INSTITUTO DE ENSINO SUPERIOR - FACULDADE LABORO
TECNÓLOGO EM REDES DE COMPUTADORES

JOSÉ RONALDO DA SILVA PEREIRA
THIAGO VINICIUS SANTANA PINHEIRO

SEGURANÇA DA INFORMAÇÃO: Aplicação de mecanismo de segurança da informação em pequenas e médias empresas

TRABALHO DE CONCLUSÃO DE CURSO

SÃO LUÍS - MA
2018

JOSÉ RONALDO DA SILVA PEREIRA
THIAGO VINÍCIUS SANTANA PINHEIRO

SEGURANÇA DA INFORMAÇÃO: Aplicação de mecanismo de segurança da informação em pequenas e médias empresas

Trabalho de Conclusão de Curso apresentado ao Curso Tecnólogo em Redes de Computadores da Faculdade Laboro, para obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Prof. Esp. Carlos Rayllan Lima Sousa

SÃO LUÍS - MA
2018

JOSÉ RONALDO DA SILVA PEREIRA
THIAGO VINÍCIUS SANTANA PINHEIRO

Trabalho de Conclusão de Curso apresentado ao Curso Tecnólogo em Redes de Computadores da Faculdade Laboro, para obtenção do título de Tecnólogo em Redes de Computadores.

Aprovado em: / /

BANCA EXAMINADORA

_____

Prof. Esp. Carlos Rayllan Lima Sousa (Orientador)

_____

Prof. Ms. Milson Louseiro Lima

_____

Prof. Ms. Yanna Leidy Ketley Fernandes Cruz

DEDICATÓRIA

“Dedico este trabalho a minha mãe, Dolores Maria Silvia Santana, por ser essencial em minha vida, por nunca ter deixado de acreditar em mim.”

“Dedico este trabalho primeiramente a Deus, por ser essencial em minha vida, autor de meu destino, meu guia, socorro presente na hora da angústia, ao meu pai José Ribamar Oliveira Pereira, minha mãe Gracinete feitosa da Silva Pereira e ao meu irmão Rogério da Silva Pereira.”

AGRADECIMENTOS

Agradeço ao meu orientador Prof. Esp. Carlos Rayllan Lima Sousa, pela sabedoria com que me guiou nesta trajetória.

Aos meus colegas de sala, em especial ao José Ronaldo, uma pessoa que me ajudou bastante, espero um dia poder retribuir.

A minha fámilia, Dolores Maria Silvia Santana, Hana Leticia Santana Pinheiro e Alanna Nascimento Delgado Mota, sem ela não teria condições de concluir nenhum desafio.

A Secretaria do Curso, pela cooperação.

Enfim, a todos os que por algum motivo contribuíram para a realização desta pesquisa.

EPÍGRAFE

“O sucesso nasce do querer, da determinação e persistência em se chegar a um objetivo. Mesmo não atingindo o alvo, quem busca e vence obstáculos, no mínimo fará coisas admiráveis.”.

José de Alencar

RESUMO

A segurança da informação é algo de extrema importância mas em muitos casos ignorada, tanto no ambiente domestico quanto no corporativo. As pequenas empresas costumam ser mais displicentes ainda com esse ponto. O objetivo deste trabalho é mostrar os principais erros e ataques que um usuário sofre diariamente e tentar conscientizar que a segurança da informação é algo que deve ser valorizado e implantado nas empresas. No trabalho também foi abordado a pontencialiazação da segurança em uma empresa, modificando a sua estrutura, com equipamentos e softwares, deixando mais segura.

Palavras-chave: Ataques. Segurança. Informação. Trabalho.

ABSTRACT

Information security is extremely important but in many cases ignored, both in the domestic and corporate environments. Small businesses tend to be more nonchalant about this point. The objective of this work is to show the main mistakes and attacks that a user suffers daily and try to make aware that information security is something that should be valued and implemented in companies. The work also addressed the safety enhancement in a company, modifying its structure, with equipment and software, making it safer.

Keywords: Attacks. Safety. Information. Work.

