UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO SEMIPRESENCIAL EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

PAULO CESAR FERNANDEZ ALCARAZ

DESENVOLVIMENTO DE UMA POLÍTICA DE SEGURANÇA PARA UMA EMPRESA REAL

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2018

PAULO CESAR FERNANDEZ ALCARAZ

DESENVOLVIMENTO DE UMA POLÍTICA DE SEGURANÇA PARA UMA EMPRESA REAL

Monografia de Especialização, apresentada ao Curso de Especialização Semipresencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. M. Sc. Luis José Rohling

CURITIBA

2018

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização Semipresencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes

TERMO DE APROVAÇÃO

DESENVOLVIMENTO DE UMA POLÍTICA DE SEGURANÇA PARA UMA EMPRESA REAL

por

PAULO CESAR FERNANDEZ ALCARAZ

Esta monografia foi apresentada em 23 de Novembro de 2018 como requisito parcial para a obtenção do título de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. M.Sc. Luis José Rohling
Orientador

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Membro titular

_____
Prof. M.Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Dedico este trabalho a Ricardo dos Reis Neto.

RESUMO

ALCARAZ, Paulo Cesar Fernandez. **Desenvolvimento de uma política de segurança para uma empresa real**. 2018. 41 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

A segurança da informação é uma parte essencial em uma organização, é nela que se documenta todas as políticas da empresa, como utilizar cada recurso, quais são os critérios para proteger um dado ou uma informação como: o controle de acesso nas dependências que determina quem pode entrar fisicamente e onde, o tipo de autenticação nas ferramentas da empresa, como elaborar uma senha que seja mais robusta e esteja nas normas da companhia, como utilizar o e-mail corporativo de forma correta, como utilizar a Internet sem que realize nenhuma irregularidade, deveres a ser cumprido nas estações de trabalho. Realizando essas ações, as informações e dados ficam mais protegidos de indivíduos que não pertencem a esse setor ou organização.

Palavras-chave: Política de Segurança. Boas práticas no ambiente corporativo. Segurança da Informação.

ABSTRACT

ALCARAZ, Paulo Cesar Fernandez. **Development of a security policy for a real company**. 2018. 41 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

Information security is an essential part of an organization, it documents all company policies, how to use each resource, what are the criteria to protect a data or information such as: access control in the dependencies that determine who can physically enter and where, the type of authentication in the company's tools, how to create a password that is more robust and is in the company's rules, how to use corporate email correctly, how to use the Internet without performing any irregularities, duties to be fulfilled in workstations. Performing these actions, the information and data are more protected from individuals who do not belong to that sector or organization.

Keywords: Security Policy. Good practices in the corporate environment. Security Information.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A segurança da informação está diretamente relacionada ao sistema onde as mesmas estão armazenadas e quando essa segurança é corrompida, acidentalmente ou não, as consequências são altamente prejudiciais para uma empresa e as pessoas que estão envolvidas. Atualmente, a informação é um dos mais importantes patrimônio de uma empresa, e por esse fator, a criação de uma política de segurança é extremamente significativa dentro, e muitas vezes, fora de uma empresa, para assegurar que seus dados estejam mais protegido possível.

A política de segurança é um procedimento de suma importância que deve ser criada para tornar a rede menos vulnerável, visando garantir uma confiabilidade (o acesso a informação deve ser feito exclusivamente pelas pessoas autorizadas), integridade (é preciso ter a garantia que a informação é confiável) e a disponibilidade (deve estar acessível quando o usuário autorizado precise). Para isso, deve-se interagir com os objetivos da empresa e o plano da política da informação, realizar uma análise para se ter o conhecimento onde estão as prioridades da organização e que impacto pode ocasionar caso não se dê uma devida atenção e proteção dos dados e dessa estrutura empresarial.

A segurança não é uma tecnologia e também não pode ser vista para resolver todos os problemas de uma organização. Segurança é um processo e pode ser aplicada em diversas partes da empresa, o foco é delimitar o acesso de usuários permitindo somente os autorizadas tanto na parte física como na parte lógica, concedendo exclusivamente o ingresso, a alteração ou até mesmo a indisponibilidade do serviço unicamente por essas pessoas. Segundo Wadlow (2000), a segurança deverá ser proporcionada ao valor do que se está protegendo. Parte desse valor é realmente um valor; outra parte é o trabalho necessário para restabelecê-lo; uma outra parte mais sutil é o trabalho que permitirá confiar em sua rede novamente. Agregando esses valores e esses conceitos, possibilita ter a confiabilidade de uma empresa e a credibilidade em sua rede tornando-a mais protegida.

1.1 OBJETIVOS

Nesta seção serão apresentadas os objetivos geral e específicos do trabalho.

1.1.1 Objetivo Geral

Criar uma proposta de uma Política de Segurança em um cenário real para uma empresa do ramo de Tecnologia de Informação com base nas informações e documentações fornecidas pela empresa.

1.1.2 Objetivos Específicos

Para atender ao objetivo geral neste trabalho de conclusão de curso os seguintes objetivos específicos serão abordados:

- Apresentar o conceito de Política de segurança e seus benefícios;
- Apresentar a estrutura atual da empresa;
- Demonstrar a necessidade de segurança física;
- Desenvolver uma política de senha e acessos;
- Demonstrar a necessidade de um conjunto de cuidados com credenciais e dados;
- Desenvolver um conjunto de boas práticas.

1.2 JUSTIFICATIVA

Quando se atua na área de redes, deve-se pensar não somente na questão lógica e física da configuração da rede mas também de como proteger essas informações e dados. Com o objetivo de tentar dificultar ao máximo invasões ou burlagens nos equipamentos e sistemas.

A política de Segurança é um conjunto de boas práticas que devem ser seguidos por todos os membros internos e externos que tem acesso a sua rede. Essa prática tem o objetivo de padronizar e aumentar a segurança das informações de uma empresa e evitar possíveis problemas na corrupção dos dados trafegados na rede.

1.3 ESTRUTURA DO TRABALHO

Esta monografia de especialização está dividida em 6 (seis) seções. Nesta primeira seção foi introduzido o assunto tema do trabalho e também foram abordados a motivação e os objetivos geral e específicos da pesquisa, a justificativa e a estrutura geral do trabalho.

A segunda seção: “CITAÇÕES”**,** engloba todo referencial teórico utilizado para realizar essa monografia, com o objetivo de enriquecer o conteúdo e ter um embasamento consolidado de autores que disponibilizaram suas obras para este assunto da monografia.

Já na terceira seção: “DESCRIÇÃO DO CENÁRIO ATUAL”**,** aborda a forma que a empresa está organizada, expondo todas as informações compartilhadas para realizar a partir do documento recebido uma análise para a proposta da Política de Segurança.

A seguir na quarta seção: “PROPOSTA DE POLÍTICA DE SEGURANÇA”**,** é a parte que realiza cada descrição e explicação da política para o cenário compartilhado da empresa. Esta parte, apresenta os métodos que podem ser aplicados na empresa e suas respectivas explicação.

Na quinta seção: “PROPOSTA DE BOAS PRÁTICAS NOS SWITCHS”, descreve como aumentar o nível da segurança com exemplos realizados na ferramenta *Cisco Packet Tracer* nos switchs da empresa, pois os roteadores são da gestão de cada operadora de Telecom.

Por último na quinta seção: “CONCLUSÃO”, serão retomados a pergunta de pesquisa e os seus objetivos e apontado como foram solucionados, respondidos, atingidos, por meio do trabalho realizado.

