UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ

***CAMPUS* LUIZ MENEGHEL - CENTRO DE CIÊNCIAS TECNOLÓGICAS**

SISTEMAS DE INFORMAÇÃO

EMERSON TURIM CARVALHO

CONTROLES DE SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO EM UMA EMPRESA DE MÉDIO PORTE

Bandeirantes

2017

EMERSON TURIM CARVALHO

CONTROLES DE SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO EM UMA EMPRESA DE MÉDIO PORTE

Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação e Licenciatura em Computação.

Orientador: Prof. Me. Carlos Eduardo Ribeiro

Bandeirantes

2017

EMERSON TURIM CARVALHO

CONTROLES DE SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO EM UMA EMPRESA DE MÉDIO PORTE

Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação e Licenciatura em Computação.

COMISSÃO EXAMINADORA

_____
Prof. Me. Carlos Eduardo Ribeiro
Orientador
UENP – *Campus* Luiz Meneghel

_____
Prof. Me. Luiz Fernando Legore do Nascimento
UENP – *Campus* Luiz Meneghel

_____
Prof. Me. Ricardo Gonçalves Coelho
UENP – *Campus* Luiz Meneghel

Bandeirantes, 05 de julho de 2017.

Dedico este trabalho aos meus familiares que de diversas maneiras me ajudaram, sempre acreditando no meu sucesso, e em especial a Deus por mais este sonho realizado.

AGRADECIMENTOS

À Deus primeiramente, por ter sempre me mostrado claramente os caminhos e me ajudado em todos os aspectos da minha vida, me abençoando sempre.

Ao meu orientador Prof. Carlos Eduardo Ribeiro, que com seu conhecimento colaborou enormemente durante a elaboração deste trabalho, obrigado por tudo.

Aos Professores Mestres Luiz Fernando Legore do Nascimento e Ricardo Gonçalves Coelho, pelo apoio e incentivo na conclusão desta pesquisa.

À minha família por participar de toda essa caminhada, me apoiando sempre, e me dando força para continuar e não desistir.

À minha namorada e sua família, pelos incentivos nos dias mais difíceis, em que a desistência batia com força nos meus pensamentos.

Aos amigos que me acompanharam durante essa caminhada longa e cheia de desafios.

Aos meus colegas de trabalho que sempre foram compreensíveis com minhas faltas, minhas falhas no serviço e pelo apoio que sempre tiveram comigo.

Por fim, agradeço a todos que não citei aqui, mas que colaboraram direta ou indiretamente.

“Nossa maior fraqueza está em desistir. O caminho mais certo de vencer é tentar mais uma vez. ”
(Thomas Edison).

RESUMO

Nesse trabalho é apresentado uma análise dos aspectos relacionados à segurança da informação em uma empresa de médio porte, em que se ressalta a importância e eficácia em adotar controles de segurança da informação. De natureza monográfica, esse trabalho é constituído por uma pesquisa de campo sobre a Segurança da Informação em uma empresa privada, na qual foi aplicado um questionário e analisado os objetivos de controles relacionados à riscos de segurança da informação. As informações foram coletadas por meio de visitas técnicas ao local, e de aplicação de um questionário ao departamento de informática da empresa. São apresentados os principais problemas, e sugestões para solucionar os principais pontos considerados problemáticos. Foram feitas análises quanto à conformidade da gestão da segurança da informação da empresa, com ênfase nos requisitos da norma ABNT NBR ISO/IEC 27002/2013 – Código de Prática para a Gestão de Segurança da informação. Por fim, foi elaborado as Controles para implementação de políticas de segurança da informação na empresa, com base na gestão de riscos.

Palavras-chave: Segurança da Informação; ABNT NBR ISO/IEC 27002/2013; Políticas de Segurança da Informação.

ABSTRACT

The work described in this research aims to perform an analysis of aspects related to information security in a medium-sized company, demonstrating the importance and effectiveness of adopting information security policies in medium-sized organizations. This monographic work presents a field research on Information Security in a private company, in which a questionnaire was applied and the control objectives related to the risks of information security were analyzed. The information was collected through site visits, and a questionnaire was applied to the person in charge of the company's IT department. The main problems are presented, and solutions are suggested for the main problem points encountered. Analyzes are made regarding the compliance of the information security management of the company, with emphasis on the requirements of the standard ABNT NBR ISO / IEC 27002/2013 - Code of Practice for Information Security Management. Finally, the guidelines for the implementation of information security policies in the furniture company were elaborated based on risk management.