LISTA DE FIGURAS E ILUSTRAÇÕES

LISTA DE ABREVIATURA E SIGLAS

PSI – Politíca de Segurança da Informação

LAN – Local Area Network

USB – *Univesal serial Bus*

AVG – Anti-virus Guard

SUMÁRIO

1. INTRODUÇÃO

Assim como no mundo real, o mundo cibernético também é passível de pessoas com má índole, que tentam se apropriar de informações de outras pessoas ou empresas. Com o crescimento da internet, diversas ferramentas para obter essas informações foram desenvolvidas. Palavras como vírus, *worms* e trojans, já não são mais novidade para quase ninguém que as lê ou ouve. Uma das principais causas para a disseminação dessas pragas virtuais, nada mais é do que a falta de conhecimento do usuário, que acreditam que foram vencedores de um concurso que nunca nem participaram, ou herdeiros de uma herança de um tio distante.

No ambiente corporativo, esse problema se torna mais grave ainda, pois informações importantes da empresa podem ser fornecidos em apenas alguns segundos. O administrador da rede não deve apenas se preocupar com os equipamentos que fazem parte do ambiente mas também com os usuários. Para isso, foram criadas as políticas de segurança da informação, ou simplesmente PSI. A segurança da informação, muita das vezes é ignorada, imaginando que nunca serão alvos, abrindo ainda mais as portas para ataques. "A segurança da informação de uma empresa garante, em muitos casos, a continuidade de negócio, incrementa a estabilidade e permite que as pessoas e os bens estejam seguros de ameaças e perigos." [BLUEPHOENIX, 2008].

Este trabalho, aborda o uso das Políticas de Segurança da Informação para a proteção desses dados.

1.1 JUSTIFICATIVA

Criar uma consciência aos usuários e diretores sobre segurança da informação em pequenas e médias empresas.

Entender a importância do conhecimento sobre Eng. Social.

Entender métodos de prevenção a ataques e espionagem empresarial.

1.2 OBJETIVOS:

1.2.1 Geral

Introduzir técnicas e políticas de segurança da informação no ambiente corporativo, principalmente nas pequenas e médias empresas, dificultando a ação de pessoas que tem como objetivo se apropriar de dados privados.

1.2.2 Específicos

Entender o valor da segurança da informação nas empresas, como forma de evitar perda de dados sigilosos.

Alertar fatores que influenciam pequenas empresas a adotarem técnicas de gestão de segurança da informação e analisar o grau de importância dos mesmos.

Incentivar a prática de treinamentos e capacitar o colaborador sobre engenharia reversa e técnicas de phishing para obtenção de dados.

Desmistificar que para obter um nível satisfatório de segurança da informação basta ter um bom antivírus instalado e atualizado no seu computador ou que o antivírus se tornou peça obsoleta no combate a ataques.

2. FUNDAMENTAÇÃO TÉORICA

2.1 INFORMAÇÃO

A Informação é um conjunto de dados que inserido dentro de um contexto passa a ter significado para organização. Hoje a informação é considerada o bem maior da empresa privada e órgãos público.

De acordo com a norma ISO 27002 (2005), informação “é um ativo, que como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente precisa ser adequadamente protegida” e ainda na mesma norma entende-se que é “qualquer coisa que tenha valor para a organização”.

Existe três conceitos de segurança voltados a informação, que são eles:

2.1.1.Segurança Física

Lugar onde ás informações tem que ser protegidas contra ameaças cibernética.

2.1.2.Segurança Lógica

Estabelecer controles de acesso lógico que tem como objetivo apenas para usuários autorizados.

2.1.3.Segurança em Recursos Humanos

Todos os colaboradores devem saber e cumprir as políticas de segurança da informação bem como participar dos treinamentos periódico estabelecido pela corporação.

2.2 SEGURANÇA DA INFORMAÇÃO

Segurança da Informação refere-se à proteção de dados valiosos e importante para corporação e ou órgãos contra acesso não autorizado e roubo de informação.

Segurança da informação é a proteção da informação contra possíveis ameaças com o intuito de garantir a continuidade do negócio, minimizar o risco ao

negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio (ISO 27002, 2005).

Abaixo considerado os três pilares da segurança da informação:

2.2.1.Confidencialidade

A privacidade dos dados em questão deve ser garantida. Os dados devem ser protegidos contra acesso não autorizado(OLIVEIRA, 2018).

