controles de segurança implementados nestes locais seja equivalente ao ambiente principal.

Informações adicionais

Convém que seja destacado que as atividades e os planos de gerenciamento de crise (ver 12.1.3) possam ser diferentes de gestão de continuidade de negócios, isto é, uma crise pode acontecer e ser suprida através dos procedimentos normais de gestão.

12.1.4 Estrutura do plano de continuidade do negócio

Controle:

Convém que uma estrutura básica dos planos de continuidade do negócio seja 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.

Diretrizes para implementação:

Convém que cada plano de continuidade do negócio descreva o enfoque para continuidade, por exemplo, o enfoque para assegurar a disponibilidade e segurança da informação.

Convém que cada plano também especifique o plano de escalonamento e as condições para sua ativação, assim como as responsabilidades individuais para execução de cada uma das atividades do plano. Quando novos requisitos são identificados, é importante que os procedimentos de emergência relacionados sejam ajustados de forma apropriada, por exemplo o plano de abandono ou o procedimento de recuperação.

Convém que os procedimentos do programa de gestão de mudança da instituição sejam incluídos para assegurar que os assuntos de continuidade de negócios estejam sempre direcionados adequadamente. Convém que cada plano tenha um gestor específico.

Convém que procedimentos de emergência, de recuperação, manual de planejamento e planos de reativação sejam de responsabilidade dos gestores dos recursos de negócios ou dos processos envolvidos.

Convém que uma estrutura de planejamento para continuidade de negócios contemple os requisitos de segurança da informação identificados e considere os seguintes itens:

a) condições para ativação dos planos, os quais descrevem os processos a serem seguidos (como se avaliar a situação, quem deve ser acionado etc.) antes de cada plano ser ativado;

b) procedimentos de emergência que descrevam as ações a serem tomadas após a ocorrência de um incidente que coloque em risco as operações do negócio;

c) procedimentos de recuperação que descrevam as ações necessárias para a transferência das atividades essenciais do negócio ou os serviços de infra-estrutura para localidades alternativas temporárias e para a reativação dos processos do negócio no prazo necessário;

d) procedimentos operacionais temporários para seguir durante a conclusão de recuperação e restauração;

e) procedimentos de recuperação que descrevam as ações a serem adotadas quando do restabelecimento das operações;

f) uma programação de manutenção que especifique quando e como o plano deverá ser testado e a forma de se proceder à manutenção deste plano;

g) atividades de treinamento, conscientização e educação com o propósito de criar o entendimento do processo de continuidade de negócios e de assegurar que os processos continuem a ser efetivo;

h) designação das responsabilidades individuais, descrevendo quem é responsável pela execução de que item do plano. Convém que suplentes sejam definidos quando necessário;

i) os ativos e recursos críticos precisam estar aptos a desempenhar os procedimentos de emergência, recuperação e reativação.

12.1.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio

Controle:

Convém que os planos de continuidade do negócio sejam testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.

Diretrizes para implementação:

Convém que os testes do plano de continuidade do negócio assegurem que todos os membros da equipe de recuperação e outras pessoas relevantes estejam conscientes dos planos e de suas responsabilidades para a continuidade do negócio e a segurança da informação, e conheçam as suas atividades quando um plano for acionado.

Convém que o planejamento e a programação dos testes do(s) plano(s) de continuidade de negócios indiquem como e quando cada elemento do plano seja testado. Convém que os componentes isolados do(s) plano(s) sejam frequentemente testados.

Convém que várias técnicas sejam utilizadas, de modo a assegurar a confiança de que o (s) plano (s) irá (ão) operar consistentemente em casos reais. Convém que sejam considerados:

a) testes de mesa simulando diferentes cenários (verbalizando os procedimentos de recuperação para diferentes formas de interrupção);

b) simulações (particularmente útil para o treinamento do pessoal nas suas atividades gerenciais após o incidente);

c) testes de recuperação técnica, se necessário (garantindo que os sistemas de informação possam ser efetivamente recuperados);

d) testes de recuperação em um local alternativo (executando os processos de negócios em paralelo com a recuperação das operações distantes do local principal);

e) testes dos recursos, serviços e instalações de fornecedores (assegurando que os serviços e produtos fornecidos por terceiros atendem aos requisitos contratados);

f) ensaio geral (testando se a instituição, o pessoal, os equipamentos, os recursos e os processos podem enfrentar interrupções).

