SERVIDOR DE DIRETÓRIO COMO AUXILIAR NA GESTÃO DAS INFORMAÇÕES, USUÁRIOS E COMPUTADORES

Andre Hoffmann*

Fabiano Wonzoski**

Lilian Jeannette Meyer Riveros***

Resumo

Esta pesquisa apresenta como um serviço de diretório juntamente com outros recursos, pode beneficiar organizações fornecendo uma forma prática de gerenciar computadores e usuários, além de fornecer permissões adequadas a cada um , garantindo maior segurança e controle perante os administradores da rede. O serviço de diretório funciona como um banco de dados contendo informações das contas dos usuários, e tais usuários só poderão conectar em uma rede interna e acessar pastas compartilhadas. O estudo exibe uma introdução aos serviços de diretório, o que são, como funcionam e como podem auxiliar na segurança dos dados, apresentando algumas ferramentas pagas e gratuitas aos sistemas operacionais Windows e Linux, para o gerenciamento dos diretórios. Serão demostradas formas de integração entre vários sistemas com diferentes funções e objetivos, juntamente com o banco de dados do diretório, como um modo de utilizar as mesmas informações para gerenciar os usuários, permissões e objetos no sistema integrado. Aborda-se assim, benefícios para a organização, na segurança, centralização e controle dos usuários, entre outras funcionalidades essenciais para a gestão da rede.

Palavras-chaves: Serviço de diretório. Gestão de usuários. Administração da rede. Segurança de redes.

1 INTRODUÇÃO

Observa-se nos dias de hoje que a segurança da informação é um quesito fundamental para qualquer empresa ou rede doméstica, seja ela pequena ou com centenas de computadores, e um ponto fundamental para garantir a segurança e a administração de uma rede, é ter um sistema ou serviço de diretório. Os sistemas de diretório armazenam informações sobre pessoas, objetos, ou qualquer matéria que possa ser catalogada em um banco de dados, e que permita consulta a qualquer momento. Porém a consulta das informações de um banco de dados de diretório pode ser controlada de várias formas e com várias ferramentas distintas, que garantem a segurança da informação (SILVA, 2015).

O principal objetivo do trabalho é demostrar como um serviço ou sistema de diretório pode beneficiar e trazer o básico de segurança para dentro de uma organização, mantendo os usuários e suas devidas informações seguras e confidenciais. Também espera-se demonstrar as vantagens, desvantagens e dificuldades em ter um ou não ter um sistema de diretórios em uma organização.

Para alcançar esse objetivo, serão analisados dois ambientes de duas organizações distintas, uma do ramo financeiro e outra do ramo supermercadista. Apesar de serem ramos completamente diferentes, os dois ambientes possuem uma grande estrutura de rede, e consequentemente vários computadores e usuários. O diferencial é que uma delas possui sistema de diretório para administrar todas as informações referentes aos usuários e a outra não.

Espera-se com este estudo passar todo o conhecimento absorvido e confirmar a importância da segurança da informação, e dos serviços de diretório.

2 **DESENVOLVIMENTO**

2.1 SEGURANÇA DA INFORMAÇÃO

A segurança hoje em dia é fundamental em qualquer empresa, seja ela do ramo que for. Existem muitas formas de se proteger dos crimes virtuais do qual as empresas podem ser vítimas, e uma delas, talvez uma das mais importantes seja ter um serviço de diretório na organização. Segundo Passos (2016), o Active Directory, além de muitos outros serviços, permite impor uma série de restrições aos usuários da rede, além de ter um ponto central para a gestão dos usuários.

Conforme Pereira (2016) existem três elementos que garantem a segurança da informação:

•Disponibilidade: essa é a garantia de que todas as informações estarão disponíveis, a todo e qualquer momento, par que usuários autorizados possam acessá-las.

•Confidencialidade: a confidencialidade está ligada ao sigilo das informações. Isso significa estabelecer níveis de acesso a determinadas informações, ou seja, restringi-las e disponibilizá-las somente aos usuários devidamente autorizados (seja do ponto de vista hierárquico, seja do ponto que for estabelecido nas políticas de segurança).

