REVISTA ELETRÔNICA AMPLAMENTE
v.1, n.4 out./ dez. 2022 DOI: 10.47538/RA-2022.V1N4
ISSN: 2965-0003

SEGURANÇA DA INFORMAÇÃO, SOB INFLUÊNCIA DA ENGENHARIA SOCIAL

Daniela da Silva Soncini
Centro Estadual de Educação Tecnológica Paula Souza; Etec Elias Nechar - Catanduva-SP.
http://lattes.cnpq.br/6992674460797738
https://orcid.org/0000-0001-6075-7847
E-mail: danielasilvasoncini@gmail.com

Fernanda da Silva Cacini
Centro Estadual de Educação Técnológica Paula Souza. Etec Prof. José Carlos Seno Júnior-Olímpia –SP.
http://lattes.cnpq.br/9711495460013196
E-mail: fer.sil@hotmail.com

DOI-Geral: http://dx.doi.org/10.47538/RA-2022.V1N4
DOI-Individual: http://dx.doi.org/10.47538/RA-2022.V1N4-05

RESUMO: A elaboração do conteúdo proporciona repensar dentro dos ambientes educacionais as ações voltadas para a segurança da informação, como podemos desenvolver uma engenharia social apropriada dentro de seus ambientes, para que possamos ter uma segurança de dados apropriada e de um acesso seguro a estes ambientes. Trabalhou-se e desenvolveram-se ações diárias que nos remetem a garantir esta segurança de informações sigilosas de todos os envolvidos destes ambientes, mostrar dentro deste contexto em como trabalhar e desenvolver estratégias com a finalidade de assegurar e garantir uma integridade de dados para que o ambiente ao qual desenvolvesse se torne confiável, garantindo qualidade em nossos resultados e refletindo em uma melhoria contínua.

PALAVRAS-CHAVE: Segurança. Integridade. Qualidade.

INFORMATION SECURITY, UNDER THE INFLUENCE OF SOCIAL ENGINEERING

ABSTRACT: The elaboration of the content allows us to rethink the actions aimed at information security within educational environments, how we can develop appropriate social engineering within their environments, so that we can have appropriate data security and secure access to these environments . Work was carried out and daily actions were developed that lead us to guarantee the security of confidential information for all those involved in these environments, to show within this context how to work and develop strategies with the aim of ensuring and guaranteeing data integrity so that the environment in which it developed becomes reliable, guaranteeing quality in our results and reflecting in continuous improvement.

KEYWORDS: Security. Integrity. Quality.

INTRODUÇÃO

REVISTA ELETRÔNICA AMPLAMENTE
v.1, n.4 out./ dez. 2022 DOI: 10.47538/RA-2022.V1N4
ISSN: 2965-0003

O desenvolvimento do conteúdo tem como foco central a Engenharia Social e a aplicação das políticas de acesso às informações, dentro das instituições educacionais, buscando focar o tema, pois estamos em um ambiente educacional onde muitas vezes não possuímos ações que nos permitem uma melhoria constante da qualidade da informação, e uma conscientização dos usuários de que devem possuir uma postura adequada durante o seu uso.

O principal foco de desenvolvimento deste tema é trabalhar com ações que possam ajudar colaboradores administrativos e alunos dentro destes ambientes com a finalidade de melhorar o uso de tecnologias e utilizá-las de forma correta para que não ocorra divulgação de informações consideradas sigilosas, pois é necessário entender e compreender o teor daquilo com o qual estamos trabalhando.

Observamos questões importantes a serem discutidas e analisadas dentro destes ambientes, tais como a divulgação de informações confidenciais e de uso restrito da instituição a terceiros, o uso de rede de dados onde estas em sua maioria estão desprovidas de tecnologia adequada para o compartilhamento e disseminação das informações em rede local ou remota, deixando acessos e espaços para que ocorra uma busca de dados não autorizado.

A proposta é desenvolver ações que torne este ambiente mais seguro para que estas informações sejam tratadas de modo integro e como agir para diminuir as incidências de divulgação inadequada de dados e o uso de tecnologias que possam atenuar a vulnerabilidade da rede local a fim de garantir uma qualidade e confiança maior para seus usuários.

