ANÁLISE DE POLÍTICAS DE CONTROLE E SEGURANÇA EM AMBIENTES EMPRESARIAIS

André Sauer Caprini[1]; Everton de Matos[2];
1 Escola Politécnica – Faculdade Meridional (IMED). andrecaprini9@gmail.com
2 Escola Politécnica – Faculdade Meridional (IMED). everton.matos@imed.edu.br

RESUMO: O presente artigo relata ferramentas de auxílio para ambientes empresariais, com foco em demonstrar como elas podem trabalhar mutuamente para melhorar a segurança digital. O objetivo da pesquisa foi demonstrar as possibilidades e algumas combinações que funcionam em conjunto. Para isso, foram efetuadas exemplificações das ferramentas e seu funcionamento. Após, efetuada a análise desses indicadores e de trabalhos relacionados já realizados no mesmo segmento. Explanada uma possível discussão a respeito do que ainda está em aberto na área e possíveis mitigações. Constata-se que ainda há muito o que ser abordado no quisto de segurança e o leque de assuntos está em aberto.
PALAVRAS-CHAVE: Digital Security, Enterprise Security, Group Policy, Active Directory, Single Sign-On.

ABSTRACT: This article reports on assistive tools for business environments, with a focus on demonstrating how they can work together to improve digital security. This research aims to demonstrate the possibilities and some combinations that work together. For this, examples of the tools and their operation were made. Afterward, the analysis of these indicators and related work already carried out in the same segment was carried out and explained a possible discussion about what is still open in the area and potential mitigations. It appears that there is still much to be addressed in the cyst of security, and the range of issues is open.

1 INTRODUÇÃO

A segurança de dados vem se tornando recorrente na medida que organizações cada vez mais possuem seus dados e informações processadas em ambiente computacional, dependendo desse ambiente para realizar seu negócio e/ou o acesso nesse ambiente está disponível a todos os colaboradores da organização (FONTES, 2017). A melhoria do desempenho das soluções de segurança em ambientes empresariais é um importante tópico de pesquisa e desenvolvimento. Esta melhoria pode ser alcançada com a utilização de ferramentas de controle de grupo, segurança de acessos entre outras funcionalidades (MICROSOFT, 2017).

Quase metade das empresas nacionais não adotam medidas de segurança digital, mesmo já tendo iniciado sua transformação digital, estudos revelam que cerca de 40 % das empresas nacionais não possuem políticas de segurança digital, sendo esta estando já estabelecida ou não (TERRA, 2020), assim, como uma alternativa para minimizar problemas de segurança em ambientes empresariais utilizam-se ferramentas para controle de acessos internos e acessos web, domínio, ferramentas contra vírus, entre demais opções para a melhoria na segurança.

Visando a importância da segurança da informação, este trabalho tem a intenção de auxiliar no âmbito em que todas as organizações possam ter um norte de ferramentas disponíveis a se utilizar para sua proteção. Para isso, se faz necessária a criação de estratégias com o objetivo de gerencias esses riscos, identidades e

incidentes, desse modo assegura-se uma reação mais eficiente, sendo as principais atividades para que se alcance o objetivo é o monitoramento, prevenção e responder as ameaças (RIBEIRO et al., 2020).

Para que se alcance o real objetivo de demonstrar a importância da utilização de ferramentas de segurança no ambiente empresarial, será feito o estudo das ferramentas, *Active Directory Domain Services*, *Group Policy Objects* e principalmente de *Single Sign-On*, avaliando como eles trabalham juntos e utilizam funcionalidades em conjunto, sendo de grande auxílio. Com a análise dos resultados de trabalhos relacionados, será proposta a discussão a respeito dos níveis de proteção conseguidos.

O restante deste trabalho é apresentado da seguinte forma. Na Seção 2 será apresentada a definição das ferramentas utilizadas, aprofundadas em cada subseção. A Seção 3 apresentara detalhes de trabalhos relacionados ao tema proposto. A Seção 4 apresenta uma discussão sobre possibilidades e futuros passos para controle de segurança em ambientes empresariais. A Seção 5 apresenta as conclusões deste artigo.

2 REFERENCIAL TEÓRICO

A presente seção define alguns conceitos comumente citados no decorrer do presente trabalho. Na Subseção 2.1 o conceito de *Active Directory Domain Server* (AD DS) é apresentado detalhadamente, assim como os diferentes níveis de aplicação presentes nesta camada, na Subseção 2.2, é apresentada a definição de *Group Policy* (GPO) ou Diretiva de Grupo. A Subseção 2.3 apresenta a funcionalidade de *Single Sign-on* (SSO), que é o controle de acesso único a vários sistemas.

