
Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Luiz Claudio Carvalho

**GESTÃO DA SEGURANÇA DA INFORMAÇÃO:
CRIAÇÃO DE UMA POLÍTICA DE INFORMAÇÃO PARA UMA
INSTITUIÇÃO DE ENSINO MÉDIO NA CIDADE DE AMERICANA – SP**

Americana, SP

2020

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

LUIZ CLAUDIO CARVALHO

**GESTÃO DA SEGURANÇA DA INFORMAÇÃO:
CRIAÇÃO DE UMA POLÍTICA DE INFORMAÇÃO PARA UMA
INSTITUIÇÃO DE ENSINO MÉDIO NA CIDADE DE AMERICANA – SP**

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana, sob orientação do Professor Francisco Carlos Mancin.

Área temática: Segurança da Informação.

Americana, SP

2020

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

C325g CARVALHO, Luiz Claudio

Gestão da segurança da informação: criação de uma política de informação para uma instituição de ensino médio na cidade de Americana – SP. / Luiz Claudio Carvalho. – Americana, 2020.

62f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Francisco Carlos Mancin

1 Segurança em sistemas de informação 2. Governança de sistemas de informação 3. Norma NBR ISO/IEC 27002 I. MANCIN, Francisco Carlos II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

LUIZ CLAUDIO CARVALHO

**GESTÃO DA SEGURANÇA DA INFORMAÇÃO:
CRIAÇÃO DE UMA POLÍTICA DE INFORMAÇÃO PARA UMA INSTITUIÇÃO DE
ENSINO MÉDIO NA CIDADE DE AMERICANA – SP**

Americana, 13 de julho de 2020.

Banca Examinadora:

Francisco Carlos Mancin (Presidente)
Mestre
Faculdade de Tecnologia de Americana - Fatec

Armando Vulcano Júnior
Especialista
Faculdade de Tecnologia de Americana – Fatec

Thais Godoy Vazquez Macetti
Doutora
Faculdade de Tecnologia de Americana - Fatec

RESUMO

Este trabalho apresenta a construção de uma política de segurança da informação para uma instituição pública de ensino médio localizada na cidade de Americana – SP, com os principais elementos necessários para o seu desenvolvimento, visando à implantação de uma cultura de segurança, contextualizada nos interesses e possibilidades de gestão pública. Como parte principal do desenvolvimento, são apresentadas as melhores práticas para a proteção e controle da informação, com a utilização de COBIT (*Common Objectives for Information and Related Technology*), ITIL (*Information Technology Infrastructure Library*) e a Norma NBR ISO/IEC 27002, interligadas.

Palavras-chave: política de segurança; COBIT; ITIL; Norma NBR ISO/IEC 27002.

ABSTRACT

This work presents the construction of an information security policy for a public high school institution located in the city of Americana - SP, with the main elements necessary for its development, aiming at the implantation of a security culture, contextualized in the interests and possibilities of public management. As the main part of the development, the best practices for the protection and control of information are presented, with the use of COBIT (Common Objectives for Information and Related Technology), ITIL (Information Technology Infrastructure Library) and the NBR ISO / IEC 27002 Standard, interconnected.

Keywords: security policy; COBIT; ITIL; NBR ISO/IEC 27002.

LISTA DE FIGURAS

Figura 1 - Organograma da Instituição de Ensino	18
Figura 2 - Layout lógico da rede antes da implantação das recomendações	19
Figura 3 - Layout lógico da rede após a implantação das recomendações	19
Figura 4 - Interface Active Directory	31
Figura 5 - Banco de Dados de Active Directory	32
Figura 6 - Automação AD	34
Figura 7 - Gerenciamento de políticas de grupo.....	35
Figura 8 - Herança de GPOS	36
Figura 9 - Criando uma GPO.....	37
Figura 10 - Vinculando uma GPO.....	38
Figura 11 - Diretiva de domínio padrão	39
Figura 12 - Configurar GPO.....	40

LISTA DE ABREVIATURAS

ABNT – Associação Brasileira de Normas Técnicas

CLT – A Consolidação das Leis do Trabalho

CRM – *Customer Relationship Management* (Gerenciamento de Relacionamento com o Cliente)

ERP – *Enterprise Resource Planning* (Planejamento dos recursos da empresa)

ISACA – *Information Systems Audit and Control Association*

IOT – *Internet of Things*

ITIL – *Information Technology Infrastructure Library*

COBIT – *Common Objectives for Information and Related Technology*

COSO – *Committee of Sponsoring Organizations of the Treadway Commission*

NBR – Norma Brasileira

PSI – Política de Segurança da Informação

SI – Segurança da Informação

TI – Tecnologia da Informação

VLAN – *Virtual Local Area Network* (Rede virtual local)

VM – *Virtual Machine* (Máquina Virtual)

SUMÁRIO

1	INTRODUÇÃO	11
1.1	Justificativa	13
1.2	Relevância	14
1.3	Viabilidade	14
2	CONTEXTUALIZAÇÃO HISTÓRICA	15
3	SOBRE A INSTITUIÇÃO	17
4	GESTÃO DA SEGURANÇA DA INFORMAÇÃO	20
4.1	Políticas e Normas	20
4.2	Padrões e melhores práticas	20
4.3	Conceitos básicos da segurança da informação	23
4.4	<i>Backup</i>	25
4.5	Backup na Nuvem	27
4.6	<i>Active Directory (AD)</i>	30
5	ESTUDO DE CASO	42
5.1	Aplicações e objetivos da PSI	42
5.2	Abrangência	43
5.3	Diretrizes gerais	44
5.4	Classificação da informação	45
5.5	Controle de acesso	46
5.6	Internet	47
5.7	Correio eletrônico	47
5.8	Rede sem fio (<i>Wi-Fi</i>)	48
5.9	Recursos de TIC institucionais	48
5.10	Recursos de TIC particulares	49

5.11	Dispositivos móveis particulares:	50
5.12	Armazenamento de informações	50
5.13	Repositórios digitais	51
5.14	Mídias sociais	51
5.15	Mesa limpa e tela limpa	51
5.16	Áudio, vídeos e fotos	52
5.17	Uso de imagem, som da voz e nome.....	53
5.18	Aplicativos de comunicação.....	53
5.19	Monitoramento	54
5.20	Combate à intimidação sistemática (<i>bullying</i>).....	54
5.21	Contratos de trabalho e de prestação de serviços.....	55
5.22	Segurança da informação	55
5.23	Papéis e Responsabilidades.....	56
5.24	Disposições Finais da PSI	58
6	CONSIDERAÇÕES FINAIS	59
	REFERÊNCIAS.....	61
	ANEXO I.....	62

1 INTRODUÇÃO

Especialistas em diversas áreas de conhecimento afirmam que vivemos no Século XXI a Era da Informação¹. No entanto, ela pode receber também outras denominações como Era Digital ou Era Tecnológica, sendo também conhecida como Terceira Revolução Industrial, entre outras denominações. Independente do termo empregado, a particularidade mais notória da atual era da informação é, sem dúvida, a ampliação da capacidade de comunicação, da geração de dados, seu armazenamento, compartilhamento e a própria geração de conhecimentos que hoje se faz em escala mundial por meio da *Internet*.

Se no final do Século passado, mais precisamente na década de 90 as pessoas acessavam a *Internet* por meio de escassos recursos tecnológicos, hoje não nos desconectamos dela. Vivemos conectados, seja por meio de *smartphone*, *smart TV*, centrais de multimídia de veículos, assistentes virtuais, eletrodomésticos, câmeras de vídeo, e até lâmpadas inteligentes, entre outros dispositivos e objetos utilizados no cotidiano que possuem características próprias de conectividade com a *Internet*, criando um novo conceito e tendência tecnológica denominada *Internet of Things – IoT (internet das coisas)*. Por meio dessa nova tendência, não apenas pessoas, mas também objetos se mantêm conectados através da *Internet* provocando uma hiper conectividade global.

No entanto, para desfrutarmos as facilidades que a conectividade global nos traz, se faz necessário voltar nossa atenção aos aspectos de segurança cibernética, uma vez que diversos são os riscos envolvidos, além da privacidade dos dados e das pessoas. Nesse sentido é eminente a necessidade de se definir políticas de segurança e adotar boas práticas na gestão de recursos informacionais a fim de resguardar o sigilo e garantir a operabilidade dos sistemas e, tais políticas se baseiam em normas, padrões e procedimentos, que são recomendados por renomadas organizações.

¹Era da Informação é um termo utilizado para se referir à realidade tecnológica como mediadora das relações humanas e das interações entre homem e máquina ou entre máquinas.

Ao contrário do que muitas pessoas pensam a segurança da informação não se resume à compra de equipamentos e sistemas caros, como *firewalls*, sistemas de detecção de intrusão ou antivírus ou ainda acham que adotar políticas de segurança e estabelecer responsabilidades funcionais, ao aparato tecnológico é suficiente, nenhum desses comportamentos consegue precaver as perdas se forem adotadas de forma isolada e inconsequente.

De forma mais ampla, podemos considerá-la como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos da segurança: Confidencialidade, disponibilidade e integridade da informação. Dessa forma, estaríamos falando da definição de regras que incidiriam sobre todos os momentos do ciclo de vida da informação: manuseio, armazenamento, transporte e descarte, viabilizando a identificação e o controle de ameaças e vulnerabilidades. O modelo de gestão corporativa de segurança da informação empresta à expressão um sentido mais amplo, considerando em primeiro plano os desafios do negócio como um todo. Diante dessa abrangente orientação, dois outros conceitos ganham autonomia: autenticidade e conformidade (anteriormente referenciada como legalidade). (SÊMOLA, 2014, p. 43)

Como pode-se ver, a segurança da informação deve sempre estar relacionada aos seus pilares, atuando em todos os âmbitos de forma com que estes funcionem de alicerces para toda e qualquer situação. Com isso, pode-se constatar que as empresas e organizações, independente se seu porte, devem se preocupar com os aspectos de segurança cibernética dos dados e da privacidade das pessoas de modo a garantir a continuidade de seus negócios.

Sendo assim, consideramos em primeiro plano os desafios do negócio e a segurança da informação que pode se tornar algo mais amplo, abrangendo ainda aspectos de autenticidade, que verifica se os processos que estão ocorrendo são autênticos e de cunho verdadeiro, e se quem está acessando é de fato a pessoa autorizada e com direitos de acesso. Por fim a conformidade, que tem o papel de garantir o cumprimento das obrigações organizacionais, englobando desde compromissos com investidores, empregados, credores etc., a aspectos legais relacionados aos planos de negócio da empresa, garantindo assim que a empresa não sofra com problemas penais, e assegure a continuidade dos seus negócios.

A Segurança da Informação abrange várias áreas, dentre elas está a gestão de riscos que tem o intuito de prover a segurança da rede, objetivando planejar, agir, auditar, educar, monitorar, gerenciar, proteger e garantir a continuidade dos negócios. Também é de extrema importância que toda empresa ou organização se atualize em conformidade com as novas tendências tecnológicas, de forma a

sempre estarem atentas a novos ataques, vírus e acessos indevidos, pois, sabe-se que o mercado está cada vez mais competitivo e conforme as novas tecnologias surgem, aumenta-se as vulnerabilidades e chances de acessos indevidos. Com isto, também aumentam as possibilidades de outras empresas ou organizações que trabalham no mesmo âmbito de negócio consigam informações privilegiadas e secretas, saindo assim à frente no que o mercado tem a oferecer, podendo até lucrar mais por conta disso.

A implantação de uma política de segurança eficaz exige que uma organização gerencie, proteja e distribua os recursos necessários para atingir seus objetivos específicos.

É necessário que a política esteja alinhada aos objetivos da organização. A partir dos objetivos de negócios, são definidos os objetivos da segurança da informação, que tem como destaque: possibilitar a realização do negócio no que depende do uso dos recursos de informação.

A política e demais regulamentos definem estratégias, regras, padrões e procedimentos que direcionarão todas as ações para atingirmos os objetivos de segurança da informação. (FONTES, 2008, p-9).

A Política de Segurança define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação².

Deve-se utilizar uma visão metódica, criteriosa e técnica em seu desenvolvimento e elaboração, de forma que possam ser sugeridas alterações na configuração de equipamentos, na escolha de tecnologia, na definição de responsabilidades e, por fim, na elaboração das políticas com o perfil da empresa e dos negócios que ela pratica.

A Gestão da Segurança da Informação tem como foco principal as características humanas, organizacionais e estratégicas relativas à segurança da informação.

1.1 Justificativa

Com o crescente uso de recursos digitais, as instituições, sejam elas públicas ou privadas, precisam lidar com uma crescente estrutura de TI. Um dos componentes mais relevantes disso é a segurança, que precisa ser mantida para evitar problemas. É nesse cenário em que entra a Política de Segurança da Informação, ou, PSI.

² Ativo: Qualquer coisa que tenha valor para a instituição e precisa ser adequadamente protegida.

A PSI é um documento imprescindível para orientar e hierarquizar o acesso aos dados, essa política garante a efetividade de ações na hora de proteger as informações.

1.2 Relevância

Apesar de parecer uma elaboração opcional, a política de segurança da informação deve ser encarada como sendo indispensável. Acima de tudo, ela garante que os dados sejam protegidos, especialmente de concorrentes e outras pessoas não autorizadas. Portanto, é uma forma de manter elementos estratégicos longe de vazamentos.

A política ainda promove a homogeneização de atuação, de modo que todos saibam o que fazer e o que evitar.

1.3 Viabilidade

A realização desse trabalho pautou-se na execução de um estudo de caso fundamentado em pesquisa bibliográfica compreendida por artigos científicos, normas técnicas e revisão bibliográfica.

2 CONTEXTUALIZAÇÃO HISTÓRICA

Se resgatarmos a história, veremos diversas fases, desde as revoluções industrial e elétrica, a abertura de mercado e o aumento da competitividade proporcionado pela globalização, passando pelos momentos relacionados à reengenharia de processos, à terceirização, à virtualização e, mais recentemente, aos efeitos da tecnologia da informação aplicada ao negócio de forma cada vez mais abrangente e profunda. Em todas essas etapas, a informação sempre esteve presente e exercia um papel crucial para a gestão dos negócios.

