RESIGeT On-Line Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica Uni-FACEF CENTRO UNIVERSITÁRIO DE FRANCA
Vol. 06- Nr. 02 - 2015

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO EM INSTITUIÇÕES PÚBLICAS

Lorena Pires de Paula

Faculdade de Informação e Comunicação - Universidade Federal de Goiás

Douglas Farias Cordeiro

Faculdade de Informação e Comunicação - Universidade Federal de Goiás

RESUMO

A evolução tecnológica, somada aos avanços das áreas relacionadas à gestão, impele grande importância à informação, que passa a se configurar como um dos mais importantes ativos dentro de um ambiente organizacional. Neste sentido, torna-se fundamental desenvolver e implantar políticas de segurança da informação, sejam em organizações privadas ou em instituições públicas. Apesar disso, muitas organizações ainda apresentam dificuldades ou apresentam falta de conhecimento a cerca da importância da segurança da informação, fato este que se torna ainda mais atenuado em instituições públicas, devido a questões como interferência política e a cultura organizacional existente. Neste contexto, este artigo se propõe a apresentar uma análise sobre questões preponderantes da gestão da segurança da informação em instituições públicas, com referência à utilização das normas ISO 27001 e ISO 27002. Além disso, é apresentado um estudo de caso, realizado no CGA – Centro de Gestão Acadêmico da Universidade Federal de Goiás (UFG). Finalmente, é apresentada uma discussão sobre a importância da criação, implantação e manutenção de políticas e controles de segurança da informação nestas instituições.

Palavras-Chave: segurança da informação; instituições públicas; análise de risco; políticas de segurança da informação.

1. Introdução

O rápido crescimento da internet, acompanhado das tecnologias da informação, proporcionou uma evolução nas organizações, dos mais variados tamanhos, incluindo organizações comerciais, setor público, privado e sem fins lucrativos, e uma produção gigantesca de informação. Através de coleta e processamento de informação, as organizações contribuíram para o aumento da transmissão e disseminação dessas informações, tornando-as insumos importantes de valor para elas competirem estrategicamente no mercado. Neste caso, entende-se como informação, todo conteúdo valioso para um indivíduo/organização, com capacidade de armazenamento ou transferência, servindo a determinado propósito e sendo de utilidade do ser humano.

Seguindo esse raciocínio, Castells (1999) aborda a atual revolução tecnológica, cujo sua caracterização não é a centralidade de conhecimento e informação, mas a aplicação deles para geração de conhecimento, ou seja, a informação gerada auxiliando a tomada de decisão.

RESIGeT On-Line Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica Uni-FACEF CENTRO UNIVERSITÁRIO DE FRANCA
Vol. 06- Nr. 02- 2015

Diante disso, uma área do conhecimento surge com o objetivo de proteção dos ativos de uma organização contra acessos não autorizados, alterações indevidas e indisponibilidade, denominada segurança da informação. Ativos são quaisquer coisas que tenham valor para a organização (ISO 27001, 2006), por exemplo: pessoas, processos, serviços, sistemas, informação, etc. Além de a informação ser um ativo organizacional, e de ter relação com outros ativos, ela tem importância destacada na tomada de decisões e aumenta o impacto das informações divulgadas por meios não autorizados.

Neste artigo será apresentado um estudo analítico sobre segurança da informação com foco em instituições públicas, com propósito de destacar fatores chave nestes tipos de organização que demandam medidas específicas de controle de segurança da informação. A partir disso, será apresentado um estudo de caso, realizado no órgão administrativo Centro de Gestão Acadêmica, da Universidade Federal de Goiás (UFG), onde, com o objetivo de identificar os fatores críticos de sucesso do local, foram realizados levantamentos no local e, sucessivamente, uma análise de risco, com o objetivo de mensurar os riscos e verificar as reais necessidades de uma política de segurança da informação.

2. Segurança da Informação

A segurança da informação visa à proteção das ameaças para garantir a continuidade dos negócios, minimizando as perdas e maximizando o retorno de seus investimentos. Ameaças surgem quando os ativos estão vulneráveis, acarretando em um incidente indesejável. Essa área não deve ficar restrita aos aspectos tecnológicos, ela deve proteger a informação em qualquer meio que se encontre (Silva e Stein, 2007, pg.48).