Key words: Information Security; ABNT NBR ISO/IEC 27002/2013; Information security policy.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas.
CI	Classificação de Impacto.
CP	Classificação de Prioridade.
GUT	Gravidade, Urgência e Tendência.
IEC	*International Electrotechnical Commission.*
ISO	*International Organization for Standardization.*
NBR	Norma Brasileira.
PDCA	Planejamento, execução, controle e ação.
RP	Relevância de Processos.
SGSI	Sistema de Gestão de Segurança da Informação.
TI	Tecnologia da Informação.

SUMÁRIO

1. INTRODUÇÃO

Alguns anos atrás viveu-se na era agrícola, evoluindo-se para era industrial e atualmente vivencia-se a era do conhecimento, o que potencializa o grau de importância das informações geradas nas empresas.

Antes as empresas não possuíam sistemas informatizados e utilizavam papéis para registrar informações, os documentos eram armazenados em pastas e armários, para protegê-los, esses eram colocados em salas restritas com segurança nas portas e alarmes, e só os responsáveis tinham acesso ao seu conteúdo.

Com a vinda dos computadores, a tecnologia chegou nas empresas, e seu uso tornou-se comum e com o objetivo de aperfeiçoar o processo de trabalho das mesmas.

Os documentos armazenados em armários foram sendo transferidos para os computadores e, com isso, a utilização de papéis, para esses fins, diminuíram. Porém, sem prevenção de perda de dados, a informatização por si só, não oferece segurança às empresas. Grandes companhias já foram prejudicadas por causa do vazamento de suas informações.

A implantação das políticas de segurança da informação é imprescindível para auxiliar as organizações a se protegerem adequadamente contra invasões e perdas de dados.

Abordar a prática de Segurança da Informação significa implementar mecanismos e ferramentas de segurança, que ofereçam principalmente, confidencialidade, disponibilidade e integridade das informações, principais pilares indispensáveis da segurança da informação.

Em nossa atual era da tecnologia, a segurança da informação nas empresas tem sido motivo de preocupação por parte de muitos empresários, que se questionam sobre a segurança que o ambiente virtual fornece contra-ataques de vírus e pessoas maliciosas.

A política de segurança da informação deve especificar os mecanismos através dos quais estes requisitos podem ser alocados, estabelecendo como será efetuado o acesso as informações de todas as formas possíveis, seja ela internamente ou externamente, e quais os tipos de mídias poderão transportar e ter acesso a esta informação.

No cenário atual, em que as empresas dependem cada vez mais da tecnologia e da informação, é vital garantir a segurança adequada deste ativo, considerado estratégico em sua missão de prestar serviços de qualidade, e a implementação da prática de Segurança da Informação no âmbito da organização compreende uma sequência de ações importantes e indispensáveis.

1.1 FORMULAÇÃO DO PROBLEMA

A pergunta chave que motivou esta pesquisa foi: Como proceder para que uma empresa venha a se adequar as Normas de Políticas de Segurança da Informação numa empresa de médio porte, minimizando os impactos de incidentes de Segurança e melhorar seus procedimentos internos e externos?

1.2 OBJETIVO GERAL

O objetivo geral desta pesquisa é analisar os riscos de segurança da informação de uma empresa, realizando uma análise dos aspectos relacionados à segurança da informação em uma, aspectos esses analisados antes e depois da implementação das diretrizes apresentadas, demonstrando a importância e eficácia em adotar controles de segurança da informação em organizações.

1.3 OBJETIVOS ESPECÍFICOS

- Definir brevemente a importância da segurança da informação no cenário econômico atual em particular nas pequenas e médias empresas, demonstrando a importância dos gestores modernos em instituir políticas de segurança, garantindo segurança e continuidade dos negócios.

- Abordar os três princípios básicos: confidencialidade, integridade e disponibilidade, que norteiam o sistema de segurança da informação, bem como a ABNT NORMA ISO/IEC 27002:2013.

- Mapear as práticas de segurança da informação formalmente estabelecidas pela empresa através de questionário, analisando os processos de negócio relacionado a segurança da informação e apresentação das Diretrizes de Segurança

e Gerenciamento de Sistemas de Informação (SGSI) com os principais itens que devem constar em uma Política de Segurança da Informação.

1.4 JUSTIFICATIVA

A presente pesquisa justifica-se pela evolução da tecnologia, das quais as informações passaram a ser armazenadas em mídias digitais, fato que as tornam mais vulneráveis à roubos e perdas.

A motivação para o desenvolvimento Controles de Segurança vem da necessidade de alcançar uma maior conscientização dos gestores e usuários, com respeito a segurança da informação em qualquer tipo de organização. Demonstrando uma necessidade crescente de implantação de políticas de segurança, tornando assim possível a utilização dessas informações em tomadas de decisão da empresa.