Evidentemente que, para tal, deve-se observar os aspectos culturais, de *marketing* e até macroeconômicos da época, com o intuito de ajustar a projeção dos impactos. Todavia é evidente que todas as empresas ou organizações, independentemente de seu segmento de mercado, de seu núcleo de negócios e porte, em todas essas fases de existência, sempre se nutriram da informação, visando melhor produtividade, atenuação de custos, ganho de mercado, aumento de competitividade, agilidade e apoio mais eficiente aos processos de tomada de decisão.

Sêmola (2014, p. 23) afirma que a todo o instante aparecem descobertas, experimentos, visões, técnicas e padrões nascidos pela movimentação de críticos estudiosos, observadores e executivos que não aceitam a indiferença da vida e visam a inovação e o rompimento com as normas estabelecidas, evidenciando, quase sempre, uma atual disposição auspiciosa. E assim as empresas têm sido influenciadas por mudanças e novidades que surgem no mercado e provocam alterações de contexto.

Décadas atrás, as informações eram tratadas de forma centralizada e ainda pouco automatizada e a tecnologia da informação engatinhava e figurava, primeiramente, apenas como uma nova e promissora ferramenta, principalmente se forem consideradas as limitações de armazenamento iniciais e os preços dos primeiros grandes computadores *mainframes*³.

³ *Mainframes* é uma plataforma integrada de computadores capaz de processar grandes volumes de informações em curtos espaços de tempo.

No entanto, os investimentos da indústria de alta tecnologia foi sendo amortizados e seus frutos foram se tornando mais acessíveis. Logo os *mainframes* foram herdando, pouco a pouco, a função de central de processamento e armazenamento de dados, e mais tarde apareceram os terminais espalhados pelos ambientes da empresa, a princípio um único por departamento, que permitiam consultas remotas.

E assim, compartilhar informação passou a ser considerado uma prática moderna de gestão necessária as empresas que buscavam maior velocidade nas ações. Então, surgiram, em seguida, as primeiras redes de computadores e, paralelamente, as informações passaram a ser mais digitalizadas e os processos mais automatizados.

A preservação da confidencialidade, integridade e disponibilidade da informação utilizada nos sistemas de informação requer medidas de segurança, que por vezes são também utilizadas como forma de garantir a autenticidade e o não repúdio.

Todas estas medidas, independentemente do seu objetivo, necessitam ser implementadas antes da concretização do risco, ou seja, antes do incidente ocorrer. As medidas de segurança podem ser classificadas, em função da maneira como abordam as ameaças, em duas grandes categorias: prevenção e proteção. A prevenção é o conjunto das medidas que visam reduzir a probabilidade de concretização das ameaças existentes. O efeito destas medidas extingue-se quando uma ameaça se transforma num incidente. A proteção, por seu lado, é o conjunto das medidas que visam dotar os sistemas de informação com capacidade de inspeção, detecção, reação e reflexo, permitindo reduzir e limitar o impacto das ameaças quando estas se concretizam. Naturalmente, estas medidas só atuam quando ocorre um incidente. (CARVALHO; SILVA; TORRES, 2003, p. 17).

Em meio a tudo isso fica o questionamento de como a Gestão da Segurança da Informação pode ajudar a amenizar esse problema.

Objetivo Geral

O objetivo deste trabalho é demonstrar as melhores práticas e procedimentos que estão sendo utilizados para a proteção da informação e seus ativos e criar uma política de segurança da informação para uma instituição de ensino fundamental e médio.

Objetivos Específicos

Analisar os recursos existentes para impedir que ameaças⁴ explorem vulnerabilidades, reduzir essas vulnerabilidades, limitar a probabilidade ou o impacto

⁴ Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano à instituição.

de sua exploração e minimizar ou mesmo evitar os riscos.

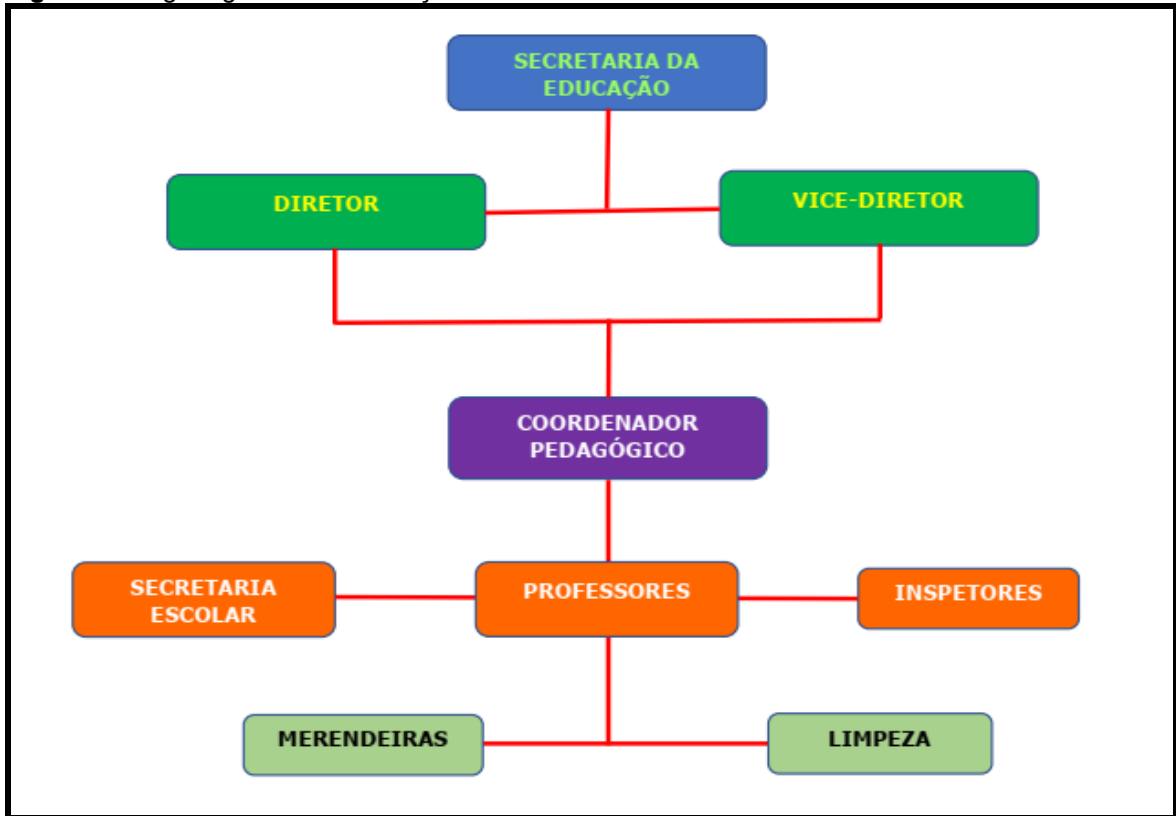
3 SOBRE A INSTITUIÇÃO

A instituição é uma instituição de Ensino Fundamental 2 (do 6º ao 9º ano) e ensino médio (1º, 2º e 3º ano) e está localizada na cidade de Americana – SP e conta com:

- 13 salas de aulas de ensino regular
- 1 sala de informática
- 1 biblioteca
- 1 sala para a secretaria
- 1 sala para a diretoria
- 1 sala de recurso para alunos especiais (8 alunos regulares e 2 não regulares)
- 80 professores
- 1 diretor
- 1 vice-diretor
- 1 coordenador pedagógico
- Secretaria com 4 colaboradores permanentes
- 2 inspetores de alunos
- 3 merendeiras
- 3 responsáveis pela limpeza

Organograma da Instituição

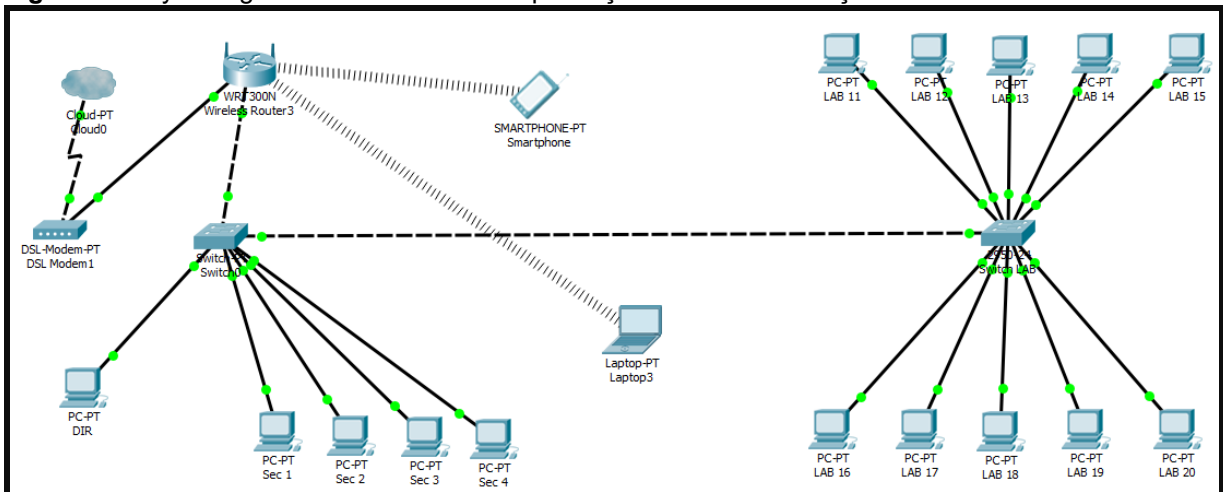
Figura 1 - Organograma da Instituição de Ensino



Fonte: própria

Sua estrutura computacional é simples, isto é, não tem uma pessoa específica para gerenciá-la. Conta com um roteador com configurações básicas e 2 *switchs*, sendo que, um na secretaria e faz a distribuição da rede para a secretaria (4 computadores), sala da diretoria (1 computador), e interliga o outro *switch* que fica na sala de informática (22 computadores), todos via cabo RJ45. Conforme figura 2.

Figura 2 - Layout lógico da rede antes da implantação das recomendações

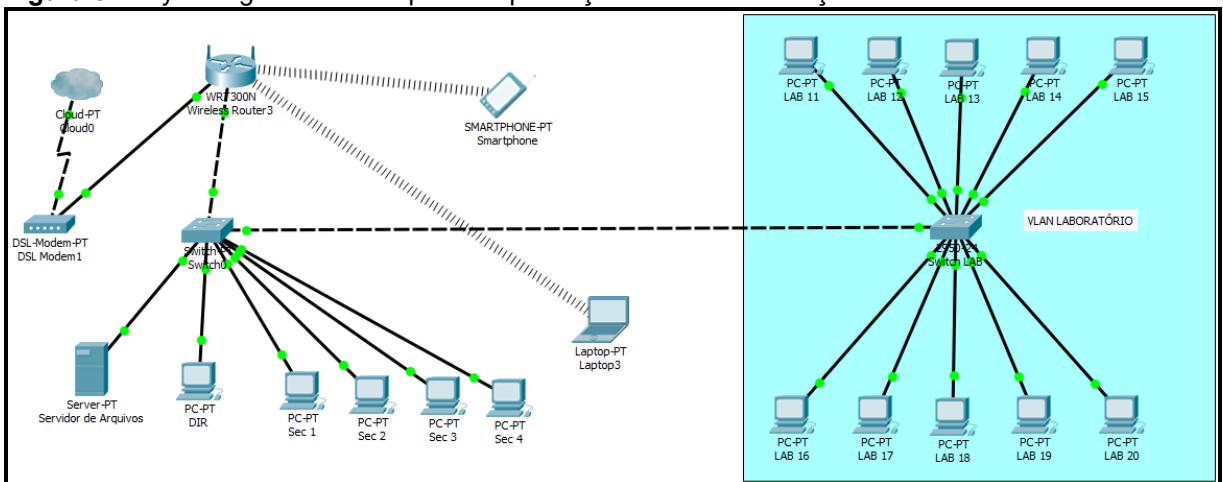


Fonte: própria (Packet Tracer)

Ao analisar o ambiente, foram encontradas algumas vulnerabilidades tais como, roteador com configuração padrão, isto é, usuário “*admin*” e senha “*admin*”. Os computadores do laboratório com acesso total a rede, podendo estes acessar as informações dos outros computadores, até mesmo os da secretaria e diretoria.

E assim conforme mostrado a figura 3, foi proposto uma configuração do roteador trocando o usuário e senha, também a criação de uma “*vlan*”⁵ separando assim a rede do laboratório do restante da rede, além da instalação de um servidor de arquivos para centralizar o armazenamento das informações, medidas simples, mas que cooperaria bastante no que diz respeito à segurança lógica da rede.

Figura 3 - Layout lógico da rede após a implantação das recomendações



Fonte: própria (Packet Tracer)

⁵ VLAN (*Virtual Local Area Network*), é uma rede logicamente independente.

4 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

A gestão da segurança da informação é um tema bastante discutido atualmente nas organizações, uma vez que a informação é um ativo valioso e necessita de cuidados quanto ao seu armazenamento, uso e segurança por parte daqueles que a detêm.

Temos de compreender que o alvo é a informação e que a mesma não se encontra mais confinada a ambientes físicos específicos ou a processos isolados. A empresa virou uma grande teia de comunicação integrada, dependente do fluxo de informações que por ela são distribuídas e compartilhadas. Essas mesmas informações, agora sujeitas a vulnerabilidades que transcendem os aspectos tecnológicos, são alvos também de interferências provocadas por aspectos físicos e humanos. (SÊMOLA, 2014, p. 37.)

4.1 Políticas e Normas

É necessário elaborar políticas, normas e procedimentos para comunicar aos usuários os fundamentos da cultura e indicar como as pessoas devem agir. Além das tarefas e ações, é preciso explicitar os critérios considerados em sua elaboração, facilitando o seu entendimento e a sua incorporação aos hábitos individuais.

Uma política é uma diretriz que descreve os requisitos básicos, indicando a filosofia da organização. Todas as ações a serem realizadas pelas pessoas precisam seguir e estar alinhadas a essa política.

Uma norma é um regulamento que define como a política será operacionalizada. Um procedimento é o detalhamento de como uma atividade deve ser realizada.

Todos esses elementos precisam ser escritos em uma linguagem simples, direta e de forma a serem entendidos por cada usuário da informação. É necessário explicitar o que é obrigatório e o que é desejável/opcional (FONTES, 2008, p. 12).