De forma geral, a segurança da informação é baseada em três pilares básicos:

- **Confidencialidade**: é responsável por garantir que o acesso às informações das organizações só se darão pelas pessoas permitidas. É também, assegurar o valor da organização. Quando outras pessoas cujo não tem permissão de acessar as informações da organização tem acesso a elas, ocorre a quebra de confidencialidade.

- **Integridade**: é a garantia de que as informações das organizações estarão corretas, verídicas, não podendo ser alteradas ou excluídas. A informação que for corrompida, falsificada, roubada ou destruída acarretará na quebra de integridade.

- **Disponibilidade**: a disponibilidade de informações das organizações deve ser realizada somente às pessoas autorizadas, e devem estar disponíveis sempre que os usuários precisarem. Se um usuário necessita de uma informação da organização e ela não está disponível para o uso, ocorrerá à quebra de disponibilidade.

Todos os pilares explicitados acima devem ser cumpridos para assegurar o bom gerenciamento da segurança da informação nas organizações. Além destes, existem outros que também são de suma importância para ajudar na proteção dos ativos organizacionais. Sendo eles:

RESIGeT On-Line Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica Uni-FACEF CENTRO UNIVERSITÁRIO DE FRANCA
Vol. 06- Nr. 02- 2015

- **Autenticidade**: é a garantia de que a informação é construída por pessoas que tem permissão para isso, e cuja informação atribuída é oriunda da fonte. Por exemplo, a pessoa que se apresenta falando que é o autor de tal, deve realmente ser.

- **Responsabilidade**: todas as pessoas, sem exceção, que participam de alguma forma da produção, manuseio, transporte e descarte de informação, devem ser responsáveis por elas, ou seja, a responsabilidade é divida por todos, também pelos seus sistemas e redes de trabalho.

- **Não repúdio**: não desvio de informação ao seu destino determinado, propiciando com que o emissor ou o receptor não aleguem a não comunicação da informação.

- **Confiabilidade**: a informação deve ser confiável garantindo a origem de uma fonte autentica, tendo por principal uma mensagem verídica.

Vários fatores, como os comportamentais e do usuário, ambiente/infraestrutura, pessoas que tem a intenção de furtar, destruir ou modificar as informações, podem afetar a segurança da informação nas organizações. Isto posto, é necessário proteger essas informações, como dito anteriormente, informações que são de suma importância para as organizações, através da implementação de controles, incluindo processos, políticas, procedimentos, estrutura organizacional e funções de software e hardware adequados para cada tipo de organização da se a segurança da informação.

Esses controles necessitam ser estabelecidos, implementados, monitorados e analisados de acordo com a necessidade de cada organização. Assim sendo, a gestão da segurança da informação requer a criação de uma política de segurança da informação, devendo ser documentada, e contando com a participação de todos colaboradores da organização. A política, a qual é o instrumento mais importante para implementar a segurança, diz respeito às regras das quais devem ser elaboradas e seguidas pelos colaboradores da organização. Para a elaboração da política é necessário levar em consideração alguns fatores como: riscos e benefícios associados à falta de segurança, e o custo de implementação.

Neste contexto, o risco pode ser descrito como a possibilidade de uma ameaça ser explorada, de um evento ocorrer e de suas consequências para a organização. Algo que pode ocorrer afetando os objetivos da organização. Ele é medido pela probabilidade de um evento ocorrer e gerar perdas. Diante disso, deve-se ficar atento aos riscos, pois quando se trata deles, é necessário sempre lembrar que é a probabilidade de ocorrer algo que irá prejudicar a segurança da informação na organização e suas consequências dessa ocorrência. A partir disso, de acordo com Casada et al. (2003), o risco pode ser calculado como: **R= C** x **P,** onde **R** refere-se ao risco, **C** à consequência, e **P** à frequência. Ainda segundo estes autores:

> A frequência é estimada em dados históricos ou calculada com base na possibilidade de combinação de eventos externos, erros humanos e falhas de equipamentos e sistemas que mais contribuem para aocorrência do risco. (CASADA et al., 2003).

