UNIVERSIDADE FEDERAL DO PARANÁ

ARMAZENAGEM E COMPARTILHAMENTO DE DADOS E INFORMAÇÕES NA UNIVERSIDADE FEDERAL DO PARANÁ

CURITIBA
2017

PAULO PEREIRA FEITOSA

ARMAZENAGEM E COMPARTILHAMENTO DE DADOS E INFORMAÇÕES NA UNIVERSIDADE FEDERAL DO PARANÁ

Monografia apresentada à disciplina SIN119 - Pesquisa em Informação II, como requisito parcial à conclusão do Curso de Gestão da Informação, Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná.

Orientador: Prof. Dr. Edelvino Razzolini Filho

CURITIBA

2017

DEDICATÓRIA

Ao meu pai, Prof. Dr. Francisco Franco Feitosa Teles (*in memoriam*), não apenas pelo exemplo de retidão e dedicação aos estudos, mas pelas oportunidades, incentivos, e demonstrações extraordinárias de amor durante nossa formação, **sempre** colocando as necessidades de seus filhos acima das dele próprio.

MEMORIA IN AETERNA

Sr.ª Edith Geny Kleina
Prof. Dr. Eldo Monteiro Silva (DBA/UFV)
Prof. Dr. Frank M. Whiting (University of Arizona)
Prof. Dr. Reginaldo Romeiro (DFP/UFV)
Prof. Dr. Walter Bruno Hans Brune (DZO/UFV)
Sr. Yuri Danielewicz (BCC/UFPR)

Mens sibi conscia recti.

AGRADECIMENTOS

A minha esposa Margareth, cujo apoio foi decisivo para meu ingresso, curso e conclusão deste bacharelado. Obrigado por ser minha “melhor metade”, e estar sempre ao meu lado - principalmente nas horas difíceis.

Aos professores Edelvino e Newton, pela orientação, apoio, incentivo, confiança e principalmente pela amizade.

Aos professores Egon, Simão e Rodrigo, pelos ensinamentos, confiança, e incentivo ao término deste trabalho.

Aos amigos Massimo Carlo e Anna Gabriella, pela amizade, companheirismo e pela colaboração na realização deste trabalho.

Ao meu tio Nelson pela apoio e presença incondicionais em minha vida, e demais familiares pela amizade e companheirismo.

Aos usuários da SUINFRA, colegas do CCE, e demais funcionários da UFPR, pela amizade, companheirismo e colaboração recebida durante o desenvolvimento do trabalho.

RESUMO

Respondeu-se a questão de como armazenar e compartilhar dados e informações em uma organização pública de forma segura, eficaz e em acordo com a legislação vigente. A demanda por educação de qualidade exige a implantação do maior número possível de ferramentas e práticas de gestão da informação para atender às necessidades e expectativas do mercado educacional. A importância dos dados é cada vez maior, visto que são um ativo valioso, oneroso e trabalhoso de se administrar, que requerem atenção para atributos como disponibilidade, confidencialidade, integridade e autenticidade. Além das questões técnicas e processuais, existem ainda as normas de legislação a serem seguidas, e no caso específico das instituições federais, o decreto Nº 8.135 de 4 de novembro de 2013 acrescenta a necessidade de utilizar somente meios do governo para o trâmite de dados e informações. No caso específico da UFPR, por falta de planejamento, não havia um sistema centralizado de compartilhamento de arquivos, e sua ausência dificultava a troca de informações digitais através da Instituição, visto que sistemas descentralizados são mais trabalhosos de serem administrados, tem maior dificuldade de atender requisitos de acessibilidade, e geram mais problemas técnicos. Um sistema centralizado de compartilhamento de arquivos traz melhor acessibilidade ao utilizar *login* unificado, oferece maior confiabilidade e segurança e menor custo operacional ao unificar tarefas em um único serviço. O método de pesquisa englobou a caracterização de um ambiente de pesquisa, descrição das práticas e políticas de compartilhamento de dados e informação existentes, identificação das necessidades e competências informacionais dos usuários. Procedeu-se à pesquisa bibliográfica, pesquisa experimental e o estudo do caso para então se propor uma solução baseada nos princípios e conhecimentos de gestão da informação e em acordo com as normas e legislações vigentes. Atingiu-se os objetivos estabelecidos, utilizando conceitos de gestão de informação, tecnologia da informação e comunicação, segurança da informação, normatização e legislação, proporcionando aumento na velocidade de acesso, ganho de segurança física (redundância), lógica (políticas de acesso bem estabelecidas) e legal (notoriamente no que diz respeito ao decreto 8135/2013), além da possibilidade de recuperar informações erroneamente apagadas (a partir de cópias de segurança).

Palavras-chave: Gestão de informação. Armazenagem em nuvem. Compartilhamento de dados.

ABSTRACT

The question of how to store and share data and information in a public organization was answered taking in consideration security, effectiveness and accordance to the current legislation. The demand for quality education requires the implementation of the greatest number of tools and practices of information management possible to meet the needs and expectations of the educational market. The importance of data is increasing, since they are a valuable, expensive and laborious asset to manage, which require attention to attributes such as availability, confidentiality, integrity and authenticity. In addition to technical and procedural issues, there are still legislation norms to be followed, and in the specific case of federal institutions, the Decree No. 8,135, of November 4, 2013, adds the need to use only government resources for the processing of data and information. In the specific case of UFPR, due to a lack of planning, there was no centralized file-sharing system, and this absence made it difficult to exchange digital information through the Institution, since decentralized systems are more troublesome to manage, have greater difficulty in achieving accessibility requirements, and generate more technical problems. A centralized file-sharing system provides better accessibility by using unified login, provides greater reliability and security, and lower operational cost by unifying tasks into a single service. The research method involved the characterization of a research environment, the description of existing data and information sharing practices and policies, and the identification of users' informational needs and competences. Bibliographic research, experimental research and case study were carried out to propose a solution based on the principles and knowledge of information management, and in accordance with the current norms and laws. The established goals were achieved, using concepts of information management, information technology and communication, information security, standardization and legislation, increasing access speed, gaining security in the physical (redundancy), logic (well-established access policies) and legal aspects (notoriously with respect to the Decree 8135/2013), and the possibility of retrieving erroneously deleted information (from backup copies).

Key words: Information management. Cloud storage. Data sharing.

LISTA DE QUADROS E FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas
ACS - Assessoria de Comunicação Social
Bit - Dígito binário, menor parcela de informação processada por um computador
Byte - Conjunto de oito *bits* que forma a unidade de informação
BVIT - *Business Value of Information Technology* (Valor de negócio da tecnologia da informação)
CCE - Centro de Computação Eletrônica
COPLAD - Conselho de Planejamento e Administração da UFPR
CPU - *Central Processing Unit*, Unidade de Processamento Central
DAU - Divisão de Apoio ao Usuário
DOS - *Denial of Service* (Negação de Serviço)
DSG - Depósito de Serviços Gerais
DSS - Divisão de Suporte e Serviços
IFES - Instituições de Ensino Superior
FTP - *File Transfer Protocol* (Protocolo de Transferência de Arquivos)
FTPS - *File Transfer Protocol Secure* (Protocolo de Transferência de Arquivos Seguro)
Gb - *Gigabit*, 10^9 *bits*
GB - *Gigabyte*, unidade de espaço, correspondente a 10^9 *bytes*
Gbps - *Gigabits* por segundo, unidade de velocidade de transmissão correspondente a 10^9 *bits* por segundo
GI - Gestão da Informação
GNU - *GNU is Not Unix* (GNU não é Unix)
HTTP - *Hyper Text Transfer Protocol* (Protocolo de Transferência de Hiper Texto)
HTTPS - *Hyper Text Transfer Protocol Secure* (Protocolo de Transferência de Hiper Texto Seguro)
LDAP - *Lightweight Directory Access Protocol* (Protocolo Leve de Acesso a Diretórios)
LPM - Licença Pública de Marca
LTS - *Long Time Support* (Suporte de Longo Prazo)

Mb - *Megabit*, 10^6 *bits*

MB - *Megabyte*, unidade de espaço, correspondente a 10^6 *bytes*

Mbps - *Megabits* por segundo, unidade de velocidade de transmissão correspondente a 10^6 *bits* por segundo

PCU - Prefeitura do Campus Universitário

PRAE - Pró-reitoria de Assuntos Estudantis

PSI - Política de Segurança da Informação

RAM - *Random Access Memory*, Memória de Acesso Randômico

SI - Segurança da Informação

SO - Sistema Operacional

SMB - *Server Message Block* (Bloco de Mensagens de Servidor)

SSH - *Secure Shell* (Cápsula Segura)

SUINFRA - Superintendência de Infraestrutura (da UFPR)

TI - Tecnologia da Informação

TIC - Tecnologia de Informação e Comunicação

TPA - *Third party auditor* (auditor terceirizado)

UFPR - Universidade Federal do Paraná

VPN - *Virtual Private Network* (Rede Privada Virtual)

ZFS - *Zeta File System* (Sistema de Arquivos Zeta)

SUMÁRIO

1. INTRODUÇÃO

No atual momento que vive nossa sociedade, a demanda por educação de qualidade exige a implantação do maior número possível de ferramentas e práticas de gestão para atender às necessidades e expectativas do mercado educacional. “A gestão da informação é a ferramenta que amplia a competitividade organizacional” (RAZZOLINI FILHO; DO NASCIMENTO, 2011, p. 29). Visando a redução dos custos e o aumento da produtividade, os gestores podem atentar à otimização de processos existentes, de forma a melhor atender as necessidades administrativas e operacionais dentro das instituições.

A importância dos dados e informações é cada vez maior, visto que são um ativo valioso, oneroso e trabalhoso de se administrar. Sua correta armazenagem e compartilhamento requer atenção para atributos como disponibilidade, confidencialidade, integridade e autenticidade.

Além das questões técnicas e processuais, existem ainda normas de legislação a serem seguidas. No caso específico das instituições federais, o decreto Nº 8.135 de 4 de novembro de 2013 acrescenta a necessidade que estas informações permaneçam em redes e computadores do governo, não podendo utilizar-se sistemas comerciais (BRASIL, 2013, p. 2).

1.1 PROBLEMÁTICA

A Universidade Federal do Paraná - UFPR possui cerca de 55.000 usuários diretos de seus sistemas de informação, que o acessam a partir das redes internas e externas à Instituição. Mas, por falta de planejamento, não há um sistema centralizado de compartilhamento de arquivos, e sua ausência dificulta a troca de informações digitais através da Instituição por diversas razões:

1. A existência de múltiplos sistemas menores dificulta a administração destes, visto que as tarefas de manutenção também se multiplicam. Atividades simples como atualizações de *software* e monitoramento dos arquivos de relatório (“*logs*”), tornam-se mais trabalhosas à medida que o número de monitoramentos passa de um para dezenas, comprometendo a confiabilidade e a segurança.

2. Múltiplos sistemas sem centralização são mais difíceis de atenderem aos requisitos de acessibilidade, por exigirem que seus usuários estejam cadastrados e memorizem um dado adicional de autenticação (usuário e senha) específico para cada sistema. Uma dificuldade adicional de acessibilidade causada pela descentralização é que nem sempre o usuário está em uma rede com acesso ao servidor que necessita.
3. Sistemas descentralizados geram mais problemas técnicos. Na falta de um sistema centralizado de grande porte, adotam-se computadores pequenos, os quais são máquinas dimensionadas para trabalhos sem necessidades críticas, cujos projetos sacrificam confiabilidade máxima em favor de economia de custos. Adequados como estações de trabalho, adotar uma máquina convencional para um serviço de compartilhamento entre múltiplos usuários submete o equipamento a uma carga de intensidade e extensão (tempo) para as quais ele não foi projetado. Por exemplo, os discos rígidos convencionais apresentam problemas muito rapidamente quando operados de forma intensa durante 24h/7d/365d (se comparados ao desgaste que sofrem quando em uso em uma estação de trabalho), comprometendo a integridade dos dados; ao passo que serviços de armazenagem de grande porte utilizam discos de alto valor de MTBF (“*Mean Time Between Failures*”, Tempo Médio Entre Falhas), que suportam bem a intensidade do trabalho, possuem monitoramento de previsão contra falhas, e são arranjados em conjuntos (RAID - *Redundant Array of Independent Drives*, Arranjo Redundante de Dispositivos Independentes) que proveem redundância, velocidade e facilidade de reparo (*Hot Swap*, Troca a Quente, permitem a substituição de discos defeituosos sem a parada do sistema). Esta característica de discos rígidos para uso em estações de trabalho serem econômicos, porém pouco duráveis (e confiáveis) em contrapartida aos destinados a servidores de grande porte suportarem trabalhos intensos por longos períodos de uso (mas serem mais caros) aplica-se a todos os demais componentes do sistema: por isso denominam-se “estação de trabalho” (para uso pessoal) e “servidor”, respectivamente.