2 CITAÇÕES

Não há dúvidas que a informática como um todo é cada vez mais utilizada pelo homem, pois a Tecnologia da Informação têm como o foco trazer facilidade, rapidez, eficiência com o objetivo de produzir maiores resultados em menos tempo. Segundo Nakamura e Geus (2007, p. 44) a rede é uma das essenciais tecnologias, pois permite conexões entre todos os elementos, desde roteadores, servidores que hospedam web sites, banco de dados. Todos esses recursos representam a Era da Informação, isso traz facilidade e flexibilidade resultando em uma maior produtividade e possibilitando a criação de novos serviços e produtos, gerando maior lucro para uma empresa.

Um dos primeiros quesitos que se deve pensar a respeito de redes é sobre a segurança dos dados de quem está utilizando esse meio, para Nakamura e Geus (2007, p. 25) a segurança é um fato que vai além do limite da produtividade e da funcionalidade, para ele a eficiência e a velocidade no conjunto do processo de negócios é uma vantagem competitiva e a falta de segurança nos meios que habilitam a eficiência e a velocidade podem gerar muitos prejuízos e uma ausência de novas oportunidades de negócio.

Já para Stallings (2015, p. 6) a área de segurança de rede e de Internet contempla de medidas para desviar, prevenir, detectar e corrigir violações de segurança que englobam a transmissão de informações. Esse autor também informa que uma definição de segurança de computadores baseado na NIST – *National Institute of Standards Technology* (federal norte americana que lida com a ciência da medição, padrões e tecnologias relacionada ao uso do governo e à promoção de inovação no setor privado dos Estados Unidos da América) a segurança de computadores se dá da seguinte forma: “[...] a proteção oferecida a um sistema de informação automatizado a fim de alcançar os objetivos de preservar a integridade, a disponibilidade e a confiabilidade dos recursos do sistema de informação [...]”.

A partir desta definição, tem-se três conceitos principais denominados de tríade CIA (acrônimo em inglês para *Confidentiality*, *Integrity* e *Availabity*) quando se trata da segurança da informação. Para Stallings (2015, p. 7) seriam as definições da seguinte forma: confidencialidade (para este termo cobre dois conceitos que estão relacionados a confidencialidade de dados que tem por objetivo assegurar que a informação privadas e confidenciais não podem estar disponíveis e nem ser revelados

a indivíduos não autorizados, e o segundo conceito é a privacidade que tem por objetivo assegurar que os indivíduos controlem ou influenciem quais informações relacionadas deles podem ser obtidas e guardadas, da mesma forma que por quem e para quem podem ser reveladas), o segundo objetivo é a integridade (também abrangem dois conceitos, o primeiro é integridade de dados que serve para assegurar que as informações e os programas sejam alterados apenas de uma forma especificada e autorizada, e o segundo conceito é a integridade do sistema que o foco é assegurar que um sistema execute as suas funcionalidades de forma ilesa, sem manipulações deliberadas ou inadvertidas do sistema) o terceiro e último objetivo é a disponibilidade (certifica que os sistemas operem prontamente e não gere indisponibilidade dos seus serviços aos usuários autorizados).

Stallings (2015, p. 7) ainda ressalta dois conceitos adicionais que são necessário quando se refere a objetivos de segurança, são eles: autenticidade (que é a propriedade de ser genuíno e capaz de ser verificado e confiável, significando que se deve verificar que os usuário são quem dizem ser e que a entrada desse sistema venha de uma fonte confiável) e o conceito de responsabilização (a meta de segurança que gera o requisito para que as ações de uma entidade sejam atribuídas somente a elas, os sistemas precisam manter registros das atividades para caso haja necessidades futuras realizar uma análise forense).

Pode-se classificar em níveis de impacto sobre a organização ou aplicar em indivíduos que podem figurar uma quebra de segurança. Stallings (2015, p. 8) descreve três níveis: o primeiro é o baixo, onde a perda representa um efeito limitado nas operações da organização, recursos da empresa ou nos indivíduos. O segundo é o moderado, onde se espera que as perdas representem graves efeitos nas operações da empresa, em seus recursos ou nos indivíduos. O último é alto, representando que a perda esperada possui um efeito muito grave nas operações da organização em seus recursos ou indivíduos.

Na área da Tecnologia da Informação as mudanças são continuas, visando um aperfeiçoamento do que está sendo utilizado em produção. Um fator que leva esse aperfeiçoamento são os ataques que são realizados e também são melhorados a cada instante, sendo assim, o que foi implementado na rede precisa ser revistas de tempos em tempos para corrigir falhas na segurança e impedir que esses ataques sejam efetivados. Para Nakamura e Geus (2007, p. 25) esses ataques são definidos por uma evolução contínua, onde novas formas de proteção são realizadas e

consecutivamente novos ataques são efetuados, assim gera um ciclo, onde a cada novo ataque há uma nova proteção, por isso a segurança deve ser contínua e evolutiva. Isso acontece pois a defesa utilizada pela empresa pode funcionar para um determinado tipo de ataque e para outros não.

Existem alguns fatores a serem considerados para justificar preocupação com a segurança. Nakamura e Geus (2007, p.25) afirmam que esses fatores são: entender a natureza dos ataques é fundamental (muitos ataques são consequências de exploração de vulnerabilidades, pois existe uma brecha no projeto ou na implementação de uma aplicação, serviço, sistema, erros de configuração, protocolos e administração de recursos computacionais). Novas tecnologias trazem novas vulnerabilidades (primeiramente é necessário saber que novas vulnerabilidades aparecem diariamente, como novos sistemas ou tecnologias são criados frequentemente isso acarreta novas vulnerabilidades). Novas formas de ataques são criadas (a combinação de diferentes técnicas, uso de tecnologias para realizar um ataque torna a defesa mais complicada). Aumento da conectividade resulta em novas possibilidades de ataque (a facilidade de acesso traz como efeito o aumento de novos curiosos e também na chance dos disfarces que podem ser usados nos ataques). Existência tanto de ataques direcionados quanto de ataques oportunísticos (ainda que a maioria dos ataques registrados sejam oportunísticos, os ataques direcionados existem em grande número. Os ataques direcionados podem ser considerados mais perigosos, já que com a intenção de atacar a estratégia pode ser pensada, estudada e executada visando explorar a parte mais fraca da empresa. Quanto maior agressivo for o ataque maior é o nível de esforço gasto para acertar o alvo específico, logo a severidade é maior pois há chances de maiores perdas). A defesa é mais complexa do que o ataque (a ausência de um único ponto na segurança, gera que os outros pontos sejam em vão, isso pode gerar uma falsa sensação de segurança na rede). Aumento dos crimes digitais (a legislação para crimes digitais, em alguns países, está em fase de crescimento que acarreta em um obstáculo para inibir ações de crimes digitais).

Nakamura e Geus (2007, p. 47) ainda relatam que a segurança deve ser vista como o componente que concede que novas oportunidades sejam aproveitadas de forma concreta, assim pode-se manter e abrir novos negócios a longo prazo, conseguindo uma credibilidade no área que a empresa está atuando.

Para determinar efetivamente as carências de segurança de uma empresa e escolher diversos produtos e políticas de segurança, é necessário de um meio sistemático para estabelecer os requisitos para a segurança e caracterizar as técnicas para supri-las. Segundo Stallings (2015, p. 10), recomenda a utilização da X.800 da ITU-T (a ITU - *Internation Telecomunication Union* é uma organização internacional dentro do sistema das Nações Unidas, possui esse setor denominado de ITU *Telecommunicaction Standardization Sector*, ou ITU-T, que tem o objetivo de realizar produção de padrões que abrangem todos os campos das telecomunicações) *Security Architecture for* OSI (*Open Systems Interconnection*). A Arquitetura de Segurança OSI é válido para organizar a tarefa de fornecer a segurança. O autor ainda afirma: “Para os nossos propósitos, a arquitetura de segurança OSI oferece uma visão geral útil, abstrata de muitos conceitos [...] Ela focaliza ataques, mecanismos e serviços de segurança.”. Resumidamente, eles podem ser definidas de três formas: a primeira é ataque a segurança (qualquer ação que afete a segurança da informação de uma organização). A segunda é o mecanismo de segurança (é um processo que é projetado para detectar, impedir ou recuperar de um ataque de segurança). A última é a serviço de segurança (serviço de processamento ou comunicação que amplia a segurança dos sistemas de processamento de dados e da transferências de informação de uma empresa).