3. As normas ISO 27001 e 27002

RESIGeT On-Line Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica Uni-FACEF CENTRO UNIVERSITÁRIO DE FRANCA
Vol. 06- Nr. 02 - 2015

Existem diversas normas de segurança da informação, entre as quais se destacam, no âmbito da gestão de segurança da informação, as normas ISO 27001 (2006) e ISO 27002 (2013). A primeira serve de guia para implementar, operar, monitorar, analisar criticamente, manter e melhorar um sistema de gestão de segurança da informação (SGSI), lembrando que um sistema de gestão de segurança da informação deve ser implementado na organização através de uma decisão estratégica e de acordo com a necessidade dela.

Qualquer que for a organização, necessita identificar e gerenciar suas atividades, para que seu funcionamento seja efetivo. Qualquer atividade que utiliza de recursos e os gerencia para habilitar as entradas e saídas, pode ser chamada de processo. Os processos funcionam como um ciclo, onde suas saídas realimentam outras entradas e assim por diante. A aplicabilidade de um sistema de processos em uma organização, junto com a identificação e interações desses processos e seu modelo gestão, podem ser considerados como "abordagem de processo", (ISO 27001, 2006, pg. 5).

Esta norma adota como modelo o *Plan-Do-Check-Act* (PDCA), utilizado para estruturar os processos do sistema de gestão de segurança da informação. Ela pode ser usada em qualquer tipo de organização como as citadas na seção anterior. A norma traz especificado os requisitos para fazer todo o processo de implementação do SGSI analisando todo o contexto de risco e de negócio da organização.

A segunda norma citada, a ISO 27002 (2013), foi elaborada com base na norma anterior. Neste sentido, esta norma foi delineada com o objetivo de servir como referência na seleção de controles de segurança durante o processo de implementação de um sistema de gestão de segurança da informação (SGSI), realizadas pelas organizações de todo tipo e tamanho (pública, privada, comerciais e sem fins lucrativos). Também tem por finalidade, ajudar no desenvolvimento de organizações e indústrias específicas de gerenciamento de segurança, alertando que é de suma importância levar em consideração os ambientes de riscos de segurança específicos. Além disso, é projetada para fazer a seleção de controles dentro de um processo de implementação de um SGSI baseado na ISO 27001 (2006), a fim de permitir a implementação desses controles selecionados e desenvolver seus próprios princípios de gestão de segurança da informação.

A norma contém quatorze seções de controles de segurança da informação, trinta e cinco objetivos de controles e cento e quatorze controles, sendo que cada seção de controle aborda um ou mais objetivos de controle declarando o que se espera, um ou mais controles que podem ser aplicados para o alcance do objetivo. Eles não se apresentam em ordem de prioridade, pois cada organização irá utilizar dos controles que são aplicáveis a ela, pela necessidade e importância para os seus processos individuais de negócio.

As definições dos controles apresentam estruturadas na norma da seguinte forma: controle - irá definir a forma para se atingir o objetivo do controle; diretrizes de implementação - nelas estão informações mais detalhadas que permitem apoiar a implementação do controle e o alcance do objetivo do controle, essas diretrizes podem não ser tão completas para atender os requisitos de controle específicos da organização; e finalmente, as informações adicionais - abrangem algumas questões legais e referências normativas.

As seções de controles citados acima são:

- **Política de segurança da informação**: esta seção de controle mostra a importância da definição de um conjunto de políticas e segurança da

RESIGeT On-Line Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica Uni-FACEF CENTRO UNIVERSITÁRIO DE FRANCA
Vol. 06- Nr. 02 - 2015

informação em uma organização, de sua aprovação pela direção, e sua necessidade de publicação e apresentação para todos os funcionários e as partes externas que são relevantes para a organização.