•Integridade: a integridade nada mais é que assegurar que as informações estarão disponibilizadas na mesma forma que foi salva. Mais precisamente, esse fundamento trata da proteção de dados, para que as informações não sejam violadas ou modificadas acidentalmente.

O controle dos usuários dentro da empresa é muito importante para garantir os três elementos citados acima, pois vários problemas com vírus, roubo, ou vazamento de informações acontecem por falta de controle interno dos acessos. Para Donda (2012), 70% dos ataques partem de usuários

legítimos do sistema, ou seja, são usuários internos, que trabalham na própria organização, porém com a intenção de fazer um ataque.

2.2 SERVIÇO DE DIRETÓRIO

Quando os computadores passaram a se comunicar uns com os outros através da rede, viu se a necessidade de intensificar a segurança dos computadores, para que os dados presentes neles não fossem perdidos ou acessados sem autorização. Silva (2015) afirma que foi a partir dessa ideia de controle de acesso a informações que várias corporações que primam por segurança da informação desenvolveram sistemas para controlar esse acesso, e entre esses sistemas está o sistema de serviço de diretório.

O Serviço de diretório é um conjunto de atributos sobre recursos e serviços existentes na rede, como por exemplo, usuários, computadores, impressoras, servidores entre outros recursos de rede. Isso significa que é uma maneira de organizar e simplificar o acesso aos recursos que estão disponíveis na rede centralizando-os, e os tornado mais seguros e protegidos (LOSANO, 2003).

Para entender bem o que é um serviço de diretório, pode-se citar o exemplo de uma agenda. Nela são organizadas todas as tarefas por dias, semanas, meses, e onde são anotados os nomes, datas e dados importantes. Rover (2012) cita que o serviço de diretório tem exatamente o mesmo sentido, o sentido de organizar e principalmente ter um local centralizado para a busca de informações necessárias.

Numa empresa que possua tal serviço hoje, quando é criado um novo usuário, é usado o banco de dados do serviço de diretório (que é como a agenda), para salvar as informações referentes ao nome, sobrenome, endereço, grupo, login e senha que o usuário possui ou irá possuir. Tudo isso ficará disponível nessa base, e poderá ser utilizada por todos os computadores da rede (ROVER, 2012).

Castro e Junior (2008) complementam que um serviço de diretório é uma ferramenta a mais que pode ser usada para complementar à utilização

de outros serviços facilitando manutenção, a busca e a localização de dados por usuários e aplicativos, onde todos os serviços compartilham o mesmo servidor e diretório, e também a mesma árvore de informações.

Seja qual for o tamanho da rede, com poucos, ou com centenas de computadores, um serviço de diretório já pode facilitar muito a vida dos administradores da rede. Imagine uma empresa com apenas dez computadores, e todas elas devem manter os dados de clientes e dos próprios usuários sempre atualizados em diversos aplicativos. Caso não utilizem um serviço de diretório, a manutenção destes teria que ser feita na base de cada aplicativo em cada computador, onde seria difícil dar a garantia de que os dados, em todos eles, ficariam 100% sincronizados (CASTRO e JUNIOR, 2008).

2.3 PROTOCOLO LDAP

Um protocolo Lightweight Directory Acess Protocol (LDAP) ou Protocolo Leve de Acesso a Diretórios, resumidamente é um conjunto de regras que controla a comunicação entre um serviço de diretório e seus clientes. Para Trigo (2003), LDAP é um padrão aberto capaz de facilitar, de forma flexível, o compartilhamento, a manutenção e o gerenciamento de grandes volumes de informações, definindo um método-padrão de acesso e atualização de informações dentro de um diretório.