Para definir ameaça e ataque, o autor Stallings (2015, p. 10) descreve como:

> Na literatura, os termos *ameaça* e *ataque* normalmente são usados mais ou menos para a mesma coisa. [...] oferece a definições retiradas da RFC4949, *Internet Security Glossary*.
>
> **Ameaça**
>
> Uma chance da violação da segurança que existe quando há uma circunstância, capacidade, ação ou evento que poderia quebrar a segurança e causar danos. Ou seja, uma ameaça é um possível perigo a explorar uma vulnerabilidade.
>
> **Ataque**
>
> Um ataque à segurança do sistema, derivado de uma ameaça inteligente; ou seja, um ato inteligente que é uma tentativa deliberada (especialmente no sentido de um método ou técnica) de fugir dos serviços de segurança e violar a política de segurança de um sistema.

Na X.800 e na RFC 4949 existe dois tipos de classificações de ataques a segurança: os ataques passivos e os ataques ativos. Para Stallings (2015, p. 11) um ataque passivo possui uma finalidade de bisbilhotar ou monitorar as transmissões, o propósito é obter informações que estão sendo transmitida na rede. Nesta categoria de ataque existe dois tipos: vazamento de conteúdo de mensagem (facilmente compreendido. Pode ser uma conversa telefônica, uma mensagem de *e-mail* que podem conter informações confidencias ou sensíveis) e o segundo tipo é a análise de tráfego (é mais ameno, onde se pode conseguir informação analisando o trafego da rede para tentar retirar informações importantes, relevantes ou sensíveis). Os ataques passivos são mais trabalhosos de se detectar porque não envolve alteração nos dados, basicamente o emissor e o receptor não tem o conhecimento de que a mensagem foi lida ou foi observado um padrão do trafego. Uma forma de se impedir a leitura da informação seria por encriptação. Os ataques ativos englobam uma modificação do fluxo de dados ou a criação de um novo fluxo de dado falso, podem ser divididas em quatro categorias: disfarce (uma entidade finge ser outra), repasse (captura passiva de uma unidade de dados e a sua retransmissão com o objetivo de produzir um efeito não autorizado), modificação da mensagem (alguma parte da mensagem que é legítima foi alterada ou que as mensagens são reordenadas ou adiadas, com a finalidade de produzir um efeito não autorizado) e a negação de serviço (inibe ou impede o uso ou o gerenciamento normal das instalações da comunicação, podendo ter um alvo específico).

Existem tipos de serviços de segurança que podem ser implementado na rede. Stallings (2015, p. 12) utiliza a X.800 e a RFC 4949 para definir esses serviços, os quais seriam: para a X.800 “[...] define um serviço de segurança como aquele fornecido por uma camada de protocolo de comunicação de sistemas abertos, que garantem a segurança adequada dos sistemas ou das transferência de dados.” Para RFC 4949 seria “[...] um serviço de processamento ou comunicação que é fornecido por um sistema para dar um tipo específico de proteção aos recursos dos sistemas; os serviços de segurança implementando políticas (ou diretrizes) de segurança [...]”.

Para Stallings (2015, p.12) não existe uma definição universal sobre os termos utilizados nas literaturas de segurança. O autor afirma que o termo integridade ocasionalmente é empregado no sentido em que se refere a todos os aspectos da segurança da informação e o termo autenticação às vezes é aplicado para se referir à verificação da identidade.

Visando garantir que a comunicação seja realmente autentica, utiliza-se o serviço de autenticação. Para uma única mensagem, como um sinal de alarme ou uma advertência, Stallings (2015, p. 12) afirma que a autenticação para esse cenário é “[...] garantir ao destinatário que a mensagem tem a origem que ele afirma ter vindo.”. Quando há uma interação entre dois equipamentos, seja ele qual for, dois aspectos são envolvidos. O primeiro aspecto é no instante do início da conexão, o serviço deve garantir que as duas entidades são autenticas, sendo que cada uma deve ser o que afirma ser. O segundo aspecto é que o serviço deve garantir que a conexão não sofra interferência de um terceiro se disfarçando de uma das duas das partes legítimas, para fins de transmissão ou recepção não autorizada. Na X.800 existem dois tipos de autenticação específica: autenticação de identidade pareada (fornece autenticação para a identidade de uma entidade pareada em uma associação, são consideradas pareadas se utilizarem o mesmo protocolo em sistemas diferentes, exemplo: TCP – acrônimo em inglês para *Transmission Control Procotol*) e a segunda é autenticação da origem de dados (fornece uma autenticação para uma origem de uma entidade de dados. Não tem proteção a duplicação ou a modificação das unidades de dados, exemplo: correio eletrônico).

Stallings e Brown (2014, p. 67) afirmam que a autenticação dos usuários é a parte fundamental e a linha de defesa primária. Os autores informam que na RFC 2828 a autenticação de usuário é definida como:

> O processo de identificação de uma identidade alegada por ou para uma identidade de sistema.
>
> **Etapa de Identificação:** Apresentar um identificador de sistema de segurança. (Identificadores devem ser atribuídos cuidadosamente porque identidades autenticadas são a base para outros serviços de segurança, como o serviço de controle de acesso.)
>
> **Etapa de verificação:** Apresentar ou gerar informações de autenticação que corroborem a vinculação entre a identidade e o identificador.

Para realizar a autenticação, existem quatro meios gerais para autenticar a identidade de um usuário, podendo ser utilizados sozinho ou combinados. Stallings e Brown (2014, p. 68) descrevem da seguinte forma: algo que o indivíduo conhece ou sabe (uma senha, um PIN – *Personal Identification Number*, uma resposta a um conjunto de perguntas previamente arranjados), algo que o indivíduo possui (um *token*

– cartões eletrônicos com senhas, smart cards e chaves físicas), algo que o indivíduo é – biometria estática (reconhecimento por impressão digital, retina, face) e algo que o indivíduo faz – biometria dinâmica (reconhecimento por padrão de voz, características de escrita, ritmo de digitação). A autenticação baseada em senha é a mais utilizada contra intrusos, praticamente todos os sistemas multiusuários, servidores baseados em rede, site de comercio eletrônico utilizam esse tipo de autenticação, assim para continuar o acesso é preciso fornecer um identificador (ID) e uma senha. O sistema de autenticação compara o usuário e a senha fornecido com o usuário e senha previamente cadastrado em uma base de dados. A senha tem por objetivo autenticar o ID do usuário que deseja acessar o sistema. O ID tem por objetivo verificar se o usuário está autorizado a ter acesso ao sistema e o tipo de privilégio que esse ID possui.

Seguindo o serviço de segurança de redes, o controle de acesso tem como objetivo precaver o uso não autorizado de um recurso, esse serviço deve controlar, limitar e dominar quem pode ter acesso a um recurso, acesso a aplicações ou a um sistema, ajustando os direitos de acesso a cada indivíduo, afirma Stallings (2015, p. 13).

Para Stallings e Brown (2014, p. 97) o controle de acesso é a parte central de segurança dos computadores. A RFC 2828 define como: “[...] medidas que implementam e asseguram serviços de segurança em um sistema de computador, em particular as que asseguram o serviço de controle de acesso.”. O controle de acesso também engloba as seguintes entidades: Autenticação (identificar se as credenciais são válidas), autorização (determina quem é confiável para uma determinada finalidade, concedendo direito ou permissão a essa entidade no sistema) e a auditoria (revisar e examinar os registros das atividades no sistema com objetivo de testar a adequabilidade dos controles do sistemas).