2.2.2.Integridade

A veracidade dos dados deve ser garantida. A existência de proteção contra mudanças não-autorizadas no sistema deve ser existir(OLIVEIRA, 2018).

2.2.3.Disponibilidade

O sistema deve fornecer as informações sempre que for solicitado. O serviço não pode ser interrompido(OLIVEIRA, 2018).

Figura 1

2.3 TIPOS DE ATAQUES

Segundo o Sebrae, existem 6,4 milhões de estabelecimentos e desse total, 99% são micro e pequenas empresas. O número de ataques a essa enorme fatia só cresce e muitos dos responsáveis por essas empresas ainda acham que estão seguros, pois quem atacaria uma pequena empresa no meio de tantas, ou por qual motivo estaria sujeito a uma falha de segurança?

Estão listados abaixo alguns dos principais ataques e falhas de segurança:

Phishing

Software desatualizados

Downloads de fontes desconhecidas

Ransomware

2.3.1.*Phishing*

O *phishing* é um ataque que tem como objetivo, ganhar a confiança do usuário leigo, com pouco conhecimento em informática, pois simula um site real, um e-mail de algum banco ou promoção de alguma loja online. Um exemplo prático de *phishing*, é o recebimento de um e-mail, informando que o produto X está com 50% de desconto, ou que a sua conta no banco Y foi invadida e você precisa clicar no *link* enviado para corrigir o problema. Realizando esses passos, as informações digitadas, serão enviadas para a pessoa que realizou o ataque e ficara de posse de seus dados.

2.3.2 *Software* desatualizados

Um problema grave, são os *softwares* desatualizados, pois a grande maioria das atualizações são correções de *bugs* e falhas do programa. Os *hackers* se aproveitam dessas falhas para conseguir obter informações. O usuário, por falta de tempo ou conhecimento, acaba negligenciando as atualizações dos *softwares*, um

bom exemplo, são os antivírus com a base de dados desatualizada, pois os vírus mais recentes, com pouco tempo de descobertos, não estão inseridos nos antivírus mais antigos, por isso o fabricante disponibiliza a atualização.

2.3.3 *Download* de fontes desconhecidas

Este e mais um tipo de ataque que busca o usuário com menor conhecimento, ao tentar fazer um *download* de um *software* ou arquivo, o usuário não se preocupa de onde está sendo feito este *download*. A internet permite o compartilhamento em esfera global, o *software* que você deseja pode estar vindo de uma fonte do outro lado do mundo, essa fonte pode ter modificado esse mesmo *software* com algum tipo de vírus ou trojan e infectar seu dispositivo. Por isso é sempre importante fazer *downloads* diretamente do site oficial do desenvolvedor, pois a garantia de que o item não foi modificado é maior.

2.3.4 *Ransoware*

Segundo o AVG, importante empresa de segurança da informação, *ransomware* é um software maligno que criptografa arquivos em seu computador e bloqueia completamente seu acesso a eles. Ele se espalha através de cibercriminosos que exigem um resgate (geralmente entre 300 e 500 dólares/libras/euros, preferivelmente pagos em *bitcoins*), declarando que, ao pagar, você receberá uma chave de descriptografia para recuperar seus arquivos

O usuário não tem garantia nenhuma que conseguirá reaver seus dados, apenas a palavra do criminoso.

2.4 BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

2.4.1 Controle de Acesso

Os controles de acesso são práticas de segurança da informação executada em um ambiente computacional com o objetivo de controlar acessos aos dados.

2.4.2 Controle de Acesso Lógico

Os controles de acesso lógico são procedimentos e medidas de controle de proteção de dados, programas e sistemas contra *malware* e tentativas de acesso feitas por pessoas não autorizadas.

Existem duas formas de encarar o controle de acesso lógico: a partir de algum recurso computacional a qual se quer proteger e ao usuário a quem foi disponibilizado alguns privilégios e acessos aos recursos.

A proteção aos recursos computacionais, é baseada na necessidade de acesso de cada usuário, quando um usuário solicita uma requisição e coloca suas credências, o sistema se encarrega de verificar a autenticidade.