Para Rouse (2008), o LDAP é um protocolo de software que permite a qualquer pessoa localizar dados como organizações, indivíduos e outros recursos como arquivos e dispositivos em uma rede sejam na internet pública ou em uma intranet corporativa. Tal protocolo é chamado de leve, pois sua versão inicial não incluía muitos recursos de segurança presentes em suas versões anteriores. Porém após sua origem diversas organizações o melhoraram e adicionar os pontos de segurança que faltavam. Rouse (2008) ainda complementa que o protocolo está presente em muitos serviços, tais como o serviço de diretório NetWare, da Novell, em equipamentos de rede desenvolvidos pela Cisco, que suportam o LDAP, e está fortemente presente

em produtos da Microsoft, como o Outlook Express e principalmente no serviço de diretório oferecido pela empresa, o Active Directory. Também está presente em serviços de diretório Open Source, distribuídos livremente pela internet, tais como o Samba e o OpenLdap.

2.4 FERRAMENTAS

Nesta seção serão apresentados alguns serviços de diretórios conhecidos presentes hoje no mercado, além de identificar seus pontos fortes e o que podem fornecer para a segurança da informação.

2.4.1 Active Directory

O Active Directory (AD) é o serviço de diretório disponível para as redes Windows e oferecido pela Microsoft. Rover (2012), afirma que o AD, utilizando como base o LDAP, assumiu a liderança do mercado de serviços de diretório, pelo seu grande desempenho, segurança e disponibilidade.

Esse serviço de diretório é composto por objetos, ou seja, todo recurso presente na rede é representado no AD como um objeto. Tais objetos possuem propriedades, chamadas de atributos dos objetos (LOSANO, 2003).

Muitos confundem o AD com o Controllers Domain (DC) ou Controlador de Domínio. Rover (2012), explica que ambas são completamente diferentes, sendo o DC a parte física e o AD a parte lógica. Os controladores de domínio são os servidores, ou seja, é a estrutura física ou virtualizada, que possui o serviço do Active Directory rodando nela. Podem existir vários DCs espelhados em uma rede para garantir a disponibilidade do serviço de diretório. Assim quando um servidor parar, algum outro poderá assumir a função de autenticador da rede, além de receber as outras solicitações.

A Active Directory possui uma grande e bem dividida estrutura lógica, formada por Florestas, Árvores, Domínios e Unidades Organizacionais (OUs). Duarte (2015) explica cada uma delas:

•Florestas: consiste no agrupamento de uma ou mais árvores de domínios. O primeiro domínio da floresta é chamado de domínio raiz ou root. O nome desse domínio faz referência a floresta.

•Árvores: os domínios agrupados em estrutura hierárquica são chamados de árvores de domínio. Quando você acrescenta um segundo domínio a uma árvore, ele se torna filho do domínio raiz.

•Domínios: Os domínios, são as principais unidades funcionais da estrutura lógica do AD, são um conjunto de objetos definidos de forma administrativa que compartilham um banco de dados de diretórios comum, diretivas de segurança e relações de confiança com outros domínios. Em outras palavras cada domínio possui seu administrador, ou seja, as definições de segurança de um domínio não se aplicam aos outros domínios.

•Unidades Organizacionais ou OUs: são os objetos do AD usados para armazenar e organizar objetos de usuários, grupos, computadores e outras unidades organizacionais. Ou seja, deve-se utilizar as OUs para distribuir de forma uniforme os objetos dentro do Active Directory.

A importância do AD não se caracteriza apenas como um simples autenticador de usuários e de máquinas, mas sim num total e completo serviço que provê recursos desde o marco inicial de uma rede, com a construção de um pequeno domínio, até a criação de um grande servidor com recursos de e-mail, compartilhamento de arquivos e pastas, segurança e controle centralizado de recursos (GUIMARÃES, 2005).

Guimarães (2005), também aponta itens importantes que o Active Directory pode fornecer para uma organização:

•Administração simplificada: organiza recursos hierárquicos, fornecendo um único ponto da administração para todos os objetos, ou seja, centralizando o gerenciamento dos recursos.