A confidencialidade de dados é o próximo serviço de segurança de redes, o foco é dar a proteção dos dados contra uma divulgação não autorizada. Para isso é preciso realizar a confidencialidade de conexão, protegendo todos os dados de um usuário na conexão, realizar a confidencialidade sem conexão, proteção dos dados em um único bloco de dados. Também deve realizar a confidencialidade de um campo seletivo, promover a confidencia de campos selecionados dentro dos dados do usuário em um bloco de dados ou conexão. Por último, confidencialidade de fluxo de

tráfego, que consiste em proteger as informações que poderiam ser derivadas do fluxo de dados, informa Stallings (2015, p. 13)

A integridade de dados no serviço de segurança de redes, refere-se que os dados que foram recebidos são exatamente iguais aos que foram enviados, não podendo conter modificação, inserção, exclusão ou repasse do dado na conexão (com ou sem recuperação dos dados), relata Stallings (2015, p. 13).

A última parte no serviço de segurança de redes é a irretratabilidade que impede que o emissor ou receptor neguem uma mensagem transmitida ou recebida em uma comunicação, desta forma não há como uma das partes negarem a participação de parte ou toda a comunicação, afirma Stallings (2015, p.14).

Para o serviço de disponibilidade, Stallings (2015, p. 14) informa que tanto para X.800 quanto a RFC 4949 definem como “[...] a propriedade de um sistema ou de um recurso do sistema de ser acessível e utilizável sob demanda de uma entidade autorizada [...]”. Assim, o sistema deve estar disponível sempre que o usuário requisitar a utilização.

Para Stallings e Brown (2014, p. 438) o gerenciamento de Segurança de Tecnologia da Informação precisa responder três principais questões: Quais ativos precisam ser protegidos? Como esses ativos são ameaçados? O que se pode fazer para contrapor essas ameaçadas? Para isso utilizamos esse processo formal afim de responder essas perguntas. Nos últimos tempos muitos padrões nacionais ou internacionais foram publicados com o objetivo de ter as melhores práticas na área. A ISO – *International Standard Organization* revisou e consolidou esses padrões na série ISO 27000. O autor descreve sete séries da ISO, os quais são: ISO 27000:2019 – “Sistema de Gerenciamento de Segurança da Informação” que define vocabulários e definições usados na família de padrões 27000; ISO 27001:2005 - “Sistema de Gerenciamento de Segurança da Informação” que especifica os requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um sistema de gerenciamento de segurança; ISO 27002:2005 – “Códigos de práticas de gerenciamento de segurança da Informação” fornece diretrizes de gerenciamento de segurança da informação e uma lista de melhores práticas; ISO 27003: 2010 – “Orientação de implementação de Sistemas de Gerenciamento de segurança da Informação” fornece os detalhes dos processos desde a concepção e implementação; ISO 27004:2009 – “Gerenciamento de segurança da informação - medição” orienta as organizações para medir e relatar a afetividade dos processos e controles dos

sistemas; ISO 27005:2008 – “Gerenciamento de riscos de Segurança da Informação” fornece a diretriz de sobre o processo de gerenciamento de riscos; ISO 27006:2007 – “Requisitos para órgãos que fazem auditoria e certificação de sistema de gerenciamento de segurança da informação”, especifica os requisitos e dá orientação a esses órgãos.

Há um material que cada empresa pode realizar e adequar para o seu cenário, visando definir conjunto de normas, métodos e procedimentos para a proteção dos dados e informações que sejam relevantes e importantes. Esse material é comumente chamado de Política de Segurança que para Ferreira e Araujo (2008, p. 36) a definição seria:

> Segundo o livro “Writing Information Securty Policies” de Scott Barman, publicado pela editora New Riders nos Estados Unidos (sem tradução no brasil) a Política de Segurança é composta por um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações e serviços importantes para a empresa recebam a proteção conveniente, de modo a garantir sua confiabilidade, integridade e disponibilidade.

Para realizar esse processo na elaboração deste documento, deve-se empregar uma visão metódica, criteriosa e técnica na elaboração e desenvolvimento de modo que permita sugestões de alteração na configuração do equipamento, na escolha da tecnologia, na definição da responsabilidade e por último na elaboração das políticas com o perfil da empresa e dos negócios que ela realiza. Um quesito de extrema importância é não esquecer que esse documento deve expressar as vontades dos proprietários ou acionistas, pois eles são responsáveis por decidir o futuro da empresa e de todos os recursos da organização em relação a todos que tem acesso as informações e dados. Tem-se como resultado os seguintes aspectos: estabelecimento do conceito de que as informações são extremamente importante para a empresa; A alta administração da empresa tem que estar presente e envolvida com relação a Segurança da Informação; Todos os operadores da empresa tem responsabilidade formal sobre a proteção e garantia dos recursos da informação, definindo o conceito de irrevogabilidade; e por último, estabelecimento de padrões para a manutenção da Segurança da Informação (FERREIRA; ARAUJO, 2008, p.36).

A Política de Segurança deve ser desenvolvida antes de algum problema com a segurança, porém pode ser desenvolvida depois de alguma ocorrência para evitar

reincidência. Ferreira e Araujo (2008, p.37) relatam que, “Ela é uma ferramenta tanto para prevenir problemas legais como para documentar a aderência ao processo de controle de qualidade.” Deve-se deixar bem explicito qual é o escopo, pois pode englobar alguns dos serviços e áreas da empresa. É preciso ter uma visão além de software e hardware que são parte os sistemas, incluindo também os processos de negócios e pessoas, ou seja, deve ser considerado software, hardware, dados e documentação, identificando quem pode ter acesso a cada parte. Os aspectos sobre a segurança dos dados, backups, propriedade intelectual e respostas a incidentes necessitam ser considerados.

Para Ferreira e Araujo (2008, p. 37) é necessário realizar uma reunião com todas as áreas da empresa:

> Recomendamos a formação de um Comitê de Segurança da Informação, constituídos por profissionais de diversos departamentos, como, por exemplo, informática, jurídico, auditoria, engenharia, infra-estrutura, recursos humanos e outros que forem necessários. O Comitê deve catalogar todas as informações da organização e agrupá-las por categorias. Cada uma dessas categorias deverá ter um proprietário que será responsável pelo controle de acesso manuseio e segurança em geral.

O objetivo da Política de Segurança é ser simples, escrita de forma clara e objetiva, homologada e assinada pela alta gerencia, estruturada de forma a permitir sua implementação por fases, deve ser alinhada com a estratégia de negócio da empresa, flexível e priorizar as informações de maior valor e de maior importância (FERREIRA; ARAUJO, 2008, p.38).

3 DESCRIÇÃO DO CENÁRIO ATUAL

A empresa, o nome da referida empresa será omitido por solicitação da mesma, atualmente possui o seguinte cenário implementado.

3.1 SEGURANÇA FÍSICA

Esta empresa possui um controle de acesso por biometria através de digitais e cartões físicos para acesso. O sistema adquirido por uma empresa terceira permite cadastrar colaboradores, terceiros e visitantes. As digitais são para acesso permanente (colaboradores e terceiros) e os cartões são utilizados para acessos de visitantes.

O cadastro dos colaboradores é realizado somente após a contratação e integração, sendo liberados o acesso somente às áreas de atuação e setores corporativos comuns as unidades. O cadastro de visitantes é realizado pela recepção e o visitante só pode acessar as dependências da empresa acompanhado de um responsável.

A portaria dupla permite uma identificação prévia do indivíduo sendo liberado o acesso pela recepcionista e confirmado através da biometria para as dependências da empresa, depois da digital ter sido aceita, na recepção existe uma catraca de acesso e em cada andar tem-se um leitor digital para permitir a entrada ou não a este ambiente. Caso seja a primeiro acesso na empresa somente a recepcionista pode abrir a segunda porta para o indivíduo.