Políticas, normas e procedimentos precisam ser divulgados e constantemente lembrados, possibilitando que os usuários de todas as áreas da organização não tenham dúvidas de como tratar a informação.

4.2 Padrões e melhores práticas

O profissional de segurança da informação precisa desenvolver ações alinhadas com as melhores práticas para a proteção e controle da informação. Como padrões

de mercado aceitos e seguidos pela grande maioria das organizações e governos encontram-se o *COBIT (Common Objectives for Information and Related Technology)*, o *ITIL (Information Technology Infrastructure Library)* e a Norma NBR ISO/IEC 27002.

Para FERREIRA (2008, p. 121), essas práticas recomendam a existência de processo formal de conscientização em segurança da informação e enfatizam que o elo mais fraco da segurança é o ser humano.

COBIT: tem uma abordagem de controle e é bastante utilizado para a realização de auditorias nos ambientes de informação e de tecnologia da informação. Foi criado pela *ISACA (Information Systems Audit & Control Association)*, entidade de profissionais de segurança, auditoria e controle. Também é empregado com a finalidade de Governança de TI, patrocinado pelo *ITGI – IT Governance Institute*, coligado à *ISACA* (SAHIBUDIN et al, 2008).

Neste trabalho será usado como base o COBIT 4.1. O *COBIT* está dividido em 4 domínios, nos quais 34 processos estabelecem os objetivos de controle necessários para a manutenção de uma estrutura de controles internos que possibilitem à organização atingir seus objetivos de negócio de maneira confiável (do ponto de vista de TI). Os quatro domínios são:

- Planejamento e Organização (*Plan and Organize*);
- Aquisição e Implementação (*Acquire and Implement*);
- Entrega e Suporte (*Delivery and Support*);
- Monitoração e Avaliação (*Monitor and Evaluate*).

O *COBIT* é um modelo e uma ferramenta de suporte que permite aos gerentes suprir as deficiências com respeito aos requisitos de controle, questões técnicas e riscos de negócios, comunicando esse nível de controle às partes interessadas. Ele habilita o desenvolvimento de políticas claras e boas práticas para controles de TI em toda a organização; e é atualizado continuamente e harmonizado com outros padrões e guias. Assim, o *COBIT* tornou-se o integrador de boas práticas de TI e a metodologia de governança de TI que ajuda no entendimento e gerenciamento dos riscos e benefícios associados com TI. A sua estrutura de processos e o seu enfoque de alto nível orientado aos negócios fornece uma visão geral de TI e das decisões a serem tomadas sobre o assunto. Os benefícios de sua implementação como um modelo de governança de TI incluem:

- Um melhor alinhamento baseado no foco do negócio
- Uma visão clara sobre o que TI faz
- Uma clara divisão das responsabilidades baseada na orientação para processos
- Aceitação geral por terceiros e órgãos reguladores
- Entendimento compreendido entre todas as partes interessadas, baseado em uma linguagem comum
- Cumprimento dos requisitos do COSO para controle do ambiente de TI.

Informações mais completas e atualizadas sobre o *COBIT* e os produtos relacionados, incluindo ferramentas *on-line*, guias de implementação, estudos de caso, notícias e material educacional, estão disponíveis no site www.isaca.org/cobit.

ITIL: tem como objetivo a gestão da tecnologia da informação e seus recursos através da execução dos processos e serviços que precisam ser considerados para uma efetiva execução da tecnologia da informação alinhada ao negócio da organização. (OGC, 2011)

Conseqüentemente, o *ITIL* é um guia direcionado para a Governança de TI. O aspecto da segurança da informação é um pequeno segmento do conjunto dessa biblioteca de boas práticas. Foi elaborado pelo *Office of Government Commerce/UK* (OGC) com o objetivo de que as organizações que se relacionassem com o governo britânico seguissem esse padrão.

A filosofia *ITIL* adota uma estratégia orientada a processos para atender qualquer tipo de organização. Ela considera o Gerenciamento de Serviços em TI como um conjunto de processos estreitamente relacionados e altamente integrados. Para atingir os objetivos-chaves do Gerenciamento de Serviços em TI, devem ser utilizados: pessoas, processos e tecnologias.

Desta forma, as organizações poderão estar seguras da entrega de serviços de TI inovadores e de alta qualidade, alinhados com os processos de negócio. Muitos países adotaram a *ITIL* como um padrão para o Gerenciamento de Serviços. Pode-se ousar dizer que a *ITIL* é o padrão mundial no Gerenciamento de Serviços.

A *ITIL* era uma série de cerca de 60 livros que foram desenvolvidos no final da década de 80, como um conjunto de melhores práticas para TI. Atualmente, ela é considerada mais do que um conjunto de livros, pois se tornou amplamente aceita para a operação dos negócios de TI.

Desde o início, a *ITIL* foi disponibilizada sem restrições, ou seja, qualquer organização pode utilizar a estrutura descrita nos livros. Por este motivo, a *ITIL* tem sido utilizada por uma grande quantidade de organizações, como os órgãos públicos e entidades privadas (manufatura, instituições financeiras etc.).

A biblioteca contempla os seguintes assuntos: Gerenciamento da Configuração, Central de Serviços, Gerenciamento de Incidentes, Gerenciamento de Problemas, Gerenciamento de Mudanças, Gerenciamento de Liberações, Gerenciamento da Capacidade, Gerenciamento da Disponibilidade, Gerenciamento da Continuidade dos Serviços de TI, Gerenciamento Financeiro para Serviços de TI, Gerenciamento do Nível de Serviço, Gerenciamento da Infraestrutura e Gerenciamento de Aplicações.

Os processos da *ITIL* podem ser utilizados como base para alcançar conformidade com as normas BS 15000 (*British Standard for IT Service Management*) e ISO/IEC 20000.

A **Norma NBR ISO/IEC 27002**, é baseada na Norma Britânica BS-7799/1 e se apresenta como um código de prática para a gestão da segurança da informação. Seu objetivo direto é a Governança da Segurança da Informação (ABNT, 2013).

Essa norma tem como objetivo estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Anteriormente esta norma era conhecida como NBR ISO/IEC 17799, mas a partir de 2005 a nova edição da ISO/IEC 17799 foi incorporada ao novo esquema de numeração como ISO/IEC 27002.

A parte principal da norma se encontra distribuída em 11 seções, que correspondem a controles de segurança da informação.

“Segurança da informação é a proteção da informação contra vários tipos de ameaças, para garantir a continuidade do negócio, minimizar riscos e maximizar o retorno sobre os investimentos e as oportunidades de negócio”. (ISO 27002:2013)

4.3 Conceitos básicos da segurança da informação

Adotou-se por referência os aspectos estabelecidos na norma ABNT NBR 27002 (ABNT, 2013).

Na Seção 5 – Política de Segurança da Informação

É necessária a criação de um documento sobre a política de segurança da informação da organização, que deve conter, entre outros, os conceitos de segurança da informação, o comprometimento da direção com a política, uma estrutura para estabelecer os objetivos de controle e os controles, a estrutura de análise e avaliação e gerenciamento de riscos, as políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização. Essa política também necessita ser comunicada a todos, bem como analisada e revisada criticamente, em intervalos regulares ou quando mudanças se fizerem necessárias.

Na Seção 6 – Organizando a Segurança da Informação

Diz que para implementar a segurança da informação (SI) em uma organização, é necessário que seja estabelecida uma estrutura para gerenciá-la. É importante ainda que sejam estabelecidos acordos de confidencialidade⁶ para proteger as informações de caráter sigiloso, bem como as informações a que são acessadas, comunicadas, processadas ou gerenciadas por partes externas, tais como terceiros e clientes.

Seção 7 – Gestão de Ativos

De acordo com a norma, “ativo é qualquer coisa que tenha valor para a organização”. Gestão de Ativos, portanto, significa proteger e manter os ativos da organização. Para que eles sejam devidamente protegidos, necessitam ser primeiramente identificados e levantados, com proprietários também identificados e designados, de tal forma que um inventário de ativos possa ser estruturado e posteriormente mantido. As informações e os ativos ainda precisam ser classificados, conforme o nível de proteção recomendado para cada um deles, e seguir regras documentadas, que definem qual o tipo de uso é permitido fazer com esses ativos.

Na Seção 8 – Segurança em Recursos Humanos

Antes de realizar a contratação de um funcionário ou mesmo de fornecedores e

⁶ Confidencialidade: Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e sejam devidamente protegidas do conhecimento alheio.

terceiros, é importante que cada um deles entenda suas responsabilidades e esteja de acordo com o papel que desempenhará. Portanto, as descrições de cargo e os termos e condições de contratação precisam estar explícitos, especialmente no que tange às responsabilidades de segurança da informação. É importante também que quaisquer candidatos sejam devidamente analisados, principalmente se o trabalho envolve o manuseio de informações de caráter sigiloso. A intenção é diminuir o risco de roubo, fraude ou mau uso dos recursos.

Durante todo o tempo em que funcionários, fornecedores e terceiros estiverem trabalhando na instituição, eles precisam estar conscientes sobre as ameaças relativas à segurança da informação, bem como de suas responsabilidades e obrigações, de tal maneira que estejam preparados para apoiar a política de segurança da informação da organização. Também precisa ocorrer o processo de treinamento nos procedimentos de segurança da informação e no uso correto dos recursos de processamento da informação. É fundamental ainda que um processo disciplinar formal seja estabelecido para tratar das violações de segurança da informação.

No momento em que ocorrer o encerramento ou uma mudança na contratação, a saída de funcionários, fornecedores e terceiros, é preciso que tudo seja feito de modo ordenado e controlado, para que a devolução de todos os equipamentos e a retirada de todos os direitos de acesso sejam concluídos.

4.4 Backup

Backup ou cópia de segurança, é a cópia de dados de um dispositivo de armazenamento para outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Meios difundidos de cópias de segurança incluem *CD-ROM*, *DVD*, disco rígido, disco rígido externo (compatíveis com *USB*), fitas magnéticas e a cópia de segurança externa (online).

Todos os *backups* devem ser feitos por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de *backup*” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pelo *backup* deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o *software* não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de *backup* (como *DAT*, *DLT*, *LTO*, *DVD*, *CD* e outros) devem ser acondicionadas em local seco e seguro conforme as normas da ABNT.

As fitas de *backup* devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de *backup* deve ser monitorado e controlado pelos

responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante. É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de *backup*.

Os *backups* imprescindíveis, críticos, para o bom funcionamento da Instituição da Instituição de Ensino, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de *backup* e/ou *restore* é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Quaisquer atrasos na execução de *backup* ou *restore* deverão ser justificados formalmente pelos responsáveis.

Testes de restauração (*restore*) de *backup* devem ser executados por seus responsáveis, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do *backup*. Por se tratar de uma simulação, o executor deve restaurar os arquivos

em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de *backups* e *restores*, deverá ter um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo conselho escolar.

Os colaboradores responsáveis descritos na planilha de responsabilidade poderão delegar a outro colaborador⁷ a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, não poderá se eximir da responsabilidade do processo.

4.5 Backup na Nuvem

Também conhecido como *cloud backup*, é uma forma de *backup* que armazena cópias das informações em um servidor na nuvem, usando um *link* de *internet*.

Nem todos os clientes estão preocupados apenas com a falta de espaço, alguns usam sistemas de armazenamento em *clouds* para garantir que, caso haja algum problema em sua infraestrutura computacional, a informação estará intacta na *cloud* de armazenamento.

Soluções de *backup* na nuvem permitem o armazenamento de qualquer tipo de informação, desde dados pessoais a dados corporativos tais como: Bancos de Dados, *VMs*, Sistemas (ERPs, CRMs e outros sistema) e outros documentos como Planilhas, Fotos, Vídeos ou quaisquer outros arquivos.

Segurança do *backup* em nuvem.

Desde que a solução contratada use serviços de qualidade, o *backup* na nuvem é uma solução segura. Isso acontece quando os dados trafegam criptografados durante todo o processo, desde a cópia até o armazenamento e o site de hospedagem tenha todos as características de segurança.

A questão do *backup* e recuperação de dados também é outro desafio na nuvem. A segurança do *backup* é tão importante quanto a do próprio dado uma vez que o mesmo contém uma cópia do conteúdo da informação original. Por isso, os *backups* devem também ser criptografados e também possuir um forte controle de acesso. A recuperação de dados também levanta preocupações quanto a velocidade em que dados perdidos sejam recuperados de forma a não comprometer os serviços e processos que utilizam esses dados. (Silva, 2013, p. 24).

⁷ Colaborador: Empregado, estagiário ou menor aprendiz da instituição.

As duas maiores preocupações acerca do armazenamento em *clouds* são a confiabilidade e a segurança. É improvável que uma organização confie os seus dados críticos a outra entidade sem a garantia que terá acesso a estes dados sempre que quiser (disponibilidade), que estes não serão corrompidos (integridade) e que mais ninguém terá acesso a eles sem a sua autorização (confidencialidade). Para garantir a segurança da informação, a maioria dos sistemas usa uma combinação de técnicas, incluindo:

- Criptografia: algoritmos criptográficos são usados para codificar a informação tornando-a incompreensível e quase impossível de decifrar sem a chave usada para cifrar a informação, normalmente uma chave secreta partilhada entre o cliente e o serviço.
- Autenticação: é necessário o registo de um cliente através da criação de credenciais de acesso (ex. *username* e *password*).
- Autorização: o cliente define quem pode acessar a sua informação.

Mesmo com estas medidas de proteção, muitas pessoas acreditam que a informação armazenada num sistema de armazenamento remoto é vulnerável. Existe sempre a possibilidade de um *hacker* malicioso, de alguma maneira, ganhar acesso à informação do sistema, devido a vulnerabilidades existentes. Além disso, há sempre a preocupação de colocar os dados críticos (e muitas vezes confidenciais) nas mãos de terceiros, que terão acesso às informações neles contidos.

Armazenar informação num sistema remoto acessado via *internet* coloca a organização vulnerável a todos os problemas de conectividade e indisponibilidade temporária da *internet*. Além disso, praticamente todos os grandes fornecedores de serviços de armazenamento já sofreram problemas de disponibilidade e/ou corromperam dados de clientes, mesmo com a redundância interna de seus sistemas (os dados são tipicamente armazenados em diferentes *data centers* do fornecedor).

Os principais problemas de gerenciamento e segurança da informação dos dados na nuvem são:

- Falta de conhecimento da arquitetura em que os dados são armazenados.