2.1 AD DS

O *Active Directory Domain Services* já se tornou uma identidade ao se tratar de sistemas operacionais Windows. Ele é a representação de um ponto central de controle e autenticação para seus objetos, como grupos, usuários e computadores. Ele armazena informações sobre os objetos na rede e faz com que essa informação seja de fácil uso e acesso tanto para administradores quanto aos usuários, utilizando de um armazenamento de dados estruturado como base para uma organização lógica e hierárquica de informações do diretório (MICROSOFT, 2017).

O AD DS usa uma base de dados para todas as informações de diretório, esse banco de dados é geralmente referido como "Diretório". O diretório contém informações sobre usuários, grupos, computadores, serviços e todo tipo de recurso de sua estrutura hierárquica, o *SysAdmin* acaba por ter a habilidade de fazer buscas organizadas aplicando configurações e opções de segurança para todos os objetos (STEFANOVIC; KRANJAC,2019).

Todo AD DS possui dois tipos de componentes, lógico e físico. Seus componentes trabalham em conjunto e para cada um há uma função própria para que o funcionamento do AD DS seja correto. A Tabela \ref{tab:adds} apresenta alguns exemplos de componentes lógicos e físicos presentes em AD DS (STEFANOVIC; KRANJAC,2019).

Tabela 1. Componentes do AD DS (STEFANOVIC; KRANJAC, 2019)

Componentes Lógicos	Componentes Físicos
Partições	Controladores de Domínio
Domínios	Controladores de Domínio – Somente Leitura
Unidades Organizacionais (OU)	Armazenamento de dados
Florestas	Catálogo de Servidores Global

Como é demonstrado em (STANEK, 2008), o *Active Directory* (AD) também possui outras funcionalidades além do *Domain Services* (DS), os seguintes itens detalham as diferentes possibilidades:

- *Active Directory Certificate Services* (AD CS), o qual é responsável pela emissão e revogação de certificados digitais para usuários, computadores-clientes e servidores.
- *Active Directory Federation Services* (AD FS), que complementa a autenticação e controle de acesso do AD DS estendendo ele ao *World Wide Web* (WWW).
- *Active Directory Lightweight Directory Services* (AD LDS), fornece um armazenamento de dados para casos que não requerem o AD DS e não incluem que sejam efetuados em controladores de domínio.
- *Active Directory Rights Management Services* (AD RMS), fornece acesso controlado a mensagens de e-mail protegidas, documentos, páginas da intranet e outros tipos de arquivos.

As previamente citadas são algumas das principais ferramentas que completam a funcionalidade do *Active Directory*.

Sua implementação deve ser feita em uma das distribuições de *Windows Server* da Microsoft, a partir do Windows Server 2012, se tornou mais simples e mais rápido que versões anteriores. O processo de instalação é construído no *PowerShell* e é integrado a funcionalidade do *Server Manager*. Existem alguns pré-requisitos a serem cumpridos antes de conseguir efetuar uma implantação bem-sucedida, como por exemplo definir um nome para seu domínio e efetuar a criação da floresta. Porém, o passo-a-passo de instalação auxilia na criação desses requisitos.

2.2 GPO

O *Group Policy Object*, ou Objeto de Diretiva de Grupo, é uma funcionalidade da família dos sistemas operacionais Microsoft Windows. É um conjunto de regras que controlam o ambiente de trabalho de contas de usuário e contas de computador, fornecendo o gerenciamento e configuração centralizado de sistemas operacionais, aplicativos e configurações dos usuários em um ambiente contendo *Active Directory*. Uma Diretiva de Grupo controla em parte as atividades que os usuários podem ou não fazer em um sistema de computadores (MICROSOFT, 2018).

As configurações de Diretiva de Grupo estão contidas em um Objeto de Diretiva de Grupo. Um GPO pode representar as configurações de diretiva do sistema

de arquivos e no *Active Directory*. As configurações de GPO são avaliadas pelos clientes usando a natureza hierárquica do *Active Directory*. Sua estrutura é proveniente de quatro itens, sendo: (i) caminho do sistema de arquivos do computador, (ii) caminho do serviço de diretório do computador, (iii) caminho do sistema de arquivos do usuário e (iv) caminho do serviço de diretório do usuário (MICROSOFT, 2018).

