# Governança de Tecnologia e Segurança de Informação em Instituição Pública de Ensino Superior Brasileira

**Luci Longo**
Professora Doutora - Universidade Estadual do Centro Oeste do PR (Brasil)

**Iago França Lopes**
Professor Doutor - Universidade Federal do Paraná (UFPR)

**Resumo**
Na última década os avanços da tecnologia de informação (TI), sistemas avançados e integrados ao ambiente virtual são alguns exemplos que vem requerendo das organizações uma série de ações para tratar de segurança das informações, que se conectam ao tema sustentabilidade e desempenho das atividades, independentemente do ramo. O objetivo deste trabalho consistiu em analisar os aspectos principais da Governança voltada à segurança da Tecnologia de Informação (TI) de uma Universidade Estadual do Centro-Oeste do Paraná, Brasil e apresentar indicadores para auxiliar nos processos operacionais e planejamento preventivo das fraudes e ameaças eletrônicas. Adotou-se uma abordagem qualitativa-descritiva em pesquisa *in-loco*, com instrumento de coleta estruturado e foram realizadas entrevistas com os técnicos e supervisores do Centro de Tecnologia de Informação da Instituição. Destaca-se como contribuição científica do artigo uma metodologia de análise dos desafios abordados, contendo adaptações para Instituições de Ensino Superior de modelos utilizados com sucesso em organizações em seus programas de governança da TI, que possibilita monitorar os problemas de segurança aos *Data Centers*. A gestão da instituição pode usufruir do levantamento das prioridades da segurança e indicadores apresentados, também para investimentos e processos evolutivos visando mitigar os riscos à informação da Universidade.

**Palavras-chave:** Tecnologia de Informação; Infraestrutura de Dados; Segurança da Informação; Controladoria.

## *Gobernanza de la Tecnología y la Seguridad de la Información en una Institución Pública de Educación Superior Brasileña*

*En la última década, los avances en tecnología de la información (TI), sistemas avanzados e integrados en el entorno virtual son algunos ejemplos de que las organizaciones ven una serie de acciones para hacer frente a la seguridad de la información, que están conectadas con el tema de la sostenibilidad y el desempeño de las actividades, independientemente de la sucursal. El objetivo de esta planificación consiste en los principales aspectos de la Gobernanza de los Indicadores del Sistema de Seguridad de la Información de la Universidad Estatal del Medio Oeste de Paraná, Brasil y*

*presentar para la planificación para ayudar en los procesos operativos y preventivos de fraude y amenazas electrónicas. . Se adoptó una metodología cualitativa de instrucción-investigación-creación-investigación y un enfoque cualitativo-construcción-investigación con el Centro de Investigación de Investigación Técnica y supervisores de investigación con el Centro de Tecnología de Instrucción de Construcción y Desarrollo de Supervisores de Tecnología de Investigación y Supervisores. Como aporte se destaca una metodología de análisis de artículos de instituciones, sus programas exitosos, que contiene conocimientos para los modelos utilizados con organizaciones en ciencia de los problemas de seguridad del Centro TI. La dirección de la institución podrá procurar relevar las medidas de seguridad y medidas adoptadas para mitigar los riesgos a la información de la Universidad.*

***Palabras-clave:*** *Tecnologías de la información; Infraestructura de datos; Seguridad de la Información; Contraloría.*

## *Governance of Technology and Information Security in a Brazilian Public Institution of Higher Education*

*In the last decade, advances in information technology (IT), advanced systems and integrated into the virtual environment are some examples that organizations see a series of actions to deal with information security, which are connected to the theme of sustainability and performance of activities, regardless of of the branch. The objective of this planning consists of the main aspects of the Governance of the Indicators of the Information Security System of the State University of the Midwest of Paraná, Brazil and to present for planning to assist in the operational and preventive processes of fraud and electronic threats. A qualitative-instruction-research-creation-research methodology and a qualitative-construction-research approach were adopted with the Technical Research Research Center and research supervisors with the Construction Instruction Technology Center and Research Technology Supervisors Development and Supervisors. A scientific contribution of the article stands out as a methodology for analyzing the challenges addressed, containing adaptations for Higher Education Institutions of models successfully used in organizations in their IT governance programs, which makes it possible to monitor security problems in Data Centers. The institution's management can take advantage of the survey of security priorities and indicators presented, also for investments and evolutionary processes aimed at mitigating the risks to the University's information.*

***Keywords:*** *Information Technology; Data Infrastructure; Information Security; Controllership.*

## 1 INTRODUÇÃO

A governança da tecnologia de informação (TI), entre outros aspectos, possibilita que a TI atenda aos propósitos da organização, inclusive quanto aos aspectos de segurança e blindagem das informações, muito além da gestão de sistemas integrados.

Os SI desempenham um papel crítico, são geradores de informação, por isso as organizações devem tomar providências especiais para protegê-los e garantir que sejam valiosos, confiáveis e seguros (Laudon & Laudon, 2015; Silva, Silveira, Dornelas & Ferreira, 2020).

Atualmente as organizações buscam aprimorar e atualizar os procedimentos de segurança (Espinel-Ortega & Carreno-Perez, 2020). A controladoria desde as primeiras definições do papel da governança (Weill & Ross, 2004; Peterson, 2004) integra em geral o comitê de governança de tecnologia de informação, conforme convenções e recomendações para as entidades, em especial de organizações certificadoras. E, como meta, espera-se o alinhamento tanto da controladoria, quanto dos setores ligados ao desenvolvimento dos negócios em relação às decisões de investimentos em TI (Henderson & Venkatraman, 1993; Chan & Reich, 2007; Löbler, Bobsin & Visentini, 2008), que se resume no alinhamento estratégico entre o Plano Estratégico de Tecnologia de Informação (PETI) e o Plano Estratégico de Negócio (PEN). Neste plano estratégico é comum enfocar a redução de riscos, incluindo um tratamento adequado aos impactos causados pelas falhas de segurança, assim como promovendo ações preventivas para redução dos riscos para a informação.

Voltado ao processo de melhoria da segurança, o trabalho de Solana-González, Vanti e Fontana (2019) destaca que a segurança da informação é um tema atual de proteção de ativos de informação que é considerada importante variável de natureza estratégica, organizacional e informática, que exige análise de conformidade com as normas internacionais que regulam as ações comerciais, com práticas e metodologia analítica. Neste sentido, cada instituição desenvolve suas regras de conduta que devem estar asseguradas por suas políticas de segurança da informação e comunicação (Rios *et al*. (2017). Entretanto, no último Levantamento de Governança de TI em 2014, elaborado pelo Tribunal de Contas da União, foi divulgado que apenas 51% dos órgãos da Administração Pública Federal adotaram integralmente a política de segurança da informação e comunicação.