Estas técnicas podem ser utilizadas por qualquer instituição. Convém que elas reflitam a natureza do plano de recuperação específico. Convém que os resultados dos testes sejam registrados e ações tomadas para a melhoria dos planos, onde necessário.

Convém que a responsabilidade pelas análises críticas periódicas de cada parte do plano seja definida e estabelecida. Convém que a identificação de mudanças nas atividades do negócio que ainda não tenham sido contempladas nos planos de continuidade de negócio seja seguida por uma apropriada atualização do plano.

Convém que um controle formal de mudanças assegure que os planos atualizados são distribuídos e reforçados por análises críticas periódicas do plano como um todo.

Os exemplos de mudanças onde convém que a atualização dos planos de continuidade do negócio seja considerada são a aquisição de novos equipamentos, atualização de sistemas/informação e mudanças de:

a) pessoal;

b) endereços ou números telefônicos;

c) estratégia de negócio;

d) localização, instalações e recursos;

e) legislação;

f) prestadores de serviços, fornecedores e usuários;

g) processos (inclusões e exclusões);

h) risco (operacional e financeiro).

13 CONFORMIDADE

13.1 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.

Convém que consultoria em requisitos legais específicos seja procurada em instituições de consultoria jurídica ou em profissionais liberais, adequadamente qualificados nos aspectos legais. Os requisitos legislativos variam de país para país e também para a informação criada em um país e transmitida para outro (isto é, fluxo de dados transfronteira).

13.1.1 Identificação da legislação vigente

Controle:

Convém que todos os requisitos estatutários, regulamentares e contratuais relevantes, e o enfoque da instituição para atender a esses requisitos, sejam explicitamente definidos, documentados e mantidos atualizados.

Diretrizes para implementação:

Convém que os controles específicos e as responsabilidades individuais para atender a estes requisitos sejam definidos e documentados de forma similar.

13.1.2 Direitos de propriedade intelectual

Controle:

Convém que procedimentos apropriados sejam 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.

Diretrizes para implementação:

Convém que as seguintes diretrizes sejam consideradas para proteger qualquer material que possa ser considerado como propriedade intelectual:

a) divulgar uma política de conformidade com os direitos de propriedade intelectual que defina o uso legal de informação;

b) manter conscientização das políticas para proteger os direitos de propriedade intelectual e notificar a intenção de tomar ações disciplinares contra pessoas que violarem essas políticas;

c) manter de forma adequada os registros de ativos (plano de classificação de documentos) e identificar todos os ativos com requisitos para proteger os direitos de propriedade intelectual;

d) não copiar, no todo ou em partes, livros, artigos, relatórios ou outros documentos, além daqueles permitidos pela lei de direito autoral.

Informações adicionais:

Legislação, regulamentação e requisitos contratuais podem estabelecer restrições para cópia de material que tenha direitos autorais. Em particular, pode ser requerido que somente material que seja desenvolvido pela instituição ou que foi licenciado ou fornecido pelos desenvolvedores para a instituição seja utilizado. Violações aos direitos de propriedade intelectual podem conduzir a ações legais, que podem envolver processos criminais.

13.1.3 Proteção de registros institucionais

Controle:

Convém que registros importantes sejam protegidos contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.

Diretrizes para implementação:

Convém que registros sejam categorizados em tipos de registros, tais como registros contábeis, registros de base de dados, registros de transações, registros de auditoria e procedimentos operacionais, cada qual com detalhes do período de retenção e do tipo de mídia de armazenamento.

Convém que cuidados sejam tomados a respeito da possibilidade de deterioração das mídias usadas no armazenamento dos registros.

Convém que, para o armazenamento de longo tempo, o uso de papel e microficha seja considerado.

Convém que sistemas de armazenamento de dados sejam escolhidos de modo que o dado solicitado possa ser recuperado de forma aceitável, dependendo dos requisitos a serem atendidos.

Convém que o sistema de armazenamento e manuseio assegure a clara identificação dos registros e dos seus períodos de retenção, conforme definido pela legislação nacional ou regional ou por regulamentações, se aplicável.