A configuração de diretivas de grupo podem ser realizados em ambientes empresariais ou residenciais e também de maneira independente, porém, é altamente recomendado que se faça em ambientes contendo *Active Directory*, devido à como podem ser utilizadas quando nesse ambiente. Geralmente é usada para restringir determinadas ações que representem potenciais riscos de segurança, como por exemplo bloquear acesso ao gerenciador de tarefas, restringir acesso a determinadas pastas, desabilitar download de arquivos executáveis, e assim por diante, e, por conter esse modelo, onde há uma organização com AD DS será mais eficaz sua implementação.

2.3 SSO

Single Sign-On é um processo de autenticação em sessão, que permite ao utilizador inserir suas credenciais de acesso apenas uma vez e aceder a múltiplas aplicações protegidas. O processo autentica em todas as aplicações que este tem direito e elimina a necessidade de se autenticar novamente ao mudar de aplicações durante sua sessão, deste modo, toda autenticação será centralizada. As infraestruturas de autenticação já são populares em sistemas de computadores, principalmente nos de grande escala. Nesse cenário, não é eficiente visando os pontos de implementação e administração, separar para cada sistema de computador, recursos e servidores um método de autenticação (ESTANQUEIRO, 2010).

Quando refere-se a configuração do *Single Sign-On* (SSO), que é independente de qualquer software, será utilizado uma autenticação de credencial única. Seu conceito não é novo e existem muitas soluções que são utilizadas por empresas. SSO ganha destaque com a LGPD (Lei Geral de Proteção de Dados) entrando em vigor, lei que dispõe do tratamento de dados e de pessoas naturais (Lei 13.709/18), por meio físico ou digital buscando o reconhecimento da finalidade da tutela desses dados ou informações para a proteção de seus direitos, como liberdade de expressão e comunicação, honra, privacidade, imagem autodeterminação informativa e livre desenvolvimento de personalidade. A lei protege situações que vão dizer respeito exclusivamente à operações de tratamento de dados, ou seja, "dos que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle, modificação, comunicação, transferência, difusão ou extração" (art; 5º, X)" (MULHOLLAND, 2018). Com essa obrigatoriedade de regulamentação no ambiente empresarial, buscas por implementação de SSO vem em uma crescente.

O SSO é recorrentemente referido como o Santo Graal da autenticação e autorização na indústria de segurança e tecnologia. Isto ocorre pelos grandes benefícios que ele tem a oferecer para as empresas, através da grande economia em gastos e mitigação nos riscos à segurança. Já para o usuário são benefícios um pouco

mais óbvios, pois com implementação correta, eles vão precisar usar apenas um par de credenciais para todos os sistemas da empresa, salvando muito tempo que se é perdido em casos de esquecimento de usuários ou senhas (IVANOVA; VODANOVICH, 2017).

Quanto a suas arquiteturas, o *Single Sign-On* também possui mais de um tipo de implementação, os seguintes itens detalham as suas arquiteturas:

- **Pseudo SSO**, trata-se de uma aproximação entre suporte-utilizador, onde fornece a gestão de suas credenciais, assim, o utilizador pode guardar suas credenciais e informações em um ficheiro encriptado ou uma base de dados segura com uma chave mestre.
- **SSO Centralizado**, como o nome indica, é ter a centralização da autenticação e da base de utilizadores, tal sistema tem que ter uma relação de confiança com cada servidor de aplicação. Pode ser baseado em *Tokens* ou PKI (*Public Key Infrastructure*).
- **SSO Federado**, por sua vez, são limitados a uma organização ou domínio. Para estabelecer uma confiança entre diferentes domínios, são necessárias Federações. Ou seja, seu objetivo é um sistema em que as credenciais sejam provenientes de seu domínio. São estruturados em Círculo de confiança, *Identity Provider* (IdP) e *Identity Federation* (IdF).

O SSO simplificou a maneira de como os usuários interagem e realizam acesso a seus aplicativos, com ele os usuários podem economizar tempo, acessando seus aplicativos VDI (*Virtual Desktop Infrastructure),* corporativos, Web e SaaS (*Software as a Service*) como se fossem compartilhamentos de arquivos de rede, simples e com apenas um conjunto de credenciais (CITRIX, 2020).