Levando em consideração, que em um passado recente a armazenagem da informação e dos dados de uma entidade, ocorria na forma física, sendo necessário um ambiente protegido para os registros feitos em papéis, pastas e arquivos. Com o avanço da tecnologia, os sistemas de informação armazenam os dados e informações digitalmente, que podem ser acessados facilmente por meio de computadores, ou remotamente, por pessoas no ambiente interno, por clientes e outros grupos externos ao ambiente da entidade. Os ataques aos dados das entidades é sempre um risco que pode ocorrer. Nesse sentido, as organizações têm tido preocupação com a segurança das informações que possam comprometer as atividades da organização (Sêmola, 2014; Solana-González *et al*., 2019).

Destarte, a coordenação do setor da TI tem atribuição de promover a segurança da informação, a começar pela infraestrutura e seguranças do banco de dados. Surgindo a motivação de desenvolver uma análise da infraestrutura para salvaguarda do ambiente digital e dos dados, tão importante para a sustentabilidade das entidades, tendo como questões e norteadores da pesquisa: Quais os instrumentos e indicadores de segurança da tecnologia de informação (STI) gerados pelo setor de Tecnologia da Universidade

Estadual do Centro-Oeste do Paraná? Quais os procedimentos atualizados para mitigar os riscos relacionados à STI?

O objetivo desta pesquisa, portanto, consiste em analisar os aspectos principais sobre Segurança da Tecnologia de Informação (STI) da Universidade Estadual do Centro-Oeste do Paraná e apresentar indicadores que podem auxiliar no planejamento e detecção de ameaças/riscos relacionados à segurança da TI da Instituição.

## 2 REVISÃO DA LITERATURA

### 2.1 Segurança da Informação e o Papel da Governança de TI

A Governança de TI torna-se necessária, sincronicamente com a segurança dos dados (Espinel-Ortega & Carreno-Perez, 2020; Weill & Ross, 2004; Chan & Reich, 2007; Henderson & Venkatraman, 1993). A segurança da informação consiste na proteção dos dados e informações contidas nos sistemas contra aos acessos, modificações, leituras, divulgações e inspeções não autorizadas. Logo, quanto maior o uso de dados dentro de uma entidade, quanto maior a visibilidade da entidade seus ambientes informatizados podem sofrer algum tipo de ataque, principalmente com o grande aumento no uso de comercio eletrônico e das redes sociais.

De acordo com a variedade de tecnologias relacionadas, faz-se necessário evoluir os procedimentos internos de segurança de dados, de maneira que protejam a infraestrutura dos softwares da entidade, sendo por meio de testes de segurança, gestão de risco, planejamento, auditorias e outras técnicas de segurança digital, portanto para essa proteção ocorrer deve-se exercer a governança de TI, que consiste em uma gama de habilidades, competências e diretrizes compartilhadas e utilizadas dentro das entidades, podendo ser pelos gestores, técnicos e usuários dos sistemas de TI, ou até conjuntos externos que realizem essa prática.

Analisado alguns trabalhos sobre governança de TI, em diferentes épocas, apresentam resultados que comprovam a sua importância e impactos para o valor e desempenho da organização (Peterson, 2004; Weill & Ross, 2004; Lunardi, Becker, Maçada & Dolci, 2014; Silva *et al*., 2020).

A governança de TI pode ser exercida e observada de inúmeras formas nas organizações, a forma mais evidente é a composição de "comitês" para elaborar a diretrizes e política em relação às decisões de TI e segurança das informações (tema foco desta pesquisa). A GTI consiste na integração dos esforços da TI juntamente com as atividades praticadas, cuja finalidade é determinar as estruturas organizacionais adequadas no que se diz respeito à gestão de pessoas, estruturas e processos, a fim de agregar valor aos negócios.

A segurança da informação pode ser impactada pelo modelo de Governança e arquitetura de TI (Silva & Moraes, 2011) explicam que compõem um modelo de governança, toda infraestrutura, processos, relacionamentos, mecanismos estabelecidos e decisões críticas para a TI. Esta infraestrutura depende de decisões dos responsáveis pela TI, ou por comitês. Os processos envolvem as decisões, as estratégias e o acompanhamento dos resultados. Nos mecanismos de relacionamento, estão incluídas as parcerias entre TI e demais áreas, o aprendizado compartilhado, comunicação e diálogo estratégico.

Compreendendo como pode ser distribuída as responsabilidades na organização, quanto ao papel e uso da TI e o modelo de Governança de TI. Peterson (2004) observa que há três modos de GTI dominantes nas organizações: centralizado, descentralizado e

federal, em que se determina o grau de centralização e organização das decisões no tocante à TI e para as atividades da organização.

Enfim, a governança de TI é um programa amplo de análise de processo, etapas de implementação, acompanhamento de medidas e melhores práticas da gestão da tecnologia de informação. O programa mais conhecido é do ISACA- *Information Systems Audit and Control Association*, com o COBIT. O modelo COBIT, foi associado a este trabalho, na fase de estruturação do instrumento de coleta junto à universidade foco da pesquisa.

O COBIT ajuda a preencher as lacunas entre os riscos do negócio, as necessidades de controle e as questões técnicas. Ele fornece boas práticas em uma estrutura de domínio e processo e apresenta as atividades em uma estrutura gerenciável e lógica. Incorpora os principais padrões internacionais, tornou-se um padrão para o controle geral de TI e segurança dos dados (ISACA, 2020).

A principal motivação para uso do guia de gestão para segurança de informação do COBIT, é devido o mesmo possuir padrões dos processos chaves que podem ser utilizados para vários tipos de organização como é o caso das IES, por meio deste modelo pode-se identificar o nível de maturidade por meio de notas e acompanhamento da evolução das rotinas e processo para ponto de maturidade global da organização, incluído o tratamento e segurança da informação. Este modelo abrange do estratégico ao operacional.

## 2.2 Segurança da Informação

A Segurança da Informação já era tratada pela literatura (Morris & Thompson, 1979; Brostoff, 2004; Whitman & Mattord, 2012; Adress, 2014) como uma proteção contra o uso ou acesso não autorizado à informação, também proteção para garantir que os usuários autorizados utilizem seus serviços, mantendo a integridade e confidencialidade dessas informações.

A informação pode existir em diversas formas, impressa em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada, seja qual for a forma, é recomendado que ela seja sempre protegida adequadamente (ABNT NBR ISO/IEC 27002, 2013).