Convém que seja permitida a destruição apropriada dos registros após esse período, caso não sejam mais necessários à instituição.

Para atender aos objetivos de proteção dos registros, convém que os seguintes passos sejam tomados dentro da instituição:

a) emitir diretrizes gerais para retenção, armazenamento, tratamento e disposição de registros e informações;

b) elaborar uma programação para retenção, identificando os registros essenciais e o período que cada um deve ser mantido;

c) manter um inventário das fontes de informações-chave;

d) implementar controles apropriados para proteger registros e informações contra perda, destruição e falsificação.

Informações adicionais:

Alguns registros podem precisar ser retidos de forma segura para atender a requisitos estatutários, contratuais ou regulamentares, assim como para apoiar as atividades essenciais do negócio. Exemplo disso são os registros que podem ser exigidos como evidência de que uma instituição opera de acordo com as regras estatutárias e regulamentares, para assegurar a defesa adequada contra potenciais processos civis ou criminais ou confirmar a situação financeira de uma instituição. O período de tempo e o conteúdo da informação retida podem estar definidos através de leis ou regulamentações nacionais. Outras informações sobre como gerenciar os registros institucionais, podem ser encontradas na ISO 15489-1.

13.1.4 Proteção de dados e privacidade de informações pessoais

Controle:

Convém que a privacidade e proteção de dados sejam asseguradas conforme exigido nas legislações relevantes, regulamentações e, se aplicável, nas cláusulas contratuais.

Diretrizes para implementação:

Convém que uma política de privacidade e proteção de dados da instituição seja desenvolvida e implementada.

Convém que esta política seja comunicada a todas as pessoas envolvidas no processamento de informações pessoais.

A conformidade com esta política e todas as legislações e regulamentações relevantes de proteção de dados necessita de uma estrutura de gestão e de controles apropriados. Geralmente isto é melhor alcançado através de uma pessoa responsável, como, por exemplo, um gestor de proteção de dados, que deve fornecer orientações gerais para gerentes, usuários e provedores de serviço sobre as responsabilidades de cada um e sobre quais procedimentos específicos recomenda-se seguir.

Convém que a responsabilidade pelo tratamento das informações pessoais e a garantia da conscientização dos princípios de proteção dos dados sejam tratadas de acordo com as legislações e regulamentações relevantes.

Convém que medidas institucionais e técnicas apropriadas para proteger as informações pessoais sejam implementadas.

Informações adicionais:

Alguns países têm promulgado leis que estabelecem controles na coleta, no processamento e na transmissão de dados pessoais (geralmente informação sobre indivíduos vivos que podem ser identificados a partir de tais informações).

Dependendo da respectiva legislação nacional, tais controles podem impor responsabilidades sobre aqueles que coletam, processam e disseminam informação pessoal, e podem restringir a capacidade de transferência desses dados para outros países.

13.2 Conformidade com normas e políticas de segurança da informação

Objetivo: Garantir conformidade com as políticas e normas institucionais de segurança da informação.

Convém que a segurança da informação seja analisada criticamente a intervalos regulares e sejam executadas com base na políticas de segurança da informação institucional.

13.2.1 Conformidade com as políticas e normas de segurança da informação

Controle:

Convém que gestores garantam que todos os procedimentos de segurança da informação dentro da sua área de responsabilidade estão sendo executados corretamente para atender à conformidade com as normas e políticas de segurança da informação.

Diretrizes para implementação:

Convém que os gestores analisem criticamente, a intervalos regulares, a conformidade dos processos de gestão da informação (dentro sua área de responsabilidade) com as políticas de segurança da informação, normas e quaisquer outros requisitos de segurança. Se qualquer não-conformidade for encontrada como um resultado da análise crítica, convém que os gestores:

a) determinem as causas da não-conformidade;

b) avaliem a necessidade de ações para assegurar que a não-conformidade não se repita;

c) determinem e implementem ação corretiva apropriada;

d) analisem criticamente a ação corretiva tomada.

Convém que os resultados das análises críticas e das ações corretivas realizadas pelos gestores sejam registrados e que esses registros sejam mantidos.