2.5 RECURSOS QUE DEVEM SER PROTEGIDOS

Uma boa proteção das informações e recursos em um ambiente computacional tende em proteger aplicativos, arquivos de dados, utilitários e sistema operacional.

2.5.1 Aplicativos

O acesso não autorizado ao código fonte dos aplicativos assim podendo ser alterado o código fonte do mesmo. Por exemplo, um sistema de uma empresa que armazena credências de cliente para acesso de portal do cliente e assim tendo acesso a todas as contas dos clientes.

2.5.2 Arquivos de dados

Base de dados onde contêm informações que devem ser protegidos para que não sejam apagados ou alterados sem autorização. Por exemplo, arquivos de configuração do sistema, informações estratégica da empresa.

2.5.3 Arquivo de senha

Geralmente as empresas não se preocupam em ter uma proteção adequada dos arquivos que contêm as senhas de usuários, sistemas e até administradores dos sistemas, então se algum usuário mal intencionado obtiver esses arquivos com

senhas ele poderá ter acesso a vários sistemas, se caso for as credencias de administrador ele poderá ter acesso à sistemas se passando por administrador sem muitos problemas.

2.5.4 Arquivos de logs

Os arquivos de log são arquivos onde ficam registrado todas as ações do sistema e usuários, nele se sabe horário e data de acesso ao sistema, qual usuário acessou o sistema, toda ação que esse usuário realizou quando logado.

A maioria dos invasores ou programa malicioso vão em busca do arquivo de log para apagar todas suas ações efetuada, para que os administradores ou especialista forense não o possa rastrear.

2.5.5 Sistema Operacional e Utilitários

Um acesso a um utilitário, como compiladores e *software* de monitoração e diagnóstico deve ser restrito devido que essas ferramentas podem ser alteradas para benefício do invasor ou *software* malicioso.

3 METODOLOGIA

Esse trabalho consiste em um estudo de caso na empresa TFMA ENGENHARIA que através desse método no processo de execução, através de uma vasta pesquisa em material especializado além de artigos científicos para uma revisão introdutória descritiva.

Feito uma análise minuciosa na infraestrutura de rede da empresa, e constava a seguinte configuração (Figura 2). A maior parte da rede é sem fio, acesso à internet sem controle de acesso, os Access Point com senhas fraca, a empresa não possui um *firewall* de rede, também não possuía um antivírus corporativo para uma melhor proteção, sem esquema de *backup* dos arquivos, os usuários tem perfis de administrador do sistema operacional, as senhas dos usuários são iguais para todos, todos os usuários conseguiam copiar informações da empresa para qualquer tipo de mídia. Em uma conversa com o técnico de informática da empresa, ele relata que a empresa sofreu um ataque do tipo *ransoware*, onde perdeu uma grande parte dos seus dados.

Através de toda a análise feita na empresa, desenvolvemos uma documentação com melhorias que se possa implantar, para que tenha uma proteção integrada dentro da empresa. Onde citarei as melhorias para implantação.

Implantação de um *firewall e* filtro no servidor *proxy*; infraestrutura de rede deve ser cabeada; Antivírus corporativo; servidor de arquivo com controle de acesso e *Active directory*; *Backup* diário dos dados em nuvem; Controle de acesso à internet; Bloqueio das portas USB e Leitores Ótico; treinamento para colaboradores de segurança da informação.