A relevância fundamental para a sua escolha foi devido a experiências vivenciadas, perceber a divulgação de informações confidenciais sendo informada e distribuída a terceiros que não pertenciam ao ambiente de trabalho, causando transtornos e prejuízos físicos e psicológicos, gerando desconforto dentro do ambiente. A metodologia de pesquisa adotada foi a qualitativa, que foi desenvolvida através de bibliografias que tratam do respectivo assunto e que façam alusão ao proposto, comprovando e mostrando como devemos aplicar a proposta de forma adequada e de acordo com experiências anteriores.

REVISTA ELETRÔNICA AMPLAMENTE
v.1, n.4 out./ dez. 2022 DOI: 10.47538/RA-2022.V1N4
ISSN: 2965-0003

A IMPORTÂNCIA DA INFORMAÇÃO NAS INSTITUIÇÕES

A informação está presente no cotidiano das pessoas, e integrada dentro das empresas, hoje vivemos conectados constantemente a um acesso a dados de forma fácil e muitos divulgados de forma aberta através dos acessos à internet. Quando falamos em empresas é válido informar que muitas informações devem ter sua integridade preservada bem como a sua respectiva segurança, pois não estamos aqui tratando com uma única pessoa, mas temos situações em que tratamos e armazenamos muitas informações de grande relevância para a vida financeira e funcional destas empresas.

De acordo com Sousa (1990, p. 58), a informação é, "uma ferramenta crucial do processo de tomada de decisão e controle das atividades da empresa", pois através destes dados é que definimos estratégias para a melhoria da gestão e a tomada de importantes decisões, tanto atual quanto futura, se faz importante compreender o que é realmente informação para o desenvolvimento e aplicação de ações dentro dos ambientes corporativos.

Entender e compreender isto se faz necessário, pois tratamos com pessoas que expões decisões e opiniões diferentes para as tomadas de decisão, e que muitas vezes estas informações devem ser sigilosas e armazenadas de modo específico restringindo o acesso.

Compreender esta sistemática é entender que a informação necessita de segurança e esta não envolve apenas equipamentos, mas também pessoas que são vulneráveis e suscetíveis a comportamento e erros, onde o papel da engenharia social dentro destes ambientes se faz necessário para manter a segurança destas informações e a qualidade e confiança destas instituições na sociedade atual.

ENGENHARIA SOCIAL

A engenharia social é um item da composição da segurança da informação, compreender o seu significado que, de acordo com Ferreira (2009), têm-se os seguintes significados para *Engenharia:* aplicação de conhecimentos científicos e empíricos e certas habilitações especificam a criação de estruturas, dispositivos e processos para converter recursos naturais em formas adequadas ao atendimento das necessidades

REVISTA ELETRÔNICA AMPLAMENTE
v.1, n.4 out./ dez. 2022 DOI: 10.47538/RA-2022.V1N4
ISSN: 2965-0003

humanas (p. 754) e *Social*: da sociedade ou relativo a ela, sociável (p. 1864), ou seja, a forma pela qual extraímos informações das pessoas através das relações sociais existentes. Podemos afirmar que é a técnica de persuasão para se conseguir informações importantes dentro da empresa como dados bancários, senhas etc. São realizadas muitas vezes por pessoas que estudam a empresa suas características, atuação de mercado, situação financeira e que desejam agir para conseguir ter acesso a informações podendo repassá-las ao "mercado negro", com a finalidade ganhos financeiros dentro desta área.

A sua construção é iniciada através de pessoas que exercem atividades remuneradas dentro da própria empresa de forma direta ou indireta ou por terceiros que tenham contato com funcionários em um ambiente externo, utilizando técnicas para conseguir retirar informações importantes para seus fins.

Devemos compreender que a segurança da informação está pautada em dois elementos os computacionais e o humano onde este é vulnerável, por isto considere a engenharia social como um dos pilares da segurança da informação mais frágeis. As fontes de vulnerabilidade identificadas são (Fonte: http://pt.wikipedia. org/w/index.php?oldid=19800887):

- **Vaidade pessoal e/ou profissional:** As pessoas aceitam de forma mais fácil os seus pontos positivos em relação aos negativos, pois reconhecer seus erros é um processo que requer um grau maio de aceitação. Aceitar os pontos positivos está ligado ao seu benefício próprio ou coletivo para demonstração destes valores.

- **Autoconfiança**: O ser humano busca em suas conversas, transmitir uma confiabilidade sobre o que está falando, fazendo com que outras pessoas acreditem que este tenha um conhecimento e experiência necessários e ações que sejam eficazes para a organização.