Os setores que necessitem de restrição controlada de acesso também possuem um equipamento de controle de exclusivo. Salas em que existem informações ou acesso a redes de clientes possuem este acesso específico para garantir que somente pessoas autorizadas estejam no local.

O sistema permite realizar relatórios de controle de acesso de modo a validar se somente pessoas autorizadas entraram nas salas bem como os horários de acesso, permitindo cruzar as informações com o sistema de vídeo monitoramento.

Para o monitoramento de vídeo é utilizado outra solução terceirizada que monitora por 24 horas as dependências da empresa e acessos a organização que são situadas na parte externa, estacionamento, recepção, acessos aos andares e salas

de operação (onde os funcionários permanecem realizando o seu trabalho). As imagens são monitoradas e gravadas para que em conjunto com o controle de acesso permita auditar para qualquer eventualidade.

3.2 SEGURANÇA DE REDE ELÉTRICA

Possui um sistema de contingência elétrica com o objetivo de garantir a continuidade das operações na empresa sem que haja riscos de corrupção de dados ou perda de informações. Para isso são disponibilizados *Nobreaks* (ou também chamados de UPS, é responsável por regular a voltagem e a pureza da energia de quem está diretamente conectados a ele, também alimenta os aparelhos por meio de uma bateria quando há queda ou variações bruscas de energia) nos ambientes de produção e no *Data Center* (ou também conhecido como Centro de Processamento de Dados, é um ambiente projetado para concentrar servidores, equipamentos de armazenamento de dados e processamento, sistemas de ativos de rede) há redundância de *Nobreaks*.

As manutenções preventivas são realizadas periodicamente. Nos ambientes operacionais de alta disponibilidade também é provido o uso de nobreak, para que não haja nenhuma interrupção do serviço até o acionamento do gerador.

O sistema de Gerador é movido a *diesel*, de uso *standby* (está ligada na energia elétrica, mas não em utilização) que monitora a rede externa acionando o gerador automaticamente em caso de queda de rede. O gerador possui a capacidade de fornecimento de energia para suprir todas as instalações da empresa.

O gerador possui um plano de testes e manutenção preventiva, sendo realizados starts semanais, manutenções preventivas mensais, por uma empresa especializa e capacitada.

3.3 ESTRUTURA DE REDE

Todos os andares são segmentados por VLANs, além destas VLANs existem as de visitantes, servidores e gestão de equipamentos, também é disponibilizados VLANs independentes para uso de salas dos clientes que seguem o modelo:

i. Rede Compartilhada:

São ambientes que utilizam uma VLAN da empresa, que distribui os endereços e utilizam o domínio da empresa, o controle de licenças, softwares de uso da equipe, antivírus e atualizações são de responsabilidade da empresa.

ii. Rede Mista

São ambientes que utilizam uma VLAN da empresa, porém é o cliente que distribui os endereços de rede e utilizam o domínio do cliente, as licenças de softwares utilizadas podem ser de responsabilidade da empresa ou do Cliente dependendo do estabelecido em contrato.

iii. Rede Isolada

São ambientes totalmente isolados da rede da empresa, onde é recebido diretamente na sala de operação a conexão disponibilizada pelo cliente. Nesta modalidade os equipamentos estão fisicamente na sede da empresa mas na rede do cliente.

A empresa disponibiliza a estrutura de rede redundante garantindo o funcionamento e a continuidade da operação com links de Internet (banda garantida e dupla abordagem em fibra ótica para acesso à Internet, além de uma contingência em fibra ótica e em rádio como operadoras distintas), Firewall (segurança das conexões e VPNs são geridas por um cluster de firewall gerenciável monitorada 24 horas), Switch Core (o isolamento das VLANS e provido pela camada de switch core CISCO 3750 em cluster que permite o correto estabelecimento, gestão e segurança dos segmentos de rede já mencionados), Proxy (para os acesso que utilizam a rede da empresa é efetuado o controle de navegação e filtro de conteúdo permitindo identificar e segregar acessos internos indevidos pelos colaboradores, além de permitir o serviço de proxy) e antivírus (são atualizadas de acordo com a distribuição de patchs automaticamente pelo fabricante, sendo monitorado pela equipe da empresa).

Os equipamentos utilizados para a parte de redes são da marca Cisco e 3COM para Switchs gerenciados pela empresa e os roteadores são gerenciados pelas empresas que fornecem os serviços de telecom.

3.4 ESTRUTURA DA TELEFONIA

O sistema contratado pela empresa permite o controle das ligações de entrada e correto direcionamento das filas de ligações e URAS de recebimento de chamadas e de pesquisas, bem como a gravação de todos os canais em áudio compatível de mercado para auditorias e gerenciamento de não conformidades nos atendimentos.

4 PROPOSTA DA POLÍTICA DA SEGURANÇA

Para a realização desta proposta, será utilizado somente as informações fornecidas e explicitas no capítulo anterior, desta forma se assume que o que não foi compartilhado não está implementado ou em uso pela empresa.

Todas as normas estabelecidas terão que ser seguidas por todos os funcionários ou terceiros da empresa que ao receber os termos da Política de Segurança compromete a respeitar todos os tópicos abordados, e também está ciente que sua navegação na internet ou intranet e os e-mails podem ser monitorados.

Um fator primordial para a proteção das informações e dados é que cada usuário adote a ação de Comportamento Seguro que consiste na proteção das informações, devendo assumir atitudes proativas e engajadas em relação à proteção das informações e dados.

A empresa necessita realizar campanhas contínuas em relação a Política de Segurança, disponibilizando quando um funcionário é contratado e de tempos em tempos realizar um reforço, seja por avisos contínuos via e-mail e por plataformas de treinamento online para realizar a reciclagem do conhecimento.

A empresa também precisa atualizar a Política de Segurança, de acordo com sua necessidade, tendo que passar por uma revisão e aprovação, geralmente a cada ano. Desta forma, se garante que o que foi implementado realmente condiz com a realidade da empresa e atende os requisitos para preservação dos dados ou informações.

Quando um funcionário tiver dúvida se aquilo afeta a Política de Segurança a primeira ação é procurar o seu supervisor direto, enviar um e-mail ou gerar um ticket para o setor de Tecnologia da Informação manifestando a sua dúvida e sendo claro e direto para sanar os seus questionamentos.

O não cumprimento da Política de Segurança pode acarretar desde advertências verbais ou escrita e dependendo da gravidade, até o desligamento do funcionário por não cumprimento dessas normas.

4.1 CONTROLE DE ACESSO AS DEPENDÊNCIAS

No ato da contratação, deve-se deixar claro quais são as dependências comuns e quais são as dependências de acesso restrito. Qualquer indivíduo que tentar entrar em uma área onde não é permitido deve ser investigado e auditado para evitar qualquer tipo de burlagem e comprometimento dos dados ou informações.

O acesso a qualquer dependência da empresa tem que obrigatoriamente autenticar cada pessoa que deseja entrar em alguma parte da organização, impedindo qualquer forma de “carona” (que é quando uma pessoa libera o acesso e outras passam junto para o ambiente). Essa informação tem que ser fornecida a partir do momento que o colaborador faz parte do quadro de funcionários e reforçada para todos que pertencem a empresa via e-mail geral corporativo e cartazes informativos espalhados pela organização. Tem que se evitar que em áreas que não são de uso comum qualquer colaborador possa entrar no ambiente.