Um exemplo das dificuldades provenientes da falta de um sistema centralizado de compartilhamento deu-se na Superintendência de Infraestrutura da UFPR (SUINFRA)[1], cujos projetos precisavam ser fisicamente copiados para uma mídia removível, e levados através de entregadores ou malotes para serem vistos por outros setores - o que gerava restrições de tamanho, prazo de entrega e por vezes a perda completa da informação (causada pela perda e/ou corrupção do dispositivo).

Um sistema centralizado de compartilhamento de arquivos traz melhor acessibilidade ao unificar as informações de autenticação ("*login*"), pois facilita o trabalho do usuário (que só memoriza um nome e senha, e só precisa acessar um único servidor), além de assegurar que o serviço seja acessível em qualquer ponto da rede da instituição. Oferece mais confiabilidade e segurança por utilizar hardware dimensionado para a intensidade da tarefa e a adoção de planos de gestão de manutenção (PPM - "*Planned Preventive Maintenance*", Manutenção Preventiva Planejada) que asseguram paradas mínimas (se existentes). O menor número de *logs* dos sistemas centralizados agiliza sua análise. Facilita a configuração de *firewalls* (sistemas de restrição de acesso, proteção necessária contra invasões e outros acessos não autorizados) de forma mais simples e eficaz. A existência física em um único local (tipicamente um *Data Center* - Centro de Dados, mas podendo chegar a ser uma "sala cofre", a qual é hermeticamente blindada) permite custos e número de pessoal técnico menores, ao mesmo tempo em que permite cuidados maiores relacionados à temperatura, umidade, eletricidade e segurança física.

Quanto ao atendimento do decreto Nº 8.135, de 4 de novembro de 2013, o qual em seu Art. 1º estabelece que:

> As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal. (BRASIL, 2013, p. 2)

Todos os *campi* da UFPR atualmente já estão interligados por meio de redes de fibra ótica do governo federal. Mas também é necessário oferecer Sistemas de Informação que atendam à referida legislação, isto é, que estas informações possam

[1] Anteriormente a SUINFRA se chamava PCU (Prefeitura do Campus Universitário).

ser armazenadas e compartilhadas utilizando-se sistemas do governo federal - se possível, dentro da própria instituição.

A questão a ser analisada é: como armazenar e compartilhar dados e informações em uma organização pública de forma segura, eficaz e em acordo com a legislação vigente?

1.2 OBJETIVOS

O objetivo geral deste trabalho é recomendar soluções para o problema de compartilhamento e armazenamento seguro para dados e informações em um ambiente organizacional público, de acordo com a legislação vigente.

1.2.1 Objetivos específicos

Os objetivos específicos são:

a) Revisar e condensar conceitos sobre Gestão da Informação (GI), Tecnologias da Ciência da Informação (TIC) e segurança da informação relacionados ao compartilhamento de dados e informações na organização.
b) Identificar um ambiente amostral para validação conceitual, compreendendo necessidades e restrições deste ambiente.
c) Apresentar uma solução para o problema de pesquisa apresentado, com base no aprendizado nas disciplinas constantes do curso de GI

1.3. JUSTIFICATIVA

Sob a dimensão pessoal, dois pontos levaram à escolha do tema deste Trabalho de Conclusão de Curso.

O autor possui interesse em aplicar e aprofundar os conhecimentos de Gestão de Informação adquiridos no curso de bacharelado em G.I. atualmente em curso, mais especificamente nas práticas de desenvolvimento de sistemas computacionais voltados para o compartilhamento de dados e informações.

Além disso, o autor é servidor da Universidade Federal do Paraná (UFPR), onde desempenha funções de suporte a sistemas de informação que possibilitaram-lhe visualizar a carência de ferramentas e processos para o compartilhamento de informações na UFPR, as quais trafegavam com dificuldade entre os usuários. Dessa vivência surgiu a segunda razão determinante do tema deste trabalho, pois ficou clara a possibilidade de elaborar uma solução de compartilhamento digital de dados e informações, com grande agregamento de valor aos sistemas de informação da UFPR.

Sob a dimensão das contribuições e relevância do estudo proposto, a UFPR tem grande demanda por informação, e a proposta oferece uma possibilidade de compartilhar dados e informações na instituição em acordo com a legislação vigente, e oferecendo grandes facilidade de acessibilidade e confiabilidade – sem perder a confidencialidade.

Sob a perspectiva do curso de GI, o trabalho não apenas permite colocar em prática conceitos e fundamentos aprendidos nas disciplinas, mas abre novas perspectivas de atuação profissional para os formados em GI, e estabelece novas fronteiras para pesquisas futuras.

2 REFERENCIAL TEÓRICO

A base teórica está organizada de forma a contextualizar o valor dos dados e informações da UFPR.

2.1 GESTÃO DA INFORMAÇÃO - GI

Dados são símbolos quantificáveis, que não apresentam semântica. (SETZER, 1999). Constituem uma fase anterior à informação.

Conceituando o que é informação, a informação serve de insumo para todas as tarefas de gestão da organização (RAZZOLINI FILHO, 2013, 2’01”). Segundo Le Coadic (1996, p. 4), “informação é a medida da organização de um sistema e ou medida da organização de uma mensagem em um caso”. Segundo Setzer (1999), “informação é uma abstração informal (isto é, não pode ser formalizada através de uma teoria lógica ou matemática), que representa algo significativo para alguém. ”

Em uma fase posterior à informação, atinge-se o conhecimento, que é uma abstração pessoal, apenas atingido após a experiência. (SETZER, 1999).

Comunicação é o processo que se dá quando o receptor da mensagem percebe semântica no conteúdo recebido. (EPSTEIN, 1986, p. 16). Nesse caso, tanto informação, quanto comunicação dependem diretamente uma da outra.

Quanto à importância da GI, embora Floridi (2010, p. 4) afirme que “apenas recentemente” o progresso e o bem-estar humano começaram a depender principalmente de uma gestão bem-sucedida e eficiente da informação, sua importância é irrefutável.

Corroborando a importância (e o valor) das informações e de uma gestão adequada, Sabherwal e Jayaraj (2015, p. 809) afirmam que o valor da tecnologia da informação para o negócio (“*business value of information technology”* - BVIT) aumenta quando os usuários têm acesso a fontes de dados primárias e têm poucos incidentes de TI (e bons procedimentos de G.I. sabidamente minimizam incidentes).

2.1.1 Ciclo da informação: compartilhamento

Não basta simplesmente compartilhar os dados, sem tratamentos ou normas. Davenport (2006, p. 74) afirma que “para serem usados pela empresa para competir, os dados devem ser padronizados, integrados, armazenados numa central e disponibilizados a todo e qualquer interessado”.

Abordando especificamente os ganhos do compartilhamento de dados e informações, estes são citados por Terpstra *et al.* (2004, p. xxxix) quando afirma que todos podem agregar valor não apenas aos seus colegas atuais, mas aos vindouros, ao contribuir com informações - bem como a sua documentação. Ainda, o autor recomenda que as ferramentas para compartilhar informações sejam flexíveis, de forma a poder atender os diferentes tipos de usuários (independendo a plataforma de acesso que estes utilizam).

O compartilhamento não apenas proporciona ganhos, mas é essencial segundo Cortada (2011), que afirma ser necessário equipar aqueles que detém o conhecimento na organização (*experts*) com as ferramentas necessárias para criar uma cultura de compartilhamento de informações e desenvolvimento do conhecimento. Menciona ainda que a dependência intensa de informações é uma característica cada vez maior nas instituições, e seu uso tem sido feito de forma cada vez mais formal e rigorosa. Outra afirmação particularmente valiosa do referido autor é que a informação em si (e não a tecnologia da informação) é quem tem principal importância como alicerce à organização (embora seja bem mais difícil lidar com informações de forma eficiente sem a tecnologia).

Gil-Garcia, Chengalur-Smith e Duchesi (2007, p. 121) afirmam que projetos de compartilhamento de informação têm se tornado cada vez mais importantes tanto em organizações privadas quanto governamentais, e que estes projetos têm como objetivos oferecer melhorias nos serviços (qualidade destes), economia operacional, e aumento na efetividade. Estende ainda sobre a necessidade de se compreender as percepções e expectativas dos usuários.

2.1.2 Ciclo da informação: armazenamento

Para que a informação esteja disponível, ela precisa ser armazenada.

Esta armazenagem pode ser feita de forma local (disco rígido interno ou unidade externa USB), ou em nuvem (em um sistema de compartilhamento central).

A armazenagem em nuvem é uma forma moderna de arquitetura de dados, que move os dados para grandes sistemas centralizados, onde a gestão dos dados e serviços é mais confiável, e os dados mais acessíveis.

Armazenagem em nuvem é a longa visão sonhada da computação como um utilitário, onde os usuários podem armazenar seus dados de forma remota na nuvem, de modo a aproveitar alta qualidade e segurança. Ao “terceirizar” a armazenagem de seus dados, os usuários podem ser aliviados do peso do armazenamento e manutenção de dados locais (WANG, 2010, p. 1). No entanto, o fato de que os usuários já não possuem posse física do - possivelmente - grande tamanho de dados terceirizados, torna a proteção da integridade de dados na nuvem uma tarefa muito desafiadora e potencialmente formidável, especialmente para usuários com recursos de computação restrita.

Armbust *et al.* (2010, p. 54) cita diversas vantagens em centralizar o armazenamento de dados em uma unidade centralizada em nuvem, das quais destacamos a disponibilidade (que permite a continuidade do empreendimento, mesmo fora do ambiente físico); confidencialidade; desempenho e escalabilidade.

2.2 TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO - TIC

As Tecnologias de Informação e Comunicação - TIC são tecnologias que interferem e medeiam os processos de informação e de comunicação entre as pessoas.

Classificam-se em hardware (computadores e equipamentos de rede) e software (sistemas operacionais e aplicativos).

Os processos das TIC são relativos a tratamento, controle e comunicação da informação, fundamentalmente através de meios eletrônicos (essencialmente ligados à informática, pelo uso de computadores e sistemas).

Os dados e informações podem ser compartilhados através de mídias removíveis (as quais precisam ser transportadas fisicamente) ou eletronicamente, através de redes de computador.

A colaboração é de fundamental importância para o sucesso da organização, e é papel da empresa assegurar sua implementação e coordenação. Para isto, a implementação de tecnologias de comunicação e informação constitui ferramenta essencial para a colaboração organizacional.

> Colaboração não significa a ausência de conflito, mas condições estratégicas e estruturais específicas podem ajudar em sua formação e sobrevivência.
> A TIC disponível atualmente possibilita altos níveis de incentivos e alavancagem para o desenvolvimento de novas estruturas organizacionais colaborativas, gerenciando processos complexos, aumentando a troca de informações e possibilitando melhores decisões. (CASTILHO JR. e DINIZ, 2005, p. 104)

2.2.1 Software

As Tecnologias de Informação e comunicação dependem de instruções lógicas para funcionar. O *software* estabelece um programa, uma rotina para este conjunto de instruções.

Dentro do *software* temos diversos níveis. Para serviços de grande porte, são adotadas duas camadas: Sistema Operacional de gestão dos recursos físicos (de forma a constituir uma nuvem), e máquinas virtuais operando sob a nuvem.

O Sistema Operacional é responsável pela gestão dos recursos físicos da máquina (processamento, armazenagem e comunicação). Já as máquinas virtuais operam sob o ambiente de nuvem, tendo seus recursos ajustados dinamicamente, conforme necessidade. É possível ajustar a capacidade de processamento (número e percentual de utilização dos núcleos do processador), a quantidade de memória RAM e espaço em disco, bem como as conexões de rede – útil para resolver necessidades pontuais de grande processamento e/ou comunicação.

Dentre os Sistemas Operacionais voltados para sistemas de grande porte, e com características facilitadoras de virtualização, está o Ubuntu, uma distribuição GNU/Linux de código aberto (permite auditoria) e gratuito, amplamente utilizada pela comunidade informacional, com atualizações frequentes e distribuições voltadas

para longo suporte. Esta política de atualizações eficiente é um de seus pontos de maior destaque, crucial em um ambiente onde as ameaças de segurança são muito dinâmicas (rapidamente divulgadas).