- **Formação profissional**: Sempre a formação profissional é valorizada com ênfase, seja ela acadêmica através de suas titulações ou de forma práticas através dos trabalhos desenvolvidos dentro das empresas, falar sobre o conhecimento é sempre importante e valorizar a formação e o que se conhece é melhor, pois isto gera em outras pessoas admiração e respeito pelo seu respectivo currículo.

REVISTA ELETRÔNICA AMPLAMENTE
v.1, n.4 out./ dez. 2022 DOI: 10.47538/RA-2022.V1N4
ISSN: 2965-0003

- **Vontade de ser útil**: A questão de ser útil se mostra quando a pessoa demonstra cortesia, e procura colaborar com o próximo.

- **Busca por novas amizades**: Através dos novos relacionamentos entre as pessoas, e gerando laços de amizade, nos sentimos confortáveis e suscetíveis a novas informações e a fornecê-las também.

- **Propagação de responsabilidade**: Dividir a responsabilidade com um grupo, ter a consciência de que não somos capazes de desenvolver as atividades sozinhos, agimos em vivemos em grupo.

- **Persuasão**: A capacidade de convencer as pessoas para se obter as informações que procuramos, agimos sobre as características das pessoas, pois cada uma age e se comporta de um modo diferente, desta forma para conseguir retirar algum tipo de informação desta pessoa, tratamos de estudar o seu comportamento e analisá-lo com a finalidade de agir para que ocorra uma manipulação de modo certo.

A engenharia social está pautada não somente na área computacional, ela envolve todos os setores, desenvolve suas ações sobre o comportamento humano, tratando e desenvolvendo técnicas através dos seus comportamentos, das suas ações psicológicas para que possamos extrair informações para serem utilizadas a outros fins, muitas vezes para um roubo eletrônico, para a venda destas concorrentes. As técnicas utilizadas são comuns até mesmo para pessoas que não exercem atividades na área computacional, vivenciamos estas situações mesmo que direta ou indiretamente sem termos a percepção de que estamos realizando, as pessoas que utilizam estas metodologias para aplicar a Engenharia Social, nos fazem sentirmos pessoas especiais, trabalham como o ego humano, a sua valorização e este por sua vez, não pondera a questão ética e sua postura dentro do ambiente de trabalho. Entender este procedimento é importante para aplicar artifícios para coibir estas ações e instrumentos para diminuir estas incidências dentro do ambiente de segurança da informação (MITNICK; SIMON, 2003).

TÉCNICAS UTILIZADAS NA ENGENHARIA SOCIAL

A Engenharia Social é a técnica de enganar as pessoas, ela não é faculdade e sim a arte de se conseguir informações.

REVISTA ELETRÔNICA AMPLAMENTE
v.1, n.4 out./ dez. 2022 DOI: 10.47538/RA-2022.V1N4
ISSN: 2965-0003

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe (MITNICK; SIMON, 2003, p. 03).

As obtenções das informações são principalmente obtidas através dos meios de comunicação principalmente pelos canais como internet, e-mail, conversa direta com a pessoa que desejamos obter as informações, telefone. Identificamos algumas técnicas como:

Vírus que se difundem por e-mail: Os vírus são criados e propagados em sua maioria por e-mail, o usuário inicialmente recebe a informação e executada o arquivo, isto acontece, pois este e-mail recebido está com informações atrativas na descrição do seu corpo como um texto especial, uma propaganda, um prêmio, que possam desperdiçar e aguçar a curiosidade de quem o lê, induzindo a pessoa a executá-lo, através desta ação este arquivo é instalado no computador da vítima monitorando suas informações e a utilizando para outros fins.

E-mails falsos (spam): Utilizado para obter informações financeiras das pessoas, com o propósito de obter informações. Esses e-mails em sua maioria solicitam informações bancárias com a finalidade de atualização de dados bancárias, o que devemos nos lembrar sempre é que as instituições bancárias não solicitam informações por e-mail.

A utilização deste método é a obtenção de uma lista de e-mails utilizando para SPAM, tendo nestes documentos digitais links que são direcionados para sites falsos e assim tendo acesso a informações de suas vítimas. Estes exemplos de técnicas são exemplos de tática utilizada dentro da Engenharia Social.