Ainda segundo ABNT NBR ISO/IEC 27002 (2013) segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio. É obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

A segurança de Informação não se restringe aos sistemas de informação, ou à informação digital por exemplo. Se aplica a todos os aspectos de proteção da informação ou dados. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer.

Conforme descrevem Salovaara, Kalle e Esko (2019) as organizações enfrentam altos riscos no universo digital e devem mitigá-los por meio de um conjunto técnico-sistêmico. Em geral almeja-se um grau de segurança ideal em que uma organização e seus ativos estejam totalmente protegidos. Mas na realidade, a segurança da informação é um processo contínuo.

Dentro desses limites de objetivos e recursos organizacionais, os riscos aos ativos de informações da organização devem ser mitigados a um nível aceitável para a administração e suas partes interessadas. O termo segurança da informação pressupõe

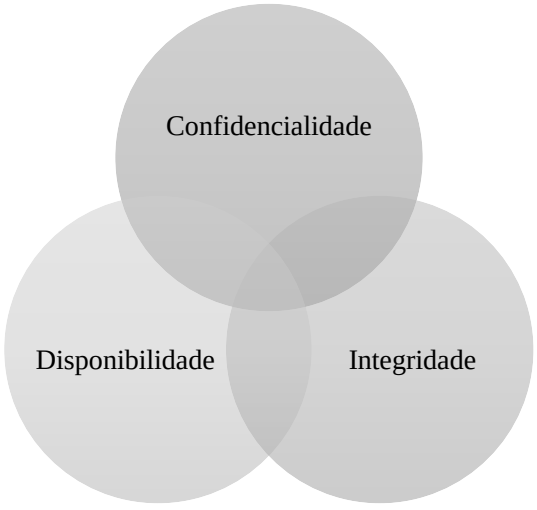
este ato de equilíbrio como a proteção da informação e seus elementos críticos, incluindo os sistemas e hardware que usam, armazenam e transmitem essas informações, por meio da aplicação de políticas, programas de treinamento e conscientização e tecnologia para equilibrar da melhor forma possível, a necessidade de proteger e de obter acesso aos ativos da organização (Whitman & Mattord, 2012).

Há várias formas da segurança de uma determinada informação ser afetada, por fatores comportamentais e de uso, pelo ambiente ou infraestrutura em seu entorno. Portanto, as ameaças à segurança dos dados afetam profundamente as organizações e os indivíduos. As ameaças são agentes ou condições que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades (Sêmola, 2014; Andress, 2014).

Em seu trabalho Andress (2014) detalha a tríade *Confidentiality*, *Integrity and Availability* (CIA), ou Confidencialidade, Integridade e Disponibilidade — representa os principais atributos que, orientam a análise, o planejamento e a implementação da segurança de informações.

O modelo CIA visa assegurar fidedignidade os dados (Figura 1). O conceito da tríade se formou ao longo do tempo e diversas fontes. A confidencialidade pode ter sido proposta pela primeira vez em 1976, em um estudo da Força Aérea dos Estados Unidos. Da mesma forma, o conceito de integridade foi explorado em um artigo de 1987 intitulado "Uma Comparação de Políticas de Segurança de Computadores Comerciais e Militares". Embora não seja tão fácil encontrar uma fonte inicial, o conceito de disponibilidade tornou-se mais difundido um ano depois, em 1988, quando se reconhece que a computação comercial necessitava de registros contábeis e dados corretos, compondo os três atributos do modelo de segurança, mais difundido depois de 1998.

**Figura 1 - Tríade modelo CIA**




Fonte adaptada: Andress (2014)

Os atributos básicos da segurança da informação, regidos pelos padrões internacionais (ISO/IEC 27002, 2013), igualmente tratados pela normativa nacional (ABNT NBR ISO/IEC 27002, 2013), são:

• Confidencialidade um atributo fundamental da proteção da informação, limitando o acesso da informação aos usuários, ou entidades autorizadas. Pode ser implementada em diferentes níveis, permitindo maior ou menor acesso aos dados.

• Integridade é a propriedade referente à capacidade de proteger a informação contra alteração, edição ou exclusão por pessoa não autorizada.

• Disponibilidade é a competência para acessar a informação quando necessário. A falta de disponibilidade pode ser causada por problemas de energia elétrica, falhas no sistema operacional, na aplicação e na rede de computadores, por ataques (internos ou externos), de hackers, entre outros fatores.

Portanto, a literatura e a prática recomendam que se deve estabelecer métricas e instrumentos para controlar e amenizar o nível de segurança existente e, com isto, determinando as bases para análise da situação de segurança existente.

## 3 MÉTODO

### 3.1 Tipo de Pesquisa

Para atender ao foco desta pesquisa, adotou-se a abordagem metodológica fundamentada na pesquisa qualitativa (Howe & Eisenhart, 1990; Yin, 2005).

Iniciou com pesquisa bibliográfica e documental e em uma pesquisa de campo, em que as informações foram coletadas no ambiente organizacional por meio de entrevista e observação não participativa analítica.

É importante destacar que a pesquisa social, detém-se na observação do contexto no qual é detectado um fato social (problema), que a princípio passa a ser examinado e, posteriormente, encaminhado para explicações, por meio dos métodos e das técnicas específicas (Fachin, 2006).

Em relação aos objetivos da pesquisa, é classificada como descritiva. Na etapa de análises foram evidenciadas as informações por meio de critérios definidos com base nas assertivas indicadas em entrevistas (semelhante a escala *likert*), porém, adotando como base o *frame* e níveis de evolução da governança (0 a 6) segundo o COBIT ® já descrito.

### 3.2 Escolha e Relevância da Instituição Analisada

A Unicentro é uma das mais jovens Universidades do Estado do Paraná. Ela surgiu no ano de 1990 da fusão de duas Faculdades regionais, nos municípios de Guarapuava e Irati. Para descrever brevemente as unidades, em Guarapuava: *Campus* Central, em que funcionam os cursos de Graduação, Pós-Graduação dos Setores de Sociais Aplicadas e Humanas, Reitoria, grande parte dos Programas de Extensão, Centros de Assistência Social à Comunidade e Centro de Tecnologia de Informação (COORTI), há também o *Campus* do CEDETEG em que encontram-se uma grande parte dos Cursos, de Graduação, Pós-graduação, Hospital Veterinário, Clínica de Fisioterapia e Reabilitação, Centro Tecnológico e Laboratórios de análise e pesquisas concentrando os Setores de Exatas, Agrárias e Saúde. A partir do ano de 1997, após concluído seu processo de reconhecimento a instituição iniciou seu processo de expansão, implantando novos cursos em diversas áreas do conhecimento, contanto, atualmente, com 38 cursos de graduação, diversos cursos de pós-graduação em nível de especialização lato sensu e 21 programas stricto sensu, sendo 16 mestrados e 5 doutorados. Instalada na região central do Estado,

a Unicentro atende mais de cinquenta municípios em sua região da abrangência, compreendendo uma população de mais de 1 milhão de habitantes.