- Falta de controles apropriados na transferência de dados para dentro e para fora da nuvem.
- Má utilização da criptografia.
- Dados em locais desconhecidos pelos clientes de nuvem.
- Dados de diferentes clientes misturados no provedor de nuvem.
- Provedores podem não excluir realmente os dados, mesmo que tal ação seja comandada pelo cliente.

A cópia e o acesso as informações armazenadas na nuvem

A cópia é muito simples, utiliza-se um aplicativo que permite uma customização de horários e uso de *link* de *internet*. No horário pré-determinado, o aplicativo coleta, comprime, criptografa e transfere os dados para a nuvem.

O acesso às informações também é bastante simples. Poderá ser feito normalmente utilizando o mesmo software que fez o *backup*, de qualquer lugar, desde que tenha as permissões e o acesso aos dados.

Serviço de *internet* (*link*)

O *backup* consome o *link* de acordo com a quantidade de dados a ser transferida diariamente. Recomenda-se sempre um *link* que comporte todos os serviços da empresa ou instituição.

Normalmente o *backup* é programado em um horário conveniente e que não prejudique os serviços da empresa ou instituição. Pode-se também definir o percentual do *link* a ser utilizado pelo serviço de cópia.

Cobrança do serviço de *backup* na nuvem

Existem fornecedores de armazenamento em *clouds* que cobram uma quantia fixa por uma quota de espaço e largura de banda de entrada e saída de dados (ex., *DivShare*, *DocStoc* e *Box.net*), enquanto outros usam um modelo *pay-per-use* (pagamento por uso) e cobram quantias variáveis conforme o espaço ocupado e a largura de banda utilizada pelo cliente (ex., *Amazon S3*, *Nirvanix*, *Windows Azure* e *RackSpace*). Em geral, o preço do armazenamento online tem baixado devido à entrada cada vez mais de empresas neste negócio.

Ao contrário das técnicas tradicionais de *backup*, o *backup* em nuvem é altamente flexível e escalável. Também é seguro e oferece um excelente custo x benefício.

4.6 Active Directory (AD)

Para um melhor “gerenciamento” dos usuários, acessos e permissões foi recomendado à Instituição de Ensino o uso do *Active Directory* (AD).

Mas o que é o Active Directory?

O *Active Directory* (AD) é uma ferramenta da *Microsoft* utilizada para o gerenciamento de usuários de rede, denominada serviço de diretório.

O *Active Directory* armazena informações sobre objetos na rede e torna essas informações fáceis de serem encontradas e usadas por administradores e usuários. O *Active Directory* usa um armazenamento de dados estruturado como base para uma organização lógica e hierárquica de informações de diretório. (Dolci, 2017).

O AD surgiu juntamente com o *Windows 2000 Server*. Objetos como usuários, grupos, membros dos grupos, senhas, contas de computadores, relações de confiança, informações sobre o domínio, unidades organizacionais, etc., ficam armazenados no banco de dados do AD. Nele ficam registrados os nomes e senhas de usuários, suas permissões de acesso a arquivos, impressoras e outros recursos da rede, as cotas de disco, os computadores e horários que cada usuário pode utilizar, etc.

Além de armazenar vários objetos em seu banco de dados, o AD disponibiliza vários serviços, como: autenticação dos usuários, replicação do seu banco de dados, pesquisa dos objetos disponíveis na rede, administração centralizada da segurança utilizando GPO (diretivas de grupos), entre outros serviços. Esses recursos tornam a administração do AD bem mais fácil, sendo possível administrar todos os recursos disponíveis na rede centralizadamente.

Como Funciona o Active Directory (AD)?

Na perspectiva do usuário o AD funciona para que eles possam acessar os recursos disponíveis na rede. Para isso basta que estes efetuem o *login* uma única vez no ambiente local de rede (normalmente, ao iniciar o sistema operacional).

Quando o usuário digita seu *login*⁸ e senha, o AD verifica se as informações fornecidas pelo usuário são válidas, e em caso positivo, realiza a autenticação. A partir daí, todo o acesso a recursos compartilhados pela rede corporativa/institucional será gerenciado pelo serviço de diretório do *Active Directory*.

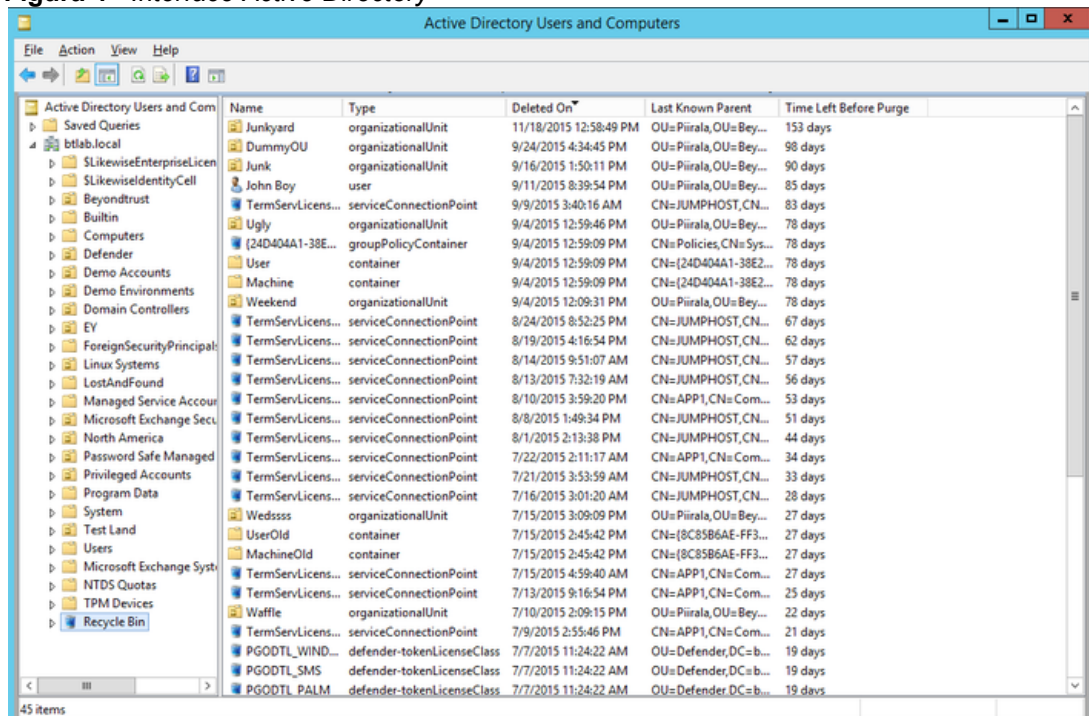
Na perspectiva técnica pode-se entender que o *Active Directory (AD)* funciona como uma base de dados (em modelo de diretório) que desempenha uma função específica dentro de uma Rede de Computadores que utiliza *Windows Server*.

Alguns exemplos de informações que normalmente são armazenadas no AD são:

- Dados de contato do usuário.
- Informações da fila da impressora.
- Dados específicos de configuração do *desktop* ou da rede.

Na figura 4 podemos ver a *interface do Active Directory*.

Figura 4 - Interface Active Directory



Name	Type	Deleted On	Last Known Parent	Time Left Before Purge
Junkyard	organizationalUnit	11/18/2015 12:58:49 PM	OU=Piirala,OU=Bey...	153 days
DummyOU	organizationalUnit	9/24/2015 4:34:45 PM	OU=Piirala,OU=Bey...	98 days
Junk	organizationalUnit	9/16/2015 1:50:11 PM	OU=Piirala,OU=Bey...	90 days
John Boy	user	9/11/2015 8:39:54 PM	OU=Piirala,OU=Bey...	85 days
TermServLicens...	serviceConnectionPoint	9/9/2015 3:40:16 AM	CN=JUMPHOST,CN=...	83 days
Ugly	organizationalUnit	9/4/2015 12:59:46 PM	OU=Piirala,OU=Bey...	78 days
{24D404A1-38E...	groupPolicyContainer	9/4/2015 12:59:09 PM	CN=Policies,CN=Sys...	78 days
User	container	9/4/2015 12:59:09 PM	CN={24D404A1-38E2...	78 days
Machine	container	9/4/2015 12:59:09 PM	CN={24D404A1-38E2...	78 days
Weekend	organizationalUnit	9/4/2015 12:09:31 PM	OU=Piirala,OU=Bey...	78 days
TermServLicens...	serviceConnectionPoint	8/24/2015 8:52:25 PM	CN=JUMPHOST,CN=...	67 days
TermServLicens...	serviceConnectionPoint	8/19/2015 4:16:54 PM	CN=JUMPHOST,CN=...	62 days
TermServLicens...	serviceConnectionPoint	8/14/2015 9:51:07 AM	CN=JUMPHOST,CN=...	57 days
TermServLicens...	serviceConnectionPoint	8/13/2015 7:32:19 AM	CN=JUMPHOST,CN=...	56 days
TermServLicens...	serviceConnectionPoint	8/10/2015 3:59:20 PM	CN=APP1,CN=Com...	53 days
TermServLicens...	serviceConnectionPoint	8/8/2015 1:49:34 PM	CN=JUMPHOST,CN=...	51 days
TermServLicens...	serviceConnectionPoint	8/1/2015 2:13:38 PM	CN=JUMPHOST,CN=...	44 days
TermServLicens...	serviceConnectionPoint	7/22/2015 2:11:17 AM	CN=APP1,CN=Com...	34 days
TermServLicens...	serviceConnectionPoint	7/21/2015 3:53:59 AM	CN=JUMPHOST,CN=...	33 days
TermServLicens...	serviceConnectionPoint	7/16/2015 3:01:20 AM	CN=JUMPHOST,CN=...	28 days
Wedssss	organizationalUnit	7/15/2015 3:09:09 PM	OU=Piirala,OU=Bey...	27 days
UserOld	container	7/15/2015 2:45:42 PM	CN={8C85B6AE-FF3...	27 days
MachineOld	container	7/15/2015 2:45:42 PM	CN={8C85B6AE-FF3...	27 days
TermServLicens...	serviceConnectionPoint	7/15/2015 4:59:40 AM	CN=APP1,CN=Com...	27 days
TermServLicens...	serviceConnectionPoint	7/13/2015 9:16:54 PM	CN=APP1,CN=Com...	25 days
Waffle	organizationalUnit	7/10/2015 2:09:15 PM	OU=Piirala,OU=Bey...	22 days
TermServLicens...	serviceConnectionPoint	7/9/2015 2:55:46 PM	CN=APP1,CN=Com...	21 days
PGODTL_WIND...	defender-tokenLicenseClass	7/7/2015 11:24:22 AM	OU=Defender,DC=b...	19 days
PGODTL_SMS	defender-tokenLicenseClass	7/7/2015 11:24:22 AM	OU=Defender,DC=b...	19 days
PGODTL_PALM	defender-tokenLicenseClass	7/7/2015 11:24:22 AM	OU=Defender,DC=b...	19 days

Disponível em: < <https://images.app.goo.gl/3PmCNnNYqw72UDZz6/>>. Acesso em 30 maio 2020.

Armazenamento de Dados no *Active Directory*

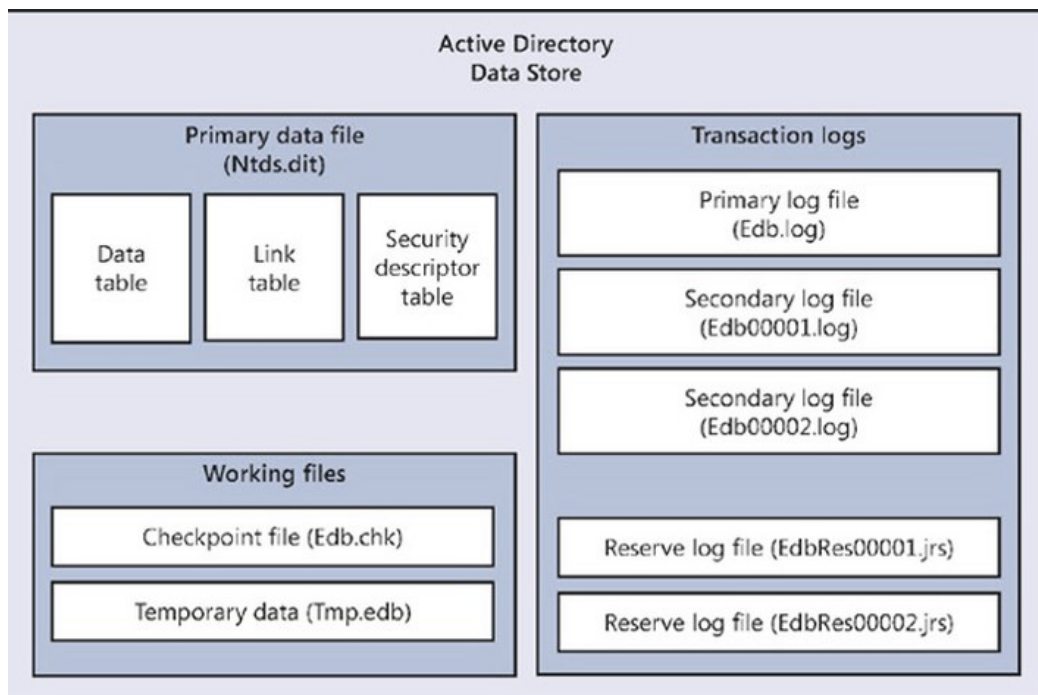
⁸ *Login*: Nome de identificação única dos usuários para acessarem sistemas computacionais ou recursos tecnológicos.

O "Active Directory data Store" (Banco de Dados de *Active Directory*) contém todas as informações do diretório, como informações sobre usuários, computadores, grupos, outros objetos e os objetos aos quais os usuários podem acessar, assim como componentes de rede. Ele permite um gerenciamento de acesso total e controlado.

Estrutura do Active Directory data Store

Na figura 5 temos a estrutura do banco de dados do AD. O arquivo *Ntds.dit* armazena no disco rígido do servidor todos os dados, em uma unidade formatada com o sistema de arquivos *NTFS*. O arquivo *Ntds.dit* é colocado na pasta *Ntds* na barra de sistema. Quando as alterações são feitas no diretório, essas alterações são salvas no arquivo *Ntds.dit*.