3 TRABALHOS RELACIONADOS

O objetivo do trabalho que está sendo desenvolvido é analisar e comprovar que com a correta implementação de um conjunto de tecnologias, a segurança dos dados em um ambiente empresarial pode ser elevada, com mais controle e facilidade. Portanto, a presente seção irá avaliar os estudos efetuados com ferramentas e ambientes relacionados à segurança, com o objetivo de verificar quais os pontos relevantes à serem analisados e levados em consideração ao aplicar em diferentes ambientes e resultados obtidos.

Gestão De Segurança Da Informação E Utilização De Firewalls Em Empresas Da Indústria Têxtil (JÚNIOR; JÚNIOR; LIMA, 2019): As tecnologias de segurança além de protegerem dados e conferirem sigilo, são importantes para manter a reputação das empresas, a proposta apresentada em seu trabalho tem seu foco na gestão de segurança da informação em ambientes empresariais, por meio da implementação de um *firewall*, que é um equipamento que vem sendo usado em larga escala (JÚNIOR; JÚNIOR; LIMA, 2019). O papel do *firewall* é de gestão e segurança de redes, ele protege contra muitos tipos diferentes de ameaças. Com ele é possível gerenciar o uso de algumas ferramentas como o *Single Sign-On*, efetuar configurações de VLANs, rotas e demais configurações de rede. Ficou demonstrado que é de grande uso em ambientes empresariais, onde quase todos optam por fazer

implementações de segurança, porém, foi apenas coletado o resultado de *firewalls* nas empresas, não de mais ferramentas, foco onde a pesquisa que estou desenvolvendo irá se aplicar.

Information security policy compliance model in organizations (SAFA; SOLMS; FURNELL, 2016): A Internet e a tecnologia da informação influenciam a vida humana significativamente, entretanto a segurança da informação é uma importante preocupação tanto para usuários quanto para suas empresas/organizações, pois ela não pode apenas garantir um lugar seguro para a informação; os aspectos humanos da segurança da informação devem ser levados em consideração. A falta de conscientização sobre segurança da informação, ignorância, negligência e a resistência é a raiz dos erros dos usuários (SAFA; SOLMS; FURNELL, 2016). Nessa pesquisa, um novo modelo demonstra como o cumprimento das políticas de segurança da informação organizacionais moldam e mitigam o risco do comportamento de seus empregados, utilizando da conceituação de diferentes aspectos como compartilhamento do conhecimento de segurança da informação, colaboração, intervenção e experiência. Observando os resultados, através da análise de dados, nota-se que os aspectos são grandes influenciadores perante a atitude dos funcionários em relação a conformidade com as políticas de segurança adotadas.

ADFS authentication for healthcare system (PENGSART et al., 2017): No modelo de funcionamento atual dos hospitais, são utilizadas aplicações para acessar os dados de saúde do paciente, portanto, o custo para o controle de identidade dos usuários aumenta conforme o número de aplicações vem aumentando. A frustração em lembrar múltiplas combinações de usuário e senha é um empecilho para os funcionários dos hospitais, o que pode acarretar em uma baixa na produtividade do trabalho e lentidão aos serviços nos hospitais. Além disso, dados dos pacientes estão passíveis a fraude devido a vulnerabilidade e a insegurança do sistema de autenticação, dificuldade em compartilhamento de dados e recursos entre os departamentos e a rede hospitalar (PENGSART et al., 2017). Analisado o cenário, foi proposto o *Active Directory Federation System* (ADFS), uma das funcionalidades do *Active Directory*, o qual se trata de um método de *Single Sign-On* e um serviço de federação de identificação, é um protótipo que utiliza de um *framework* do ADFS para que seja possível ao usuário efetuar um login único e seguro. Usuários podem acessar todas as aplicações disponíveis, assim como torna fácil a identificação entre os sistemas de saúde, aumentando a segurança dos usuários e reduzindo os custos citados anteriormente. Outro benefício está ligado a manter os dados do paciente e do usuário protegidos e seguramente compartilhados através dos sistemas hospitalares.