No ano de 2018, a Universidade abrigou 11.904 alunos matriculados no ensino de graduação e pós-graduação. Destes, 7.212 matriculados no ensino de graduação presencial, distribuídos nos 41 cursos ofertados, e 2.627 no ensino a distância, em sete cursos distintos. Na pós-graduação, a Universidade ofertou 38 cursos, sendo 17 lato sensu, com 1.351 alunos matriculados, e 21 cursos stricto sensu, com 569 acadêmicos vinculados a 16 cursos de mestrado e 145 a cinco programas de doutorado (Anuário-UNICETRO 2018).

A coleta das informações foi por meio de visitas e entrevistas com os analistas e Coordenador do setor de tecnologia de informação e comunicação (TIC) da Instituição (COORTI) que atende as três unidades: *Campus* de Guarapuava, *Campus* CEDETEG e *Campus* de Irati.

O período de desenvolvimento foi de Outubro de 2019 a março de 2020, antes das interrupções de aulas presenciais devido a pandemia. No instrumento de coleta foram avaliadas 62 afirmativas/quesitos sobre os processos, que se encontram no Apêndice do artigo e a elaboração do modelo de análise dimensionando os quatro (04) pontos de enfoques, visando avaliar os níveis de evolução declarado com a atribuição de pontos (scores) de determinados processos críticos da segurança de TI.

## 4 RESULTADOS

### 4.1 Ameaças Eletrônicas no Ambiente da Universidade

A Coordenadoria de TI da UNICENTRO (COORTI) é responsável pela ampliação e desenvolvimento de ações futuras que visem prevenir a segurança da informação.

Trecho da entrevista realizada em fevereiro de 2020 com o analista de tecnologia da informação, destacando aspectos da amplitude e colaboração dos usuários para segurança da informação, e dando ênfase que a Instituição atende aos protocolos de segurança, determinações governamentais e reguladores para o setor de TI.

> “Segurança de dados é algo bastante abrangente, diz respeito tanto a segurança física quanto segurança dos dados contra invasão. Além disso, depende muito da contribuição dos usuários. Não existe nenhum ambiente informatizado que seja totalmente seguro e não somos exceção. O que se busca é aprimorar os mecanismos de segurança prevendo determinados tipos de ameaças ou como respostas a determinados incidentes sofridos” (Analista Chefe da COORTI).

O especialista explicou que ocorrem ataques e ameaças dos dados e informações armazenados nos sistemas, contudo, essas ameaças ocorrem de maneira esporádica e leve. Ocorrem na forma de tentativa de acesso, quando não há o cadastro no banco de dados dos usuários e também por *Phishing*, que nada mais é do que a tentativa de “roubo” de senhas de acesso para *login.* Ficou evidente a preocupação e dedicação dos analistas para atualização de técnicas visando aperfeiçoar a segurança de dados. Declaram também que está sendo possível obter proteção da informação no mesmo ritmo que ocorrem as ameaças, destacam que a segurança dos dados deve ser dinâmica e estar continuamente se atualizando.

Como apresentado existe sempre ocorrências indesejadas, apresentando algum nível de risco, seja por meio de ameaças, ou fatores que representem vulnerabilidades, gerando prováveis impactos e demandando o trabalho contínuo do setor de TI (ações de detecção e prevenção). Na tabela 1, apresenta-se o modelo de avaliação da segurança de TI indicando os tipos de riscos para compreender como podem ser prevenidos:

**Tabela 1 - Modelo Cia e formas de intercepção**

| Atributos | Tipo de Ameaça |
|---|---|
| Confidencialidade | Intercepção |
| | Interrupção |
| | Modificação |
| Integridade | Fabricação de dados |
| | Interrupção |
| | Modificação |
| Disponibilidade | Fabricação de dados |

Fonte Adaptada: Andress, 2014

As informações apresentadas neste estudo representam um primeiro passo, contudo, não se pode mensurar os níveis diretamente conforme apresentado no modelo CIA. Observa-se que há uma centralização das informações da TI da universidade, também não foi possível ter acesso aos indicadores específicos dos níveis de ameaças ou outros instrumentos para controlar e amenizar o nível de segurança dos dados. Da mesma forma, não foi possível compreender o grau efetivo de Governança para o Setor de Tecnologia, dificultando a obtenção de um mapeamento completo da confidencialidade-integridade e disponibilidade. O instrumento a seguir oferece uma ferramenta mais detalhada dos processos e por isso possibilitou um diagnóstico importante para dar maior clareza aos níveis de segurança da informação.

## 4.2 Modelo e indicadores Propostos

Na sequência elaborou-se uma análise com base nos processo de governança adaptado do modelo ITIL (2011), do *Information Systems Audit and Control Association* (ISACA), que propôs uma avaliação com a indicação de pontos (*scores*) para determinados processos críticos a segurança de TI. Estes resultados podem oferecer um levantamento imparcial sobre aspectos da segurança de informação que requerem mais atenção dos gestores (Tabela 2). Imparcial pois a nota foi atribuida após o processo de visitas, levantamentos e observação e a nota foi com base no guia de boas práticas do modelo citado.