Dentre os aplicativos disponíveis para o ambiente GNU/Linux mencionamos o Samba, igualmente de código aberto e gratuito, que permite compartilhar arquivos mediante o protocolo SMB – *Server Message Block* (Bloco de Mensagem do Servidor), popularizado pelo fabricante Microsoft em seu popular sistema operacional Windows (a partir da versão 3.11), suportado pela maioria dos dispositivos atualmente em fabricação (computadores, *tablets* e celulares), independendo o sistema operacional (GNU/Linux, Windows ou Apple OS).

Outro aplicativo de interesse é o LDAP- "*Lightweight Directory Access Protocol*" (protocolo leve de acesso a diretório), que permite centralizar a autenticação de usuários. Este aplicativo traz duas vantagens desejáveis à implementação da centralização (mencionada no item 1.1), sendo elas a facilidade para o usuário memorizar uma única combinação de nome e senha, e a confiança dos dados de autenticação (como ficam em um único lugar, reduz-se a possibilidade de discrepâncias).

Todo sistema deve ser passível de administração, e este acesso administrativo requer atenção para não comprometer a segurança em favor da acessibilidade. Uma solução amplamente utilizada para acessar administrativamente recursos informacionais com segurança é o uso de VPN – *Virtual Private Network* (Rede Privativa Virtual), uma conexão criptografada entre equipamentos, formando um "túnel" seguro de comunicação, sem interferências ou acessos de terceiros. Essencial para proteger a comunicação de ataques de *sniffing* (captura de dados que são transmitidos por uma rede), visto que passa a se assegurar que a conexão entre os equipamentos será direta e segura. Cada usuário possui chave de criptografia única, a qual deve ser entregue em mãos, em mídia removível – não deve ser transmitida por meios digitais para assegurar sua confidencialidade. Recomenda-se ainda que a partição onde a chave esteja escrita (na máquina cliente) seja criptografada, e que o perfil de usuário que permita acesso à chave seja protegido por autenticação segura.

2.2.2 Hardware

Hardware é qualquer utensílio necessário para realizar uma determinada atividade. No âmbito da informação, destacamos computadores (quer sejam celulares, *tablets*, computadores pessoais – portáteis ou de mesa - ou servidores de rede) e equipamentos de rede (*switches*, roteadores, transmissores, repetidores, cabos).

Conforme mencionado no item 1.1, ao planejar os computadores para a função de Servidor de Rede, deve-se atentar para o fato que seus componentes sejam dimensionados para a intensidade da tarefa planejada e que sejam adotados planos de gestão de manutenção (PPM) que assegurem paradas mínimas (se existentes).

Em relação aos sistemas em nuvem, ao contrário dos computadores pessoais, estes possuem seus componentes distribuídos em vários equipamentos: unidades de processamento (agrupando CPU – *Central Processing Unit*, Unidade Central de Processamento e memória RAM – *Random Access Memory*, Memória de Acesso Randômico); unidades de armazenagem (*Storage* - Armazenagem, contendo as unidades de disco); unidades de cópias de segurança (*Backup* – Cópia de Segurança, podendo ser em mídias fixas ou removíveis) e equipamentos para a distribuição dos dados e informações em rede, notoriamente os s*witches* (que fazem a distribuição física) e os roteadores (que fazem a distribuição lógica).

Em relação ao compartilhamento de dados e informações em um ambiente organizacional, é essencial que a rede de comunicação seja de projeto adequado à necessidade, caso contrário pode-se ter perdas de desempenho ou mesmo de acesso. Sempre que possível deve-se dar preferência que os clientes acessem o serviço através de redes cabeadas; conexões sem fio só devem ser utilizadas por dispositivos móveis. Deve-se projetar os equipamentos e pontos de distribuição de forma a assegurar o tráfego de dados e informações sem pontos de gargalo, assegurando a acessibilidade. É ainda essencial o estabelecimento de uma política de manutenção da rede, não apenas para atender falhas, mas também para planejar as necessárias expansões (principalmente quanto às redes móveis, cuja demanda cresce com velocidade maior que a necessidade de pontos de rede fixos, visto que estes últimos requerem também expansões físicas no mobiliário ou nas edificações).

2.3 SEGURANÇA DA INFORMAÇÃO - SI

Turban, McLean e Wetherbe (2004, p. 146) estabelecem diversas questões a serem abordadas durante a implementação da TI como suporte da comunicação e do trabalho cooperativo. Uma delas é a segurança.

Turban, Rainer e Potter (2007, p. 59) afirmam que as tecnologias da informação, se mal utilizadas, podem ter consequências devastadoras, e que atentar a esse possível mal-uso das tecnologias da informação está à frente de qualquer discussão sobre TI.

A segurança e confidencialidade são importantes, e de grande valor para Matsuda (1992, p. 222), que afirma ser necessário abordar informações secretas e confidenciais, que estas são as de maior valor para executivos da organização, e que são o produto mais avançado e importante para o processo de inteligência organizacional de mais alta ordem.

Para assegurar a segurança da informação, a norma ABNT NBR ISO/IEC 27002:2007 (baseada na norma britânica BS 7799) recomenda atentar para quatro aspectos: confidencialidade (garantir que apenas pessoas autorizadas possam acessar as informações); integridade (garantia que dados/sistemas estejam corretos); disponibilidade (os usuários autorizados devem ter acesso às informações necessárias); confiabilidade (a imagem da instituição deva ser protegida) (ABNT, 2005). A seção 10 da referida norma recomenda que a manutenção da integridade do sistema seja de responsabilidade da função do usuário ou do grupo de desenvolvimento a quem pertence o sistema de aplicação ou software (corroborando a vantagem da centralização para este caso). A seção 12 recomenda ainda que as trocas de informações e software entre organizações sejam controladas e estejam em conformidade com toda a legislação pertinente. (BELLI, 2011)

Dentre as vulnerabilidades de segurança dos sistemas de informação, Castilho Jr. (2012) cita incêndio, falha elétrica, falhas de hardware e comunicações, erros de software, mau uso do computador, e ações pessoais. Menciona ser essencial compreender as necessidades informacionais da organização, atentando para o que precisa ser protegido, como os bens críticos estão sendo protegidos, e como estes bens deveriam estar protegidos. Propõe que um programa de segurança de informação deve abranger aspectos envolvendo riscos, políticas, implementação, administração e auditoria, de fora cíclica.

Castilho Jr. (2012) discorre ainda sobre a norma ABNT NBR ISO/IEC 27001:2006, ressaltando como principais áreas de controle política de segurança (comprometimento da alta-direção, documento aprovado); organização para a segurança (estrutura, medidas, responsabilidades, áreas de atuação, papéis das pessoas); classificação e controle dos ativos (classificação, identificação dos proprietários, inventário); aderência às regras e conformidades legais; segurança física e ambiental (áreas restritas, controle de acesso, mesa limpa, retirada de materiais, equipamentos, infraestrutura, transporte); gerenciamento de computadores e redes (procedimentos e responsabilidades, separação de responsabilidades, segregação de ambientes, controle de mudanças, controle de vírus, *backups*, logs, correio eletrônico); controle de acesso a sistemas (computadores, redes, aplicativos) através de senhas, restrições de privilégios, sistemas de monitoração e alarme; desenvolvimento e manutenção de sistemas; desenvolvimento de um plano de continuidade de negócio.

2.4 OUTRAS FERRAMENTAS DE COMPARTILHAMENTO

Para efeito de comparação, pesquisou-se outras ferramentas para compartilhamento de dados e informações.

2.4.1 Comparação com outras ferramentas de compartilhamento.

Existem diversas ferramentas comerciais para o compartilhamento online de dados e informações. Todas possuem a característica de serem pagas, porém oferecerem acesso gratuito com funcionalidades limitadas (restrições de espaço, limitações quanto às políticas de compartilhamento), conforme descrito no Quadro 1. Os preços foram levantados em 21 de novembro de 2017, no website dos referidos serviços, conforme nota de rodapé respectiva a cada serviço.

QUADRO 1 – COMPARATIVO ENTRE FERRAMENTAS DE COMPARTILHAMENTO

Nome	Espaço (GB)	Custo mensal (R$)	Custo por GB (R$)*
Google Drive[2]	15	-	-
	100	6,99	0,0699
	1.000	34,99	0,03499
	10.000	349,99	0,03499
Microsoft OneDrive[3]	5	-	-
	50	7	0,14
	1.000	24	0,024
Dropbox[4]	2	-	-
	1.000	34,99	0,03499
	1.000 com recursos avançados	69,98	0,06998
UFPR Docs[5]	427[6]	-	-

*Obs.: utilizou-se mais de duas casas decimais em virtude de que os valores são muito pequenos

FONTE: O autor, baseado em informações dispostas no *website* dos referidos serviços em 21 nov. 2017, conforme nota de rodapé respectiva a cada serviço.

[2] https://www.google.com/drive/pricing/
[3] https://onedrive.live.com/about/pt-BR/plans/
[4] https://www.dropbox.com/buy
[5] http://www.cce.ufpr.br/portal/2014/02/24/cce-lanca-o-servico-de-armazenamento-institucional-docs-ufpr-br/
[6] Capacidade máxima do sistema todo, em 21 de novembro de 2017. Não há cota por usuário, neste momento.

2.4.2 Similaridades e diferenças

Todas as ferramentas permitem acesso via página *web*. Mas as similaridades param por aí.

O *Google Drive* e o *Microsoft Onedrive* oferecem ferramentas de pesquisa e indexação para todos seus planos, inclusive o gratuito. Já o *Dropbox* só oferece estas funcionalidades na versão “paga, com recursos avançados”.

Quanto a acesso direto via explorador de arquivos, somente o UFPR Docs o permite sem instalar nenhum aplicativo (por utilizar o protocolo SMB, que possui suporte nativo aos Sistemas Operacionais) – notar que todos os demais oferecem aplicativo próprio que permite o recurso, mas é necessário instalá-lo.

Privacidade e confidencialidade são características desejáveis à informação. *Google*[2], *Microsoft*[3] e *Dropbox*[4] explicitamente afirmam que pesquisam metadados de interesse comercial (embora sejam escusos quanto a como e por quem estes metadados são utilizados). Já o UFPR Docs não compartilha dados nem informações com terceiros.

2.4.3 Razões da inadequação das ferramentas comerciais à UFPR

Existem diversas limitações dos serviços comerciais avaliados, que impossibilitam seu uso pela UFPR.

A mais séria é o empecilho legal. Por ser uma entidade da Administração Pública Federal, a UFPR sujeita-se a legislação específica. A Portaria Interministerial Nº 141, de 2 de maio de 2014, em seu capítulo 1 determina que:

> As comunicações de dados da Administração Pública Federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da Administração Pública Federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias, observado o disposto nesta Portaria. (BRASIL, 2014, p. 82)

[2] https://www.google.com/policies/terms/
[3] https://privacy.microsoft.com/pt-br/privacystatement
[4] https://www.dropbox.com/pt_BR/privacy

O único serviço a atender tais requerimentos é o UFPR Docs. Os demais utilizam redes comerciais alheias à Administração Pública Federal (o que pode comprometer a segurança).

Existe ainda a limitação do acesso direto via explorador de arquivos sem a instalação de aplicativos de terceiros, também oferecida exclusivamente pelo UFPR Docs.

2.5 LEGISLAÇÃO E NORMATIZAÇÃO APLICÁVEIS

Toda organização está sujeita a leis e normas que se aplicam para evitar conflitos, prevenir problemas, e assegurar o atendimento das necessidades. Foram identificados itens de legislação e normatização, como se segue.

2.5.1 Legislação

O decreto Nº 8.135, de 4 de novembro de 2013, estabelece em seu Art. 1º que:

> As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal. (BRASIL, 2013, p. 2)

A portaria ministerial Nº 141, de 2 de maio de 2014, regulamenta o cumprimento do referido decreto, incluindo em seu escopo “empresas públicas e sociedades de economia mista da União e suas subsidiárias” (BRASIL, 2014, p. 82). No capítulo 1, define-se como atender à legislação, destacando-se:

> § 1º O disposto no caput não se aplica às comunicações realizadas através de serviço móvel pessoal e serviço telefônico fixo comutado.
>
> § 2º Os órgãos e entidades da União a que se refere o caput deverão adotar os serviços de correio eletrônico e suas funcionalidades complementares oferecidos por órgãos e entidades da Administração Pública Federal.
>
> § 3º Os programas e equipamentos destinados às atividades de que trata o caput deverão possuir características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, na forma definida nesta Portaria.
>
> § 4º O armazenamento e a recuperação de dados a que se refere o caput serão realizados em centro de processamento de dados fornecido por órgãos e entidades da Administração Pública Federal. (BRASIL, 2014, p. 82)

2.5.2 Normas internas à UFPR e da ABNT

O COPLAD - Conselho de Planejamento e Administração, é o órgão normativo, consultivo e deliberativo da Administração Superior da UFPR[5].