GLOSSÁRIO[12]

As definições a seguir devem ser entendidas no contexto desta Norma.

Acervo	totalidade dos documentos de uma entidade produtora ou de uma entidade custodiadora.
Acesso	direito, oportunidade ou meios de encontrar, recuperar e usar a informação.
Ameaça	causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou instituição [ISO/IEC 13335-1:2004].
Análise de riscos	uso sistemático de informações para identificar fontes e estimar o risco [ABNT ISO/IEC Guia 73:2005].
Análise/avaliação de riscos	processo completo de análise e avaliação de riscos [ABNT ISO/IEC Guia 73:2005].
Arquivamento	1. sequência de operações intelectuais e físicas que visam à guarda ordenada de documentos; 2. ação pela qual uma autoridade determina a guarda de um documento, cessada a sua tramitação.
Arquivo	1. conjunto de documentos produzidos e recebidos por uma entidade coletiva, pública ou privada, família ou pessoa, no desempenho de suas atividades, independente da natureza dos suportes; 2. instituição ou serviço que tem por finalidade a custódia, o processamento técnico, a conservação e acesso de documentos arquivísticos.

[12] Para este glossário foi utilizado os seguintes referenciais: ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC27002** - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação (Conteúdo técnico idêntico ao da ABNT NBR ISO/IEC 17799), 2005. CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS. **Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos:** e-ARQ**.** Conarq, 2006. Disponível em: <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/earqbrasilv1. pdf>. Acesso em: 09 out. 2007. DICIONÁRIO BRASILEIRO DE TERMINOLOGIA ARQUIVÍSTICA. Rio de Janeiro: Arquivo Nacional, 2005.

Ativo	qualquer coisa que tenha valor para a instituição [ISO/IEC 13335-1:2004].
Avaliação arquivística	processo de análise de documentos de arquivo, que estabelece os prazos de guarda e a destinação, de acordo com os valores que lhes são atribuídos.
Avaliação de riscos	processo de comparar o risco estimado com critérios de risco pré-definidos para determinar a importância do risco [ABNT ISO/IEC Guia 73:2005].
Classe	primeira divisão de um plano de classificação ou de um código de classificação.
Classificação	1. análise e identificação do conteúdo de documentos, seleção do descritor sob o qual o documento será recuperado, podendo-ser-lhe atribuir um código. 2. atribuição a documentos, ou às informações neles contidas, de graus de sigilo, conforme legislação específica.
Código de classificação	conjunto de símbolos, normalmente letras e/ou números, derivado de um plano de classificação. Ver também: Classificação; plano de classificação.
Controle	forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas institucionais, que podem ser de natureza administrativa, técnica, de gestão ou legal *NOTA:* Controle é também usado como um sinônimo para proteção ou contramedida.
Destinação	decisão, com base na avaliação, quanto ao encaminhamento de documentos para guarda permanente, descarte ou eliminação.
Diretriz	descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas [ISO/IEC 13335-1:2004].

Documento/informação arquivístico (a)	documento produzido e/ou recebido por uma pessoa física ou jurídica, no decorrer das suas atividades, qualquer que seja o suporte, e dotado de organicidade. (I) Record.
Eliminação	destruição de documentos que, na avaliação (arquivística), foram considerados sem valor permanente. Também chamada expurgo de documentos.
Entidade custodiadora	entidade responsável pela custódia e acesso(2) a um acervo.
Evento de segurança da informação	ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação [ISO/IEC TR 18044:2004].
Gestão arquivística de documentos	conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos arquivísticos em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente.
Gestão de riscos	atividades coordenadas para direcionar e controlar uma instituição no que se refere a riscos [ABNT ISO/IEC Guia 73:2005] *NOTA:* A gestão de riscos geralmente inclui a análise/avaliação de riscos**,** o tratamento de riscos**,** a aceitação de riscos e a comunicação de riscos.
Incidente de segurança da informação	um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação [ISO/IEC TR 18044:2004].
Integridade	estado dos documentos que se encontram completos e que não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada.
Plano de classificação	esquema de distribuição de documentos em classes, de acordo com métodos de arquivamento específicos, elaborado a partir do estudo das estruturas e funções de uma instituição e da análise do arquivo por ela produzido. Expressão geralmente adotada em arquivos correntes.