**Tabela 2 - Frame para Avaliação dos serviços e segurança da informação**

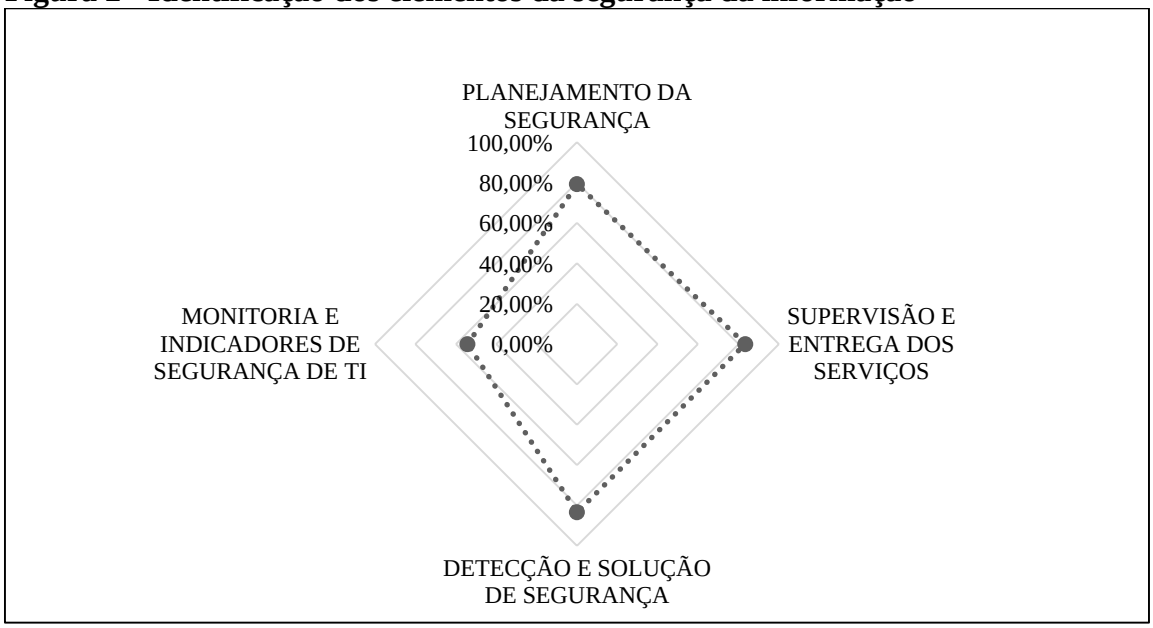
| Foco | Descrição / Avaliação Interna | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|---|
| **PLAN** | PLANEJAMENTO DA SEGURANÇA | | | | | | | |
| **DS1** | Definir e Gerenciar Níveis de Serviço | | | | | | ■ | |
| **DS2** | Gerenciar Serviços de Terceiros | | | | | | ■ | |
| **DS3** | Gerenciar Capacidade e Desempenho | | | | | | ■ | |
| **DS4** | Assegurar Continuidade e segurança dos serviços | | | | | ■ | | |
| **SUPER** | SUPERVISÃO E ENTREGA DOS SERVIÇOS | | | | | | | |
| **DS6** | Identificar e Alocar Custos | | | | | | ■ | |
| **DS7** | Educar e Treinar Usuários | | | | | ■ | | |
| **DS8** | Gerenciar a Central de Serviço e os Incidentes | | | | | | | ■ |
| **DS9** | Gerenciar a Configuração e problemas | | | | | | ■ | |
| **SOL** | DETECÇÃO E SOLUÇÃO PROBLEMAS DE SEGURANÇA | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **DS10** | Gerenciar os Problemas | | | | | | | ■ |
| **DS11** | Gerenciar os Dados | | | | | ■ | | |
| **DS12** | Gerenciar o Ambiente Físico | | | | | | ■ | |
| **DS13** | Gerenciar as Operações | | | | | | ■ | |
| **MONIT** | MONITORAR A SEGURANÇA | | | | | | | |
| **ME1** | Monitorar e Avaliar o Desempenho por meio de indicadores, quais? | | ■ | | | | | |
| **ME2** | Monitorar e Avaliar os Controles Internos | | | | ■ | | | |
| **ME3** | Assegurar a Conformidade com Requisitos Externos | | | | | ■ | | |
| **ME4** | Prover a Governança de TI | | | | | ■ | | |

Fonte: Desenvolvido na pesquisa adaptada ITIL/COBIT ®

O gráfico em radar foi adotado após processar as informações coletadas segundo os analistas de forma a evidenciar quais setores necessitam maior atenção dos gestores, a fim de focar nos processos e tarefas para ter seus níveis de efetividade dos serviços de TI melhorados (Figura 2).

**Figura 2 - Identificação dos elementos da segurança da informação**



Fonte: Elaborado na pesquisa (2020)

Para ficar facililitar a visualização dos níveis pontuados em porcentagens de 0% a 100% (tabela 3) para as dimensões: i) planejamento das questões de segurança; ii) supervisão dos serviços; iii) identificação e solução dos problemas de segurança eos quadrantes e vi) monitoria e indicadores, encontram-se evidenciados nos respectivos quadrantes, em que o quadrante 4 (monitoria e indicadores de segurança de TI) possui o menor índice com pouco mais de 54% avaliados pelos responsáveis pela TI, conforme descrito anteriormente.

**Tabela 3 - Resumo e resultados dos quadrantes**

| Etapas/Áreas | Descrição | Nível |
|---|---|---|
| **PLAN** | PLANEJAMENTO DA SEGURANÇA | 79,17% |
| **SUPER** | SUPERVISÃO E ENTREGA DOS SERVIÇOS | 83,33% |
| **DET-SOL** | DETECÇÃO E SOLUÇÃO DE SEGURANÇA | 83,33% |
| **MONIT** | MONITORIA E INDICADORES DE SEGURANÇA DE TI | 54,17% |

Fonte: Elaborado na pesquisa (2020)

## 5 DISCUSSÃO DOS RESULTADOS

Adotou-se por estratégia de pesquisa o estudo de caso, com as referidas justificativas e pertinência para pesquisar o assunto segurança de informação e outros processos relacionados aos riscos dos dados da instituição. Aplicou-se um roteiro de coleta (Apêndice 1).

Os resultados apresentados possibilitam apresentar um panorama do setor de tecnologia, adotando uma composição de intrumentos de avaliação dos serviços de tecnologia e segurança da informação. O processo pode ser considerado relevante e imparcial, pois foi desenvolvido semelhantemente de uma auditoria de processos, sendo as classificações ocorream com base no guia de boas práticas do modelo ISACA e após o processo de visitas, levantamentos e observação.

A instituição analisada possui grande representatividade para a região, sendo uma referência para outras IES, bem como, é parte da estrutura da demais Universidades Estaduais do Paraná, que possuem infraestrutura e modelo de gestão semelhantes. Estes resultados dão ciência dos mecanismos concretos, conectando o fenômeno com a literatura, por meio de um estudo intensivo *(in loco).* Desenvolveu-se um modelo de avaliação da segurança da informação detalhadas nas normativas e boas práticas, conforme descrito no item 4.

A estratégia de pesquisa adotada possibilitou a análise sobre segurança de informação deste ambiente organizacional específico. Não muitas pesquisas que tratam deste tema no ambiente das IES, das Universidades Estaduais e da segurança de dados e até mesmo de e-Governo. Sendo assim, somente por meio da coleta e aprofundamento do ambiente estudado, tornou-se possível apresentar um instrumento exploratório em consonância com a literatura, podendo ampliar o conhecimento acadêmico, fazendo contribuições para a gestão da TI podendo servir de modelo para outras entidades com demandas e estrutura semelhante.