É assessorado por três comitês[6], sendo eles o Comitê de Segurança da Informação, o Comitê de Recursos de Tecnologia da Informação e o Comitê de Usuários de Recursos de Tecnologia da Informação.

O Comitê de Segurança da Informação é responsável por monitorar o ambiente informacional da Universidade, sob a perspectiva da segurança da informação e propor políticas de segurança da informação, resolver conflitos de recursos técnicos e monitorar projetos e níveis de serviço, bem como avaliar a incorporação de melhorias[7]. Dentre as suas atribuições está a de propor política de segurança da informação para a universidade, em consonância com a legislação vigente.

Sua PSI – Política de Segurança da Informação[8] estabelece princípios, objetivos e diretrizes destinadas à proteção da informação e à disciplina de sua utilização, emanados no âmbito da Universidade. Vale lembrar que recomenda a observância da publicidade como preceito geral e do sigilo como exceção, ou seja, divulgar informações de interesse público, independentemente de solicitações, utilizando meios de comunicação viabilizados pela tecnologia da informação, para fomentar o desenvolvimento da cultura de transparência pela administração pública.

Um ponto a favor dos gestores da informação é que o COPLAD, na resolução Nº21/13, inciso XII, descreve claramente o papel deste:

> Gestor da Informação: unidade ou projeto da Universidade que, no exercício de suas competências, produz informações ou obtém, de fonte externa à Universidade, informações de propriedade de pessoa física ou jurídica. (COPLAD, 2014, p. 2)

Um breve resumo das normas do COPLAD que se relacionam a este trabalho é apresentado no Quadro 2 – Resumo de Resoluções do COPLAD.

---

[5] http://www.soc.ufpr.br/wp-content/uploads/2016/07/Regimento_do_COPLAD.pdf
[6] http://www.soc.ufpr.br/wp-content/uploads/2016/07/resolucao_coplad_05012012-634.pdf
[7] http://www.soc.ufpr.br/wp-content/uploads/2016/07/resolucao_coplad_28062012-679.pdf
[8] http://www.soc.ufpr.br/wp-content/uploads/2016/07/resolucao_coplad_05012012-634.pdf

QUADRO 2 – RESUMO DE RESOLUÇÕES DO COPLAD

Resolução Nº	Ação principal
22/11[9]	Cria os comitês de Recursos de TI, e Usuários de TI.
13/12[10]	Cria o comitê de Segurança da Informação.
21/14[11]	Estabelece a Política de Segurança da UFPR.

FONTE: O autor, baseado em informações dispostas no *website* da SOC/UFPR[12], acessadas em 5 dez. 2017.

Existem, ainda, as normas da ABNT as quais além de apoiar as agências reguladoras, facilitam aos profissionais de TI o desempenho de suas atividades. Proporcionam ainda a comunicação aos usuários sobre as características dos produtos de informação oferecidos. Destas, destacamos as normas brasileiras ABNT NBR ISO/IEC 27002:2005 (que trata de informações locais) e ABNT NBR ISO/IEC 27017:2105 (segurança da informação para serviços em nuvem), extensivamente comentadas no item 2.3., estabelecem referências para o uso da computação em nuvem.

A nível internacional merece destaque a ISO/IEC 22123 - *Information Technology - Cloud Computing - Concepts and Terminology* (Tecnologia da Informação, Computação em Nuvem, Conceitos e Terminologia), a qual, como o nome sugere, não apenas descreve o cenário da Tecnologia da Informação e da Computação em Nuvem, mas define ainda Conceitos e Termos sobre o assunto.

[9] http://www.soc.ufpr.br/wp-content/uploads/2016/07/resolucao_coplad_05012012-634.pdf
[10] http://www.soc.ufpr.br/wp-content/uploads/2016/07/resolucao_coplad_28062012-679.pdf
[11] http://www.soc.ufpr.br/wp-content/uploads/2016/07/resolucao_coplad_17112014-959.pdf
[12] http://www.soc.ufpr.br/

3 METODOLOGIA

O objetivo do presente trabalho é analisar a questão de como armazenar e compartilhar dados e informações em uma organização de forma segura, eficaz e em acordo com a legislação vigente.

Metodologia é a descrição detalhada de como será realizada a pesquisa. Lakatos e Marconi (2003, p. 216) recomendam em sua “estrutura do projeto” que a descrição da metodologia de um trabalho de pesquisa responda às questões “onde”, “como”, “com que” e “quanto”.

3.1 CARACTERIZAÇÃO DO AMBIENTE DE PESQUISA

O ambiente de pesquisa é a Universidade Federal do Paraná e, para efeitos de pesquisa, restringiu-se o escopo inicial à Superintendência de Infraestrutura da UFPR (SUINFRA).

A SUINFRA está situada no Centro Politécnico da UFPR, em edificação própria, moderna e de boa qualidade de construção (sem infiltrações, e com boa rede elétrica). Possui localização física que facilita este projeto, por estar fisicamente próxima ao Centro de Computação Eletrônica (CCE).

3.1.1 Caracterização do compartilhamento de dados e informações no início do projeto

Quando do início deste projeto, a SUINFRA compartilhava seus dados e informações através de um computador pessoal comum, com sistema operacional *Windows 2003 Server*, sem configurações de domínio (“*Active Directory*”), sem restrições hierárquicas, e com várias falhas de segurança. A rede de comunicação de dados local era de 100Mbps, com diversos gargalos de dados (notoriamente o uso de *hubs* em vez de *switches*).

3.1.2 Usuários da SUINFRA

A SUINFRA possui cerca de 50 usuários. Este número varia constantemente, devido à presença de estagiários e colaboradores terceirizados cuja aderência ao setor é atrelada a projetos em andamento. Estes usuários estão

divididos em três grupos de trabalho: projetos, financeiro e administrativo. Há diferenças hierárquicas complexas entre os usuários, seus dados e informações.

3.2 MÉTODOS

Pretende-se oferecer uma solução baseada nos princípios e conhecimentos de Gestão da Informação para armazenar e compartilhar dados e informações da SUINFRA de forma segura, eficaz e em acordo com a legislação vigente.

3.3 MATERIAL

Inicialmente foram utilizados os exatos equipamentos que estavam em uso (microcomputador pessoal com um disco de 1TB), apenas com uma nova configuração de *software* (sistema de compartilhamento centralizado de dados e informações baseado em Ubuntu e Samba). Solução escalável, podendo ser expandida no futuro.

3.4 MÉTODO DE ABORDAGEM

O método dedutivo “pressupõe a existência de verdades gerais já afirmadas que servem de premissa para se chegar, por meio dele, a novos conhecimentos” (FARIAS, 2003).

Neste sentido, baseado nos conhecimentos de Gestão de Informação adquiridos no curso de bacharelado em G.I. atualmente em curso, mais especificamente nas práticas de desenvolvimento de sistemas computacionais voltados para o compartilhamento de dados e informações, pretende-se propor novas soluções para os problemas encontrados.

Resumidamente, este trabalho adota os seguintes procedimentos técnicos:

a) **Pesquisa Bibliográfica**: “a pesquisa bibliográfica tem por finalidade conhecer as diferentes formas de contribuição científica que se realizaram sobre determinado assunto ou fenômeno” (OLIVEIRA, 2001, p. 119). Portanto, a partir das definições iniciais, como tema, objetivos e hipóteses, se inicia uma pesquisa bibliográfica, com a consulta de livros, anais de congressos, periódicos nacionais e internacionais (jornais e revistas), bases de dados de

Universidades e Centros de Pesquisa obtidos junto à *world wide web* (www) e, ainda, através do intercâmbio com outros pesquisadores;

b) **Pesquisa experimental**: uma vez se selecionou um objeto de estudo, e se realizou a aplicação prática da proposta; e,
c) **Estudo de Caso**: uma vez que o objeto de estudo (SUINFRA) é uma unidade organizacional da UFPR e foi exaustivamente analisada para que a solução proposta atendesse às demandas daquela unidade.

3.5 PROCEDIMENTOS METODOLOGICOS

A partir do desenho teórico e metodológico, definiu-se a implementação do projeto para ser efetuada em cinco fases, conforme descrição a seguir.

3.5.1 Levantamento das necessidades.

Todo sistema visa solucionar um problema. Para compreender o problema, deve-se buscar as suas necessidades e requerimentos.

O primeiro ponto a ser considerado são as necessidades dos usuários. Estas podem ser identificadas por meio de análise de pedidos previamente feitos, em conjunto com entrevistas diretamente com aqueles que sofrem com o problema pesquisado (como compartilhar dados e informações dentro dos limites legais). Estas necessidades abordam:

3.5.1.1 Espaço físico necessário

O espaço em disco necessário deve levar em consideração todo o volume de dados a serem arquivados. Mas este desenho deve levar em consideração dois aspectos: a real necessidade dos dados atuais, e qual o aumento esperado da demanda de dados.

Muitas vezes dados e informações se encontram repetidas, redundantes ou sumariamente duplicadas dentro de grupos de trabalho. Mesmo quando houver necessidade da informação estar disponível para dois grupos, isto pode ser mais bem feito com o uso de atalhos em vez de copias completas do arquivo.

Existem ainda casos do dispendioso espaço em disco estar ocupado por assuntos alheios ao trabalho. Uma política de informação bem elaborada (como o que se propõe no item 3.5.1.3) evita o problema.

Já a previsão do aumento de demanda pode ser feita com uma simples curva de uso (quanto o espaço requerido em disco tem aumentado durante determinado período de tempo), mas esta informação precisa ser monitorada e a demanda de dados monitorada de perto.

Esta informação de demanda do espaço em disco é importante porque, em caso de falta de espaço em disco, o sistema pode apresentar falhas (principalmente de escrita). Uma medida para evitar o esgotamento do espaço em disco é limitar o acesso dos usuários estabelecendo-se cotas de espaço de uso. Mas tal procedimento não resolve completamente o problema, visto que, se todos os usuários utilizarem suas contas ao máximo, o sistema esgotará o espaço em disco. Por esta razão, é interessante colocar um limite de aviso (avisando que o limite de espaço está próximo, comumente estabelecido a 80%), e um outro estabelecendo um limite propriamente dito (100%, usuário recebe mensagem que o espaço se esgotou).

3.5.1.2 Nomes dos usuários

Para assegurar a segurança dos dados e informações, seu acesso precisa ser controlado por autenticação. O primeiro passo é levantar dados sobre os usuários (nome, *login*, senha), para então atribuir-lhes acesso aos compartilhamentos de acordo com as políticas de uso, conforme comentado no item 3.5.1.3.

3.5.1.3 Políticas de uso.

Para utilizar de forma eficiente o espaço em disco, e assegurar que as informações estejam disponíveis a todos a quem ela deve chegar (e somente a estes), faz-se necessário uma política de uso. Esta deve abranger as necessidades, e as restrições.

Como necessidades, devem ser consideradas os ciclos e demandas da informação para criar grupos que contenham todos os que dela precisarem – ao mesmo tempo em que deve protege-la daqueles que não podem ter acesso a ela.

Para conter o volume de dados e informações, recomenda-se estabelecer políticas de uso, definindo que tipo de dados e informações poderão (e deverão) ser armazenadas.

Para evitar a duplicidade de arquivos, é interessante estabelecer uma política de uso que defina onde ficará a informação (um único lugar), e, se necessário, criar-se somente atalhos para aquele documento principal, sem duplicá-lo. Alguns sistemas de arquivo (como o ZFS, *Zeta File System* – Sistema de Arquivo Zeta) fazem correção de duplicidade automaticamente, mas não é tão eficaz quanto uma gestão de duplicidade a nível de política de uso, pois só considera como duplicação quando dois arquivos forem absolutamente iguais (mesmo *hash*).

Estas Políticas de Uso devem ainda atentar para os aspectos de legislação vigentes que delimitem o serviço.

3.5.1.4 Requerimentos de rede

O acesso ao servidor de arquivos requer conexão de rede ao mesmo, e estes requerimentos dependem de diversas situações.