•Segurança da informação: o controle de acesso dos usuários pode ser definido para cada objeto do diretório ou seus atributos.

•Políticas administrativas: podem ser criadas várias regras de acesso para determinados usuários e computadores da rede, sem precisar aplicar a regra em cada máquina.

•Escalabilidade: armazena informações organizando o diretório nas seções que permitem o armazenamento de inúmeros objetos.

•Flexibilidade: o sistema de busca é muito flexível para a procura de usuários ou outros itens.

•Replicação: fornece disponibilidade das informações, tolerância a falhas, balanceamento de carga e desempenho.

•Integração com serviços: o AD permite compartilhar suas informações com diversos outros serviços da rede, ou com outros serviços de diretório.

2.4.2 OpenLDAP

O OpenLDAP é uma implementação do LDAP, e surgiu com o objetivo de facilitar o uso do LDAP. Foi desenvolvido pela Universidade de Michigan nos Estados Unidos, porém como é um software livre, cresceu rapidamente, e teve seus problemas corrigidos por desenvolvedores do mundo todo. Para Trigo (2007, p.30), as principais características do OpenLDAP são:

•Suporte a IPv4 e IPv6.

•Controle rígido de acessos.

•Pode-se escolher entre mais de um banco de dados para armazenar as informações.

•Atende a múltiplos bancos de dados simultaneamente.

•Alta performance em múltiplas chamadas.

•Replicação da base de dados, garantindo a disponibilidade do serviço.

Para Junior (2008), o OpenLDAP é um pacote de software que trabalha vinculado com o protocolo LDAP, e que juntos podem oferecer um serviço diretório prático e seguro, com várias funcionalidades como autenticação de usuários e armazenamento de informações, além da facilidade de backup e funcionamento em redes IPv4 e Ipv6. Apesar de ser um software livre, ele é muito completo, e pode ser apresentado como uma alternativa ao Active Directory, que é o serviço pago da Microsoft.

Um ponto importante, é que se pode fazer com que todos os serviços e aplicativos da rede o usem para buscar informações, de forma em que todos compartilhem uma única árvore, e ficando integrados a ele, facilitando muito a administração da rede. Dessa forma tudo será centralizado na rede, e ignora-se o fato de que toda aplicação que exija autenticação do usuário, necessite de um banco de dados separado para armazenar tais informações.

2.5 RESULTADOS

Como mencionado no início, foram analisadas duas organizações presentes na região para entender como funcionam as autenticações dos usuários, a segurança das informações de cada um deles, a centralização das informações e a integração do serviço de diretório com os softwares presentes na rede. Uma emprese será um Supermercado da Região que será chamado de SR, e a outra é uma Instituição Financeira (IF), a qual será chamada de IF.

Primeiramente foi analisada a IF, esta instituição possui em torno de 150 computadores e usuários, divididos entre uma matriz e outros 15 postos de atendimento espalhados na região e em outro estado (Rio Grande do Sul), sem contar outros dois postos que funcionam apenas um dia durante a semana. Todos os computadores estão interligados pela rede, e os servidores ficam presentes na matriz. Além disso, apenas alguns servidores possuem sistema operacional Linux, o restante das máquinas é Windows.

A IF possui o serviço de diretório da Microsoft, o Active Directory, que armazena todas as informações de todos os usuários da rede. Existe um servidor de Domínio principal, que é replicado para outros três (totalizando quatro), ou seja, caso algum servidor de autenticação pare, outros três podem assumir o seu lugar, garantindo plena disponibilidade do serviço de autenticação. Em alguns momentos ocorrem falhas nos servidores, atrasos ou problemas para a replicação das informações, mas nada que possa

atrapalhar a autenticação dos usuários, pois os outros servidores estarão operantes.