Várias pesquisas ao longo de pelo menos duas décadas, vem apresentando sob vários contextos, discussões sobre a adequação de instrumentos que permitam a avaliação da infraestrutura de TI (Hu & Plant, 2001; Weill & Ross, 2004; Mahmood & Mann, 2005; Carcary, 2008; Lim, Dehning, Richardson & Smith, 2011; Longo & Meirelles, 2016),

nestes trabalhos discutem os impactos no desempenho das atividades das organizações e por conseguinte, enfatizam desde as potencialidades como dos riscos a ela atriuída. A tecnologia de informação está presente em todos os tipos de organizações, os serviços de TI além de atender aos propósitos da organização, também precisar atuar na proteção de ameaças aos dados conforme abordado. Este gerenciamento deve ser contínuo, supervisionados por meio de métricas ou indicadores de qualidade dos serviços, neste trabalho com ênfase nas questões de segurança de dados.

A complexidade e incertezas enfatizadas a respeito da TI não devem impedir que os gestores assumam sua responsabilidade em garantir que a mesma seja utilizada na sua amplitude e com eficiência (Weill & Ross, 2004; Flyvbjerg & Budzier, 2011).

A gestão da segurança de informação (em vigor ABNT NBR ISO/IEC 27002, 2013) pode ser obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware (Coelho, Araújo & Bezerra, 2014). Portanto, é fundamental que se evidencie os serviços de proteção dos dados em um processo contínuo, cuja finalidade é se adequar a todos os tipos de ameaças, considerando também os aspectos vigentes de legislação e direito digital. Os modelos e certificações de governança amplamente aceitos no ambiente corporativo, são essenciais para estabelecer processos, soluções de estabilidade, manutenção de métricas dos sistemas e do trabalho dos profissionais de TI.

Novos achados da literatura também apontam para a conjugação de ações e supervisão humana e também por meio da tecnologia. Segundo Salovaara, Kalle e Esko (2019) as organizações que enfrentam altos riscos e operam em domínios puramente digitais devem atender a dois objetivos contraditórios: precisam identificar ameaças digitais em escala e velocidade, evitando erros resultantes do processamento automatizado. Nesta pesquisa os resultados apontam para desafios de confiabilidade e maneiras de mitigá-los. Em tal cenário, a atenção plena coletiva por meio de uma constelação sistêmica cuidadosamente em camadas de operações (humanas) conscientes e (digitais) inconscientes.

Ospina-Díaz e Sanabria-Rangel (2020) abordam o tema da segurança da informação contra ameaças cibernéticas no contexto de governo, da situação atual na Colômbia e adotaram uma pesquisa qualitativa, teórica, documental e descritiva, fizeram um percurso histórico particularmente sobre segurança da informação. Neste trabalho expuseram diversos aspectos da segurança da informação, em especial de sistemas de gestão e padrões de qualidade. Estas questões atingem empresas, a sociedade e países, potencializados pela pandemia do COVID-19.

Citando o contexto vivenciado devido a pandemia, a presente pesquisa teve início um semestre antes do atual momento de grande transformação das atividades da universidade, especialmente pela mudança formato das aulas presenciais, desde abril de 2020 com a autorização do Conselho de Ensino e Pesquisa e Extensão para os Setores e Departamentos dos Cursos de Graduação e Pós-Graduação atuarem de modo remoto (EAD), estas mudanças trarão efeitos ainda a serem dimencionados para a segurança dos dados.

As imposições da pandemia no ensino e forma de trabalho das universidades, acrescentaram um novo elemento em relação a segurança de informação, como por exemplo, a adaptação de eventos acadêmicos-científicos presenciais na modalidade virtual, que possibilitou o acesso a centenas e milhares de participantes, da instituição e externos, ampliando ainda mais as fronteiras. Todos estes elementos, possivelmente vão acarretar novos desafios para segurança da informação nos próximos anos.

## 6 CONSIDERAÇÕES FINAIS

Esta pesquisa teve como objetivo central analisar os aspectos principais da Governança voltada à segurança da Tecnologia de Informação (TI) de uma Universidade Estadual do Centro-Oeste do Paraná, Brasil e após o desenvolvimento do trabalho e suas etapas de análise, foi possível identificar a sistemática da segurança da TI da instituição, que podem ser úteis tanto nos processos operacionais, bem como para o planejamento com visão estratégica e sustentável, em especial para aspectos preventivo das fraudes e ameaças eletrônicas.

Alguns destaques para o tema tão urgente na atualidade, o trabalho pode identificar processos, áreas de prioridades do setor responsável pela TI e seus gestores, bem como elementos que podem ter evolução e necessidade de melhorias em um futuro próximo.

Com a pesquisa foi possível apresentar algumas contribuições tanto no aspecto acadêmico, quanto para a governança da TI: A contribuição científica do artigo é especialmente por apresentar um estudo empírico, adotando uma metodologia com base na literatura alinhada aos desafios da atualidade, possibilitando identificar e monitorar os problemas de segurança das informações (Banco de dados). Quanto à contribuição para a gestão, refere-se ao levantamento de prioridades da segurança e indicadores, que poderão auxiliar em processos evolutivos do planejamento e detecção dos riscos à informação da Instituição.

Os resultados apresentados possibilitaram dar visibilidade à segurança da informação, que em geral é abordada em gestão e governança de TI. Apesar de não ser suficiente para esgotar o assunto e ter limitações, uma vez que se trata de um caso específico. Mas que pode haver aproveitamento por outras Instituições de Ensino Superior, encontrando familiaridades com esta pesquisa e suas contribuições teórico-prática. A originalidade do trabalho é pela escolha do ambiente de segurança de dados das Instituições de Ensino, ainda pouco exploradas - as novas demandas do manuseio de dados, tanto sob o aspecto da infraestrutura interna de tecnologia, do aumento de acessos dos usuários internos e externos aos bancos de dados e ainda da necessidade contínua de barrar as tentativas de acessos não-autorizados.

Futuras pesquisas podem adotar outros meios de análise das informações, com diferentes técnicas, ou pesquisa ao longo dos períodos, proporcionando uma comparabilidade da evolução da segurança de informação da instituição, incluindo os impactos pós-pandemia do COVID, para averiguar as alterações na maneira de atuar e desenvolver as atividades da universidade.