Os meios físicos a serem utilizados devem ser escolhidos de acordo com a necessidade e disponibilidade de recursos. O uso de conexões ópticas permite velocidades altas (superiores a 1Gbps), mas devido ao seu custo elevado costuma ser limitado a conexões entre equipamentos de rede (roteadores e *switches*). As conexões físicas por cabo de par metálico são bastante rápidas (até 1Gbps), apresentam baixa latência e garantia de acesso (já que são únicas), mas são limitadas ao local físico da tomada. As conexões sem fio possuem a vantagem da liberdade física, mas requerem autenticação forte (para assegurar a identidade do usuário), são lentas (mesmo as mais modernas redes padrão AC atingem somente 433Mbps por antena), possuem latência alta, e tem desempenho irregular, visto que são suscetíveis a intempéries e interferências.

Por esta razão, deve-se adotar conexões óticas entre equipamentos de rede; cabeamento por par metálico em postos fixos; e só usar conexões sem fio quando a liberdade de acesso físico for absolutamente necessária.

Deve-se ainda atentar para quais protocolos de rede serão utilizados, visto que cada um tem suas vantagens e limitações, conforme disposto no Quadro 3 – Comparativo entre protocolos de rede, o qual apresenta os parâmetros para determinar quais protocolos de rede são mais adequados para um serviço.

QUADRO 3 - COMPARATIVO ENTRE PROTOCOLOS DE REDE

	Rede local	Rede externa	Página pessoal (acesso livre)
Protocolo de rede	SMB	FTPS	HTTPS
Segurança	Média[13]	Alta	Alta
Confidencialidade	Alta	Alta	Nula (pública)
Velocidade	Alta	Média	Alta
Flexibilidade	Alta	Baixa[14]	Nula (estática)

FONTE: O autor

O protocolo SMB é o protocolo de rede mais flexível entre os abordados, por ser o único a permitir a cópia de múltiplas pastas e subpastas em uma única operação. Mas possui limitações de segurança pelo fato de sua criptografia ser opcional: por padrão, não é ativada. Isto para assegurar a comunicação com múltiplas plataformas (como celulares e computadores com variados sistemas operacionais), mas acessibilidade e segurança são características opostas, e ao utilizar o protocolo SMB com a criptografia desativada o sistema fica passível de uma ação de espionagem por um usuário que tenha acesso à rede local em questão. Este problema é resolvido com o uso de criptografia a nível de arquivo,

[13] Com o uso concomitante a uma "*firewall*", esta segurança torna-se alta. A transmissão é criptografada, mas portas SMB são difíceis de se proteger contra ataques DOS ("*Denial of Service*" - Negação de Serviço). Mas se o servidor ficar atrás de uma "*firewall*" que impeça o acesso a partir de redes externas, ele fica vulnerável a este tipo de ataque somente se provindo de dentro da rede da instituição, e, neste caso, é rápido e fácil de identificar e bloquear o IP do atacante.

[14] Possui limitações quanto a cópias de pastas inteiras, notoriamente quando o caminho possui muitas subpastas e/ou caracteres estendidos.

quando for desejada compatibilidade com dispositivos que não suportem comunicação via protocolo SMB com criptografia ativada. Note que em redes locais o controle de acesso é bastante eficaz, e é possível proteger ações de espionagem com a adoção de uma política de acesso a rede bem planejada, com registro individual por máquina e/ou usuário. Embora flexível, uma curiosidade é que a porta 437 utlizada pelo protocolo SMB não é ativada por padrão em redes externas, dificultando seu uso em locais externos à rede local.

Quando o acesso for a partir de uma rede externa, esta proteção do registro individual possível na rede local cai por terra, e passa a ser necessária uma comunicação efetivamente criptografada. O protocolo FTPs (*File Transfer Protocol – Secure*, Protocolo de transferência de arquivo seguro) passa a ser mais indicado. Mas possui a limitação de só permitir uma operação por vez, restringindo sua flexibilidade. Com o uso de aplicativos de gestão de transferências, até é possível automatizar processos de cópia de pastas inteiras, mas estes são apenas gestores do processo de enviar várias solicitações cópia, as solicitações são individuais.

Existem casos onde a confidencialidade não é requerimento, apenas a autenticidade, quando então o protocolo HTTP (*Hyper text transfer protocol*, Protocolo para transferência de hipertexto) passa a ser interessante. Rápido, amplamente acessível, é bastante adequado para divulgar informações sem restrições. Mas só é eficaz para divulgar informações estáticas, visto que para disponibilizar informações dinâmicas requer acesso a um banco de dados externo.

3.5.2 Implementação e testes iniciais do servidor

A implementação deve ser gradual. Os testes iniciais devem ser efetuados pelo próprio desenvolvedor. Inicialmente com um único usuário e compartilhamento, até atingir todo o escopo desenhado nas Políticas de Uso estabelecidas no item 3.5.1.3.

Uma vez completado o sistema, passa-se a testá-lo com mais de um usuário físico, mais de uma máquina física, e mais de um sistema operacional de acesso. Buscando simular as mais diversas condições desenhadas nas Políticas de Uso estabelecidas no item 3.5.1.3, o objetivo é experimentar todas as condições que possam vir a ocorrer quando do uso em produção, evitando surpresas.

A partir do momento que todos os requisitos tenham sido atendidos, e seu uso tenha se mostrado estável nos testes iniciais, passa-se a um período de testes em um ambiente amostral.

3.5.3 Período de testes em um ambiente amostral

A escolha do ambiente amostral deve levar em conta a demanda pela solução, aliada à facilidade de implementação (deve-se começar pelo local de implantação mais simples, para somente então seguir para o mais complexo). Deve-se priorizar usuários de teste com competência informacional para tal, para facilitar a implementação do sistema. Uma vez escolhido o ambiente amostral, pode-se seguir ao processo implementação.

Como o foco de toda ação de um gestor deve ser o cliente, deve-se iniciar a implementação conversando com eles: os usuários.

> Toda mudança enfrenta algum tipo de resistência pois as pessoas não aceitam aquilo que incomoda, tendem a só perceber o que lhes convém, desconfiam das novidades, receiam perder as coisas boas conquistadas. O desconhecimento ou a falta de controle da nova situação geram insegurança pessoal. (AMARAL, 1999/2000, p. 173)

Sanar dúvidas, ouvir solicitações, treinar usuários e técnicos locais no uso do sistema. Um sistema de informações só é eficiente à medida que seus usuários tenham competência informacional para utilizá-los - e a transmissão desta competência é função do gestor.

Deve-se atentar para o controle do projeto, sempre revisitando os usuários para avaliar a eficiência do sistema, e, se necessário efetuar ajustes no mesmo – ou retornar ao treinamento dos usuários, até atingir os objetivos estabelecidos.

3.5.4 Efetivação no ambiente amostral (com desligamento do sistema anterior).

Uma implementação é mais fácil de ser implementada e avaliada ao se restringir o número de usuários, e usar como critério para a seleção destes a sua competência informacional. É recomendável começar com técnicos locais (fase 3.5.3), para somente então passar aos demais usuários.

Conforme estabelecido no item 3.5.3, é fundamental que o gestor ofereça informações e treinamento sobre o uso do sistema, para assegurar o uso eficiente dos usuários.

É ainda importante que os técnicos locais estejam capacitados a dar suporte às necessidades mais corriqueiras, evitando uma sobrecarga da administração central do serviço, e oferecendo mais agilidade às solicitações dos usuários.

3.5.5 Extensão do serviço ao restante da Instituição.

Uma vez que no espaço amostral o sistema tenha se mostrado estável e atendendo às demandas estabelecidas, pode-se passar então a sua aplicação no restante da Instituição.

Recomenda-se que sua implementação seja feita aos poucos, repetindo todos os passos descritos no item 3.5.4 para cada setor. É ainda desejável estender um setor por vez, sempre procurando treinar técnicos locais (ou pelo menos usuários com notória competência informacional) para dar agilidade ao suporte.

4 IMPLEMENTAÇÃO

Como todo projeto, iniciou-se buscando levantar-se as necessidades, para melhor compreender o problema.

4.1 LEVANTAMENTO DE NECESSIDADES

O serviço não foi proposto pelo autor, e sim solicitado pelo então prefeito do campus; assim sendo, iniciou-se pedindo-lhe que relatasse os seguintes parâmetros:

4.1.1 Espaço físico necessário

Os arquivos da SUINFRA totalizavam 1TB, mas após inspeção detalhada, percebeu-se que somente cerca de 250GB eram dados pertinentes ao serviço.

4.1.2 Nomes dos usuários

A autenticação dos usuários é única e centralizada, através de servidor LDAP:

> LDAP é um protocolo de aplicação aberto, livre de fornecedor e padrão de indústria para acessar e manter serviços de informação de diretório distribuído sobre uma rede de Protocolo da Internet - IP. (YEONG, HOWESE e KILLE, 1993, p. 1-2).

Como o serviço de correio eletrônico também utiliza os serviços de autenticação do LDAP da UFPR, a maneira mais fácil de verificar se o usuário tem acesso ao LDAP é verificar se consegue acessar sua conta de e-mail institucional. Como utilizam o mesmo servidor de autenticação centralizado LDAP, se um usuário consegue acessar o correio.ufpr.br, não terá problemas com o docs.ufpr.br.

Uma vez levantados os nomes dos usuários, percebeu-se que nem todos tinham acesso às suas contas de e-mail da UFPR (as quais são criadas automaticamente para todo servidor quando de seu ingresso na Instituição). Estes usuários foram orientados a contatar a DAU - Divisão de Apoio ao Usuário, para corrigir esta dificuldade acesso.

4.1.3 Políticas de uso

Nesta etapa foram considerados os nomes dos grupos e hierarquias de acesso dos usuários a estes.

Inicialmente os usuários propuseram que, a exemplo do Servidor anterior, houvessem dezenas de subgrupos. Mas, após, discutir melhor o assunto, foi decidido que seria criado um único grupo (“PCU”), ao qual todos os usuários da SUINFRA teriam acesso - mas somente eles: demais usuários da Instituição somente veem que o compartilhamento existe, mas não o que há dentro dele.

Dentro deste grupo PCU há a possibilidade dos próprios usuários (sem a interferência do CCE) criarem pastas, contextualizando os conteúdos. Mas, reforçando, todos os usuários da SUINFRA têm acesso a elas.

4.2 IMPLEMENTAÇÃO DO SERVIDOR SMB

A implementação do servidor SMB - “*Server Message Block*” (Bloco de Mensagens de Servidor) (MICROSOFT, 1999), levou em conta aspectos legais e técnicos, descritos a seguir.

4.2.1 Aspectos legais da implementação

Um dos aspectos mais importantes da legislação vigente a ser considerado durante a implementação do servidor foi a Portaria Interministerial Nº 141, de 2 de maio de 2014, que em seu Capítulo I, Art. 1°, § 3º determina que:

> Os programas e equipamentos destinados às atividades de que trata o caput deverão possuir características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, na forma definida nesta Portaria. (BRASIL, 2014, p. 82)

Características de auditoria implicam no uso de programas de código aberto, que possam ser inspecionados quanto ao seu funcionamento. A mesma Portaria, em seu Capítulo I, Art. 2º, itens XXII e XXIII define:

> XXII - software livre: software cujo modelo de licença livre atende a liberdade para executar o programa, estudar como o programa funciona e adaptá-lo para as suas necessidades, redistribuir cópias do programa e aperfeiçoar o programa e liberar os seus aperfeiçoamentos sem restrição;

> XXIII - software público brasileiro: software que adota um modelo de licença livre para o código-fonte, a proteção da identidade original entre o seu nome, marca, código-fonte, documentação e outros artefatos relacionados por meio do modelo de Licença Pública de Marca - LPM e é disponibilizado na Internet em ambiente virtual público, sendo tratado como um benefício para a sociedade, o mercado e o cidadão; (BRASIL, 2014, p. 82)

Por esta razão, adotou-se como sistema operacional o GNU/Linux (STALLMAN, 2017). Para manter a padronização no centro de dados do CCE, optou-se pela distribuição *Ubuntu*, mais especificamente a versão servidor LTS 64 bits por oferecer suporte de longo prazo às atualizações (LTS - "*Long Time Support*", Suporte de Longo Prazo) e permitir alocar mais de 4GB de memória RAM ("*Random Access Memory*", Memória de Acesso Randômico) (visando a escalabilidade futura) (UBUNTU, 2017).

Como sistema de compartilhamento de dados escolheu-se o componente Samba, que oferece fácil compartilhamento de dados e informações sob protocolo SMB.