Como os acessos as dependências da empresa são através de um sistema terceiro que permite o cadastro de colaboradores, terceiros e visitantes, é necessário que seja implementado no processo de desligamento de um colaborador o bloqueio a entrada física na empresa, se o mesmo não pertence ao quadro de funcionários da organização, não pode ter mais acesso a qualquer dependência desacompanhado. Também é necessário a devolução no ato da rescisão contratual de todos os tipos de todas as propriedades do empregado como: crachás, chaves de acesso, hardware, software, todos os documentos em qualquer formato (notas, atas de reuniões, lista de clientes, diários e livros de endereço, impressões de computador, planos, projeções, custo de dados, dados de mercado, desenhos) juntamente com todas as suas cópias. Esses quesitos são primordiais para evitar que colabores desligados de nenhuma forma consigam qualquer acesso físico ou através de seu e-mail coorporativo da empresa com o objetivo de furtar alguma informação ou dado e repassar a terceiros.

Nenhum equipamento de rede pode estar desprotegido fisicamente pela empresa, ou seja, o *rack* sempre deve permanecer trancado e somente pessoas autorizadas podem ter acesso para o desbloqueio do *rack* e dessa forma ter o acesso ao equipamento. Esse controle deve ser realizado pelo setor de Tecnologia da Informação da área de Redes, desta forma se evita que qualquer funcionário tenha acesso aos *hardwares*.

Nenhum equipamento gerenciável deve estar desprotegido com um usuário e senha especifica para cada funcionário, e também deve-se ter cada privilégio dependendo do tipo de acesso que o funcionário pode realizar. Esses acessos tem que estar atualizados e assim evitar que um funcionário tenha algum tipo de acesso que não pertence mais a sua função atual. É dever do administrador da rede permitir ou não um acesso a um funcionário, bem como seus privilégios. De nenhuma forma pode-se informar ou disponibilizar o acesso à senha *enable* (privilégio maior no equipamento).

4.2 AUTENTICAÇÃO

A autenticação nos sistemas da empresa é através de usuários e senhas, em virtude de ser o meio mais utilizado, fácil de implantar e possui uma manutenção de baixo custo, porém esse é o meio mais inseguro e precauções devem ser tomadas. Senhas com combinações simples (1234abcd), substantivos (caderno, mesa, computador), datas (01012018) são fáceis de descobrir e burlar.

4.3 POLÍTICA DE SENHAS

Todo usuário deve ter uma identificação única, pessoal e intransferível e para uma senha com mais segurança deverá conter no mínimo 8 caracteres contendo: letras minúsculas, letras maiúsculas, carácter especial (!@#$) e números. Pode-se utilizar padrões mnemônicas (baseado em formas simples de memorizar maiores construções) como: R3de$!10 (redes!10), c1$c0*07 (cisco*07), sW1tCh!9(switch!9). Utilizar um método próprio para lembrar-se da senha, de modo que ela não precise ser anotada em nenhum local, em nenhuma circunstância.

As senhas terão um prazo de validade de 90 dias corridos e passando esse tempo sem a troca da senha, o usuário não poderá acessar os sistemas.

Em nenhuma hipótese a senha deve ser compartilhada com outra pessoa dentro ou fora da empresa. Quando o funcionário sentir desconfiado por qualquer motivo, o mesmo pode trocar sem esperar a validade da senha chegar.

Qualquer ação que for executada com a senha do usuário é de responsabilidade dele, sendo assim, é dever de cada um proteger sua senha da melhor forma que achar conveniente.

4.4 POLÍTICA DE E-MAIL

E-mail corporativo deve ser usado para assuntos corporativos, não utilize e-mail da empresa para os assuntos pessoais. É vedado o uso de sistemas webmail externo.

É proibido o uso do correio eletrônico para envio de mensagens que possam comprometer a imagem da empresa perante seus clientes e a comunidade em geral e que possam causar prejuízo moral e financeiro.

Por questões de vírus e outros tipos de software maliciosos, não devem ser abertos anexos com as extensões *.exe*, *.bat*, *.src*, *.lnk*, caso não haja a total certeza de que foi solicitado isso.

Não utilizar o e-mail para enviar grande quantidade de mensagens (caracterizada por *spam*) que possam comprometer a capacidade da rede da empresa, não reenviando e-mails do tipo corrente, aviso de vírus, avisos da *Microsoft/Symantec*, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e qualquer tipo boatos virtuais.

Utilizar o correio eletrônico para comunicações oficiais internas, as quais não necessitem do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura de documentos.

Deve-se desconfiar de todo o e-mail recebido com assuntos totalmente desconhecidos ou até mesmo estranhos, pois muitos vírus dos últimos tempos tinham assuntos que não eram assuntos de ambientes corporativos.

4.5 POLÍTICAS DE ACESSO A INTERNET

As navegações na Internet devem ser para uso corporativo, enriquecimento intelectual ou como ferramenta de busca de informação para conclusão de uma tarefa, seu uso deve ser consciente. Não se pode utilizar em horário de trabalho para outras

funções como: jogos, bate-papo, site de apostas, pornográfia, redes sociais (se não é da função do empregado).

As ferramentas *peer-to-peer* (P2P) não podem também ser utilizadas sem uma autorização do setor de Tecnologia da Informação.

Utilizar no ambiente de trabalho ferramentas de mensagem instantânea (IM) não autorizadas ou homologadas é expressamente proibido sem a devida autorização e liberação da área de Tecnologia da Informação.

O uso da Internet é auditado constantemente e por qualquer irregularidade ou suspeita de irregularidade o usuário poderá prestar contas do uso indevido.

4.6 POLÍTICA DE USO DAS ESTAÇÕES DE TRABALHO

Cada funcionário possui a sua estação de trabalho, sendo assim, tudo que venha a ser executado nesta estação é de responsabilidade do usuário. Sempre ao sair da sua estação de trabalho, deve-se certificar que o computador foi bloqueado (*logoff*) ou travou o console.

É expressamente proibido instalar qualquer tipo de software sem a autorização do setor de Tecnologia da Informação. Todos os equipamentos já vem com os *softwares* necessário para executar a função e necessitando de alguma acessão, deverá ser solicitado.

Filmes, músicas e qualquer outro tipo de pirataria não pode estar nos computadores.

Todos os dados da empresa devem ser mantido em um servidor, desta forma se evita que dados sensíveis estejam a vista de outros funcionários.

As mídias removíveis como *pen drive*, CDs, HD externo, não deve ser utilizada sem a devida autorização do setor de Tecnologia da Informação, justificando o motivo do seu uso para a liberação dessas mídias removíveis. A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais.

Quando o expediente de trabalho finalizarr, o funcionário deve desligar o seu equipamento.

4.7 ENGENHARIA SOCIAL

Engenharia social é um termo utilizado para definir um método de ataque a uma pessoa, com o objetivo de obter informações sigilosas ou importantes, desta forma, o engenheiro social manipula psicologicamente a pessoa para execução de ações ou divulgar alguma informação sigilosa. Pode se manifestar de muitas formas, o mais comum é dividí-las em duas formas: direta (caracterizado pelo contato direto entre o engenheiro social e a vítima) e indireta (caracterizado pela utilização de software ou ferramentas de invasão como os vírus, cavalos de troia através de e-mails ou sites).

Essa prática se aproveita a falta de treinamento com relação a Política de Segurança da empresa, na qual o funcionário não considera a informação que está passando como importante. Em alguns casos, o engenheiro social não está interessado em conseguir senhas ou ter acesso a uma área restrita e sim informações privilegiadas.

4.8 CLASSIFICAÇÃO DA INFORMAÇÃO

O supervisor ou gerente de cada setor é responsável por definir os critérios relativos ao nível de confiabilidade de alguma informação de acordo com os seguintes critérios: Pública (informação da empresa dedicado à divulgação do público em geral, sendo seu carácter informativo, comercial ou promocional); Interna (informação da empresa que ela não tem interesse em divulgar, onde o acesso por indivíduos é restrito); Confidencial (informação crítica para os negócios da empresa) e Restrita (toda a informação que pode ser acessada somente por usuários da empresa, explicitamente indicado pelo nome ou pela área que pertence).