## APÊNDICE 1:

### Instrumento para coleta das informações

Setor de Tecnologia de Informação e Comunicação – Análise de sensibilidade dos quesitos sobre TI/Unicentro

| Q | Mapeamento das decisões e gestão dos serviços da Tecnologia de Informação | scores (0) inexistente e (6) 100% | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
| Q1 | A TI ajuda a organização a manter a posição competitiva | | | | | | | |
| Q2 | Capacidade de TI é adequada para desenvolver novos requisitos de TI | | | | | | | |
| Q3 | Iniciativas de TI estão alinhadas com as expectativas de negócios | | | | | | | |
| Q4 | Os gestores envolvem-se ativamente nas decisões de TI | | | | | | | |
| Q5 | Comunicação eficiente sobre as metas da Organização | | | | | | | |
| Q6 | Nível de atenção dada pelos gestores para o foco estratégico da TI | | | | | | | |
| Q7 | Há planos estratégicos para TI | | | | | | | |
| Q8 | Grau de alinhamento entre estratégia de TI e estratégia de negócios | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Q9 | Há planos estratégico para a segurança de dados | | | | | | | |
| Q10 | Grau de integração dos Sistemas de Gestão e de Apoio Acadêmico | | | | | | | |
| Q11 | Grau de influência do Governo em Sistemas Utilizados pela IES | | | | | | | |
| Q12 | Há comitês/Conselhos para tratar das tendências de TI a nível da Instituição | | | | | | | |
| Q13 | Grau de interação entre a Reitoria e o Gerente de TI (CIO) | | | | | | | |
| Q14 | Atrasos na entrega de projetos de TI | | | | | | | |
| Q15 | Estouros de orçamento significativos | | | | | | | |
| Q16 | Satisfação do usuário em soluções de falhas | | | | | | | |
| Q17 | Auditoria regulares para avaliar a segurança da informação | | | | | | | |
| Q18 | Avaliação de investimentos em TI, tomada de decisão de investimento | | | | | | | |
| Q19 | Qualidade do serviço de modo geral - desempenho | | | | | | | |
| Q20 | Capacidade de TI para apoiar inovações para o setor | | | | | | | |
| Q21 | Capacidade de TI para aproveitar as vantagens de novas tecnologias | | | | | | | |
| Q22 | Grau de confiança nos especialistas de TI | | | | | | | |
| Q23 | Possibilidade de negociar os contratos com os fornecedores/terceirizados de TI | | | | | | | |
| Q24 | Projetos de inovação e novas tecnologias, biometria entre outros | | | | | | | |
| Q25 | Há análise dos custos total de propriedade (TCO) para avaliar o desempenho | | | | | | | |
| Q26 | Quanto ao grau de comprometimento financeiro, custos de suporte e manutenção de rede | | | | | | | |
| Q27 | Controle das falhas por meio de indicadores | | | | | | | |
| Q28 | Grau de atualização dos sistemas que atendem a Universidade (suporte e atividade fim) | | | | | | | |
| Q29 | Resiliência e disponibilidade contínua | | | | | | | |
| Q30 | Restabelecimentos de eventos e ameaças externas | | | | | | | |
| Q31 | Organização dos dados e armazenagem dos dados | | | | | | | |
| Q32 | Desenvolvimento de Treinamentos para pessoal de TI | | | | | | | |
| Q33 | Treinamentos para pessoal das outras áreas da Instituição para melhoria do uso da TI | | | | | | | |
| Q34 | Retenção de habilidades | | | | | | | |
| Q35 | Infraestrutura de TI flexível e ágil (para atender mudanças e necessidades) | | | | | | | |
| Q36 | Implementação da Governança de TI (de qualquer tipo e/ou certificada) | | | | | | | |
| Q37 | Garantias físicas e ambientais da gestão dos dados | | | | | | | |
| Q38 | Avaliação e compreensão dos riscos de TI e gestão de riscos (indicadores/registros) | | | | | | | |
| Q39 | Integridade das transações | | | | | | | |
| Q40 | Preocupação com reputação e confiança | | | | | | | |
| Q41 | Recuperação de negócios em caso de sinistro com os dados em grande proporção | | | | | | | |
| Q42 | Políticas de verificação da qualidade dos Fornecedores e parceiros de Tecnologia | | | | | | | |
| Q43 | Utilização de indicadores para mensurar os investimentos em TI | | | | | | | |
| Q44 | Identificação de indicadores próprios da Universidade para medir custos relacionados a TI | | | | | | | |
| Q45 | Desempenho e geração de informação tempestivamente | | | | | | | |
| Q46 | Velocidade/qualidade do "ciclo de vida" de desenvolvimento do sistema | | | | | | | |
| Q47 | Grau de sobrecarga dos funcionários de TI | | | | | | | |
| Q48 | Necessidade de cortar custos / restrições de orçamento | | | | | | | |
| Q49 | Otimização dos serviços de TI em toda a organização | | | | | | | |
| Q50 | Problemas e incidentes de TI (indicadores/registros/*help desk*) | | | | | | | |
| Q51 | Capacidade da TI e Sistemas de suportar processos críticos de negócios | | | | | | | |
| Q52 | Perda de disponibilidade do serviço | | | | | | | |
| Q53 | Atendimento ao usuário externo (CRM) | | | | | | | |
| Q54 | Capacidade da TI quanto ao atendimento aos usuários internos | | | | | | | |
| Q55 | Níveis de melhores práticas e políticas claras | | | | | | | |
| Q56 | Acesso não autorizado à rede corporativa | | | | | | | |
| Q57 | Vírus/Ameaças/Ataques | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Q58 | Privacidade / divulgação de informações confidenciais | | | | | | | |
| Q59 | Infraestruturas de redes | | | | | | | |
| Q60 | Capacidade de atender as demandas atuais quanto a gestão e segurança de dados | | | | | | | |
| Q61 | Capacidade de atender as demandas Futuro próximo (até 5 anos) quanto a gestão e segurança de dados | | | | | | | |
| Q62 | Capacidade de atender as demandas Futuro longo prazo (10 anos ou mais) quanto a gestão e segurança de dados | | | | | | | |

Fonte: Adaptações do modelo *Information Technology Infrastructure Library* (ITIL)

## REFERÊNCIAS


ABNT NBR ISO/IEC 27002. (2013). Associação Brasileira de Normas Técnicas. Recuperado em 02 julho, 2020, de https://www.abntcatalogo.com.br/norma.aspx?ID=306582#.

Andress, J. (2014) The basics of information security: understanding the fundamentals of InfoSec in theory and practice. 2nd ed. Recuperado em 27 outubro, 2020, de https://search.ebscohost.com/login.aspx?direct=true&db=cat08036a&AN=sbfgv.000197342&lang=pt-br&site=eds-live.