Cada pessoa possui seu usuário e uma senha que expira a cada 40 dias e exige uma quantidade mínima de caracteres, além de números e caracteres especiais, por questões de segurança. No AD, são definidas as permissões dos usuários e os grupos nos quais os mesmos pertencem, sendo assim, um usuário só conseguirá acessar computadores e pastas compartilhadas do seu próprio posto de atendimento, impedindo que ele veja arquivos de outras unidades. Isso serve para todos os postos e para a matriz. Apenas o setor de TI possui um grupo especifico que garante o acesso a todos os computadores e pastas de toda a rede para prover suporte. Também existe um usuário Administrador que somente o gerente de TI possui, usado para alguns acessos que somente ele deve possuir.

Existem alguns problemas com autenticações na rede, principalmente para usuários dos postos do Rio Grande do Sul, pois como a distância é grande, existe muita latência e perca de pacotes na rede, e devido a essas instabilidades, em determinadas ocasiões os usuários não conseguem acessar algumas máquinas na rede, porque seu usuário não obtém a autenticação no servidor de domínio que fica na matriz. Porém isso acontece em casos raros, e normalmente reiniciando a máquina o problema já é corrigido.

Além da autenticação dos usuários nas máquinas, o AD também compartilha seu banco de dados com outras funcionalidades presentes na rede. O servidor de e-mail da IF utiliza da base do AD para autenticar a conta do usuário. Quando é criado o usuário de um novo funcionário por exemplo, no próprio Active Directory, já é vinculado seu e-mail, então o usuário passa a ter o mesmo usuário e senha do computador para acessar seu e-mail interno.

Outro serviço disponível para todos os usuários e que compartilha da base do AD é o OpenFire juntamente com o Spark, que é um mensageiro interno, para que todos os usuários possam conversas enviar arquivos, sem precisar, ligar ou usar o e-mail toda hora. O Spark é o mensageiro em si,

porém ele precisa de um servidor, que no caso é o OpenFire, e é ele que busca as informações no AD para automaticamente criar o acesso do usuário no mensageiro. Para que o acesso funcione, é necessário que o usuário esteja presente em um grupo lá no Active Directory. Como cada posto de atendimento possui um grupo diferenciado, os contatos no Spark também irão aparecer separadamente, facilitando ainda mais a busca pelo contato desejado.

Além do e-mail e do mensageiro, ainda existe outro sistema presente na IF que também busca as informações dos usuários no AD. Porém não é 100% automatizado, ainda deve-se acessar o sistema, adicionar o usuário e suas permissões, feito isso, o sistema busca o usuário no AD e cria seu acesso com a mesma senha que o usuário utiliza para acessar o computador.

Em muitos casos, ocorrem erros dizendo que o nome do usuário ou a senha estão incorretos, tanto para acessar o computador, quando para o Spark, E-mail ou o sistema. Para solucionar isso, deve-se encontrar o usuário da pessoa no AD e redefinir a senha dela para um padrão, que deverá obrigatoriamente ser alterada no próximo acesso ao computador. Feito isso tudo será novamente acessado sem maiores problemas, porém ainda não se sabe porque esse problema ocorre na IF.

Após essa análise na instituição financeira, foi feita a análise em uma rede de supermercados presente na região. O SR (como será chamada a organização), não possui nenhum serviço de diretório na rede, e é de porte um pouco menor, possuindo em torno de 100 computadores e usuários.

Nenhuma informação referente a usuários é centralizada em algum servidor. A um tempo atrás era usado apenas um usuário para login em cada filial, que ao todo são quatro. Depois de algum tempo isso foi ajustado para um usuário para cada setor, por exemplo, um usuário caixa, um deposito, outro retaguarda e assim por diante. Além disso, poucos usuários possuem senhas.

Existem muitos problemas referentes a esses usuários, pois todo mundo sabe e tem acesso a todas as máquinas da empresa, e como todos tem essa liberdade, não existe segurança na informação de quem usa o

computador, pois qualquer um pode acessar e pegar ou apagar arquivos que não devem. O principal problema encontrado é de arquivos que são apagados indevidamente por outros usuários.