Figura 5 - Banco de Dados de *Active Directory*



Disponível em: < <https://images.app.goo.gl/UKLxUpJEYQar4oze7/> >. Acesso em 30 maio 2020.

Este processo gera uma vantagem em relação a disponibilidade destes dados. A disponibilidade de dados é otimizada pelo fato de todos serem armazenados de forma distribuída: significa menos duplicação e menor esforço em administrar.

Cada controlador de domínio hospeda uma cópia de gravação do diretório do *Active Directory*. Isso significa que, se um controlador de domínio não estiver disponível, usuários, computadores e programas ainda podem acessar o armazenamento de

dados do *AD* hospedado em um controlador de domínio diferente no domínio específico.

Quando as alterações são feitas no armazenamento de dados em um controlador de domínio, essas alterações são replicadas para o restante dos controladores dentro do domínio. É importante notar que não é a base de dados inteira, mas apenas os dados de configuração e esquema.

Para que são usados os diretórios?

São utilizados para gerenciar pacotes de *software*, arquivos e contas de usuários finais dentro da organização/instituição. O administrador utiliza os conceitos de árvore e floresta do *AD*, não sendo necessário visitar os *desktops* individualmente.

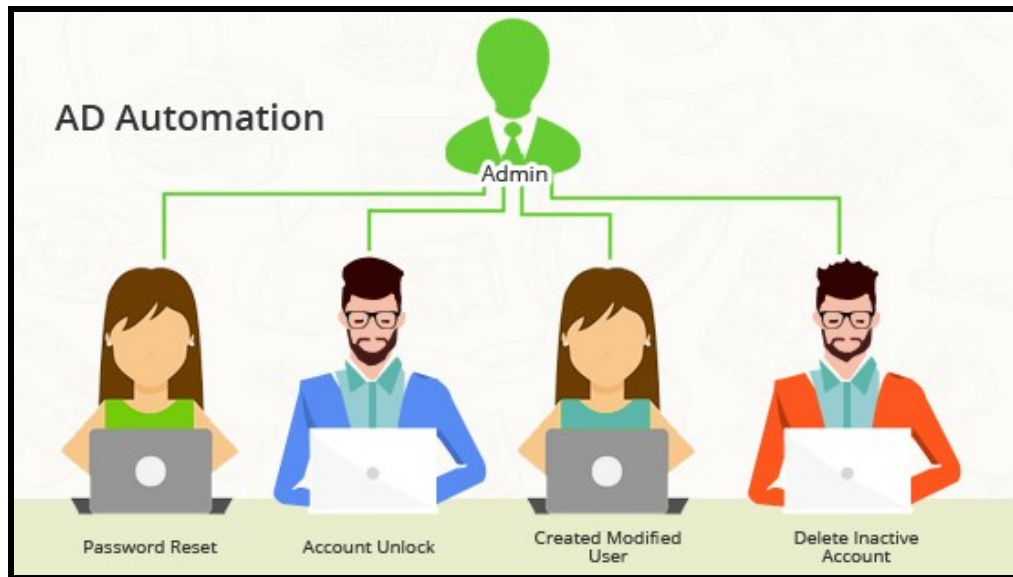
Da mesma forma, o *AD* oferece a capacidade de conceder ou remover acesso no nível de usuário para uma ou várias aplicações ou estruturas de arquivos, que podem estar parametrizadas previamente em uma espécie de grupos de serviços.

Automatização com *AD*

Assim, os diretórios ativos são utilizados para organizar redes e dados em organizações. Embora a curva de aprendizado para operar um *Active Directory* seja significativa, quando operados corretamente, eles podem resultar em uma operação de rede maior e eficiente.

Na figura 6 vemos como o administrador pode organizar as operações para cada grupo de usuário.

Figura 6 - Automação AD



Disponível em: < <https://images.app.goo.gl/mKSapoVaYsb6pQCJA/> >. Acesso em 30 maio 2020.

O que é GPO?

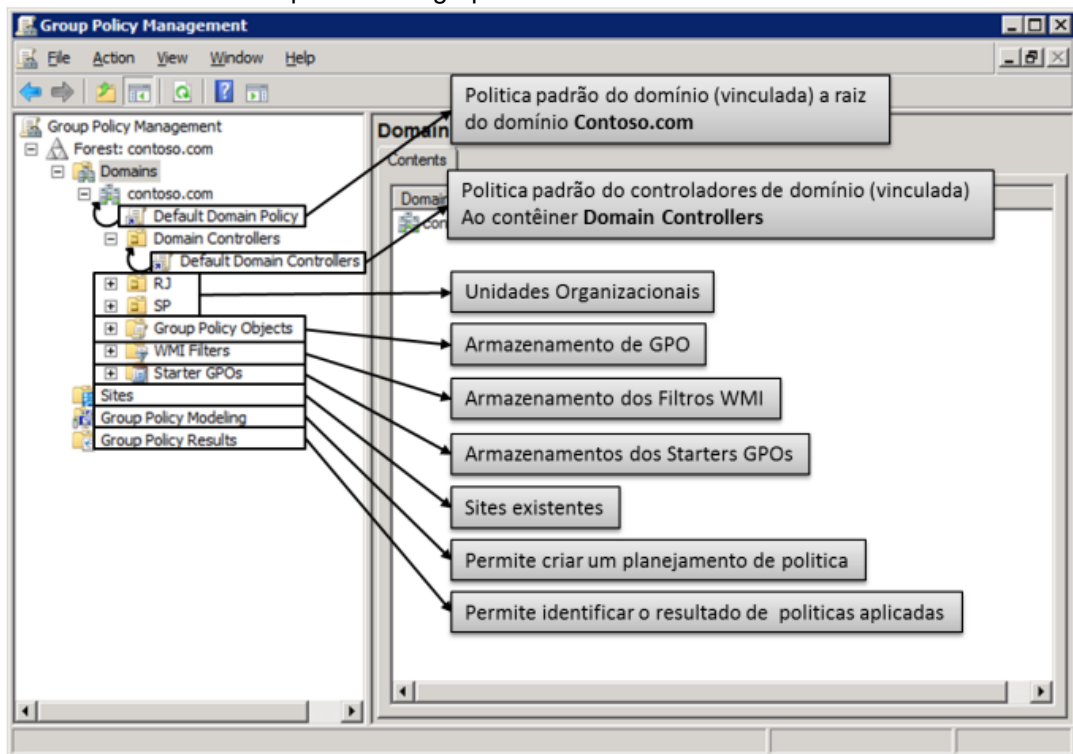
É uma implementação da *Microsoft* de uma metodologia de gerenciamento de computadores e usuários de maneira centralizada, em um ambiente do *Active Directory*. Os Objetos de Diretiva de Grupo (*GPOs*) são as coleções de várias configurações de aplicativo e Registro que foram definidas por um administrador para impor um comportamento específico para um objeto de usuário ou computador. (Gouveia, 2019)

As principais funções das *GPOs* são facilitar o trabalho do administrador da rede, oferecendo recursos que podem ser implementados tanto em sites, domínio ou até mesmos em *OUs* específicas, oferecendo uma segurança e tranquilidade no gerenciamento da rede. Seus principais recursos podem ser designados somente para os usuários que fazem parte do domínio na estação de trabalho quanto para qualquer usuário, que esteja no domínio, localmente na estação de trabalho. As *GPOs* disponíveis no *Windows Server 2008* permitem que as definições configuradas sejam efetivadas em estações de trabalho com *Windows XP* ou posterior. As configurações padrão para as *GPOs* são delimitadas em *enable*, *disable* e *Not Configured*, sendo a primeira função explicitando que a *GPO* escolhida será ativada e as configurações dela replicadas para a situação escolhida, a segunda função informa que a *GPO* estará desabilitada, não sendo configurada e a terceira função, sem alterações, ou seja, não ativa nem desativa o item escolhido. Para realizar a configuração de uma *GPO*, um item importante deve ser analisado com cautela, a hierarquia das *GPOs*. Possui três níveis diferentes: *sites*, domínios e

OUs. Qualquer GPO que seja adicionada ao *site*, será replicado para todos os domínios que fazem parte do *site*, GPOs adicionadas ao domínio, será replicado para todos os usuários e grupos que fazem parte deste domínio e as GPOs adicionadas nas OU será aplicado exclusivamente aos usuários que façam parte dela.

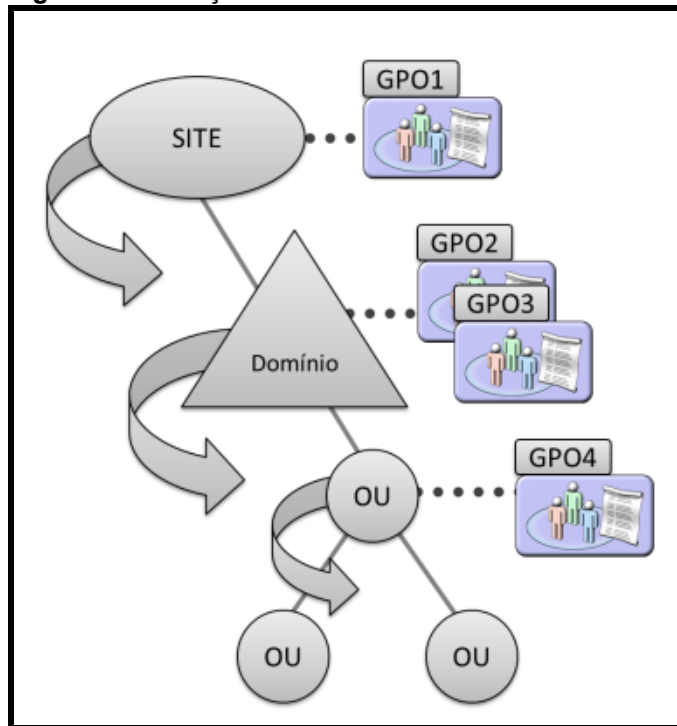
Na figura 7 vemos o *Group Policy Management*, ferramenta para o gerenciamento de política de grupo (GPO).

Figura 7 - Gerenciamento de políticas de grupo



Disponível em: < <https://images.app.goo.gl/d3n81w92S4kR3bjD9/> >. Acesso em 30 maio 2020.

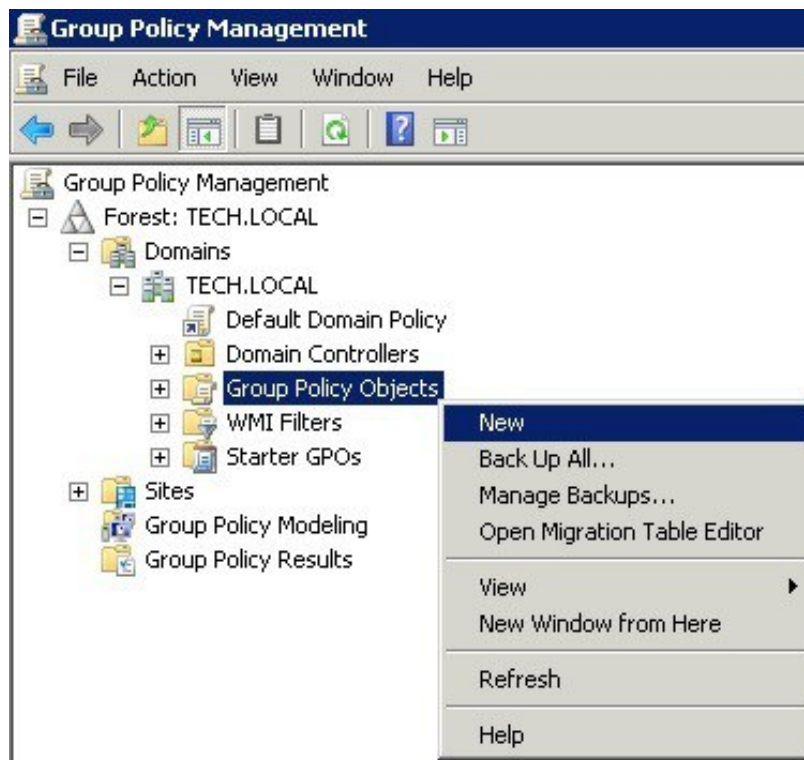
Na figura 8, se houver um computador/usuários em qualquer OU este receberá a GPO1, depois a GPO2, depois a GPO3 e por último a GPO4.

Figura 8 - Herança de GPOS

Disponível em: < <https://images.app.goo.gl/yk7rkcbhHwqyQbHW7/> >. Acesso em 30 maio 2020.

Criar uma GPO.

Criar uma *GPO* não significa que ela faz alguma coisa. Aliás você pode criar um monte de *GPO* que nada acontece até você configurar e vincular (*linkar*). Se você desejar poderá criar uma *GPO* já vinculando em um *OU*. Conforme figura 9 no *Group Policy Management* (Gerenciamento de políticas de grupo) clique com o lado direito em *Group Policy Object* (Objeto de diretiva de grupo) e selecione Novo (*New*).