Anuário-UNICETRO (2019). Unicentro em números. Diretoria de Avaliação Institucional, da Pró - Reitoria de Planejamento, DIRAI/PROPLAN. Editora UNICETRO. Recuperado em 02 março, 2020, de https://www3.unicentro.br/anuario/wp-content/uploads/sites/7/2020/03/Unicentro-em-N%C3%BAmeros-2018.pdf

Brostoff, S. (2004). Improving password system effectiveness. Tese de Doutorado. University College London.

Carcary, Marian. (2008). The Evaluation of ICT Investment Performance in terms of its Functional Deployment. *A Study of Organisational Ability to Leverage Advantage from the Banner MIS in Institutes of Technology in Ireland.* Thesis Doctorate Limerick Institute of Technology.

Chan, Y. E., & Reich, B. H., (2007). IT alignment: what have we learned? Journal of Information Technology, v. 22, p. 297–315.

Coelho, F.E.S, Araújo, L. G. S., & Bezerra, E.K. (2014). Gestão da Segurança da Informação NBR 27001 e NBR 27002. Rio de Janeiro-RJ: RNP/ESR.

COORTI-2020. (2020). Coordenação de Tecnologia de Informação da UNICENTRO Entrevistas concedidas, mar-2020.

Espinel-Ortega, Alvaro, & Carreno-Perez, Juan Carlos. (2020). Identificación de activos y ciberactivos críticos en sistemas de transmisión de energía eléctrica. *Tecnura*, *24*(65), 27-38. Recuperado em 02 novembro, 2020, de https://dx.doi.org/10.14483/22487638.15388

Fachin, O. (2006) Fundamentos de metodologia. São Paulo: Saraiva.

Flyvbjerg, B., & Budzier, A. (2011). Why Your IT Project May be Riskier Than You Think. Harvard Business Review, p. 23-25.

Henderson, J. C. & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. IBM System Journal, v. 1, n. 32, p. 4-16.

Howe, K., & Eisenhart, M. (1990). Standards for Qualitative and Quantitative Research: A Prolegomenon. *Educational Researcher*, *19*(4), 2–9, https://doi.org/10.3102/0013189X019004002

Hu, Q., & Plant, R. (2001). An empirical study of the causal relationship between IT investment and firm performance. Information Resources Management Journal, 17, (1), 37-62.

ITIL service design (2011). Best Management Practice. ISBN 978- 0-11-331305-1. 2nd ed. London: TSO. Recuperado em 01 outubro, 2019, de http://www.bestmanagement-practice.co.

ISACA- *Information Systems Audit and Control Association.* (2020). COBIT Seu roteiro para sistemas e tecnologia de informação - Use as estruturas certas para agregar valor à sua função e empresa. Recuperado em 10 novembro, 2019 de https://www.isaca.org/resources/frameworks-standards-and-models.

Laudon, K. C., & Laudon, J. P. (2015). Sistemas de Informação Gerenciais. São Paulo: Prentice Hall.

Lim, J.H., Dehning, B., Richardson, V.J., & Smith, R.E. (2011). A Meta-Analysis of the Effects of IT Investment on Firm Financial Performance. Journal of Information Systems. v. 25, n.2, p. 145-169.

Löbler, Mauri Leodir, Bobsin, Debora, & Visentini, Monize Sâmara. (2008). Alinhamento entre o plano de negócio e o plano de tecnologia de informação das empresas: análise comparativa através dos níveis de maturidade e fatores críticos de sucesso. *JISTEM - Journal of Information Systems and Technology Management, 5*(1), 37-60. https://doi.org/10.4301/S1807-17752008000100003

Longo, Luci, & Meirelles, Fernando De S. (2016). Impacto dos investimentos em tecnologia de informação no desempenho financeiro das indústrias brasileiras. *REAd. Revista Eletrônica de Administração (Porto Alegre), 22*(1), 134-165. https://doi.org/10.1590/1413-2311.0142014.48853

Lunardi, G. L., Becker, J. L., Maçada, A. C. G., & Dolci, P. C. (2014). The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms. International Journal of Accounting Information Systems, 15(1), p.66-81, http://doi.org/10.1016/j.accinf.2013.02.001.

Mahmood, M.A., & Mann, G.J. (2005). Information Technology Investments and Organizational Productivity and Performance: An Empirical Investigation. *Journal of Organizational Computing Electronic Commerce.* 15(3), 185–202.

Morris, R., & Thompson, K. (1979). Password security: a case history. Communications of the ACM, 22, 594-597.

Ospina-Díaz, M. R., & Sanabria-Rangel, P. E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Rev. Crim., Bogotá, D. C, v.62 (2).

Peterson, R. R. (2004). Crafting Information Technology Governance. Information Systems Management.

Remenyi, D., Bannister, F. & Money, A. (2007). The effective measurement and management of ICT costs and benefits, 3. Ed. Elsevier CIMA Publishing, Oxford.

Rios, O. K. L., Teixeira-Filho, J.G & Rios, V. P. S. (2017). Gestão de segurança da informação: práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação. Navus, Florianópolis-SC, v.7, n.2, p. 49-65.

Salovaara, Antti, Lyytinen, Kalle & Penttinen, Esko. (2019). High Reliability in Digital Organizing: Mindlessness, the Frame Problem, and Digital Operations. MIS Quarterly. 43. 555-578. 10.25300/MISQ/2019/14577.

Sêmola, M. (2014). Gestão de segurança da informação: uma visão executiva. 2.ed. Rio de Janeiro: Elsevier.

Silva, H.C.C., Silveira, D. S., Dornelas, J.S., & Ferreira, H. S. (2020). Information technology governance in small and medium enterprises – a systematic mapping. *JISTEM Journal Information Systems Technology Management.* v 17, http://dx.doi.org/10.4301/s1807-1775202017001.

Solana-González, P., Vanti, A.A., & Fontana, K. H. S. (2019). Multicriteria analysis of the compliance for improvement of information security. *JISTEM - Journal of Information Systems and Technology Management*, *16*, https://doi.org/10.4301/s1807-1775201916007

Silva, B.A.M., & Moraes, G.H.S.M. (2011). Influência dos Direcionadores do Uso da TI na Governança de TI. *Revista Brasileira de Gestão de Negócios*, *13*(38), 41-60. https://dx.doi.org/10.7819/rbgn.v13i38.689

Weill, P., & Ross, W.J. (2004). IT Governance: how top performers manage IT decision rights for superior result. Boston, MA: Harward School Press.

Whitman, M.E., & Mattord, H.J. (2012). Principles of Information Security – Course Technology. USA. CENGAGE Learning.

Yin, R. K. (2005). Estudo de caso: planejamento e métodos. 3. ed. Porto Alegre: Bookman.