Política	intenções e diretrizes globais formalmente expressas pela direção.
Processamento da informação	processos utilizados para codificar, armazenar e recuperar informações.
Risco	combinação da probabilidade de um evento e de suas consequências [ABNT ISO/IEC Guia 73:2005].
Segurança da informação	preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.
Sistema de gestão arquivística de documentos	conjunto de procedimentos e operações técnicas cuja interação permite a eficiência e a eficácia da gestão arquivística de documentos.
Sistema de informação	conjunto organizado de políticas, procedimentos, pessoas, equipamentos e programas computacionais que produzem, processam, armazenam e proveem acesso à informação. (I) Information systems.
Terceira parte	pessoa ou organismo reconhecido como independente das partes envolvidas, no que se refere a um dado assunto [ABNT ISO/IEC Guia 2:1998].
Tratamento do risco	processo de seleção e implementação de medidas para modificar um risco [ABNT ISO/IEC Guia 73:2005].
Vulnerabildade	fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

BIBLIOGRAFIA

ABNT NBR ISO 10007:2005 – Sistemas de gestão da qualidade - Diretrizes para a gestão de configuração

ABNT NBR ISO 19011:2002 – Diretrizes para auditorias de sistema de gestão da qualidade e/ou ambiental

ABNT NBR ISO/IEC 12207:1998 – Tecnologia de informação - Processos de ciclo de vida de software

ABNT NBR ISO/IEC27002 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação (Conteúdo técnico idêntico ao da ABNT NBR ISO/IEC 17799), 2005.

ABNT ISO/IEC Guia 2:1998 – Normalização e atividades relacionadas – Vocabulário geral

ABNT ISO/IEC Guia 73:2005 – Gestão de riscos – Vocabulário – Recomendações para uso em normas

CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS. **Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos:** e-ARQ**.** CONSELHO NACIONAL DE ARQUIVOS – CONARQ, 2006. Disponível em: <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/earqbrasilv1.pdf>. Acesso em: 09 out. 2007.

CONSELHO NACIONAL DE ARQUIVOS – CONARQ. Recomendações **para Digitalização de Documentos Arquivísticos Permanentes**, 2010. Disponível em: <http://www.conarq.arquivonacional.gov.br/media/publicacoes/recomenda/recomendaes_para_digitalizao.pdf>. Acesso em: 08 nov. 2011.

DICIONÁRIO BRASILEIRO DE TERMINOLOGIA ARQUIVÍSTICA. Rio de Janeiro: Arquivo Nacional, 2005.

ISO 15489-1:2001 – Information and documentation – Records management – Part 1: General

ISO/IEC 9796-2:2002 – Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms

ISO/IEC 9796-3:2000 – Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms

ISO/IEC 11770-1:1996 – Information technology – Security techniques – Key management – Part 1: Framework

ISO/IEC 13335-1:2004 – Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management

ISO/IEC 13888-1: 1997 – Information technology – Security techniques – Non-repudiation – Part 1: General

ISO/IEC 14516:2002 – Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services

ISO/IEC 14888-1:1998 – Information technology – Security techniques – Digital signatures with appendix – Part 1: General

ISO/IEC 15408-1:1999 – Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model

ISO/IEC 18028-4 – Information technology – Security techniques – IT Network security – Part 4: Securing remote access

ISO/IEC TR 13335-3:1998 – Information technology – Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT Security

ISO/IEC TR 18044 – Information technology – Security techniques – Information security incident

IEEE P1363-2000: Standard Specifications for Public-Key Cryptography

OECD Guidelines for the Security of Information Systems and Networks: 'Towards a Culture of Security', 2002

OECD Guidelines for Cryptography Policy, 1997

Apêndice D – Documento da Política de Segurança da Informação para o DAG

UNIVERSIDADE FEDERAL DE SANTA MARIA - UFSM

DEPARTAMENTO DE ARQUIVO GERAL - DAG

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA NÃO DIGITAL

1 INTRODUÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas do Departamento de Arquivo Geral da UFSM para a proteção dos ativos de informação não digitais e prevenção de responsabilidade legal para funcionários, usuários e terceiros. Deve, portanto, ser cumprida e aplicada em todas as áreas do departamento.