O COMPORTAMENTO ÉTICO DENTRO DAS EMPRESAS

As empresas hoje procuram e visam lucro, porém para obtê-lo é necessário desenvolver o seu capital humano, é importante conhecermos e termos a consciência de nossa responsabilidade diante do ambiente que trabalhamos. Mudar a postura das pessoas e trabalhar para que esta desenvolva suas ações requer tempo e conscientização para que possamos ter uma nova formação e uma dedicação maior deste colaborador (MASIEIRO, 2009).

REVISTA ELETRÔNICA AMPLAMENTE
v.1, n.4 out./ dez. 2022 DOI: 10.47538/RA-2022.V1N4
ISSN: 2965-0003

Procuramos dentro dos ambientes coorporativos, colaboradores que tenham responsabilidade com a empresa, mas nos questionamos sobre o que queremos sobre estas ações, dentro destes ambientes tratamos informações que sejam sigilosas, e importantes para a vida econômica da empresa, é necessário compreender como isto deve ser tratado, desenvolvemos atividades em departamentos diferentes e cada um com diretrizes voltadas para o ciclo de vida desta empresa, muitas vezes devemos compreender que assunto de um departamento A não pertence ao departamento B, e tratamos isto com a ajuda dos sistemas computacionais que buscam facilitar e agilizar o trabalho, porém tratar o capital humano é importante para sanar estas dificuldades (MASIEIRO, 2009).

De acordo com (MASIEIRO, 2009, p. 454), "uma ação ética torna-se utilitária quando é empregada em prol do bem comum e beneficia um número significante de pessoas", ter a ética voltada para o interesse da empresa e assim atingir bons resultados é aumentar a confiabilidade desta no mercado externo e a valorização do profissional que presta serviços a esta empresa.

Este comportamento passar a ser efetivo quando passamos da teoria para a prática, aplicando as propostas em ações diárias coordenadas dentro destes ambientes. As atividades das pessoas são direcionadas pela sua moral, que é construída dentro da sua cultura, no ambiente familiar em suas crenças e educação, cada pessoa tem uma moral, não somos todos iguais, vivemos em uma sociedade onde recebemos formações diferentes devido a cultura em que estamos inseridos, entendemos que é necessário se adequar para poder vivenciar em cada ambiente e assim de adequar as políticas de trabalho das empresas (MASIEIRO, 2009).

Segundo Vazquez (1985, p. 12), a "ética é a teoria ou ciência do comportamento moral dos homens em sociedade. Ou seja, é a ciência de uma forma específica do comportamento humano", as pessoas possuem princípios de ética diferentes, porém não devemos confundir estas definições com moral, pois possuem sentidos distantes (SROUR, 1998, p. 270):

> Enquanto a moral tem uma base histórica, o estatuto da ética é teórico, corresponde a uma generalidade abstrata e formal. A ética estuda as morais e as moralidades, analisa as escolhas que os agentes fazem em situações concretas, verifica se as opções se conformam aos padrões sociais. (...) Distingue-se das morais históricas que imbuem

REVISTA ELETRÔNICA AMPLAMENTE
v.1, n.4 out./ dez. 2022 DOI: 10.47538/RA-2022.V1N4
ISSN: 2965-0003

> coletividades amplas (nações, classes ou categorias sociais) e que remetem a conceitos específicos ou de "espécie".

A ética sofre influência, quando convivemos em grupo, sofremos estas influências pois somos suscetíveis a mudanças, pois começamos a ter contato com culturas diferentes, entrando em conflito dentro do ambiente coorporativo com o princípio moral que cada um de nós possuímos.

O aprendizado da ética dentro das empresas passa a ser considerada, para que se torne uma constante de ações, sua concretização ocorre pelos exemplos, orientando como devemos agir dentro das empresas, o que fazer e como agir, porém nem tudo é correto devido aos valores pessoais que envolvem este estágio (MASIEIRO, 2009).

> A maioria dos problemas éticos no ambiente de trabalho surge quando se pede às pessoas que façam – ou quando elas percebem que estão a ponto de fazer – algo contrário às suas crenças pessoais. (...) A questão ética se estende aos valores pessoais – as crenças e atitudes intrínsecas que ajudam a determinar o comportamento individual. Considerando que esses valores variam de pessoa para pessoa, é de se esperar que existam diferentes interpretações sobre qual comportamento é ético ou antiético em uma determinada situação (SCHERMERHORN, 2007, p. 51).