5 PROPOSTA DE BOAS PRÁTICAS NOS SWITCHS

Nos Switchs da marca Cisco (os modelos não foram disponibilizados pela empresa que impede as especificações), para exemplificar a implementação e trazer mais para a realidade possível, será utilizado o *Switch Generic* no Cisco Packet Tracer. A primeira boa prática a ser inserida é um padrão de nomenclatura para cada Switch que está alocado fisicamente, como por exemplo: SW_1AND_SL01 (Figura 1). Para isto, deve-se entrar no modo global e utilizar o comando *hostname* em seguida o nome e pressionar enter.

Figura 1 - Hostname Switch

```
Switch(config)#hostname SW_1AND_SL01
SW_1AND_SL01(config)#
```

Fonte: Autoria própria.

A segunda boa prática é inserir um *banner* que serve para alertar o usuário que deseja entrar no equipamento, isso tem que ser visto como um aviso e não “boas vindas”. Para realizar essa ação, o comando *banner motd [delimitador] TEXTO [delimitador]* deve ser inserido no modo global, como mostra a Figura 2.

Figura 2 - Banner Switch

```
Switch(config)#banner motd $
Enter TEXT message.  End with the character '$'.
##############################################################################
#                                                                            #
#          **UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED**              #
#                                                                            #
#   You must have explicit, authorized permission to accessor configure this #
#   device. Unauthorized attempts and actions to access or use this system   #
#   may result in civil and/or criminal penalties.                           #
#                                                                            #
#   All activities performed on this device are logged and monitored.        #
#                                                                            #
##############################################################################
$
```

Fonte: Autoria própria.

Todo equipamento Cisco vem por padrão com a VLAN 1 e é assignada a todas as portas. É a VLAN 1 de gerencia por padrão. Ela não deve ser utilizada para evitarmos problema de segurança e também porque todas as portas estão no mesmo domínio de broadcast. Não se consegue deletar essa VLAN 1, quando se tenta aparece uma mensagem: “Default VLAN 1 may not be deleted” e também não se consegue renomear. Para contornar essa situação, cria-se outras VLANs, como a 10

representando a sala 10 e a 11 representando a sala 11 da empresa, e assigna a cada porta que pertence essa VLAN. Para isso, utiliza o comando *vlan 10*, depois *name [nome da VLAN]*, como apresentado na Figura 3.

Figura 3 - VLAN 10 e VLAN 11

```
SW_lAND_SL01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_lAND_SL01(config)#vlan 10
SW_lAND_SL01(config-vlan)#name salal0
SW_lAND_SL01(config-vlan)#exit
SW_lAND_SL01(config)#vlan ll
SW_lAND_SL01(config-vlan)#name salall
SW_lAND_SL01(config-vlan)#exit
SW_lAND_SL01(config)#
```

Fonte: Autoria própria.

Para assignar cada VLAN a sua porta pertencente, deve-se entrar na interface, escolher o modo acesso, atribuir essa VLAN a esta porta, como mostra a Figura 4. Não é possível inserir mais de uma VLAN para a mesma porta física.

Figura 4 - Atribuir VLAN na porta

```
SW_lAND_SL01(config)#interface fastEthernet 0/1
SW_lAND_SL01(config-if)#switchport mode access
SW_lAND_SL01(config-if)#switchport access vlan 10
SW_lAND_SL01(config-if)#interface fastEthernet 3/1
SW lAND SL01(config-if)#switchport mode access
SW_lAND_SL01(config-if)#switchport access vlan ll
```

Fonte: Autoria própria.

Com o comando *show vlan* é possível ver a configuração realizada, desta forma tem que retirar todas as portas físicas da VLAN 1, como mostra a Figura 5.

Figura 5 - Verificando as VLANs

```
SW_1AND_SL01#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   sala10                            active    Fa0/1, Fa1/1, Fa2/1
11   sala11                            active    Fa3/1, Fa4/1, Fa5/1
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
11   enet  100011     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Fonte: Autoria própria.

Todas as portas as físicas que não são utilizadas devem ser desligadas com o comando *shutdown* em cada porta, como apresentado na Figura 6.

Figura 6 - Shutdown na porta

```
SW_1AND_SL01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_1AND_SL01(config)#interface fa2/1
SW_1AND_SL01(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet2/1, changed state to administratively
down
SW_1AND_SL01(config-if)#interface fa5/1
SW_1AND_SL01(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet5/1, changed state to administratively
down
```

Fonte: Autoria própria.

O comando *show ip interface brief* verifica quais portas estão administravelmente desligada e seus status, como mostra a Figura 7.

Figura 7 - Status das portas

```
SW_1AND_SL01#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual down                  down
FastEthernet1/1        unassigned      YES manual down                  down
FastEthernet2/1        unassigned      YES manual administratively down down
FastEthernet3/1        unassigned      YES manual down                  down
FastEthernet4/1        unassigned      YES manual down                  down
FastEthernet5/1        unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

Fonte: Autoria própria.

As vantagens de se utilizar VLANs é que proporciona uma segurança maior, pois os tráfegos das redes não se misturam com outros segmentos. O custo é reduzido, sendo que um equipamento pode separar logicamente vários segmentos da rede, desta forma permite que um hardware realize múltiplas tarefas. Desempenho melhor na rede já que os domínios de *broadcast* serão aplicados somente nas VLANs que pertence e não na rede toda.

Para que se possa gerenciar esses equipamentos, o primeiro passo é inserir um usuário e uma senha em cada equipamento. Por questão de limitação do *Cisco Packet Tracer*, nenhum *Switch* permitiu a configuração do *radius* (servidor de autenticação). Para configurar um usuário e senha, deve-se utilizar o nome da chave RSA, criar a chave de criptografia escolhendo a quantidade de bits, determinar um tempo em segundos para encerrar a sessão, número máximo de tentativas de acesso, criar um usuário com o privilégio que deseja (1 a 15) e a senha, entrar na configuração *ssh* e inserir o *login* local, habilitar o *ssh* versão 2 e replicar para a porta console o usuário e senha criado, como mostra a Figura 8.

Figura 8 - Implementando usuário e senha local

```
SW_1AND_SL01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_1AND_SL01(config)#ip domain-name empresa.com
SW_1AND_SL01(config)#crypto key generate rsa
The name for the keys will be: SW_1AND_SL01.empresa.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SW_1AND_SL01(config)#ip ssh time-out 120
*mar 1 2:14:37.925:  %SSH-5-ENABLED: SSH 1.99 has been enabled

SW_1AND_SL01(config)#ip ssh authentication-retries 2
SW_1AND_SL01(config)#username adminsw1 priv 15 secret Alc@r259
SW_1AND_SL01(config)#line vty 0 15
SW_1AND_SL01(config-line)#transport input ssh
SW_1AND_SL01(config-line)#login local
SW_1AND_SL01(config-line)#exit
SW_1AND_SL01(config)#ip ssh version 2
SW_1AND_SL01(config)#line console 0
SW_1AND_SL01(config-line)#login local
SW_1AND_SL01(config-line)#exit
SW_1AND_SL01(config)#
```

Fonte: Autoria própria.

Para configurar o *radius*, no equipamento Cisco que permite, deve-se aplicar as linhas de comando apresentadas na Figura 9.

Figura 9 - Habilitar radius

```
# aaa new-model
# aaa authentication login default group radius local
# aaa authorization exec default group radius local
# radius-server host [IP_SERVIDOR_RADIUS]
# radius-server key [SENHA_RADIUS]
# crypto key generate rsa
# [bits]
# ip ssh version 2
# line vty 0 15
#   login authentication default
#   transport input ssh
#   exit
```

Fonte: Autoria própria.

A configuração de acesso de gerenciamento remoto, para funcionar de uma forma correta, deve ser criada uma *Switch Virtual Interface* (SVI) que é uma interface virtual que representa uma determinada VLAN. A SVI da VLAN não aparecerá “up/up” até que a VLAN seja criada e haja um dispositivo conectado a uma porta do *Switch* associado a esta VLAN (Figura 10).