Implementation of Indirect Single Sign-On Approach to Integrate Web-Based Applications (KRIDALUKMANA; SATOTO, 2014): O gerenciamento da credencial do usuário é um ponto crítico na organização que tem um ambiente de ilha de aplicação, como na Universidade de Diponegoro. Ao realizar a pesquisa e aplicação do objetivo, os usuários tiveram o auxílio de manter apenas um par de credenciais para login em suas aplicações. Não alterar a função de login de cada aplicação é o limite definido ao gerenciar credenciais, devido a essa motivação, a abordagem utilizada é a de um *Single Sign-On* (SSO) indireto enquanto as aplicações foram integradas utilizando de um modelo baseado em ambiente *web*. Utilizando de um *framework* do *CodeIgniter*, foi desenvolvido um portal de SSO para lidar com o

login das aplicações disponíveis na universidade. Como resultado, foi descoberto que usando essa aproximação indireta, quase todas as variáveis de sessão do domínio secundário podem funcionar bem através da aplicação do domínio primário (KRIDALUKMANA; SATOTO, 2014). Ou seja, foi efetuada uma relação de confiança de domínios, funcionalidade do *Active Directory* para integrar todas as aplicações do ambiente em que foi elaborada a pesquisa, porém, utilizou-se de uma parte de desenvolvimento de um portal para o gerenciamento do SSO e organização.

Towards the Trust-Enhancements of Single Sign-On Services (BAO et al., 2019): O *Single Sign-On* (SSO) se tornou muito popular em termos de gerenciamento de identidade e em infraestrutura de autenticação na Internet. Um usuário recebe um *ticket* de SSO depois de ser autenticado pelo *Identity Provider* (IdP), e esse *ticket* permite que ele faça seu logon. Entretanto, existem vulnerabilidades que permitem que os atacantes intermedeiem um desses *ticket* e então possam realizar logon em qualquer sistema se passando por um usuário. Enquanto muitos incidentes das autoridades de certificação também indicam que os serviços confiáveis de terceiros não são tão confiáveis quanto o esperado e podem sofrer um ataque de *man-in-the-middle*. Essa pesquisa investiga as estratégias de defesa desses certificados de serviços de confiança reforçada e tentativas de aplicar essas estratégias no serviço de SSO, analisando que há alguns *designs* de segurança que são comumente utilizados nos serviços de autenticação com SSO e também nos sem SSO. Ainda na pesquisa de (BAO et al., 2019), são analisadas as seguintes estratégias de defesa dos certificados de serviço com aprimoramento de confiança:

- ***Pinning*:** As chaves públicas são mantidas localmente pelos clientes, os certificados não-combinatórios são detectados e rejeitados.
- ***Public Logging*:** Todos os certificados são necessários ficarem publicamente visíveis, então qualquer fraudulento será detectado pelo domínio.
- ***Restricted scopes of services*:** Os certificados são restritos para servir apenas a alguns escopos do domínio e as regras são reforçadas pelos navegadores, então um certificado que esteja violando regras irá ativar avisos do navegador.
- ***Multi-path verification*:** Um servidor certificado recebe, compara com outras cópias recebidas de diferentes caminhos e então aceita somente se forem idênticos.
- ***Subject-controlled policies*:** É definido algumas políticas específicas para o certificado, caso esteja violando alguma delas será considerado inválido ou suspeito.
- ***Multi-authority certification*:** Quando o certificado é confirmado e assinado por múltiplas autoridades de certificação então uma autoridade comprometida não é permitida para avaliar por si própria.

4 DISCUSSÃO

Analisando os trabalhos relacionados citados anteriormente, observa-se que todos tem seu foco em alguma parte da área de segurança da informação, utilizando de diferentes métodos de pesquisa, abordagem e meios de analisar seus dados para chegar a uma conclusão. Pode-se perceber que são em grande parte focados na implementação de *Single Sign-On* em ambientes diversificados e diferentes

abordagens. É um desafio da área o desenvolvimento de soluções que possam englobar as diferentes tecnologias e abordagens de segurança da informação, formando um modelo melhorado com foco no ambiente empresarial. Nota-se uma grande deficiência em pesquisas voltadas para a implementação de um grupo de ferramentas e tecnologias de segurança da informação, então o foco de trabalhos para a expansão e melhoria da área é a utilização de um conjunto de técnicas em prol de uma melhoria da segurança de sistemas empresariais.

Um grande desafio que se percebe é a integração de diversas ferramentas, como existe uma gama de ferramentas por muitas vezes não se sabe corretamente o que aplicar e em qual ambiente é o mais favorável, pois busca-se sempre a simplificação para os usuários e a complexidade para a segurança. O *Single Sign-On* já se provou ser a chave para o sucesso em grande parte dos casos, devido sua flexibilidade de compatibilidades e funcionalidade, sendo assim, deve ser feito como um próximo passo um *Proof of Concept* (PoC), termo que é utilizado para quando será feita a comprovação de algo que foi estabelecido por pesquisa ou artigo técnico, cunho cujo se encaixa perfeitamente para essa pesquisa.