4.2.2 Aspectos técnicos da implementação

Criou-se uma máquina virtual na nuvem do CCE, inicialmente com um único processador, 1GB de RAM, e 1TB de espaço em disco - todas configurações facilmente escaláveis. O espaço em disco foi alocado em uma unidade externa com redundância ("*Storage*"), proporcionando agilidade nos reparos, e ainda mais escalabilidade.

4.2.3 Escolha dos protocolos de rede

Conforme as características dos protocolos de rede mencionadas no item 3.5.1.4, notoriamente no Quadro 3, escolheu-se os protocolos de rede conforme as necessidades de acesso.

Desta forma, escolheu-se o protocolo SMB como protocolo de rede principal de acesso ao docs.ufpr.br, e, face as necessidades de segurança, somente este protocolo foi habilitado para atender os usuários na rede local. Existe acesso via SSH -"*Secure Shell*" - Cápsula segura- (OPENBSD, 2017), mas somente para administração, sendo este acesso restrito aos técnicos do CCE (melhor comentado

no item 4.2.4). Considerou-se acesso via FTP/HTTP (para permitir acesso externo), mas, nesta fase, não foi implementado.

4.2.4 Escolha do protocolo de acesso administrativo

O acesso administrativo é por protocolo SSH a uma rede VPN.

Detalhando melhor, por tratar-se de máquina virtual, o acesso administrativo ao servidor só é possível por acesso remoto. Por padrão do CCE é utilizado o protocolo SSH -um protocolo de rede criptográfico para operação de serviços de rede de forma segura sobre uma rede insegura (YLONEN, 2006).

Como segurança adicional, a acesso administrativo é restrito a uma VPN - "*Virtual Private Network*" (Rede Virtual Privada), a qual requer chave criptográfica previamente configurada, individual para cada administrador. Esta chave é a maior garantia de restrição ao acesso administrativo do servidor, por esta razão, nunca é passada por meios eletrônicos ao administrador: é necessário ir pessoalmente ao CCE retirá-la com uma unidade flash USB. Mason (2002, p. 7) define que "Aplicações executadas através de VPN podem se beneficiar da funcionalidade, segurança e gerência da rede privada". Ou seja, mesmo remotamente, se tem acesso local à máquina - com segurança.

Para manter a adequação à legislação anteriormente comentada no item 4.2.1, utiliza-se como aplicação de rede virtual o "*OpenVPN*", o qual, por ser de código aberto, assegura possibilidade de auditoria. Tem ainda a vantagem de ser gratuito (OPENVPN).

4.3 HOMOLOGAÇÃO NA SUINFRA

Antes de se implementar um sistema em caráter de produção, é necessário testá-lo e validá-lo, para antecipar problemas.

> Homologação é a aprovação, ratificação ou confirmação, por autoridade competente, de certos atos particulares, a fim de que possam investir-se de força executória ou apresentar-se com validade. (Adaptado de SEGUNDO, 2015, p. 59)

Seguindo as recomendações dispostas no item 3.5.3, prestou-se notória atenção a tentar minimizar o impacto da mudança, e o processo foi efetuado com a maior transparência possível.

4.3.1 Comunicação aos usuários

A comunicação aos usuários do sistema se deu com o apoio do prefeito do campus, que fez a apresentação inicial do serviço aos usuários, explicando ainda que haveria a implementação de uma política de uso mais restrita no acesso ao servidor, notoriamente no que tange ao fato que o mesmo só deve ser utilizado para assuntos pertinentes ao trabalho.

Reforçou-se que não fossem utilizados serviços de nuvem de terceiros (como "*Google Drive*", "*Dropbox*" e "*Microsoft OneDrive*") para armazenagem de dados e informações da Instituição, por ferir a legislação vigente, notoriamente o §4º do decreto presidencial N° 8.135 de 04 de novembro de 2013:

> "§4º O armazenamento e a recuperação de dados a que se refere o caput deverá ser realizada em centro de processamento de dados fornecido por órgãos e entidades da administração pública federal." (BRASIL, 2013, p. 2)

Para conquistar a confiança dos usuários do sistema, foi explicado que o novo servidor possui redundância de discos, backups completos dos últimos 7 dias (de rápido acesso), além de backups mensais (de acesso mais demorado, por estarem em fitas).

Ressaltou-se, entretanto, que esta confiabilidade custa caro, e que é necessário fazer uso deste espaço com parcimônia. Foi mostrado que ¾ do espaço em disco do servidor antigo estava ocupado com dados e informações que não eram pertinentes ao serviço. Recomendou-se (primeiro verbalmente, depois por escrito, em correio eletrônico assinado pelo chefe do setor) que os usuários mantenham informações pessoais em meios de armazenagem também pessoais, e lembrou-se que os equipamentos da Instituição são para uso exclusivo de trabalho.

Não se apagou "de pronto" estes dados dos usuários os quais eram pessoais, não relacionados ao trabalho - mas tampouco importamo-los para o servidor novo. Abrimos um prazo de 30 dias para que os usuários fornecessem mídias pessoais (discos rígidos portáteis e/ou "*pendrives*") para onde pudéssemos

copiá-los. Reforçamos que, para o servidor novo, só foram copiados dados pertinentes ao serviço.

4.3.2 Usuários iniciais

Inicialmente foram escolhidos três usuários de um único setor (setor de suporte técnico da SUINFRA). A escolha se deu pelo fato de serem o grupo com melhor conhecimento de informática dentre os colegas. Configuramos o acesso na máquina do primeiro usuário, já ensinando estes três usuários a como fazê-lo. As outras duas, eles mesmos já fizeram, apenas supervisionados.

Estes usuários iniciais utilizaram o serviço por três dias sem problemas. Após este período, estendeu-se o serviço aos demais usuários.

4.3.3 Demais usuários

Os demais usuários tiveram seus acessos configurados pelos usuários iniciais que descrevemos no item anterior. Em alguns casos, houve problemas pontuais, os quais foram resolvidos à distância, com uso de telefone e e-mails. Em um único dia foi configurado o acesso em todas as máquinas da SUINFRA. E todos já perceberam o notório ganho de velocidade de acesso.

4.3.4 Mensuração de disponibilidade

Durante esta fase de homologação foram constantemente monitorados dados sobre o serviço. Em nenhum momento houve atrasos ou falta de acesso - mesmo quando provocada, propositalmente, para testar a redundância do serviço: retirou-se um dos discos do arranjo de armazenagem, e mesmo assim o serviço não foi interrompido. Ao reinserir-se o disco no arranjo, este imediatamente passou a se recompor, automaticamente.

4.4 EFETIVAÇÃO NA SUINFRA

Após cerca de duas semanas em homologação com perfeito desempenho, passou-se à etapa de produção, com a efetivação do sistema.

Para os usuários, não houve nenhuma mudança. Mas o servidor antigo foi desligado, e removido fisicamente do local. Após poucas semanas, foi encaminhado ao DSG - Depósito de Serviços Gerais da Instituição, para que fosse destinado a quem dele viesse a precisar. Por razões de segurança, seus discos foram antes formatados, para não comprometer o sigilo das informações que ainda permaneciam escritas neles.

4.5 EFETIVAÇÃO NO RESTANTE DA INSTITUIÇÃO

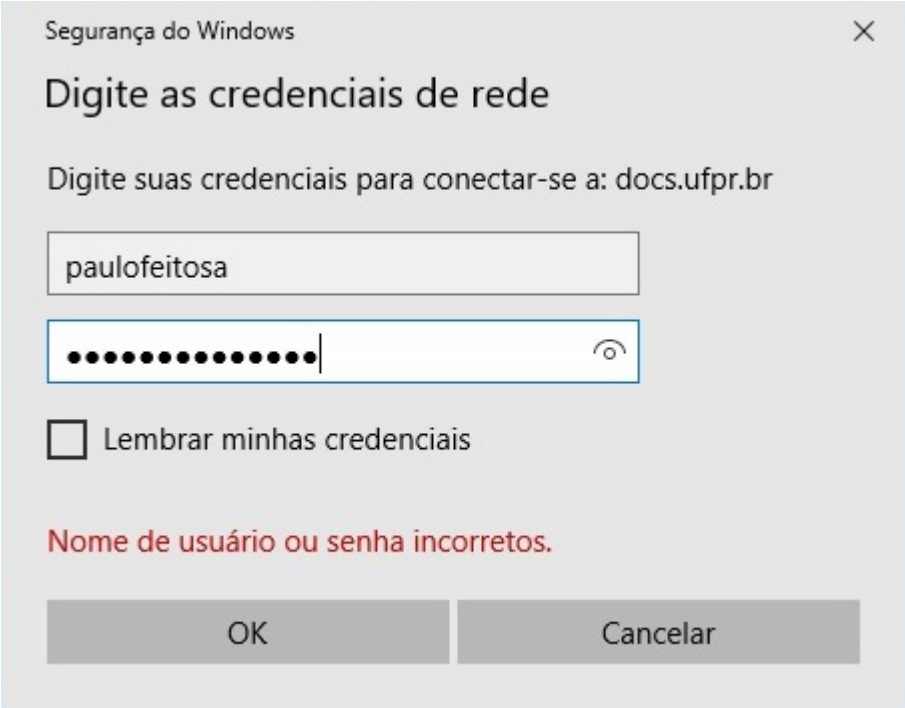
A segunda unidade da Instituição a ser atendida pelo sistema docs.ufpr.br foi a ACS - Assessoria de Comunicação Social. Foram seguidos os mesmos procedimentos efetuados na SUINFRA, e os resultados foram similares: em poucos dias, o serviço foi efetivado.

A terceira unidade da Instituição a ser atendida foi a PRAE - Pró-reitoria de Assuntos Estudantis. A quarta foi o gabinete do reitor, e, subsequentemente, todos os setores da Instituição passaram a utilizar o serviço, que hoje está em pleno uso - inclusive nos campi localizados fora de Curitiba.

4.6 EXEMPLOS DE COMPARTILHAMENTOS.

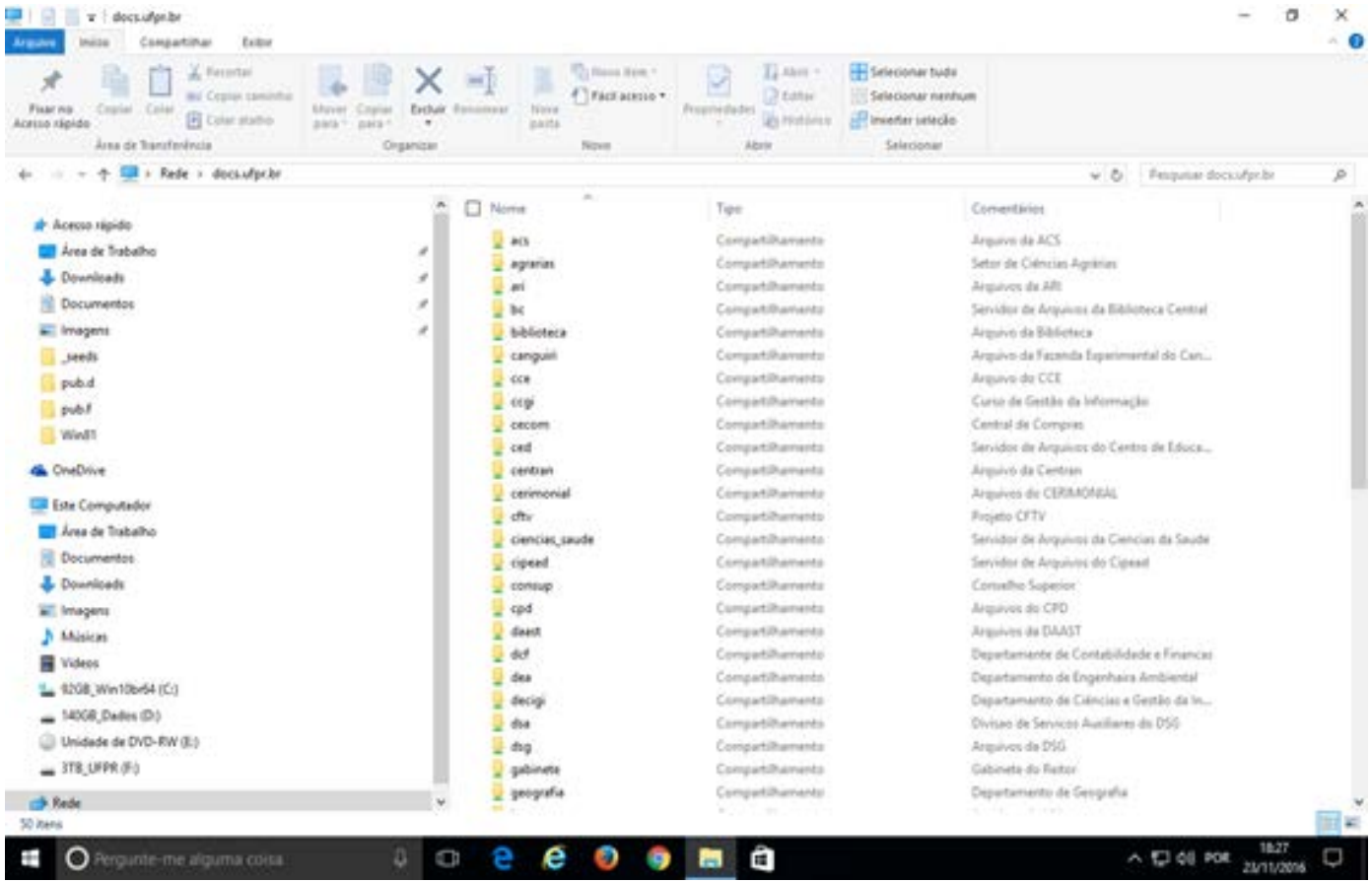
As figuras 1 a 5 ilustram os principais grupos de compartilhamento oferecidos pelo docs.ufpr.br quando acessados a partir de uma conexão da rede interna da instituição. Nos casos a seguir a conexão foi por meio físico (cabo de rede CAT 6a conectado diretamente a um “*Switch*” sem nenhum intermediário, velocidade de conexão 1Gbps.