- **Organização da segurança da informação**: nesta seção é abordada a definição e atribuição das responsabilidades de segurança da informação.
- **Segurança em recursos humanos**: visa a garantia de que todos os funcionários e partes externas entendam suas responsabilidades e estejam em conformidade com as funções para as quais foram selecionados.
- **Gestão de ativos**: tem por objetivo identificar os ativos da organização e fazer a definição das responsabilidades de cada funcionário para a proteção deles.
- **Controle de acesso**: instiga a organização a limitar o acesso a informações e aos seus recursos de processamento.
- **Criptografia**: assegura o uso adequado de criptografia em prol da proteção da confidencialidade, integridade da informação.
- **Segurança física e do ambiente**: foco na prevenção de acesso físico não autorizado, danos e interferência com os recursos de processamento das informações e as informações da organização.
- **Segurança nas operações**: confirma que a operação dos recursos de processamento de informação esteja segura e correta.
- **Segurança nas comunicações**: visa garantir a proteção das informações em redes e dos recursos de processamento que os apoiam.
- **Aquisição, desenvolvimento e manutenção de sistemas**: tem como objetivo a garantia de que a segurança da informação integre todos os ciclos de vida dos sistemas de informação. Incluindo também os requisitos para os sistemas de informação que fornecem serviços sobre as redes públicas.
- **Relacionamento na cadeia de suprimento**: visa garantir a proteção dos ativos cujo, os fornecedores têm acesso.
- **Gestão de incidentes e de segurança da informação**: assegura o gerenciamento dos incidentes de segurança da informação incluindo a comunicação sobre fragilidades e eventos de segurança da informação.
- **Aspectos da segurança da informação na gestão da continuidade do negócio**: recomenda-se que seja considerada no sistema de gestão da continuidade do negocio a continuidade da segurança da informação.
- **Conformidade**: conscientiza a organização a evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais que estão relacionadas à segurança da informação e dos requisitos.

A ISO 27002 (2013) é de suma importância para uma organização que busca implementar uma política de segurança da informação, pois ela orienta na elaboração da política, que por sua vez, deve orientar na criação de normas especificas e procedimentos, para o tratamento seguro das informações e dos outros ativos organizacionais. Ela sugere as seções de controles citados à cima com a intenção de ajudar e facilitar na proteção dos ativos informacionais da organização.

4. Cultura Organizacional

Para entender melhor o fenômeno organizacional é preciso compreender o que compõe ele, como por exemplo: as pessoas, que além da informação, também, possibilitam a vantagens competitivas nas organizações. As organizações, como dito,

RESIGeT On-Line Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica Uni-FACEF CENTRO UNIVERSITÁRIO DE FRANCA
Vol. 06- Nr. 02- 2015

estão inseridas em um ambiente de constante interação, onde influenciam e são influenciadas, e, neste cenário, as pessoas ou colaboradores que atuam nelas, são responsáveis para que esse intercâmbio ocorra, e seus valores são objetos para que a cultura da organização se construa.

Adentrando no contexto da cultura organizacional, Mintzberg et al. (2000) descrevem-na como a base da organização, onde as crenças comuns refletem nas tradições e nos hábitos, manifestando-se de forma mais tangível. Os autores afirmam que a força da cultura organizacional está no ato de tornar verdadeiro as crenças e valores compartilhados pelos colaboradores da organização, ou seja, não existe cultura organizacional sem a existência de pessoas.

A cultura organizacional é uma ideia essencial à construção das estruturas de uma organização, onde cada organização tem a sua, cujas características se diferenciam das outras. As organizações expressam sua cultura através de hábitos, crenças, rituais comuns aos membros produzindo normas de comportamentos aceitos por todos.

Os conceitos apresentados aplicam-se não somente no contexto das instituições privadas, como também no âmbito das públicas. Nesse sentido, as instituições públicas mostram um cenário onde há necessidade do novo, quanto em aspectos administrativos quanto em políticos.

Para compreender melhor sobre instituições públicas, Dussault (1992) argumenta como elas funcionam:

> "As organizações de serviços públicos dependem em maior grau do que as demais ao ambiente sociopolítico: seu quadro de funcionamento é regulado externamente a organização. As organizações públicas podem ter autonomia na direção dos seus negócios, mas, inicialmente seu mandato vem do governo, seus objetivos são afixados por uma autoridade externa."