Uma grande questão que pode ser debatida a respeito desse assunto é a de como, no modelo atual, demonstrar que o empreendedor realmente está vulnerável e necessita dessas ferramentas ao seu lado. Apesar de ser considerado indispensável pelos que estão por dentro do assunto, é comumente verificado que empresas, principalmente MPME's estão desprotegidas e extremamente vulneráveis à ataques cibernéticos. Falta de instrução, hardware e qualificação são alguns dos principais pontos que podem ser observados e considera-se uma boa prática para sua mitigação, principalmente a informação. Informação a respeito do que pode acontecer, de como agir, como prevenir. Consequentemente será necessário colocar um investimento na empresa, em cima de firewalls, técnicos de TI entre outras necessidades do ambiente, para que se resolvam os problemas que antes não se acreditavam existir.

5 CONCLUSÃO

Através desse artigo realizamos o estudo de Estados da Arte para ferramentas de segurança de dados e como elas podem trazer melhorias para o ambiente empresarial, juntamente com uma pesquisa de trabalhos relacionados que proporcionam uma visão com maior peso analítico sobre o assunto. Possibilitando uma discussão sobre as ferramentas e o tema apontado, assim como o vislumbre de possíveis dificuldades e problemas além de maneiras e estratégias para que se seja possível ter uma mitigação dos mesmos.

REFERÊNCIAS BIBLIOGRÁFICAS

BAO, X. et al. *Towards the trust-enhancements of single sign-on services*. In: IEEE.2019IEEE *Conference on Dependable and Secure Computing* (DSC). [S.l.], 2019. p. 1–8.

CITRIX. O que é logon único (SSO)? 2020. Disponível em: (https://www.citrix.com/pt-br/glossary/what-is-single-sign-on-sso.html). Acessado em: 2020-05-03.

ESTANQUEIRO, F. W. T. *Single sign-on* na FCUL. Tese (Doutorado) — Universidade de Lisboa, 2010.

FONTES, E. L. G.Segurança da informação. [S.l.]: Editora Saraiva, 2017.

IVANOVA, A. I.; VODANOVICH, S. Single sign-on taxonomy. In: *2017 IEEE 21st International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. [S.l.: s.n.], 2017. p. 151–155.

JÚNIOR, C.A. de S.; JÚNIOR, E. C. B.; LIMA, A. S. Gestão de segurança da informação e utilização de firewalls em empresas da indústria têxtil. *Revista Eletrônica ACTA SAPIENTIA*, v. 6, n. 1, p. 25, 2019.

KRIDALUKMANA, R.; SATOTO, K. I. Implementation of indirect single sign-onapproach to integrate web-based applications.International Journal of Computer ScienceIssues (IJCSI), *International Journal of Computer Science Issues* (IJCSI), v. 11, n. 3,p. 21, 2014..

MICROSOFT. *Active Directory Domain Services Overview*. 2017. Disponível em: (https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview). Acessado em: 2020-05-03.

MICROSOFT. *Group Policy Objects*. 2018. Disponível em: (https://docs.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-objects). Acessado em:2020-05-03.

MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, v. 19, n. 3, p. 159–180, 2018.

PENGSART, P. et al. Adfs authentication for healthcare system. In: IEEE. *2017 2nd International Conference on Information Technology (INCIT)*. [S.l.], 2017. p. 1–6.

RIBEIRO, R. et al. Cibersegurança e segurança da informação contábil: Uma análise da percepção do profissional contábil. *RAGC*, v. 8, n. 32, 2020.

SAFA, N. S.; SOLMS, R. V.; FURNELL, S. Information security policy compliance model in organizations. *computers & security*, Elsevier, v. 56, p. 70–82, 2016.

STANEK, W. *Windows Server 2008 inside out*. [S.l.]: Pearson Education, 2008.

STEFANOVIC, V.; KRANJAC, S. *Identity with Windows Server 2016: Microsoft 70-742 MCSA Exam Guide: Deploy, configure, and troubleshoot identity services and Group Policy in Windows Server 2016*. [S.l.]: Packt Publishing Ltd, 2019.

TERRA. *Segurança digital: 40% das empresas brasileiras não tem políticas de cibersegurança.* 2020. Disponível em: (https://www.shorturl.at/fqGMP). Acessado em: 2020-06-14.