A prática da ética nos segmentos da empresa expõe a confiança nas ações desenvolvidas por ela, acrescentando o seu valor social, pois dentro da sociedade nos remete uma maior confiança nos produtos ou serviços prestados por esta no mercado, assim também ocorre uma valorização do profissional que está exercendo suas atividades, promovendo um melhor aproveitamento do seu desempenho e estimulando este a ter uma maior participação e colaboração nas responsabilidades desta empresa, promovendo meios constantes para sua melhoria (MASIEIRO, 2009).

De acordo com Masieiro (2009, p. 455):

> Quando essa postura é adotada e colocada em prática, começam a surgir diversos pontos positivos entre os funcionários, como a formação de um clima ética na organização. Assim, o moral e o orgulho por trabalhar na empresa são elevados, gerando maior comprometimento com a empresa e um bom diferencial competitivo.

Compreendemos a importância da ética dentro das ações envolvendo a Engenharia Social, pois através da postura do profissional, estamos vulneráveis quanto a segurança da informação, o comportamento das pessoas dentro das instituições e sua

REVISTA ELETRÔNICA AMPLAMENTE
v.1, n.4 out./ dez. 2022 DOI: 10.47538/RA-2022.V1N4
ISSN: 2965-0003

responsabilidade junto a empresa, colabora para a diminuição das ações relacionadas a fraudes computacionais (SCHERMERHORN, 2007).

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

A aplicação das políticas de segurança da informação tende a diminuir e tornar o ambiente mais seguro dentro das empresas, podemos definir essa política como sendo uma ferramenta importante para diminuir os problemas que surgem dentro destes ambientes.

Com os avanços tecnológicos e com um aumento crescente da qualidade do conhecimento dos profissionais, precisamos definir ações para tornar o ambiente mais seguro, através de regras para proteger das ameaças constantes (MASIERO, 2009).

Para Krause (1999) existem três princípios para a segurança da informação:

- **Confidencialidade**: O acesso a informação é permitido somente a pessoas autorizadas, desta forma temos a proteção dos sistemas de informação para que o acesso não ocorra.
- **Disponibilidade**: Informação disponível de acordo com a necessidade.
- **Integridade**: A informação deverá ser íntegra sem alteração, ou seja, original de acordo como foi armazenada.

Compreendemos que sistemas informatizados, envolvem pessoas, tecnologia e educação, esta conexão ocorre através da implantação de boas práticas e regras do seu uso de forma adequada e, portanto, reflete no mercado externo, adicionando uma maior competência e crédito (KRAUSE, 1999).

IMPLANTAÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Com os avanços tecnológicos a implantação das práticas de políticas de segurança da informação, tendem a ficar cada vez mais evidente, pois para se obter uma qualidade no setor é necessário estar certificada. Portanto para Castro (2012), uma política de segurança deve ser aplicada na empresa de forma esclarecedora para o funcionário no sentido de agir e deverá incluir os itens abaixo:

a) **Política de senhas**: determina normas sobre a utilização de senhas, definindo através delas níveis de acesso aos recursos computacionais, como tamanho mínimo e máximo, regra de formação e periodicidade de troca;

b) **Política de backup**: determina como será realizado as cópias de segurança, o tipo de mídia utilizado para armazenamento, período de arquivamento e assiduidade de execução;

c) **Política de privacidade**: determina como será definido as informações pessoais, de clientes, usuários ou funcionários;

d) **Política de confidencialidade**: determina como será definida as informações institucionais, ou seja, se elas podem ser repassadas a terceiros;

e) **Política de uso aceitável (PUA) ou Acceptable Use Policy (AUP)**: também chamada de "Termo de Uso" ou "Termo de Serviço", definição de regras paras o uso de recursos computacionais, os direitos e as responsabilidades das pessoas que utilizam e quais situações que são consideradas abusivas.

Entendemos que as empresas passam por novas mudanças organizacionais para a implantação e funcionamento da implantação das políticas de segurança, requerendo investimentos financeiros, tanto para o setor de tecnologia da informação, com aquisições de softwares computacionais, bem como em treinamento com os colaboradores, para que assim consigam alcançar os objetivos determinados para a implantação deste processo e adquirir um padrão de qualidade para o seu reconhecimento e certificação no mercado externo (MITNICK; SIMON, 2003).