Pode-se perceber que as organizações de serviços públicos apresentam um grau de vulnerabilidade maior à interferência do poder político do que outros tipos de instituições, devido a seu gerenciamento ser realizado pelo próprio poder público. A missão fundamental destas instituições é prestar serviços à sociedade, a qual espera qualidade e com rapidez. Apesar disso, é comum que haja contradição entre os resultados necessários em relação aos recursos recebidos, ou por outro lado, quando há essa disponibilidade de recursos, elas acabam caindo na dependência da decisão política e da capacidade do estado.

Alguns serviços públicos são oferecidos pelas instituições com baixa qualidade, e isto gera uma baixa expectativa também em relação ao que pode ser ofertado tanto pelos usuários quanto pelos colaboradores, onde eles se tornam insatisfeitos e frustrados com o serviço. Diante disso, nota-se, o quanto instituições públicas são sistemas complexos, por apresentar em seu funcionamento um alto índice de burocracia, centralizadora contraria a mudanças.

Carbone (2000) cita seis características das organizações públicas cujas são responsáveis pela dificuldade de mudanças, organizadas respectivamente:

- **Burocratismo**: controla excessivamente os procedimentos, onde a administração acha-se engessada, complicada e desfocada das reais necessidades do país.

RESIGeT On-Line Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica Uni-FACEF CENTRO UNIVERSITÁRIO DE FRANCA
Vol. 06- Nr. 02 - 2015

- **Autoritarismo/Centralização**: marcada pela centralização no processo de tomada de decisão, e estrutura hierárquica excessivamente verticalizada.
- **Aversão aos empreendedores**: não existe comportamento empreendedor, para modificação e oposição ao modelo de produção vigente.
- **Paternalismo**: autoridade da movimentação de pessoal e da distribuição de empregos, cargos e comissões, dentro da lógica dos interesses políticos dominantes.
- **Levar vantagem**: indivíduos injustos recebem constante promoção de punições com o objetivo de obter vantagens dos negócios do estado.
- **Reformismo**: desinteresse por avanços conquistados, desencadeamento administrativo, desparecimento de tecnologia e desconfiança generalizada.

Essas características representativas à instituições públicas acabam por se tornar um grande empecilho para implantação de inovações tecnológicas, uma vez que, em geral, os processos são longos, requerendo tempo para desenvolvimento e aperfeiçoamento, e dificilmente esses projetos restringem a um único mandato governamental, o que acaba gerando um conflito por essa substituição de trabalhadores.

5. A Cultura Organizacional de Instituições Públicas e a Segurança da informação

A cultura organizacional tem sua formação dentro de uma organização, seja ela de qualquer tipo ou tamanho, provinda de pessoas, ou de colaboradores que nela atuam. A forma com que as pessoas agem, pensam, sentem, transmitem seus pensamentos, caracteriza a cultura de cada organização, e determina como será realizada a administração dela. E isso faz com que as organizações recebam o tempo todo, uma forte influência dessa cultura, que se diferencia das outras organizações pelos colaboradores de cada uma.

No contexto instituições púbicas, pode-se notar, como já dito anteriormente, a existência da necessidade do novo, não só em aspectos administrativos, mas também em políticos. Apesar disso, a insatisfação de alguns colaboradores que atuam nessas organizações acaba por gerar um serviço de má qualidade, devido à interferência do poder político, o qual possui grande influência, agindo principalmente na tomada de decisão, e consequentemente provocando lentidão nos serviços. Isso caracteriza a cultura de uma organização que não aceita mudanças, cuja atuação ocorre de forma desfocada na real necessidade do país e onde os serviços realizados estão voltados somente a interesses políticos.

Embora a segurança da informação, caracterizada pela proteção dos ativos informacionais, possa existir dentro dessas organizações, a cultura organizacional acaba por interferir na gestão e nos resultados obtidos, gerando um cenário desfavorável à continuidade de negócios. Neste contexto, informações importantes que acabam sendo omitidas ou falsificadas, em alguns casos pelo próprio poder político, tornam a organização pública vulnerável a diversos tipos de ameaças, tais como vazamento de informações valiosas, indisponibilidade de acesso a informações importantes, e outras, fatores estes que podem ser observados na análise apresentada na próxima seção.