FIGURA 1 - TELA INICIAL DE *LOGIN*.



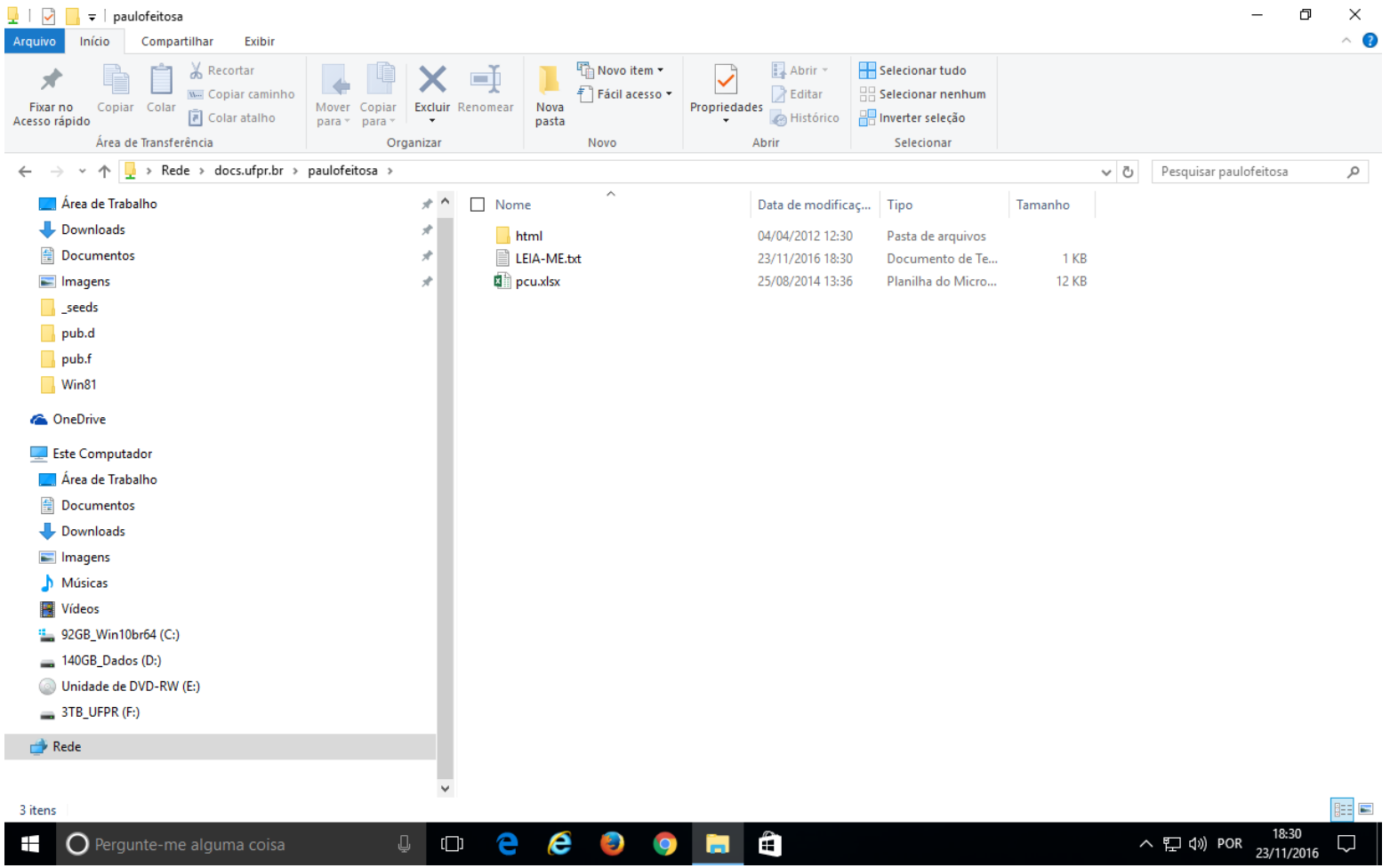
Para efetuar o login, basta abrir qualquer navegador de arquivos (no caso, o aplicativo “Windows Explorer”, em uma estação rodando SO (Sistema Operacional) “Microsoft Windows 10 Pro”, versão 1703, “build” 10.0.15063, em português do Brasil.

FIGURA 2 - PASTAS NO CAMINHO RAIZ SMB:\\DOCS.UFPR.BR\.



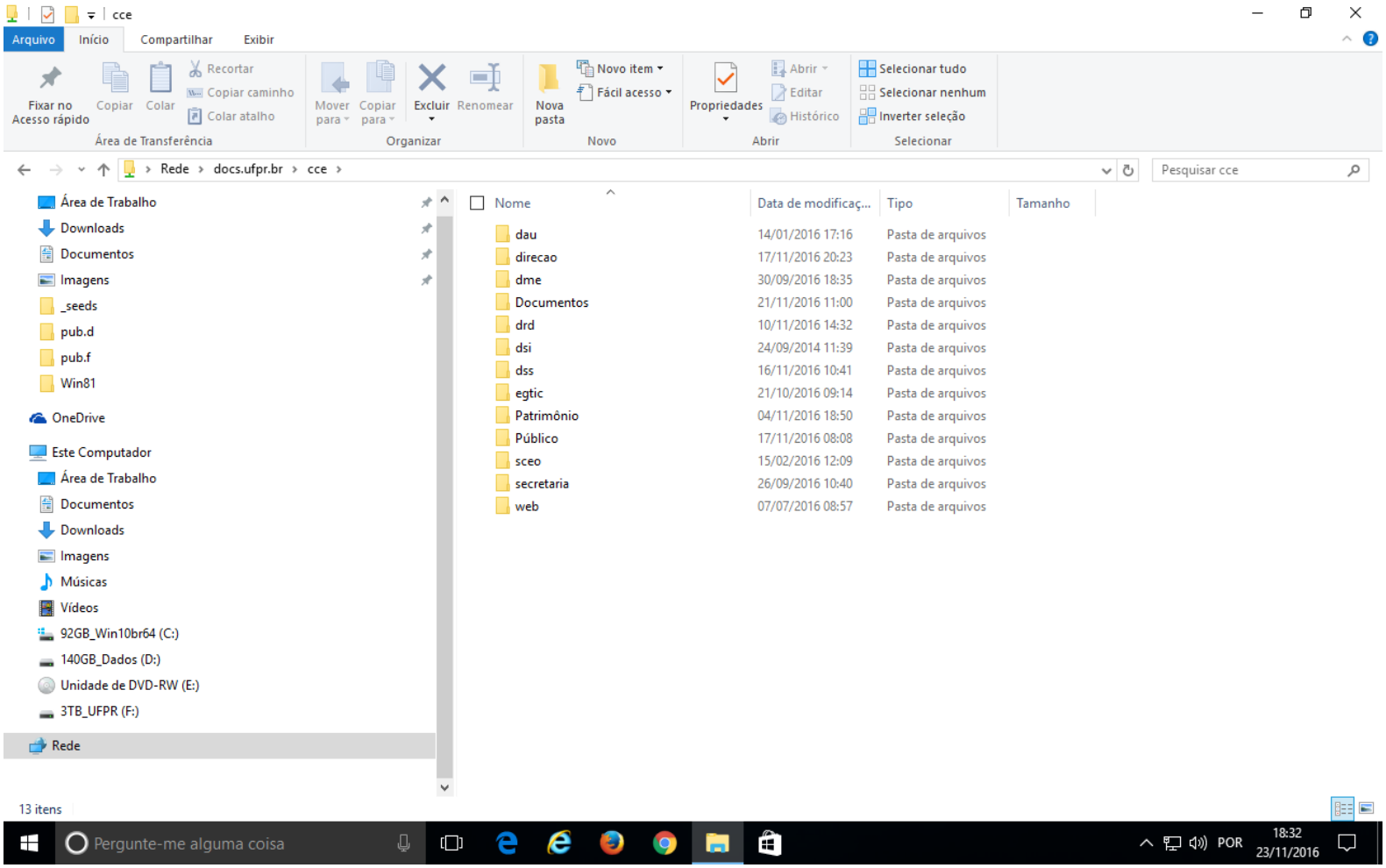
Todos os usuários com um e-mail @ufpr.br válido têm acesso a este compartilhamento.

FIGURA 3 - PASTAS DO CAMINHO DO USUÁRIO, <SMB:\\DOCS.UFPR.BR\PAULOFEITOSA>.



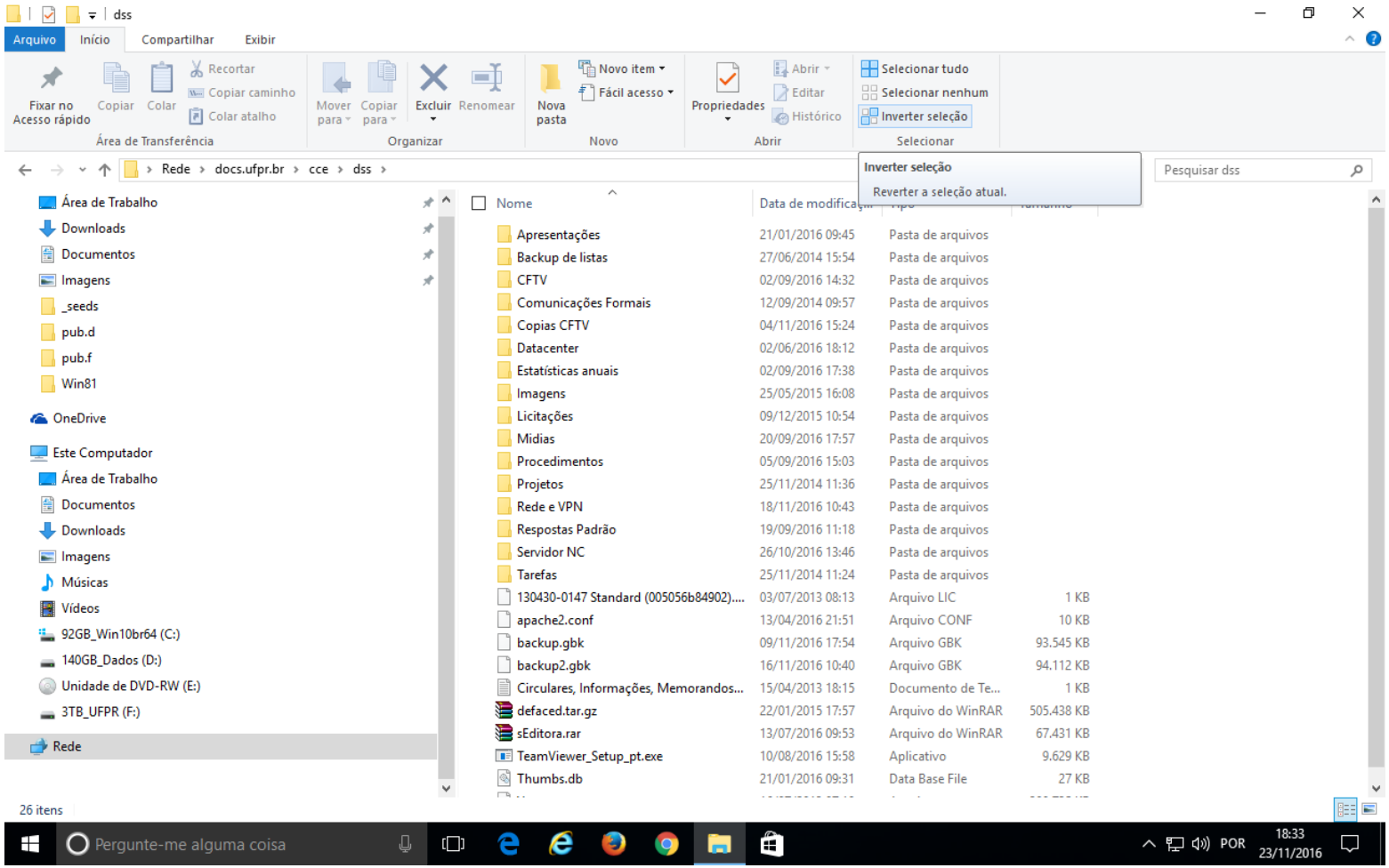
Conteúdos dentro pasta HTML são acessíveis por qualquer um via <https://docs.ufpr.br/~paulofeitosa>. Os demais, fora desta pasta (exemplo: pcu.xls) só podem ser lidos pelo próprio usuário.