Figura 10 - SVI de gerência

```
SW_1AND_SL01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_1AND_SL01(config)#interface vlan 99
SW_1AND_SL01(config-if)#ip address 192.168.99.10 255.255.255.0
SW_1AND_SL01(config-if)#no shutdown
SW_1AND_SL01(config-if)#end
SW_1AND_SL01#
%SYS-5-CONFIG_I: Configured from console by console

SW_1AND_SL01(config)#interface fastEthernet 0/1
SW_1AND_SL01(config-if)#switchport access vlan 99
% Access VLAN does not exist. Creating vlan 99
SW_1AND_SL01(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

SW_1AND_SL01(config-if)#
```

Fonte: Autoria própria.

Para completar o gerenciamento remoto, a partir de redes que não estão diretamente conectadas, deve-se configurar o *gateway* padrão, como apresentado na Figura 11. Este *gateway* é o reteador ao qual o switch está conectado. Como não foi compartilhado informações de roteadores, os quais pertencem as operadoras de Telecom, não se tem conhecimento do IP real implementado, desta forma será abstraído essa informação e focado em como implementar no equipamento.

Figura 11 - Gateway padrão

```
# configue terminal
# ip default-gateway 192.168.99.1
# end
```

Fonte: Autoria própria.

A senha *enable secret* (Figura 12), é a senha mais forte de um equipamento Cisco, tem o privilégio 15. Ela é requerida quando se tenta entrar no modo EXEC privilegiado. A diferença entre a *enable secret* e a *enable password* é que a primeira é criptografada por padrão e a outra não. Esta senha não deve ser compartilhada, somente o administrador que tem a total permissão pode ter acesso a essa informação.

Figura 12 - Enable

```
SW_1AND_SL01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_1AND_SL01(config)#enable secret Sw1*1@nD4r
SW_1AND_SL01(config)#exit
SW_1AND_SL01#
```

Fonte: Autoria própria.

Uma estratégia utilizada para proteger as portas do switch é aplicar em cada porta um regras de segurança, podendo fixar um endereço *MAC* específico que se conecta nesta porta e um modo de violação e aplicar o modo de violação: a) *protect* (número de endereços MAC seguros atinge o limite permitido na porta, pacotes com endereços de origem desconhecidos são ignorados até que se remova um número suficiente de endereços MAC seguros ou aumente o número máximo de endereços permitidos. Não notifica quando houve uma violação de segurança), b) *restrict*, apresentado na Figura 13, (número de endereços MAC seguros atinge o limite permitido na porta, pacotes com endereços de origem desconhecidos são ignorados até que você remova um número suficiente de endereços MAC seguros ou aumente o número máximo de endereços permitidos. Avisa. Notifica que houve uma violação de segurança, através de uma interceptação SNMP que é enviada, uma mensagem syslog é registrada em log e o contador de violação é incrementado), ou c) *shutdown* (neste modo a violação de segurança de porta faz com que a interface seja desabilitada para erro imediatamente e apaga o LED da porta. Envia uma interceptação SNMP, registra em log uma mensagem syslog e incrementa o contador de violação. Habilitada por padrão).

Figura 13 - Restrição na porta: Estático

```
SW_1AND_SL01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_1AND_SL01(config)#interface fastEthernet 1/1
SW_1AND_SL01(config-if)#switchport port-security
SW_1AND_SL01(config-if)#switchport port-security mac-address
0006.2AA0.6A63
Port-security not enabled on interface FastEthernet1/1.
SW_1AND_SL01(config-if)#switchport port-security violation
restrict
SW 1AND SL01(config-if)#
```

Fonte: Autoria própria.

Também é possível aprender dinamicamente os MAC utilizando o *sticky* que é salvo na configuração de execução. Podendo aplicar a quantidade de MAC que

pode aprender. Para isso, deve-se entrar na porta desejada e inserir os comandos apresentados na Figura 14.

Figura 14 - Restrição na porta: Dinâmico

```
SW_1AND_SL01(config)#interface fastEther 3/1
SW_1AND_SL01(config-if)#switchport port-security
SW_1AND_SL01(config-if)#switchport port-security maximum 3
SW_1AND_SL01(config-if)#switchport port-security mac-address
sticky
SW_1AND_SL01(config-if)#
```

Fonte: Autoria própria.

Cada alteração deve ser salva com o comando *copy running-config startup-config*, apresentado na Figura 15, desta forma evita que quando o switch for reiniciado as configurações sejam perdidas.

Figura 15 - Salvando as alterações

```
SW_1AND_SL01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW_1AND_SL01#
```

Fonte: Autoria própria.

Uma boa prática é manter uma rotina de backup das configurações do equipamento, caso aconteça do switch queimar ou necessitar da configuração por qualquer motivo, ela esteja salva e segura. Cada empresa tem que atentar a necessidade de quanto tempo é necessário para realizar os backup, podendo ser mensal, semestral, anual ou a cada modificação no equipamento. Para salvar o arquivo, pode-se utilizar FTP ou TFTP, estar com o privilégio 15, inserir o comando *copy running-config tftp: (ou ftp:)*, o endereço do serviço e o nome do arquivo, como apresentado na Figura 16.

Figura 16 - Utilizando TFTP para salvar

```
# copy running-config tftp:
Address or name of remote host []? [IP_SERVIDOR_TFTP]
Destination filename [SW_1AND_SL01-confg]? BKP_SW1_04012019
```

Fonte: Autoria própria.

Para recuperar a configuração, pode-se utilizar tanto FTP quanto TFTP, para isso, deve estar no equipamento com privilégio 15, inserir o comando *copy tftp (ou*

ftp): running-config, ip do servidor e o nome do arquivo, como apresentado na Figura 17.

Figura 17 - Utilizano TFTP para recuperar

```
# copy tftp: running-config
Address or name of remote host []? [IP_SERVIDOR_TFTP]
Source filename []? BKP_SW1_04012019
Destination filename [running-config]?
```

Fonte: Autoria própria.

6 CONCLUSÃO

A política de Segurança é um dos fatores essências em uma organização, é ela que define como se deve comportar no ambiente corporativo em relação a segurança, o que se pode realizar com as informações da empresa, como se deve atuar com as ferramentas que estão dispostas e como proceder caso tenha algum problema ou precise de alguma exceção. Um funcionário que é mal orientado, pode gerar grandes perdas a empresa, inclusive financeira.

Cada pessoa possui seu padrão de profissionalismo exclusivo de cada profissão, padrões presentes no código de ética da profissão e princípios morais. A integridade, imparcialidade e cuidado deve ser exercidas diariamente e cabe a cada funcionário cumprir que os valores da empresa seja efetivo e realizado.

No cenário atual, os clientes estão zelando por cada dado e informação, a partir do momento que se perde essa relação, pode haver rompimento de contrato, gerar incredibilidade no mercado empresarial e a empresa ser vista como inconfiável para gerir, tratar ou resolver o seguimento que a companhia escolheu.

REFERÊNCIAS

FERREIRA, Fernando Nicolau Freitas; ARAUJO, Márcio Tadeu de. **Política de segurança da informação: Guia prático para elaboração e implementação**. 2 ed. Rio de Janeiro: Ciência Moderna, 2008.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes coorporativos**. 1. ed. São Paulo: Novatec, 2007.

STALLINGS, William. **Criptografia e segurança de redes: Princípios e práticas**. 6. ed. São Paulo: Pearson, 2015.

STALLINGS, William; BROWN, Lawrie. **Segurança de Computadores: Princípios e práticas**. 2 ed. Rio de Janeiro: Elsevier, 2014.

WADLOW, Thomas. **Segurança de redes: projeto e gerenciamento de redes seguras**. Rio de Janeiro: Elsevier, 2000.