Como não existem serviços de diretório, os usuários devem ser criados localmente nas máquinas. Sempre que um computador é formatado, ou é novo, por exemplo, deve ser criado o usuário referente ao setor que aquele computador ficará. Dessa forma quando o usuário utilizá-lo o usuário já estará criado. Caso ocorra algum problema com um acesso também, como por exemplo, uma senha bloqueada, o suporte deverá entrar com uma conta de administrador naquele computador, e redefinir a senha localmente para o usuário. Se acontecer esse problema em todas as máquinas da rede, esse processo deverá ser feito em todas elas.

Existe um servidor de arquivos na rede, que de início era apenas para compartilhar fotos e vídeos de palestras ou confraternizações com todos. Porém após um tempo, todos começaram a guardar informações importantes nele, e usá-lo como um backup pessoal de arquivos. O problema, é que nele possuíam várias informações que só Diretores e gerentes podem ter acesso, inclusive informações de folhas de pagamento dos funcionários, mas todo mundo que utiliza um computador e com qualquer usuário, teria acesso a todas essas informações. Por padrão, quando algum computador era formatado, ou era criado um novo usuário, já era mapeada a pasta do servidor de arquivos para todos os usuários da máquina, sem restrições. Em muitos casos, arquivos importantes presentes no servidor eram apagados de forma indevida.

Nenhum software, objeto, serviço ou funcionalidade presente na rede do SR, pode compartilhar informações de usuários de alguma base, pois não há serviços de diretórios presentes. Existem vários softwares, como por exemplo, sistema de consultas de cheques e CPF, o sistema de folha de pagamentos e o sistema contábil/fiscal que era separado do ERP utilizado, e o próprio ERP, além de outros sistemas presentes na rede, poderiam utilizar da base de um serviço como, por exemplo, o AD, para autenticar os

usuários, onde cada um poderia ter seu próprio usuário para todos os sistemas.

Quem utilizava de todos esses softwares, principalmente o setor administrativo, possui um usuário e senha para cada um deles, causando muitos problemas de perca de senhas ou bloqueio das mesmas por digitar várias vezes a senha errada confundindo com outro sistema, e isso ocorre com muita frequência. Em alguns casos ainda existe no próprio ERP um usuário apenas para todo o setor, por exemplo o deposito, possui um usuário deposito, onde todos tem acesso a todas as funcionalidades disponíveis para aquele usuário. O principal problema que ocorre no SR, é que quando ocorrem erros em algum processo que os usuários do depósito fizeram, ninguém sabe identificar qual usuário cometeu o erro.

3 **CONCLUSÃO**

Diante das análises apresentadas, pode-se notar que um serviço de diretório, seja ele qual for, é de suma importância para qualquer organização, seja ela com poucos computadores e usuários, ou com milhares deles. Os serviços de diretórios facilitam muito o processo de gestão da rede e controle dos acessos, possibilitando que tudo seja administrado de um único lugar e de uma única base, sem precisar passar por várias máquinas ou sistemas ajustando usuário por usuário. Além disso, a base do serviço pode ser replicada para garantir sua disponibilidade, e a autenticação de todos os usuários da rede, sem perder suas informações.

Com tal serviço rodando na rede, se obtém a garantia da segurança das informações de cada usuário, sem nos preocupar com arquivos deletados, ou até mesmo roubados por outras pessoas com más intenções na rede. O uso adequado de uma ferramenta como essa é indispensável, e pode trazer inúmeros benefícios para quem possuí uma rede para administrar.

Nota-se também a dificuldade para o controle e administração dos usuários nas empresas que não possuem um serviço de diretório. A falta de

segurança é completamente visível, pois nenhuma informação é armazenada de forma segura sabendo que vários usuários possuem o mesmo acesso as mesmas máquinas. Os problemas com senhas são mais corriqueiros, e não existe integração entre os sistemas da empresa e o serviço de diretório, exigindo que cada pessoa possua vários usuários e senhas de acesso.