FIGURA 4 - PASTAS DO CAMINHO DO CCE, SMB:\\DOCS.UFPR.BR\CCE.



Somente funcionários do CCE têm acesso a este compartilhamento.

FIGURA 5 - PASTAS DO CAMINHO SMB:\\DOCS.UFPR.BR\CCE\DSS .



Somente servidores da Divisão de Suporte e Serviços têm acesso.

5 CONSIDERAÇÕES FINAIS

Consideram-se atingidos todos os objetivos estabelecidos. Foram utilizados conceitos sobre GI, TIC e segurança da informação, relacionados ao compartilhamento de dados e informações em uma organização, como base teórica; por ser uma organização do âmbito federal, esta teve necessidades e restrições próprias, destacando-se a necessidade de uso de software de código aberto, e o trânsito e armazenamento de dados e informações exclusivamente em redes digitais federais.

O novo serviço de compartilhamento de dados e informações que se implementou na UFPR ofereceu acesso aos dados e informações da Instituição com ganho de segurança física (redundância), lógica (políticas de acesso bem estabelecidas) e legal (notoriamente no que diz respeito ao decreto 8135/2013). Proporcionou um grande aumento na velocidade de acesso. A nova política de cópias de segurança ("*backup*") já possibilitou, diversas vezes, resgatar informações erroneamente apagadas. Como todo bom sistema, na maioria das vezes, os usuários sequer se lembram que "ele está lá".

Mas ainda há questões a serem estudadas no futuro. Notoriamente, no que tange ao acesso de estagiários, os quais no momento são impedidos de fazê-lo, por limitações legais. Outra questão que se deixou em aberto é a implementação de sistemas similares nos campi mais distantes (notoriamente o do litoral, mas também os de Palotina, Jandaia do Sul e Toledo), pois a conexão de rede para estes locais é lenta, e por vezes instável. A implementação de sistemas locais de compartilhamento de dados e informações - notoriamente as que só fossem pertinentes a cada um destes campi - agilizaria o acesso às mesmas.

É ainda possível fazer processos de mineração de dados, para encontrar padrões dos dados e informações que possam vir a aumentar o desempenho informacional da Instituição, notoriamente na busca e recuperação das informações, e com isto evitar a duplicidade de trabalhos.

Também há a possibilidade e se aplicar análises infométricas para medir os dados e informações não apenas quanto a suas dimensões, mas estabelecer mapas de relacionamento que determinem os pontos de centralidade e outras informações pertinentes.

REFERÊNCIAS

ABNT - Associação Brasileira de Normas Técnicas. **Norma brasileira ABNT NBR ISO/IEC 27002**. Rio de Janeiro. 2005. 120p.

AMARAL, S. A. do. O profissional da informação e as técnicas de marketing. **Revista de Biblioteconomia de Brasília**, v. 23/24, n.2, p. 173-188, especial 1999/2000. Disponivel em <http://repositorio.unb.br/bitstream/10482/17522/3/ARTIGO_OProfissionaldaInformacaoeasTecnicas.pdf>. Acesso em 22 jul. 2017.

ARMBRUST, M.; FOX, A.; GRIFFITH, R.; JOSEPH, A. D..; KATZ, R.; KONWINSKI, A.; LEE, G.; PATTERSON, D.; RABKIN, A.; STOICA, I.; ZAHARIA, M. A View of Cloud Computing. **Communications of The ACM**. Nova Iorque, EUA, abr. 2010, V. 53, N. 4, P. 50-58. Disponível em <https://dl-acm-org.ez22.periodicos.capes.gov.br/ft_gateway.cfm?id=1721672&ftid=757661&dwn=1&CFID=1003631287&CFTOKEN=22097145>. Acesso em 11 out. 2017.

BRASIL. Decreto Nº 8.135 de 4 de novembro de 2013. Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 5 nov. 2013. N. 215, p. 2. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8135.htm>. Acesso em 12 abr. 2017.

BRASIL. Portaria interministerial Nº 141, de 2 de maio de 2014. Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 2 mai. 2014. N. 83, p. 82. Disponível em <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=82&data=05/05/2014>. Acesso em 17 jul. 2017.

BELLI, M. J. Segurança da Informação. **Notas de aula da disciplina SIN132 - Segurança da Informação**. DECIGI-UFPR. Curitiba. 2011.

CASTILHO JR., N. C.; DINIZ, E. H. Implementação e Uso de Colaboração Digital entre Organizações. **Tecnologia de Informação**: Desafios da Tecnologia de Informação Aplicada aos Negócios. Editora Atlas. São Paulo. 2005. P. 104-121.

CASTILHO JR., N. C.; Vulnerabilidades dos SI. **Notas de aula da disciplina SIN098 - Sistemas de Informação**. DECIGI-UFPR. Curitiba. 2012.

COPLAD. Resolução Nº 21/14, de 24 de setembro de 2014. **Resoluções Vigentes do COPLAD**. Conselho de Planejamento e Administração. Secretaria dos Órgãos Colegiados. Universidade Federal do Paraná. Curitiba, PR, 24 set. 2014. P. 1-9.

CORTADA, J. W. **Information and the modern corporation**. Cambridge, EUA: The MIT Press, 2011. 159p.

DAVENPORT, T. Analisar para competir. **Harvard Business Review Brasil**, São Paulo, v. 84, n. 1, Ed. Especial, p. 66-75, jan. 2006.

EPSTEIN, Isaac. **Teoria da Informação**. São Paulo: Ática,1986.

FARIAS, K. L. O Problema do Método na Filosofia do Direito. **Universo Jurídico**, Juiz de Fora, ano XI, 08 de jul. de 2003. Disponivel em: <http://uj.novaprolink.com.br/doutrina/1414/O_PROBLEMA_DO_METODO_NA_FILOSOFIA_DO_DIREITO>. Acesso em: 26 mai. 2017.

FLORIDI, L. **Information**: A very short introduction. Nova Iorque, EUA: Oxford University Press, 2010. 130 p.

GIL-GARCIA, J. R.; CHENGALUR-SMITH, I.; DUCHESI, P. Collaborative e-Government: impediments and benefits of information-sharing projects in the public sector. **European Journal of Information Systems**, Londres, Reino Unido, v.16, n.2, p. 121-133, abr. 2007.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica**. Atlas, São Paulo, 2003, 5ª Ed., 311 p.

LAUDON, K., LAUDON, J. **Sistemas de Informações Gerenciais**. 9ª edição em português. São Paulo. Editora Pearson, 2010. 428 p.

LE COADIC, Y. **A ciência da informação**. Brasília: Briquet de Lemos, 1996. Disponível em <http://www.restaurabr.org/siterestaurabr/CICRAD2011/M1%20Aulas/M1A3%20Aula/20619171-le-coadic-francois-a-ciencia-da-informacao.pdf>. Acesso em 11 mar. 2017. 61 p.

MASON, A. **Cisco Secure Virtual Private Network.** Cisco Press. Indianapolis, Indiana, EUA. 2002. P. 7.

MATSUDA, T. Organizational Intelligence: It's significance as a Project and as a Product. Proceedings of the International Conference on Economics / Management and Information Technology 92, 31 de ago. a 4 de set. 1992. **The Japan Society for Management Information**, Tóquio, Japão, p. 219-222, 1992.

MICROSOFT. **Common Internet File System**. 1999. Disponível em <https://technet.microsoft.com/en-us/library/cc939973.aspx>. Acesso em 17 jul. 2017.

MICROSOFT. **SMB Security Enhancements**. 9 de mar. de 2017. Disponível em <https://msdn.microsoft.com/EN-US/library/dn551363(v=ws.11).aspx>. Acesso em 17 jul. 2017.

OPENBSD. **Manual search: SSH**. 9 de jul. de 2017. Disponivel em <https://man.openbsd.org/ssh.1>. Acesso em 17 jul. 2017.

OPENVPN. **Terms of use**. Disponível em <https://openvpn.net/index.php/terms-of-use.html>. Acesso em 17 jul. 2017.

RAZZOLINI FILHO. **Ciência da Informação**. Vídeo aula da disciplina - Introdução à Gestão da Informação, do Curso de Gestão da Informação da UFPR, ministrada a distância. Curitiba, 9 de out. de 2013. Disponível em <https://youtu.be/Fep-Lxg2wI4?t=2m1s>. Tempo total: 8m13s. Trecho utilizado disponível aos 2m01s. Acesso em 17 jul. de 2017.

RAZZOLINI FILHO, E.; DO NASCIMENTO, A. Gestão da informação e competências necessárias ao gestor. **Revista Iberoamericana de Ciencias Empresariales y Economía**, v. 2, n. 2, 2014. P. 29-43. Disponível em <https://pt.slideshare.net/fcerevista/ricee-n-2>. Acesso em 12 abr. 2017.

SABHERWAL, R.; JAYARAJ, R. Information technology impacts on firm performance: an extension of Kohli and Devaraj (2003). **MIS Quarterly**, Minneapolis, EUA, v.39, n.4, p. 809-836, dez. 2015.

SEGUNDO, H. de B. M. **Processo Tributário**. 8ª ed. São Paulo, Atlas, 2015.

SETZER, V.W. Dado, Informação, Conhecimento e Competência. **DataGramaZero**: Revista de Ciência da Informação, n.zero, dez. 1999. Disponível em <https://www.ime.usp.br/~vwsetzer/dado-info.html>. Acesso em 20 abr. 2017.

STALLMAN, R. **Linux and the GNU System**. Disponível em <https://www.gnu.org/gnu/linux-and-gnu.en.html>. Acesso em 17 jul. 2017.

TERPSTRA, J. H. *et alii*. **The official Samba-3 howto and reference guide**. Upper Saddle River, NJ, EUA: Prentice Hall PTR. 2004. 674 p.

TURBAN, E.; McLEAN, E.; WETHERBE, J. **Tecnologia da informação para gestão**. Bookman, 2004. 3ª Ed. 659 p.

TURBAN, E.; RAINER JR., K.; POTTER, R. E. **Introdução a sistemas de informação**. Elsevier, 2007. 2ª reimpressão. 364 p.

UBUNTU. **LTS - Long Time Support**. Ubuntu Wiki. Disponível em <https://wiki.ubuntu.com/LTS>. Acesso em 17 jul. 2017.

WANG, C.; QIAN, W. REN, K. Lou, W. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing**. IEEE INFOCOM 2010**. San Diego, EUA, 14-19 mar. 2010, 9 p. Disponível em <http://ieeexplore.ieee.org.ez22.periodicos.capes.gov.br/stamp/stamp.jsp?arnumber=5462173>. Acesso em 08 out. 2017.

YEONG, W.; HOWES, T.; KILLE, S. **X.500 Lightweight Directory Access Protocol**. The Internet Engineering Task Force (IETF®). Fremont, California, EUA. Jul. 1993. 21 p. Disponível em <http://www.ietf.org/rfc/rfc1487.txt?number=1777>. Acesso em 18 jul. 2017.

YLONEN, T.; **The Secure Shell (SSH) Protocol Architecture**. Cisco Systems, Inc. Network Working Group. Ed. C. Lonvick. Jan. 2006. Disponível em <https://tools.ietf.org/html/rfc4251>. Acesso em 22 jul. 2017.