Figura 9 - Criando uma GPO

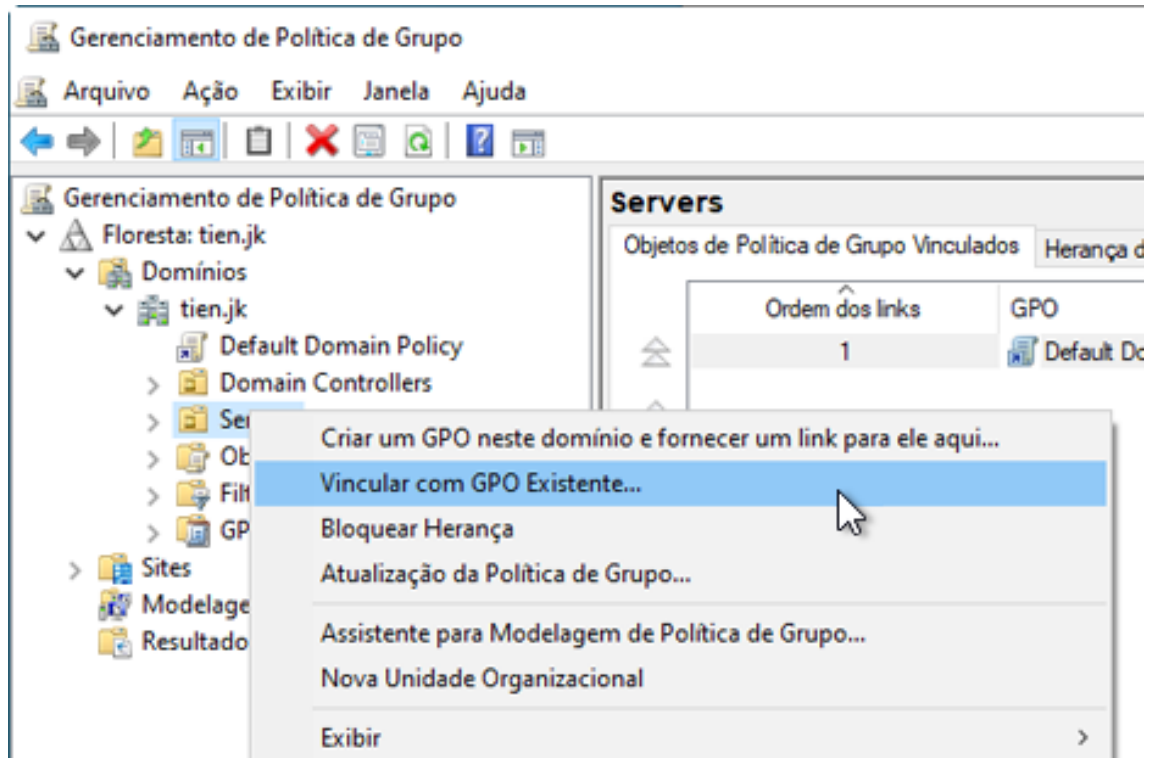
Disponível em: < <https://images.app.goo.gl/bHchz5iD6mdo86sz9/> >. Acesso em 30 maio 2020.

Vinculando GPO.

Você pode criar as GPOs no nó⁹ *Group Policy Objects* e depois vincular, ou você pode criar uma GPO já vinculando a uma OU ou domínio, conforme mostrado na figura 10.

⁹ Nó em redes de comunicação, é um ponto de conexão, seja um ponto de redistribuição ou um terminal de comunicação.

Figura 10 - Vinculando uma GPO

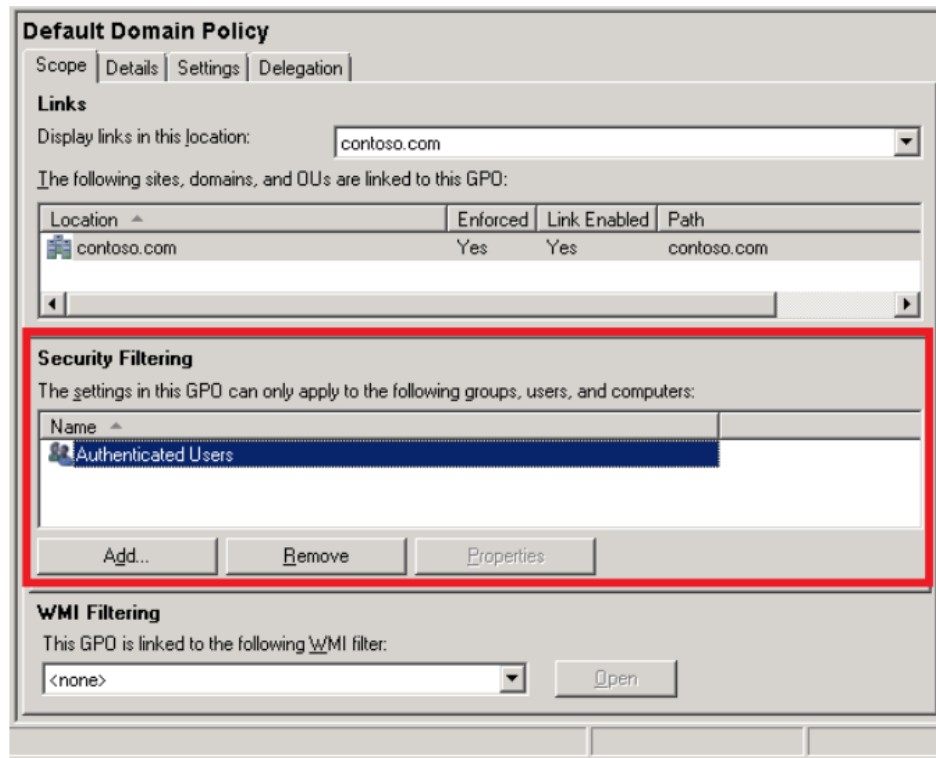


Disponível em: < <https://images.app.goo.gl/MYDfGqJwYHfHVBjCA> >. Acesso em 30 maio 2020.

Criando Filtros de segurança

Após vincular uma GPO você pode ainda criar filtros de usuários ou grupos, assim as diretivas somente serão aplicadas para os grupos de usuários ou computadores que você desejar. Conforme figura 11.

Figura 11 - Diretiva de domínio padrão



Disponível em: < <https://images.app.goo.gl/GKC5TnoVwy3JWZNq7> >. Acesso em 30 maio 2020.

Pense bem, você pode aplicar uma política no Domínio, mas somente o grupo que você definir receberá a política.

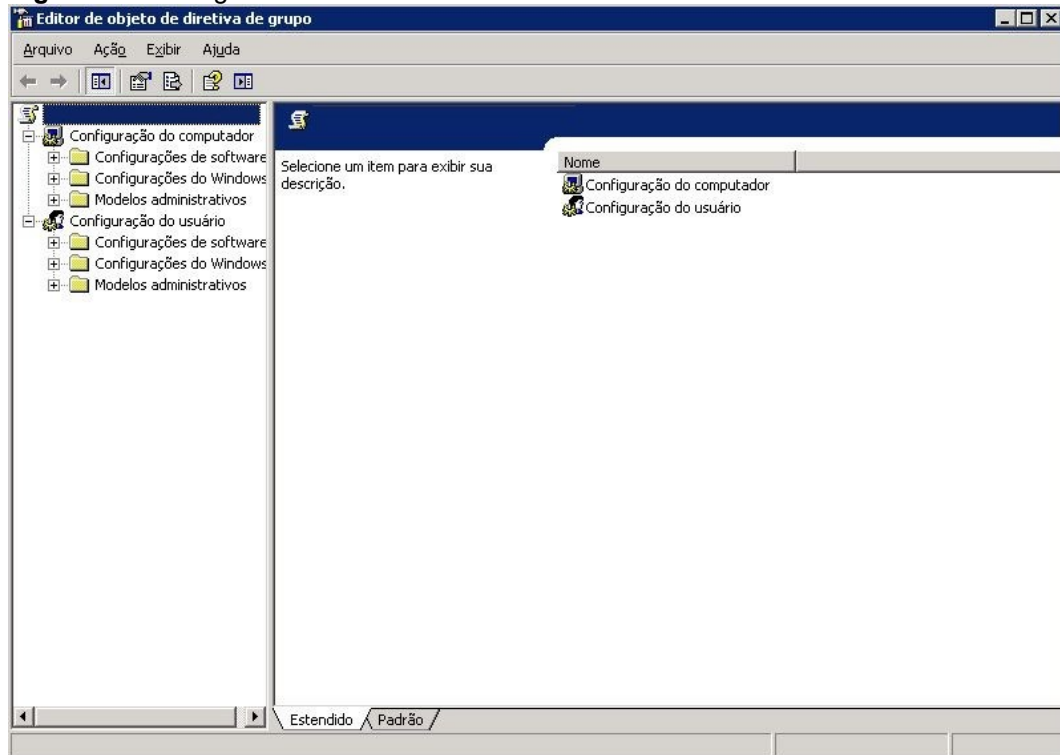
Por padrão recebem as políticas os usuários autenticados.

Configurar (Editar) uma GPO

Agora sim vamos definir o que será aplicado ao computador/usuário.

Você criou e vinculou uma GPO agora é só clicar com o lado direito e selecionar *Edit* (Editar) para que você escolha quais políticas serão definidas. Conforme figura 12.

Figura 12 - Configurar GPO



Disponível em: < <https://images.app.goo.gl/2v99dsrhYKqgK8bi9> >. Acesso em 30 maio 2020.

Nele podemos definir diretivas para:

Computador que são aplicadas quando o *Windows* é carregado e depois entre 90 e 120 minutos.

Usuário que é aplicada quando um usuário faz *login* e depois disso também é atualizada entre 90 e 120 minutos.

Computer Configuration

- **Policies**
- **Software Settings** > Usado para instalação de softwares
- **Windows Settings** > Configuração de *Scripts*, Segurança (senhas, auditoria), *firewall*, *NAP*, restrição de *softwares*.
- **Administrative Templates** > São definições de configuração de registro. Nas versões anteriores ao *Windows* vista a extensão era *ADM*, hoje *ADMX* (bem menor também).

Você pode obter *templates* administrativos no *Microsoft Download Center*, por exemplo, para configurar o *Office*.

- **Preferences** > Recurso no *Windows Server 2008*.

- *Windows Settings*
- *Control Panel Settings*

User Configuration

- ***Policies***
- *Software Settings* > Usado para instalação de *softwares*.
- *Windows Settings* > Configuração de *Scripts* de *logon/Logoff*, restrição de *softwares*. Redirecionamento de pastas, Configuração do *IE*.
- *Administrative Templates* > Assim como para computador são definições de configuração de registro.
- **Preferences** > Recurso novo no *Windows Server 2008*.
- *Windows Settings*
- *Control Panel Settings*

São muitas as diretivas (mais de 3 mil), cada organização/instituição deverá estudar e escolher as que mais se adequam as suas necessidades. No site <https://www.microsoft.com/en-us/download/details.aspx?id=25250> podemos baixar planilhas com todas as diretivas

5 ESTUDO DE CASO

Política de Segurança da Informação (PSI)

Documento de Diretrizes e Normas Administrativas

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da Instituição de Ensino para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

5.1 Aplicações e objetivos da PSI

A Política de Segurança da Informação (PSI) é aplicável ao ambiente estudantil, acadêmico e administrativo e tem por objetivos:

- Estabelecer as diretrizes estratégicas e os princípios para a proteção dos ativos tangíveis e intangíveis, a exemplo da imagem, reputação, e conhecimento, além das informações dos alunos.
- Nortear a tomada de decisão e a realização das atividades profissionais e educacionais de todos os colaboradores da instituição, em ambientes presenciais ou digitais, sempre de acordo com as normas da instituição e a legislação nacional vigente.
- Estabelecer os princípios para o desenvolvimento de atividades educacionais seguras, que afastem danos à reputação da instituição.
- Construir uma cultura de uso seguro das informações, formando indivíduos mais preparados para agir com responsabilidade e segurança na sociedade digital.

- Preservar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a legalidade das informações.
- Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

5.2 Abrangência

Esta PSI é um normativo interno, com valor jurídico e aplicabilidade imediata e irrestrita a todos os alunos e colaboradores, para os ambientes estudantil, acadêmico e administrativo, que venham a ter acesso e/ou utilizam as informações e/ou demais ativos tangíveis ou intangíveis da Instituição de Ensino.

5.3 Diretrizes gerais

5.3.1 Interpretação

- I. Esta PSI deve ser interpretada de forma restritiva, ou seja, casos excepcionais ou que não sejam por ela tratados só podem ser realizados após prévia e expressa autorização do conselho escolar juntamente com a direção.
- II. Qualquer caso de exceção ou permissão diferenciada ocorrerá de forma pontual, aplicável apenas ao seu solicitante, dentro dos limites e motivos que a fundamentaram, cuja aprovação se dará por mera liberalidade da Instituição de Ensino e com duração limitada, podendo ser revogada a qualquer tempo e sem necessidade de aviso prévio.

5.3.2 Propriedade

- I. As informações geradas, acessadas, recebidas, manuseadas ou armazenadas, bem como a reputação, o conhecimento e demais ativos tangíveis e intangíveis são de propriedade e de direito de uso exclusivos da Instituição de Ensino.
- II. Os recursos fornecidos pela Instituição de Ensino, para o desenvolvimento de atividades estudantis, acadêmicas e profissionais, são de propriedade da Instituição de Ensino ou estão a ela cedidos, permanecendo sob sua guarda e posse para uso restrito e, por isso, devem ser utilizados apenas para o cumprimento da finalidade a que se propõem.

- III. Todos os ativos tangíveis e intangíveis da Instituição de Ensino só podem ser utilizados para o cumprimento das atividades profissionais e educacionais, limitados à função do aluno ou colaborador.
- IV. Todos os alunos e colaboradores poderão fazer menção da Instituição de Ensino em conteúdos e materiais, para citação do local onde trabalha, ministra aula ou estuda, mas, em hipótese alguma, poderá a instituição ser utilizada para criação de perfis em mídias sociais em seu nome e/ou se fazendo passar por ela.

5.4 Classificação da informação

- I. Para que as informações sejam adequadamente protegidas, cabe ao colaborador realizar a classificação no momento em que for gerada a informação, para garantir a devida confidencialidade, especialmente no caso de conteúdos e dados pessoais.
- II. Informação pública: informação que pode ou deve ser tornada disponível para distribuição pública. Sua divulgação não causa nenhum dano à instituição e aos alunos.
- III. Informação interna: informação que pode ser divulgada para os alunos e colaboradores da instituição, enquanto estiverem desempenhando atividades educacionais e profissionais. Sua divulgação não autorizada ou acesso indevido podem causar impactos institucionais.
- IV. Informação confidencial: informação exclusiva a quem se destina. Requer tratamento especial. Contém dados pessoais e/ou sigilosos, que, se divulgados, podem afetar a reputação e a imagem da instituição ou causar impactos graves, sob o aspecto legal e normativo.
- V. Rotulagem da informação: quando se tratar de informações não públicas, devem ser rotuladas no momento em que forem geradas, armazenadas ou disponibilizadas.
- VI. Para informações geradas e/ou armazenadas em mídias removíveis ou papel, utilizar carimbo, etiqueta ou texto padronizado para identificação do nível de classificação da informação: interna ou confidencial.