CONCLUSÃO

Ao realizar uma análise contínua da proposta do estudo concluímos que todos nós estamos inclusos e conectados constantemente em um mundo onde recebemos informações em tempo real, muitas vezes de face verdadeira outras vezes falsa, e estas são disseminadas de forma constante e a uma velocidade que não conseguimos controlar. Ao adaptar esta nova realidade para as empresas, sejam elas instituições públicas ou privadas, buscamos compreender em como realizar uma organização de forma a garantir uma integridade e confidencialidade dos dados de forma correta e idônea, nos dias atuais.

REVISTA ELETRÔNICA AMPLAMENTE
v.1, n.4 out./ dez. 2022 DOI: 10.47538/RA-2022.V1N4
ISSN: 2965-0003

Trabalhamos e desenvolvemos nossas ações através de uma conciliação entre "pessoa e software", gerenciando corporações, cientes da responsabilidade pela qual temos em assegurar e garantir que os serviços prestados tenham qualidade e segurança. Desenvolvesse um novo perfil de funcionário que venha a fazer parte de uma equipe onde este tenha a característica de colaborador e uma corresponsabilidade sobre estas ações, cabe então ao departamento de RH e em conjunto com a área de tecnologia da informação traçar este novo perfil e tornar o seu colaborador ativo a atender suas reais necessidades.

A aplicação das políticas de segurança da informação dentro dos ambientes coorporativos é uma necessidade constante para podermos diminuir os erros e tratarmos as falhas tão almejadas na engenharia social, onde busca de forma ardilosa e surdina retirar informações importantes no mundo empresarial e usufruir de seus benefícios com a finalidade de obtenção de lucro, não falamos aqui em uma formação acadêmica, mas sim na arte de tratar e persuadir pessoas, afim de se conseguir o que se deseja e forma rápida e fácil, trabalhando e agindo nas falhas e decepções concentradas no ego humano, repleto de vaidade concorrência em suas ações.

A criação e desenvolvimento de programa de segurança da informação traz nova perspectiva, pois desta forma buscamos implantar novas políticas de segurança da informação pautada em certificações que nos garantem a qualidade, refletindo em uma consolidação no mercado externo, na questão da qualidade e confiança da empresa nos mercados em que atua. Ao aplicar todas estas propostas conclui-se que mesmo possuindo recursos e investimentos necessários precisamos ter um capital humano com um comportamento que tenha como característica agregar e somar junto a empresa onde está atuando para que assim possa-se obter o sucesso tão almejado.

REFERÊNCIAS

CASTRO, Vander de. **Internet nas empresas**: bloquear ou liberar o uso para Atividades pessoais? 2012.Disponível em:<http://corporate.canaltech.com.br/materia/seguranca/Internet-nasempresasbloquear-ou-liberar-o-uso-para-atividades-pessoais/>. Acesso em: 27 maio 2015.

ENGENHARIA SOCIAL: segurança da informação. Disponível em http://pt.wikipedia.org/w/index.php?oldid=19800887, Acesso em: 25 setembro de 2017.

FERREIRA, A. B. H. **Novo Dicionário Aurélio da Língua Portuguesa**. 4ª. Ed. Paraná: Positivo, 2009.

KRAUSE, Micki e TIPTON, Harold F. **Handbook of information security management**. AuerbachPublications, 1999.

MASIEIRO, Gilmar. **Administração de empresas:** teoria e funções com exercícios e casos. 2 ed.rev e atual. São Paulo: Saraiva, 2009.

MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar:** ataques de hackers – controlando o fator humano na segurança da Informação. São Paulo: Makron, 2003.

SCHERMERHORN. Jr., John R. **Administração.** Tradução: Mário Persona. Rio de Janeiro.LTC, 2007.

SOUSA, António. *Introdução à gestão: uma abordagem sistémica*. Lisboa: Verbo, 1990.

SROUR, Robert Henry. **Poder, Cultura e Ética nas Organizações.** 2. ed. Rio de Janeiro. Editora Campus, 1998.

VAZQUEZ, Adolfo Sanchez et. al. **Ética.** 8. Ed. Rio de Janeiro. Civilização Brasileira, 1985.

Data de submissão: 12/11/2022. Data de aceite: 18/11/2022. Data de publicação: 20/11/2022.