RESIGeT On-Line Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica Uni-FACEF CENTRO UNIVERSITÁRIO DE FRANCA
Vol. 06- Nr. 02 - 2015

Durante o processo de implementação da segurança da informação, o qual inclui processos, políticas, procedimentos, estrutura organizacional, e gestão de controles, que necessitam ser estabelecidos, monitorados e analisados de acordo com os requisitos de segurança de cada instituição, há necessidade de conscientização de todos colaboradores e da alta administração em vários pontos como:

- **Acesso, transmissão e armazenamento de informações**: é importante que as informações da organização sejam acessadas, transmitidas e armazenadas, somente por colaboradores que tenham permissão para isso. E na hora certa.
- **Uso dos recursos computacionais**: somente pessoas permitidas podem ter acesso a determinados recursos computacionais disponíveis na organização.
- **Proteção e sigilo de informações e processos críticos**: informações valoradas da organização devem ser protegidas.

Essa conscientização deve acontecer para que a gestão da organização flua de forma mais tranquila, e alcance a segurança da informação, pois caso aconteça algum problema, os colaboradores responsáveis saberão detectar de onde vem o erro, o que devem fazer, e quem procurar.

O estabelecimento de controles de segurança está atado às legislações e normas que regulamentam uma instituição pública, por isso para implementar esses controles é necessária a criação de uma política de segurança da informação que será documentada e contará com a participação dos colaboradores da instituição.

6. Estudo de caso: a segurança da informação no CGA-UFG

Com o propósito de validar as informações descritas anteriormente, a cerca da relação segurança da informação e instituições públicas, foi realizado um estudo de caso no Centro de Gestão Acadêmico (CGA) da Universidade Federal de Goiás (UFG). Neste estudo, concretizou-se a realização de levantamento de dados e de uma análise de risco, verificando quais são as ameaças aos ativos informacionais do órgão, e medindo o risco dessas ameaças acontecerem, com intuito de verificar a real situação da segurança da informação no local.

O Centro de Gestão Acadêmica (CGA) está vinculado à Pró-Reitoria de Graduação (PROGRAD), e tem por objetivo: gerenciar os dados acadêmicos dos discentes de graduação; coordenar o processo de preenchimento das vagas disponíveis dos cursos de graduação de acordo com as normas e procedimentos legais; atender as atribuições normativas sobre expedição e registro de diplomas dos cursos de graduação e pós-graduação; e, assessorar a PROGRAD acompanhando as atividades desenvolvidas, objetivando contribuir para o funcionamento eficiente e eficaz da política de graduação.

Para realizar uma análise de risco em uma organização, é necessário antes, identificar os recursos críticos, também chamados de fatores críticos de sucessos, do órgão escolhido. Silveira (2003) define fatores críticos de sucessos, como algo que diz respeito ao negócio da organização, ou o ramo de atividade em que ela atua. Também podem ser atribuídos de forma geral aos vários componentes da organização, enquanto outros são específicos de cada unidade. Diante disso, com intuito de identificar os fatores críticos relevantes ao funcionamento do serviço prestado pelo CGA-UFG, foi realizada uma entrevista local com pessoal alocado ao setor de direção, tendo contato com todas as coordenadorias existentes, e os processos envolvidos para realização do

RESIGeT On-Line Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica Uni-FACEF CENTRO UNIVERSITÁRIO DE FRANCA
Vol. 06- Nr. 02 - 2015

serviço. A partir disso, foram destacados os seguintes ativos e seus respectivos fatores críticos de sucesso:

- **Hardware:**
  - **Servidor de dados** - é acessado somente por duas coordenadorias (CRD) Registros de diplomas e (CERD) Expedição de Registros de Diplomas UFG, nele são guardados documentos e planilhas para a confecção do senso, também está presente documentos em relação às IES não universitárias.
  - **Conjunto de CPU** – utilizados para prestação de serviços, tais como: emissão de documentos solicitados, consulta de processo, protocolar requerimentos, dentre outros. Sendo ele o único meio utilizado pelo órgão.
  - **Impressoras** – são utilizadas na impressão de todos os documentos importantes solicitados pelos clientes.
- **Software:**
  - **Sistema Acadêmico** - é a interface que os servidores usam para realizar grande parte do serviço prestado pelo Centro.
- **Dados:**
  - **Banco de Dados** - o papel do banco de dados é armazenar todas as informações em relação à vida acadêmica dos estudantes da Universidade Federal de Goiás. Pessoas - memória organizacional. Nas organizações o *Know How* das pessoas é de extrema importância, pois problemas complexos podem ser resolvidos facilmente por aquelas pessoas que atuam no CGA há mais tempo, por possuírem experiências maiores.
- **Documentação:**
  - **Processos** - são requerimentos protocolados por estudantes ou não, de acordo com a legislação específica em vigor.
  - **Dossiês** - é a documentação (certificado de conclusão do ensino médio, histórico do ensino médio e outros) armazenada dos ingressantes na Universidade Federal de Goiás.

Todos os recursos críticos identificados pela entrevista realizada no CGA-UFG foram considerados de extrema importância para que o serviço prestado seja alcançado de forma eficiente.

A partir disso, a fim de realizar uma análise de segurança da informação no CGA-UFG, o cenário analisado teve como base os últimos dois anos de serviços prestados, sendo investigadas situações que ocorreram nesse período definido para a análise, com o objetivo de identificar os fatores que são ameaças para o local. São fatos que ocorreram e cujo se deve chamar a devida atenção, pois a ocorrência deles pode prejudicar o funcionamento dos serviços oferecidos. Diante disso, a investigação resultou nas seguintes ameaças: erros humanos, instalação de software não autorizado, bugs no sistema acadêmico, desastres naturais, desastres causados por pessoas, falhas em equipamentos, uso de senhas, frágeis, falhas de fornecimento de energia elétrica e falhas no serviço de *backup*.

RESIGeT On-Line Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica Uni-FACEF CENTRO UNIVERSITÁRIO DE FRANCA
Vol. 06- Nr. 02 - 2015

As ameaças identificadas foram utilizadas consequentemente para realizar a análise de risco, que é um processo que visa identificar e avaliar de forma sistemática, metodológica e repetível os riscos de segurança a que os recursos críticos se encontram sujeitos, possibilitando a definição dos meios através dos quais estes podem ser protegidos. Definiram-se os seguintes critérios para fazer a avaliação de risco: impacto, probabilidade e prevenção das ameaças, devido ao fato de serem pontos cruciais da política de segurança da informação de uma organização. Onde:

- **Impacto (i) -** é a gravidade que a ameaça gera nos serviços prestados pelo CGA:
  - 0 - irrelevante (Não causa nenhum dano relevante nos serviços);
  - 1 - baixo (afeta, mas não prejudica as funcionalidades dos serviços);
  - 2 - médio (afeta parcialmente os serviços);
  - 3 - alto (Afeta gravemente os serviços).

- **Probabilidade (p) - é** a probabilidade das ameaças ocorrerem no Centro de Gestão Acadêmica.
  - Varia de 0 a 1.
- **Prevenção (prev) -** são os artifícios existentes para prevenir que o evento ocorra e cause danos:
  - 1 - alta (possui métodos para prevenir que o evento ocorra);
  - 2 - médio (previne parcialmente);
  - 3 - baixo (não possui métodos para prevenir).
- **Risco (r) -** fórmula para calcular o risco:
  - **r = (2i + prev) * p**.

Atribuiu-se um peso maior ao impacto, devido a sua importância, adiciona-se a ele a prevenção, que caracteriza um aspecto negativo, definido por: quanto maior for o índice menor é o grau de prevenção da organização. Multiplica-se pela probabilidade que varia 0 a 1. Baseando nessa formula, pode-se identificar o risco. Neste sentido, pode-se mensurar a variação do risco como:

- 1 - 0.0 a 2.2 (baixo) - representa baixo risco da ameaça acontecer no CGA;
- 2 - 2.3 a 4.5 (médio) – acontece, mas uma vez ou outra;
- 3 - 4.6 a 6.8 (moderado) – acontece algumas vezes sem muita frequência;
- 4 - 6.9 a 9.0 (risco altíssimo) – acontece com frequência.