- VII.** Para informações geradas ou mantidas em ambientes lógicos, utilizar documentação específica para definir o nível de classificação da informação, a exemplo de, mas não se limitando a, Políticas de Uso.
- VIII.** Em respeito à classificação da informação, todos os alunos e colaboradores devem respeitar o nível de segurança requerido pela classificação indicada na informação que manusear ou com que vier a tomar contato.
- IX.** Em caso de dúvida, todos deverão tratar a informação como de uso interno, não passível de divulgação ou compartilhamento com terceiros ou em ambientes externos à instituição, incluindo a *internet* e mídias sociais, sem prévia e expressa autorização da Instituição de Ensino.
- X.** Todo colaborador deve respeitar o sigilo profissional e contratual. Por isso, não pode revelar, transferir, compartilhar ou divulgar quaisquer informações confidenciais ou internas, incluindo, mas não se limitando a, informações de outros colaboradores, alunos, fornecedores, prestadores de serviços ou demais detalhes institucionais críticos.
- XI.** Os alunos devem respeitar o sigilo das informações confidenciais ou internas, incluindo, mas não se limitando a, informações de outros alunos e colaboradores da instituição.
- XII.** Toda informação envolvendo dados pessoais de alunos, especialmente o prontuário escolar, e de colaboradores deve ser tratada como sigilosa, utilizada com cautela e apenas por pessoas autorizadas.

5.5 Controle de acesso

- I.** Para cada aluno e colaborador é fornecida um *login* e senha, de uso individual e intransferível, para acesso físico e lógico aos ambientes e recursos da Instituição de Ensino.
- II.** O *login* de cada usuário é monitorado e controlado pela Instituição de Ensino.
- III.** O aluno e o colaborador são responsáveis pelo uso e o sigilo de seu *login* e senha. No caso de uso não autorizado, não é permitido compartilhar, divulgar ou transferir a terceiros.

- IV. Todos os colaboradores, prestadores de serviços e visitantes, enquanto presentes nas dependências físicas da instituição, precisam estar devidamente identificados, portando o crachá individual de forma visível.
- V. O crachá de identificação é de uso individual, não sendo autorizado o compartilhamento com outro colaborador ou terceiro, tampouco o seu uso fora das dependências da Instituição de Ensino.

5.6 Internet

- I. Os recursos de conectividade são fornecidos para atender ao propósito administrativo e educacional, visto que o acesso à *internet* é um direito essencial para o exercício da cidadania no Brasil. No entanto, os alunos e os colaboradores devem fazer uso da *internet* em estrita observância das leis em vigor, respondendo pelo seu descumprimento.
- II. O acesso à *internet* é concedido aos alunos e colaboradores por meio da identidade digital (*login* e senha) pessoal e intransferível, sendo o titular o único responsável pelas ações e/ou danos, se houver.

5.7 Correio eletrônico

- I. A utilização do correio eletrônico educacional deve se ater à execução das atividades profissionais e educacionais, respeitando as regras de direitos autorais, licenciamento de *software*, direitos de propriedade e privacidade.
- II. A utilização de correio eletrônico particular ou público é permitida apenas para a transmissão ou recebimento de conteúdo ou informações particulares, e desde que não lhe seja dada prioridade sobre as atividades profissionais ou acadêmicas, não provoque efeitos negativos para qualquer outro usuário, não viole ou prejudique a rede interna e não viole norma vigente da Instituição de Ensino.
- III. O correio eletrônico particular deverá ser usado somente para interesses particulares do usuário, não podendo ser utilizado para o envio ou recebimento de informações da Instituição de Ensino.

5.8 Rede sem fio (*Wi-Fi*)

- I. A Instituição de Ensino oferece aos seus alunos e colaboradores, limitados ao perímetro físico da instituição, uma rede sem fio (*Wi-Fi*) própria para finalidades educacionais e administrativas.
- II. Somente os alunos e colaboradores expressamente autorizados podem ter acesso à rede sem fio (*Wi-Fi*) da instituição e devem comprometer-se a fazer uso seguro desse recurso.
- III. Em casos excepcionais, visitantes e fornecedores poderão ter acesso à rede sem fio com a prévia autorização da direção e/ou conselho escolar.

5.9 Recursos de TIC institucionais

- I. Os recursos de TIC¹⁰ da Instituição de Ensino são destinados a finalidades estritamente profissionais e educacionais, reservadas às atividades e permissões designadas para os usuários.
- II. É vedado o armazenamento de arquivos pessoais nos recursos de TIC da Instituição de Ensino.
- III. Para a proteção das informações, os arquivos digitais contendo informações da Instituição de Ensino devem ser armazenados no servidor de arquivos da Instituição de Ensino, com acesso restrito, considerando que ameaças externas, tais como vírus, interceptação de mensagens eletrônicas e fraudes eletrônicas podem afetar a segurança de tais informações.
- IV. O conselho escolar juntamente com a direção deverá delegar um responsável por realizar as cópias de segurança dos arquivos digitais (*backup*) armazenados no servidor de arquivos da Instituição de Ensino.

¹⁰ Recursos TIC (recursos de tecnologia de informação e comunicação) - Todos os recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação. Exemplos: computadores, *notebooks*, *smartphones*, *tablets*, discos externos, mídias, impressoras, *scanner*, entre outros.

- V. Só é permitida a utilização de *softwares* e *hardwares* legítimos, previamente homologados ou autorizados pela Secretaria Estadual de Ensino, sejam eles onerosos, gratuitos, livres ou licenciados.
- VI. A utilização de recursos deve ser monitorada, de forma a realizar projeções constantes para que os recursos de TIC suportem necessidades tecnológicas futuras.
- VII. É vedado o uso de recurso de TIC da Instituição de Ensino para acessar, baixar, utilizar, armazenar ou divulgar qualquer conteúdo ilícito, impróprio, obsceno, pornográfico, difamatório, discriminatório ou incompatível com o propósito profissional e educacional da Instituição de Ensino.

5.10 Recursos de TIC particulares

- I. É vedada a conexão dos recursos de TIC particulares na rede da instituição.
- II. Os docentes são autorizados a utilizar os recursos de TIC particulares, conectados à rede, exclusivamente para as suas funções no âmbito educacional, atendendo aos princípios desta Política.
- III. A Instituição de Ensino não tem qualquer responsabilidade sobre a utilização dos *softwares*, arquivos digitais, suporte técnico e manutenções dos recursos de TIC particulares utilizados pelos docentes.
- IV. Os recursos de TIC particulares previamente autorizados a acessar os conteúdos e serviços fornecidos pela instituição devem ser protegidos com uso de métodos de bloqueios de acesso e ferramentas de segurança como antivírus, a fim de mitigar os riscos de exposição da instituição a ameaças.
- V. Todo recurso de TIC particular trazido para as dependências da Instituição de Ensino é de inteira responsabilidade de seu proprietário, incluindo os dados e *softwares* nele armazenados ou instalados.
- VI. A Instituição de Ensino não será responsabilizada por qualquer perda, furto ou avaria dos recursos de TIC particulares.

5.11 Dispositivos móveis particulares:

- I. O uso de dispositivos móveis¹¹ particulares é permitido dentro do perímetro físico da Instituição de Ensino, desde que não interfira nas atividades profissionais e educacionais e esteja de acordo com as leis em vigor.
- II. Convém que o uso de dispositivos móveis particulares pelos alunos, dentro da sala de aula, seja para finalidades educacionais e didáticas. Caso contrário, o uso deve ocorrer com o prévio conhecimento do docente.

5.12 Armazenamento de informações

- I. Todos devem manter as informações da Instituição de Ensino armazenadas no local apropriado e destinado a esse fim.
- II. Os colaboradores devem armazenar as informações digitais da Instituição de Ensino no servidor de arquivos da rede que possui controle de acesso e cópia de segurança. As informações físicas devem ser guardadas em gavetas, armários trancados ou local apropriado e seguro quando não estiverem sendo utilizadas, principalmente quando envolver, mas não se limitando a, documentação de identificação de aluno, provas ou trabalhos educacionais.
- III. A Instituição de Ensino deve solicitar o apagamento e/ou a remoção de conteúdos que estejam nos dispositivos móveis particulares, na *internet*, nas mídias sociais e/ou em aplicativos, sempre que os mesmos oferecerem riscos aos alunos, colaboradores e à instituição, que forem contrários à legislação nacional vigente ou possam configurar algum tipo de dano à instituição.

¹¹ Dispositivos móveis: Equipamentos de pequena dimensão que têm como características a capacidade de registro, armazenamento ou processamento de informações, possibilidade de estabelecer conexões e interagir com outros sistemas ou redes, além de serem facilmente transportados devido à sua portabilidade. Exemplos: *smartphone*, *notebook*, *tablet*, equipamento reprodutor de MP3, câmeras de fotografia ou filmagem.

5.13 Repositórios digitais

- I. Os repositórios digitais são destinados ao armazenamento, à criação, ao compartilhamento e à transmissão de arquivos (*upload*) de informações.
- II. A utilização dos repositórios digitais para o uso institucional deve estar de acordo com os requisitos de segurança descritos nesta Política.
- III. Os repositórios digitais¹² para uso educacional ou acadêmico, objetivando o aprendizado, avaliação ou testes, podem ser utilizados desde que previamente autorizados e homologados pela Instituição de Ensino.
- IV. É vedado armazenar, criar, compartilhar ou transmitir arquivos (*upload*) contendo informações da Instituição de Ensino para repositórios digitais particulares, principalmente, mas não se limitando a, informações sobre alunos e informações pessoais dos colaboradores.

5.14 Mídias sociais

- I. Os alunos devem adotar um comportamento seguro no acesso e utilização das mídias sociais, em conformidade com todos os direitos e deveres estabelecidos no Regimento Escolar.
- II. A participação institucional do colaborador, por meio de acesso e/ou conexão a mídias sociais a partir do ambiente da instituição e durante o horário de trabalho, deve ser diretamente relacionada à sua função profissional e aos objetivos da Instituição de Ensino, sendo o colaborador responsável por qualquer ação ou omissão resultante de sua postura e comportamento.

5.15 Mesa limpa e tela limpa

- I. Os papéis contendo informações da Instituição de Ensino não devem ficar expostos em impressoras, fax, scanner, salas de aula, pátios, telas de computadores, áreas comuns, locais de trânsito de pessoas, refeitório e nas salas de reunião, principalmente quando não estiverem sendo utilizados.

¹² Repositórios digitais: Coleções de informação digital ou serviços de armazenamento, que podem ser mantidos internamente ou armazenados na internet, a exemplo de, mas não se limitando a, Wikipédia, *Microsoft One Drive*, *Google Drive*, *SkyDrive*, *Dropbox*, *iCloud*.

- II. Todos os colaboradores são responsáveis por realizar o bloqueio com senha ao se distanciar do recurso de TIC que estiverem usando, especialmente da sua estação de trabalho ou dispositivo móvel, inclusive quando estiverem em sala de aula.

5.16 Áudio, vídeos e fotos

- I. Não é permitido tirar fotos, gravar, filmar, publicar e/ou compartilhar imagens da Instituição de Ensino, seja da sala de aula, pátios, corredores, banheiros, ou qualquer outro local pertencente ao perímetro físico, e também dos alunos e colaboradores, sem prévia autorização.
- II. Exceto para situações já previamente avisadas e autorizadas, a exemplo de, mas não se limitando a, eventos educacionais, administrativos, sociais e/ou esportivos, por sua natureza pública e de compartilhamento de informações e desde que o teor do conteúdo não exponha ao ridículo ou gere constrangimento aos envolvidos.
- III. Os alunos dependem da autorização prévia do docente para captar ou reproduzir quaisquer imagens, vídeos ou sons, de dentro da sala de aula, inclusive para o registro por imagem da lousa ou do próprio docente, que devem tão somente ser utilizados para fins pessoais, sendo vedado o seu compartilhamento público, seja pela internet ou por outros meios tecnológicos, bem como a divulgação/reprodução do conteúdo a terceiros não integrantes da instituição.
- IV. Exceto em situações já previamente avisadas e autorizadas, a exemplo de, mas não se limitando a, eventos educacionais, sociais e/ou esportivos, passeios, excursões e campeonatos.
- V. Os colaboradores da Instituição de Ensino não devem captar, reproduzir ou compartilhar através de qualquer meio tecnológico, inclusive na *internet*, quaisquer imagens, vídeos ou sons que:
 - a) Possam comprometer a segurança dos alunos, de outros colaboradores e do ambiente estudantil, acadêmico ou administrativo;
 - b) Possam comprometer o sigilo das informações; ou
 - c) Envolvam diretamente a imagem dos alunos, de outros colaboradores,

visitantes, prestadores de serviço e fornecedores, sem a prévia e expressa autorização desses ou do gestor responsável, exceto quando autorizados em razão da sua função ou em situações já previamente avisadas e autorizadas a exemplo de, mas não se limitando a, eventos educacionais, sociais e/ou esportivos, passeios, excursões, campeonatos, por sua natureza pública e de compartilhamento de informações.

5.17 Uso de imagem, som da voz e nome

- I. A Instituição de Ensino pode capturar, guardar, manipular, editar e usar a imagem dos alunos para fins de identificação, autenticação, segurança, registro de atividades, acervo histórico, uso institucional, educativo e social, o que inclui os eventos promovidos pela instituição, inclusive em seus perfis oficiais nas mídias sociais, quadro de avisos, vídeos educacionais, entre outros conteúdos que possam ser criados ou produzidos em razão da atividade educacional, tendo, por isso, pela própria característica técnica da *internet*, alcance global e prazo indeterminado, podendo inclusive alcançar *sites* e outros ambientes digitais externos.
- II. Para o uso de imagem, som da voz e nome dos alunos, estão ressalvados os direitos sobre a integridade da sua honra, sua reputação, boa fama ou respeitabilidade, sendo feito apenas nos limites acordados, sem, de forma alguma, expor o aluno ao ridículo ou a situações constrangedoras, atendendo às leis em vigor no Brasil.

5.18 Aplicativos de comunicação

- I. O uso de aplicativos de comunicação¹³ no ambiente estudantil ou acadêmico, pelos alunos ou docentes, a partir de recursos institucionais ou particulares, para compartilhar informações acadêmicas, deve ser feito de forma responsável para evitar riscos desnecessários que comprometam atividades, projetos ou a própria instituição.

¹³ Aplicativos de comunicação: Programas de computador, geralmente instalados em dispositivos móveis, usados para troca rápida de mensagens, conteúdos e informações multimídia, a exemplo de *Whatsapp*, *Telegram*, *Skype* e *Snapchat*.