A presente PSI está baseada nas recomendações propostas pela Adaptação da Norma ABNT NBR ISO/IEC 27002 (código de prática para a gestão da segurança da informação) para a Segurança das Informações Arquivísticas não digitais.

2 OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação do DAG é uma declaração formal do departamento acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus funcionários, usuários e terceiros. Seu propósito é estabelecer as diretrizes a serem seguidas pelo departamento no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação não digital.

3 RESPONSABILIDADES

A Política de Segurança da Informação estabelece a responsabilidades dos funcionários, dos usuários e daqueles que realizam serviços terceirizados para com a segurança da informação no Departamento de Arquivo Geral da UFSM.

3.1 Da Direção - Em relação à segurança da informação, cabe à Direção do Departamento:

- Aprovar a Política de Segurança da Informação e suas revisões;
- Tomar as decisões administrativas referentes aos casos de descumprimento da Política e/ou de suas Normas encaminhados pelos Gestores de Segurança da Informação.

3.2 Dos Gestores de Segurança da Informação

Deve ser designado um gestor para cada divisão/setor do departamento. Assim os Gestores da Informação corresponderão aos chefes de acordo com a estrutura organizacional do mesmo:

- Direção;
- Divisão de Protocolo;
- Divisão de Apoio Técnico aos Arquivos Setoriais;
- Divisão de Arquivo Permanente;
- Laboratório de Reprografia;

Cabe aos gestores de Segurança da Informação do DAG:

- Propor ajustes, aprimoramentos e modificações desta Política;
- Propor melhorias e aprovar as Normas de Segurança da informação;
- Analisar os casos de violação desta Política e das Normas de Segurança da Informação;

- Propor projetos e iniciativas relacionados à melhoria da segurança da informação do departamento;

- Propor o planejamento de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação não digital;

- Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação;

- Conscientizar e treinar os usuários de modo a garantir a aplicação adequada dos recursos e o atendimento às normas e políticas de segurança da informação, a fim de reduzir os riscos de erro humano e;

- Divulgar as normas e procedimentos de segurança da informação adotados pelo departamento.

3.3 Dos Funcionários Tecnico-Administrativos do DAG

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação do DAG;

- Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

- Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento;

- Sempre usar o crachá de identificação;

- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pelo departamento;

- Comunicar imediatamente à Direção ou aos Gestores de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos;

- Não divulgar informações privilegiada, sob pena sofrer as punições estabelecidas pelo Departamento (Aplicação de Medida Disciplinar) e previstas em Lei.

3.4 Dos Usuários do Arquivo

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação do DAG;

- Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

- Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento;

- Não acessar ambientes institucionais sem a presença de algum responsável do departamento;

- Usar o crachá de identificação (para os funcionários da UFSM);

- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pelo departamento;

- Comunicar imediatamente à Direção ou aos Gestores de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos;

- Não divulgar informações privilegiada, sob pena de sofrer as punições estabelecidas pelo Departamento (Aplicação de Medida Disciplinar) e previstas em Lei.

3.5 Dos Serviços Terceirizados

- Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento;

- Usar o crachá de identificação da prestadora de serviço;

- Não acessar ambientes institucionais sem a presença de algum responsável do departamento;

➢ Não divulgar informações privilegiada, sob pena de sofrer as punições estabelecidas pelo Departamento (Aplicação de Medida Disciplinar) e previstas em Lei.

➢ As empresas e prestadores de serviços terceirizados obrigam-se a adicionar no contrato de prestação de serviços que a contratada está ciente da Política e das Normas de Segurança da Informação.

4 DIRETRIZES PARA A SEGURANÇA DA INFORMAÇÃO NÃO DIGITAL

4.1 Termo de compromisso

O termo de compromisso (Anexo I) é utilizado para que os funcionários, usuários e terceiros se comprometam formalmente em seguir a política de segurança, tomando ciência das punições impostas ao seu não cumprimento. No termo de compromisso podem ser reforçados os principais pontos da política de segurança, e deve ser renovado sempre que necessário.