A partir da metodologia apresentada, os resultados são apresentados na Tabela 1. Com base nos serviços prestados pelo CGA-UFG, pode-se concluir que não existem efetivamente ameaças com alto grau de risco, porém as ameaças existentes, entre as quais estão: instalação de software não autorizado, *bugs* do sistema acadêmico, falhas no fornecimento de serviços de rede com, entre outras, podem ser consideradas ameaças que demandam cuidados ou precauções específicas, pois elas podem afetar o serviço oferecido pelo órgão. A utilização das diretrizes apresentadas nas normas ISO 27001 e 27002 para selecionar e implementar os controles adequados, com referência às questões inerentes à cultura organizacional das instituições públicas, podem ser consideradas alternativas interessantes para solução deste problema.

Ameaças	Impacto	Probabilidade	Prevenção	Risco

RESIGeT On-Line Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica Uni-FACEF CENTRO UNIVERSITÁRIO DE FRANCA
Vol. 06- Nr. 02- 2015

Erros Humanos	1	0,2	2	0,8
Instalação de software não autorizado	1	0,8	2	3,2
Bugs no sistema acadêmico	2	0,3	3	2,1
Desastres naturais	3	0,05	3	0,45
Desastres causados por pessoas	2	0,1	3	0,7
Falhas em equipamentos	2	0,2	2	1,2
Uso de senhas frágeis	1	0,1	1	0,3
Falhas de fornecimento de energia elétrica	3	0,15	3	1,35
Falhas no fornecimento de serviços de rede	3	0,2	2	1,6
Falhas no serviço de backup	2	0,05	1	0,25

Tabela 1 – Estudo de segurança da informação no CGA-UFG.

8. Conclusão

Neste trabalho foi apresentado um estudo analítico sobre segurança da informação, que tem como foco a proteção de ativos informacionais de uma organização, com cerne em instituições públicas, abordando sua cultura organizacional, que é um fator crucial para implementação de uma política de segurança da informação. O estudo de caso realizado no CGA-UFG identificou ativos que precisam ser protegidos, com seus respectivos fatores críticos de sucessos. Realizou-se uma análise de risco, para identificação dos riscos mais altos, com objetivo de tratá-los e preveni-los das ameaças encontradas, mostrando que a segurança da informação é um fator crítico e deve ser levado em conta na gestão de projetos e no plano estratégico de uma organização, também como uma forma de obtenção na qualidade dos negócios.

REFERENCIAS

CASTELLS, M. **Sociedade em rede: a era da informação. Economia, sociedade e cultura**. São Paulo: Paz e Terra, 1999.
ISO 27001. **ABNT NBR ISO/IEC 27001**. Rio de Janeiro, 2006.
ISO 27002. **ABNT NBR ISO/IEC 27002**. Rio de Janeiro, 2013.
SILVA, D. R. P.; STEIN, L.M. Segurança da Informação: uma reflexão sobre o componente humano. **Ciências & Cognição.** V.10, pg.46-53, mar. 2007.
CASADA, Myron; Thomas Nolan; David Trinker; and David Walker.**Guide for Port Security**. Houston: ABS Consulting, October, 2003.
MINTZBERG, H. et al. **Sáfari de estratégia: um roteiro pela selva do planejamento estratégico**. Porto Alegre: Bookman, 2000.
DUSSAULT, G. A gestão dos serviços públicos de saúde: características e exigências. **Revista de Administração pública**, Rio de Janeiro, v. 26, n. 2, p.8-19, abr./jun. 1992.
CARBONE, P. P. Cultura organizacional no setor público brasileiro: desenvolvendo uma metodologia de gerenciamento de cultura. **Revista de Administração Pública**, v. 34, n. 2, p. 133-144, mar./abr. 2000.

RESIGeT On-Line Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica
Uni-FACEF CENTRO UNIVERSITÁRIO DE FRANCA
Vol. 06- Nr. 02 - 2015

SILVEIRA, Henrique. F. R. **Motivações e fatores críticos de sucesso para o planejamento de sistemas interorganizacionais na sociedade da informação.** Tese Doutorado em Ciências da Informação, Brasília, 2003.