- II. O uso de aplicativos de comunicação no ambiente de trabalho ou fora dele, pelos colaboradores da Instituição de Ensino, a partir dos recursos institucionais ou particulares, para compartilhar informações institucionais, deve respeitar sempre o sigilo da informação, atender aos requisitos de segurança previstos nesta Política e respeitar as leis nacionais em vigor para evitar riscos desnecessários relacionados ao vazamento da informação ou que comprometam a instituição.

5.19 Monitoramento

- I. A Instituição de Ensino realiza o registro e armazenamento de atividades (*logs*) e monitora seus ambientes físicos e lógicos, com a captura de imagens, áudio ou vídeo, inclusive com a finalidade de proteção de seu patrimônio e reputação, assim como a proteção daqueles com os quais se relacionam de alguma forma.
- II. O armazenamento dos dados monitorados é utilizado para fins administrativos e legais, além de colaborar com as autoridades em caso de investigação.
- III. Em casos de incidentes de segurança e eventos que comprometam a integridade física e lógica dos alunos e colaboradores, a instituição têm o dever de fornecer informações ao órgão competente para apuração, e quando necessário, disponibilizar provas que estiverem em seu poder ou de cuja existência tiverem conhecimento.

5.20 Combate à intimidação sistemática (*bullying*)

- I. Todos os alunos e colaboradores devem se comprometer a participar de campanhas de conscientização promovidas pela instituição contra atos de violência e intimidação sistemática, bem como a cooperar de todas as formas em situações críticas para a melhor aplicação de medidas preventivas e reativas, e também contribuir para a apuração de fatos e de pessoas envolvidas em casos de *bullying*, comprometendo-se inclusive a fornecer depoimentos, quando necessários, e provas que estiverem em seu poder ou de cuja existência tiverem conhecimento.

5.21 Contratos de trabalho e de prestação de serviços

- I. O mero porte de dispositivos institucionais e o acesso aos recursos de TIC e/ou às informações institucionais, inclusive de forma remota, fora do horário normal do expediente, em qualquer meio ou canal, incluindo, mas não se limitando a, mensagens de alunos e colaboradores em mídias sociais, mensagens SMS, aplicativos e comunicadores instantâneos, por si só, não configuram sobrejornada, sobreaviso ou plantão do colaborador, visto que isso pode ocorrer por ato de liberalidade e/ou conveniência do próprio colaborador sem expressa e prévia requisição da instituição.
- II. Em casos de desligamento, rescisão contratual ou término do contrato, a instituição deve desativar todas as identidades digitais do aluno ou colaborador.
- III. Nesse caso, o aluno ou colaborador deve excluir todas as informações e contas da Instituição de Ensino, disponíveis no dispositivo móvel particular, caso tenham sido cadastradas.

5.22 Segurança da informação

- I. Ao repassar ou transmitir informações da Instituição de Ensino ou sob sua responsabilidade, seja de forma presencial, via telefone, comunicadores instantâneos, mensagens eletrônicas ou mídias sociais, os alunos e colaboradores devem agir com cautela, confirmando antes a identidade do solicitante e a real necessidade do compartilhamento da informação solicitada.
- II. Os alunos e colaboradores devem ter cautela ao acessar *softwares*, informações e conteúdos disponibilizados gratuitamente na *internet*, a exemplo de aplicativos, músicas, vídeos, trabalhos completos, livros físicos digitalizados e *e-mails* com propostas suspeitas, pois podem ser vetores de ataques criminosos.
- III. A Instituição de Ensino deve manter um processo de salvaguarda e restauração dos arquivos digitais críticos, a fim de atender aos requisitos operacionais e legais, além de garantir a continuidade das operações em caso de falhas ou incidentes.

- IV. As informações confidenciais, assim como os recursos de TIC que as contenham, quando descartados, devem passar por procedimento de destruição que impossibilite sua recuperação e o acesso às informações armazenadas por pessoas não autorizadas.
- V. Para a proteção das informações e recursos de TIC críticos, a Instituição de Ensino deve elaborar um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre.
- VI. A Instituição de Ensino está comprometida com o dever de orientar constantemente seus alunos e colaboradores no uso seguro das informações e da tecnologia. Por isso, podem realizar programas de educação em segurança da informação para aumentar o nível de cultura em segurança na instituição.

5.23 Papéis e Responsabilidades

5.23.1 De todos

- I. Conhecer e disseminar as regras e princípios da Política de Segurança da Informação.
- II. Preservar e proteger os ativos tangíveis e intangíveis de propriedade ou sob a custódia da Instituição de Ensino, inclusive todas as suas informações e conteúdo, independentemente do formato ou suporte utilizado, contra todo e qualquer tipo de ameaça, como acesso, compartilhamento ou modificação não autorizada.
- III. Zelar pela proteção do patrimônio da Instituição de Ensino, usando com responsabilidade os recursos físicos e lógicos fornecidos;
- IV. Evitar a exposição desnecessária das informações, projetos, trabalhos e dependências da Instituição de Ensino, inclusive nas mídias sociais e na *internet*, além de agir com responsabilidade no uso dos recursos de TIC e das informações.
- V. Prevenir e/ou reduzir os impactos gerados por incidentes de segurança da informação, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

- VI. Cumprir e manter-se atualizado com relação a esta Política, ao Regimento Interno e às demais Normas de Segurança da Informação da Instituição de Ensino.
- VII. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela Instituição de Ensino.
- VIII. Cumprir o dever de combater a intimidação sistemática (*bullying*), por meio da adoção de medidas preventivas e reativas, bem como da conscientização para coibir e conter toda forma de violência dentro da escola.
- IX. Reportar os incidentes que possam impactar na segurança das informações da Instituição de Ensino imediatamente, por meio do endereço seguranca@instituicaodeensino.com.br.
- X. Ler, preencher e assinar o termo de compromisso de manutenção de sigilo disponibilizado pela Instituição de Ensino e constante no anexo I desta política.

5.23.2 Do Conselho Escolar

- I. Orientar constantemente os alunos e colaboradores quanto ao uso seguro dos ativos tangíveis e intangíveis, e dos valores adotados pela Instituição de Ensino, instruindo-os, inclusive, a disseminar a cultura para os demais alunos e colaboradores.
- II. Suportar todas as consequências das funções e atividades que delegar a outros colaboradores.
- III. Assegurar o cumprimento desta Política e das demais regulações por parte dos alunos e colaboradores supervisionados.
- IV. Participar da investigação de incidentes de segurança relacionados às informações, ativos, alunos e colaboradores sob sua responsabilidade.

5.23.3 Dos colaboradores

- I. Ser cauteloso em relação ao excesso de exposição de sua vida particular, a exemplo de rotinas, trajetos, contatos e intimidades, além do dever de sempre preservar o sigilo profissional nas mídias sociais, a imagem e reputação da instituição, alunos e docentes.
- II. Durante a comunicação, presencial ou digital, com demais colaboradores, alunos, visitantes, fornecedores, prestadores de serviços e outros profissionais, utilizar linguagem respeitosa e adequada, condizente com o ambiente estudantil, acadêmico e administrativo, sem o uso de termos indefinidos, com dupla interpretação, que exponham a intimidade ou que denotem excesso de intimidade, abuso de poder, perseguição, discriminação, algum tipo de assédio moral ou sexual.
- III. Utilizar as mídias sociais evitando excessos de exposição e riscos para a sua própria imagem e reputação, bem como para a instituição.

5.24 Disposições Finais da PSI

O presente documento deve ser lido e interpretado sob o amparo das leis brasileiras, no idioma português, em conjunto com outras normas e procedimentos aplicáveis pela Instituição de Ensino.

Quaisquer atitudes ou ações indevidas, ilícitas, não autorizadas ou contrárias ao recomendado por esta Política ou pelas demais normas e procedimentos de segurança da informação, serão consideradas violações por si só e estarão sujeitas às sanções previstas nos contratos de prestação de serviços, contratos de trabalho e nas demais normas da instituição.

Em caso de dúvidas quanto a esta Política ou aos demais procedimentos de segurança da informação da Instituição de Ensino, o aluno, docente e colaborador podem solicitar os esclarecimentos necessários pelo e-mail: seguranca@instituicaodeensino.com.br.

Os casos de incidente, infração ou suspeita dessas ocorrências deverão ser comunicados imediatamente, pessoalmente ou por meio do endereço seguranca@instituicaodeensino.com.br.

6 CONSIDERAÇÕES FINAIS

Por meio desta pesquisa, e do estudo realizado, foi possível realizar a avaliação de uma instituição de ensino quanto à sua gestão de segurança da informação e métodos de segurança da informação, analisando seus controles e à observação as normas e legislações a que está sujeita.

Foi possível perceber a inexistência de uma gestão da segurança da informação na instituição analisada, e a direção ainda não implementou itens importantes relacionados a política de segurança que continua sendo um assunto crítico, principalmente por não contar com uma política de segurança definida e de acesso a colaboradores e alunos.

Um dos fatores chaves observadas dentro da instituição de ensino analisada é a questão de definições de *GPOs* (diretivas de grupos), na qual definem as políticas de acesso aos serviços: *Internet*, correio eletrônico, redes sem fio, acesso às máquinas laboratoriais, dentre outros. Tais listas protegem os ativos contra tentativas de invasões por parte do corpo discente/docente ou ataques externos à instituição.

Pode-se se observar também que por se tratar de uma instituição pública a direção, não tem plena autonomia para deliberar sobre as questões relacionadas à infraestrutura de tecnologia, o orçamento direcionado aos recursos de TI e a segurança da informação. Existe a falta de uma equipe para tratar dos assuntos relacionados a TI, contando com a boa vontade de colaboradores que possuem algum conhecimento na área para tratar de assuntos como manutenção de dispositivos de tecnologia da informação.

Foi possível também ter a percepção da necessidade de determinadas melhorias em alguns processos tais como a prática de backup e a necessidade de incentivar uma melhor conscientização dos funcionários no que se refere à utilização de senhas de acesso à rede.

Outra observação importante é que a instituição não conta com um servidor de arquivos, ficando os arquivos/informações armazenados nos computadores de uso pessoal necessitando assim do *login* e senha do colaborador que os criou e/ou

salvou.

Após a análise completa é feita a seguinte conclusão: a instituição necessita de cuidados mais sérios sobre a segurança da informação, e a implementação da política de segurança será um bom começo. Essas políticas terão benefícios em curto prazo como a formalização e documentação dos procedimentos de segurança adotados pela instituição, implementação de novos métodos de controles, prevenção de acessos não autorizados.

Fica também a recomendação para que a instituição instale um servidor de arquivos para centralizar o armazenamento e conseqüentemente a busca de informações. Medida simples que irá contribuir muito para a disponibilidade e acesso as informações por ela manipulada.

Para a instituição este trabalho tem relevância porque com a atribuição de políticas de segurança ela ganha uma maior confiança no serviço prestado, além de dar maior estabilidade e credibilidade, devido às boas práticas que deverão ser adequadas aos processos atuais. As melhores práticas além de auxiliar na segurança auxiliam na cultura interna da instituição, auxiliando seus funcionários a prestar um serviço de melhor qualidade.

REFERÊNCIAS

- ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação**. ABNT, 2013.
- CARVALHO, Hugo; SILVA, Pedro; TORRES, Catarina, **Segurança dos sistemas de informação - gestão estratégica da segurança empresarial**. 1ª ed. Lisboa, Portugal: Centro Atlântico, 2003.
- DOLCI, N. Visão geral dos serviços de domínio Active Directory. **Microsoft Docs**, 2017. Disponível em <https://docs.microsoft.com/pt-br/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>. Acesso em 23 de maio.2020.
- FERREIRA, F. N. G, ARAÚJO, M. T. **Política de Segurança da Informação – Guia prático para elaboração e implementação**. 2ed. Rio de Janeiro, Edit. Ciência Moderna, 2008.
- FONTES, E. L. G. **Praticando a segurança da informação**. Rio de Janeiro, Brasport, 2008.
- GOUVEIA, D. Uma introdução básica sobre Group Policy. **TechNet**, 2019. Disponível em <https://social.technet.microsoft.com/wiki/pt-br/contents/articles/52566.uma-introducao-basica-sobre-group-policy.aspx>. Acesso em 23 de maio.2020
- ISACA; **Control Objectives for Information and related Technology (COBIT) – IT Governance Institute**, USA, 2007.
- OFFICE OF GOVERNMENT COMMERCE. **ITIL Security Management**. Londres: The Stationary Office, v3, 2011.
- SAHIBUDIN, S., SHARIFI, M., AYAT, M. “**Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations**”, in *Modeling & Simulation*. AICMS 08. Second Asia International Conference on, 2008.
- SÊMOLA, Marcos, **Gestão da segurança da informação: uma visão executiva**. 2ª ed. Rio de Janeiro: Elsevier, 2014.
- SILVA, P. M. **Recomendações de segurança da informação para soluções de tecnologia da informação e comunicação baseadas em computação em nuvem**. Monografia - UnB, Brasília. 2013. Disponível em https://www.bdm.unb.br/bitstream/10483/14032/1/2013_PauloMatheusNicolauSilva.pdf. Acesso em 11 de jun.2020.

ANEXO I**TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO**

Eu _____, portador (a) do RG nº _____ e inscrito no CPF nº _____, comprometo-me a manter sigilo sobre dados, processos, informações, documentos e materiais que eu venha a ter acesso ou conhecimento no âmbito do ORGÃO, em razão das atividades profissionais a serem realizadas e ciente do que preceituam a Lei 10.406, de 10 de janeiro de 2002 (Código do Processo Penal), no art. 229, inciso I; o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código do Processo Penal), nos arts. 153, 154, 314, 325 e 327; o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), no art. 207; a Lei nº 5.689, de 11 de janeiro de 1973 (Código de Processo Civil), nos arts. 116, 117, 132 e 243; a Lei nº 8.159, de 8 de janeiro de 1991 (Lei de Arquivos), nos arts. 4, 6, 23 e 25; a Lei nº 9.983, de 14 de julho de 2000 (Alteração do Código Penal); o Decreto nº 1.171, de 22 de junho de 1994 (Código de Ética Profissional do Servidor público Civil do Poder Executivo Federal); e o Decreto nº 4.553, de 27 de dezembro de 2002 (Salvaguarda de dados, informações, Documentos e materiais sigilosos).

E por estar de acordo com o presente Termo, assino-o na presença das testemunhas abaixo mencionadas.

Americana, _____ de _____ de 20 _____