4.2 Segurança física e do ambiente

A questão da segurança física e ambiental deve ser revista pela direção e pelos gestores de segurança da informação do DAG. Deve, também, ser revisada a questão de prevenção de incêndio, como também realizado um planejamento para compra de equipamento de segurança incluindo câmeras de monitoração, controlando as entradas e saídas das dependências do departamento. Um projeto específico compreendendo estas e outras ações para a segurança física, além de amenizar os riscos de segurança, previne a ocorrência de incidentes mais graves.

4.3 Controle de acesso físico e à informação não digital

➢ Todo acesso às informações e aos ambientes do DAG devem ser controlado, de forma a garantir acesso apenas às pessoas autorizadas pelos gestores da informação.

➢ Registrar a entrada e saída de visitante nas dependências do departamento;

- Utilização de crachá de identificação para funcionários da UFSM, crachá da prestadora de serviços para terceiros e crachá de visitante para os demais;

- Manter a porta de entrada principal do departamento fechada durante o horário de expediente, evitando o acesso não autorizado;

- Qualquer pessoa que necessitar ter acesso às salas de acervo documental deve ser acompanhada por um funcionário do departamento.

4.4 Gestão de incidentes em segurança da informação

- Relatar para a direção ou gestores da informação a ocorrência de eventos suspeitos de segurança da informação;

- Anotar todos os detalhes importantes imediatamente (por exemplo, tipo de não-conformidade ou violação, comportamento estranho, etc.);

- Não tomar nenhuma ação própria, mas informar imediatamente o evento ao ponto de contato.

- A análise de incidentes de segurança da informação pode indicar a necessidade de melhorias ou controles adicionais para limitar a frequência, danos e custos de ocorrências futuras.

Os eventos e incidentes de segurança da informação não digital no DAG podem ser:

1 - roubo ou extravio de informação;

2 - acesso não autorizado (violação de acesso);

3 - erros humanos;

4 – não conformidade com políticas ou diretrizes;

5 - violações de procedimentos de segurança física;

6 - desastres naturais que danificaram a informação (documentação arquivística);

7 - divulgação de informações sigilosas

4.5 Planos de continuidade do negócio

- Em caso de extravio de processos, proceder à reconstituição do mesmo;

- Assegurar que as atividades referentes a informação não digital no departamento sejam recuperadas antes da ocorrência de incidentes;

- O plano de continuidade do negócio deve ser testado e revisado periodicamente.

4.6 Conformidade

Esta política deve ser utilizada em conjuntos com as demais regras, normas, diretrizes, estatutos, leis e manuais institucionais.

5. MEDIDA DISCIPLINAR

O funcionário, usuário ou terceiro que infringir qualquer uma das diretrizes de segurança expostas neste instrumento receberá uma advertência por escrito e a ocorrência da transgressão imediatamente comunicada ao seu chefe imediato, ou à diretoria correspondente, se for o caso.

6 REVISÕES, VIGÊNCIA E VALIDADE

O Departamento de Arquivo Geral da UFSM se reserva ao direito de revisar, adicionar ou modificar essa Política para aprimorar e garantir o perfeito funcionamento das normas e regras por ela definidas. Assim, a presente política passa a vigorar a partir da data de sua homologação e publicação como resolução, sendo válida por tempo indeterminado.

Elaborada pela Mestranda: Josiane Ayres Sfreddo
Professor Orientador: Andre Zanki Cordenonsi

ANEXO I

TERMO DE COMPROMISSO

Identificação do Funcionário/Usuário/Terceiro

NOME:_____

RG/CPF:_____

MATRÍCULA:_____

Comprometo-me a:

1. Executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança e com as Normas e Padrões vigentes.

2. Evitar o acesso indevido aos ambientes institucionais aos quais não estarei habilitado.

3. Acessar as informações somente por necessidade de serviço e por determinação expressa do superior hierárquico.

4. Reportar imediatamente à direção ou aos gestores de segurança em caso de violação, acidental ou não, da Política de Segurança da Informação.

Declaro estar ciente das determinações acima, compreendendo que quaisquer descumprimentos dessas regras podem implicar na aplicação das sansões disciplinares cabíveis.

Santa Maria, _____ de _____ de _____.

_____.

Assinatura do Funcionário/Usuários/Terceiro