Infraestrutura com falhas

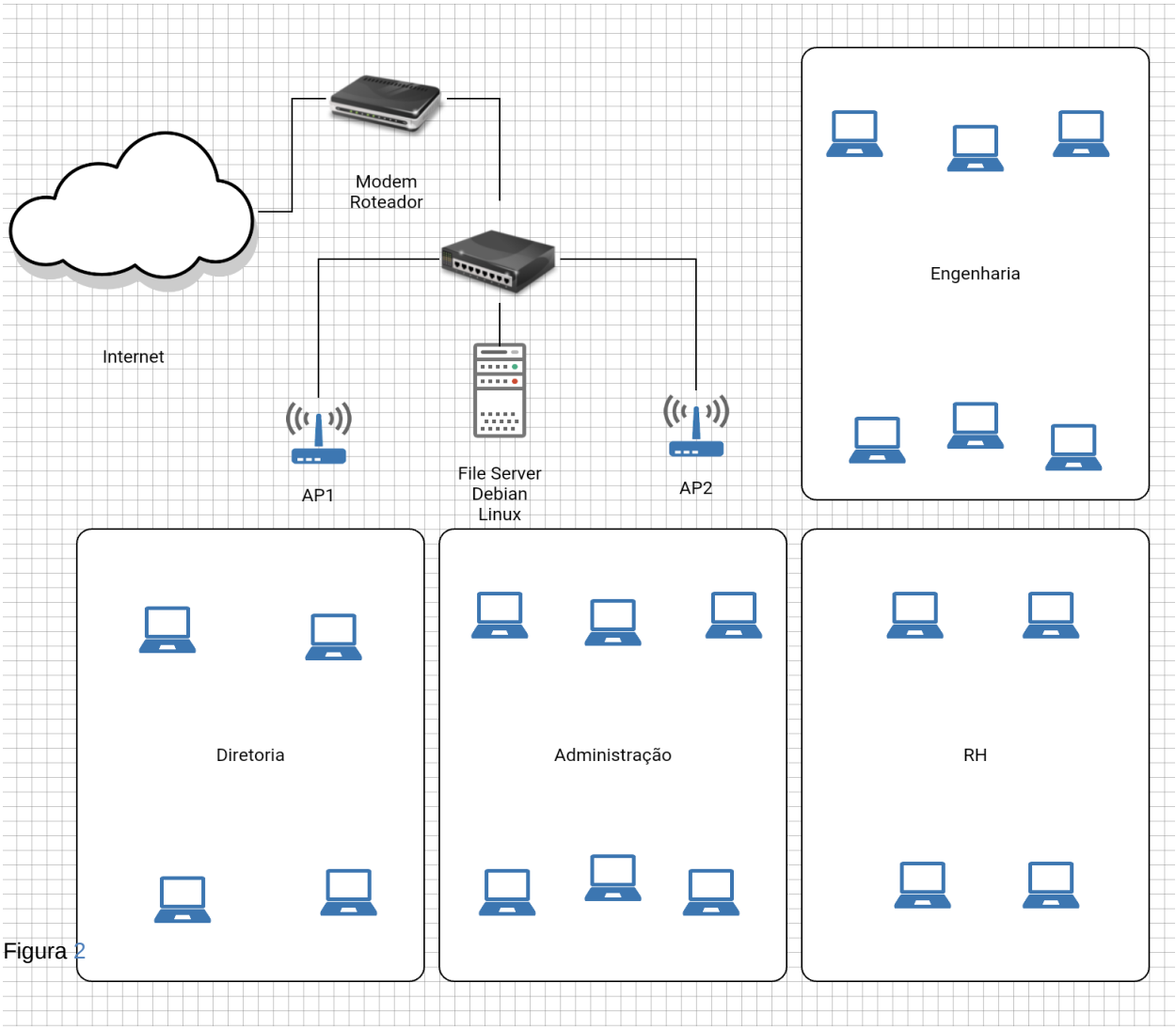

Figura 2

Infraestrutura com segurança

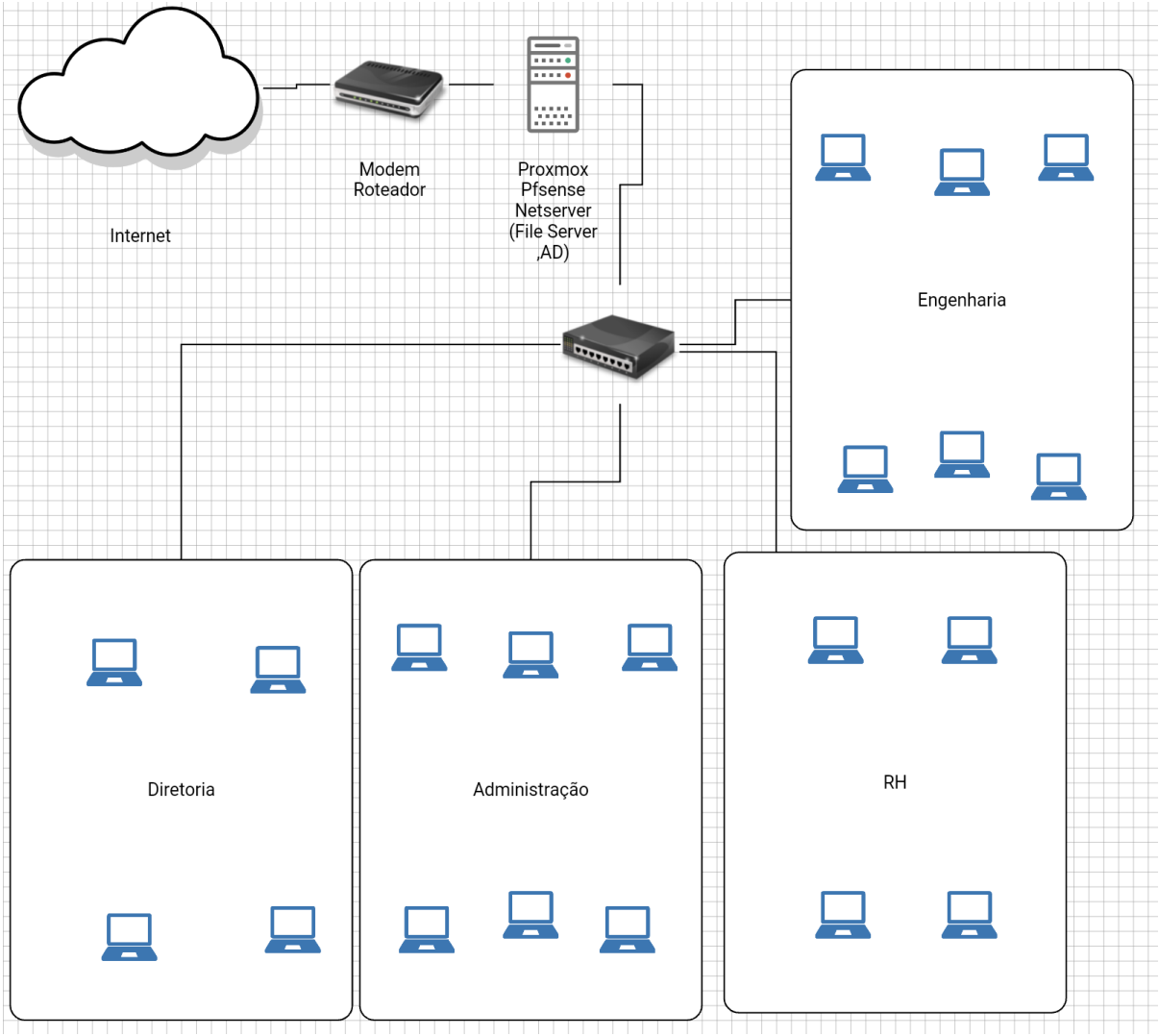

Figura 3

4 CONSIDERAÇÕES FINAIS

A segurança da informação é algo extremamente importante, seja no ambiente pessoal ou corporativo. Criar essa mentalidade nas instituições é algo difícil, principalmente por gerar custos elevados na maioria dos casos e os investidores insistirem em reduzir gastos em setores tão importante como o de tecnologia da informação. Nesse trabalho, foi abordado formas de ataques e os principais alvos, mostrando que praticamente em todos os casos, os usuários leigos são as principais vítimas. É importante lembrar que de nada vale a empresa adquirir super equipamentos ou um firewall extremamente bem configurado, se o usuário não for conscientizado e treinado para ter uma melhor performance no mundo virtual.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 17799. ABNT, Rio de Janeiro, (2005).

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002. ABNT, Rio de Janeiro, (2007).

BLUE PHOENIX. “Boas práticas de segurança”. In OLIVIERI, Luigi “No que consiste a segurança de redes empresariais" Disponível em: https://segurancaonline.wordpress.com/2016/04/12/seguranca-redes-empresarias/ Acessado em: 15/06/2018

OLIVEIRA, Waldes; “Principíos básicos da segurança da informação” disponivel em: https://www.techtem.com.br/principios-basicos-da-seguranca-da-informacao/ Acessado em 10/07/208

BRASIL. Tribunal de Contas da União. Boas práticas em segurança da informação / Tribunal de Contas da União. – 4. ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.