Analisando os resultados pode-se ter uma noção de como é feito o controle dos usuários e acessos com e sem um serviço de diretório. As facilidades e dificuldades estão bem visíveis nas duas organizações. Além disso, a segurança da informação presente na instituição financeira é muito mais completa e confiável.

REFERÊNCIAS

CASTRO, Mário César de; JUNIOR, Jaime Ribeiro. Protocolo LDAP I: Acesso Remoto a Diretórios em Redes de Dados. Teleco Inteligência em Telecomunicações. 2008. Disponível em <http://www.teleco.com.br/tutoriais/tutorialldap1/default.asp>. Acesso em 27 nov. 2016.

DONDA, Daniel. Segurança no Active Directory. Quest Community. 2016. Disponível em: <https://www.quest.com/community/b/pt/posts/seguranca-no-active-directory> Acesso em 7 jan. 2017.

DUARTE, Leonardo. O que é Active Directory ?. Como aprender Windows. 2015. Disponível em: <http://comoaprenderwindows.com.br/active-directory/o-que-e-active-directory/>. Acesso em 7 jan. 2017.

GUIMARÃES, Nilton Sango. Active Directory – Serviço de Diretório em Redes Corporativas. Linha de código. 2005. Disponível em <http://www.linhadecodigo.com.br/artigo/1631/active-directory-servico-de-diretorio-em-redes-corporativas.aspx>. Acesso em 26 nov. 2016.

JUNIOR, Jaime Ribeiro. OpenLDAP: a chabe é a centralização. Viva o Linux. 2008. Disponível em: < https://www.vivaolinux.com.br/artigo/OpenLDAP-a-chave-e-a-centralizacao?pagina=1 > Acesso em: 10 dez. 2016.

LOSANO, Monique. Introdução ao Active Directory – Parte 1. Technet Microsoft. 2003. Disponível em <https://technet.microsoft.com/pt-br/library/cc668412.aspx>. Acesso em: 27 nov. 2016.

PASSOS, Eduardo. Dicas de segurança para sua empresa. Infobusiness. 2016. Disponível em <http://infob.com.br/dicas-de-seguranca-para-sua-empresa/> Acesso em: 10 dez. 2016

PEREIRA, Alisson Alcantara. Entenda o que é Segurança da Informação e reduza riscos na empresa. 2016. Disponível em <https://pt.linkedin.com/pulse/entenda-o-que-%C3%A9-seguran%C3%A7a-da-informa%C3%A7%C3%A3o-e-reduza-riscos-pereira> Acesso em: 7 jan. 2017.

ROUSE, Margaret. LDAP (Lightweight Directory Acess Protocol). 2008. Disponível em < http://searchmobilecomputing.techtarget.com/definition/LDAP> Acesso em 26 nov. 2016.

ROVER, Marinho. O que é Active Directory, topologia física e lógica ?. Technet Microsoft. 2012. Disponível em <https://technet.microsoft.com/pt-br/library/jj206711.aspx>. Acesso em 27 nov. 2016.

SILVA, Leonardo Costa Lima. Um estudo sobre serviços de diretório e ferramentas de segurança da informação. Centro universitário de Brasíli. Brasília, 2015. Disponível em <http://repositorio.uniceub.br/bitstream/235/8153/1/51203326.pdf>. Acesso em: 27 nov. 2016.

TRIGO, Clodonil Honório. OpenLDAP Uma abordagem integrada. 2003. Disponível em <http://www.martinsfontespaulista.com.br/anexos/produtos/capitulos/249318.pdf>. Acesso em 26 nov. 2016.

Sobre o(s) autor(es)
* Graduado do curso de Ciência da computação, da Unoesc Videira. E-mail: andreh998@gmail.com
** Mestre em Ciência e Biotecnologia. Professor titular as Unoesc-Videira. E-mail: fabiano.wonzoski@unoesc.edu.br
*** Mestre em Ciência da Computação pela UFSC. Professora titular da Unoesc Videira. E-mail:lilian.riveros@unoesc.edu.br