1.5 METODOLOGIA

A pesquisa tem uma proposta metodológica, que a caracteriza como descritiva com estudo campo. Para isso será realizada uma pesquisa bibliográfica, sobre a importância da segurança da informação no cenário econômico atual, nas pequenas e médias empresas e a importância dos gestores modernos em instituir políticas de segurança. Para realização deste estudo a pesquisa será restrita a uma empresa de médio porte.

A presente pesquisa apresenta-se qualitativa e, quantitativa apenas nas coletas de alguns pontos que irão auxiliar no embasamento do trabalho. Para isso foi feita uma análise riscos e elaborado um questionário (Apêndice A), contendo 19 (dezenove) questões que foi respondido através de entrevista realizada com o profissional responsável do setor de informática da empresa, do qual selecionou-se os procedimentos considerados pertinentes para elaboração de Diretrizes de SGSI contendo procedimentos e técnicas para uma possível ajuda organizacional na elaboração de Políticas de Segurança de Informação, com base nos itens definidos na norma NBR ISO/IEC 27002:2013 - Técnicas de segurança – Código de prática

para controles de segurança da informação. Nas Diretrizes constará normas e procedimentos claros, que deverão ser seguidos por toda a equipe interna e externa da empresa.

Após a coleta de dados, foi feita uma análise da empresa e apresentado os controles, para implantação do mesmo dentro da organização de Tecnologia da Informação (TI), observando cada etapa do processo e as ações realizadas, demonstrando como é fundamental proteger as informações gerenciais, tanto para a empresa quanto para o profissional.

1.6 ORGANIZAÇÃO DO TRABALHO

No Capítulo 2 constam os conceitos básicos de segurança, informação e seu ciclo de vida, possibilitando que o leitor tenha uma visão mais abrangente sobre o assunto.

No Capítulo 3 é apresentado a importância de Segurança da Informação e seus princípios. O Capítulo 4 é apresentado o universo da pesquisa e os procedimentos da coleta de dados, realizada por um questionário, elaborado com 19 questões do tipo fechada, ordenado de acordo com os objetivos específicos da pesquisa. No capítulo 5 é abordada a análise e discussão dos resultados.

Por fim, no Capítulo 5 são descritas algumas considerações finais desta pesquisa, que afirmam a importância da Segurança da Informação não só para as empresas, mas em todas as áreas de vida de cada indivíduo.

2. FUNDAMENTAÇÃO TEÓRICA

Todos os níveis que envolvem as informações de uma empresa seja ela de pequeno, médio ou grande porte, deve ter a sua importância levada em consideração, pois trata-se de dados que nem sempre pertencem somente a empresa detentora desses dados, mas de parceiros, clientes, colaboradores e fornecedores, que confiam suas informações a elas por se sentirem seguros nesta relação empresarial.

A nível de segurança desses dados, constata-se que, principalmente em empresas pequenas e médias, não possuem procedimentos de segurança da informação, pois, nem sempre tem disponibilidade financeira para investir muito nesta área. Atualmente vive-se num ambiente global de muita competitividade, e qualquer informação pode ser de grande importância para a conquista de espaço no mundo dos negócios.

Os tópicos teóricos a seguir apresentarão as principais abordagens relacionadas à Segurança da Informação, Qualidade da Informação, importância dos gestores modernos em instituir políticas de segurança, princípios básicos que norteiam o sistema de segurança da informação, e a ABNT NORMA ISO/IEC 27002:2013, com o objetivo de auxiliar na compreensão do tema desta pesquisa.

2.1 CONCEITOS BÁSICOS DE SEGURANÇA

Para discorrer sobre a segurança da informação, faz-se necessário o entendimento sobre o valor e a definição da informação. Com o passar do tempo a informação adquiriu importância significativa para as organizações, pois, a qualidade e a solidez da mesma conduzirá os gestores a tomarem as melhores decisões. A atual sociedade, principalmente empresarial, dependente da informação, o que torna a informação um patrimônio de caráter essencial em uma empresa, e, portanto, o seu ativo mais visível e desejado.

2.1.1 Informações

De acordo com Manoel (2014, p.1) “A informação pode ser constituída por um conjunto de dados que representam um ponto de vista diferente, revelando um significado novo ou trazendo elementos antes desconhecidos para quem a manipula”. Assim, a informação é um importante produto da era atual, podendo ser e visualizada de diversas maneiras.

O autor Barreto (1994; apud ALVES, 2011), afirma que a informação sintoniza a humanidade participando da evolução e da revolução das civilizações.

Assim, pode-se concluir que na medida em que a informação circula pelos mais variados ambientes, pode ser acessada, lida, modificada ou até mesmo apagada. Neste sentido, Nobre; Ramos; Nascimento, (2010), explicam, que a informação se tornou, um ativo intangível valioso para muitas organizações e o acesso a ela tem sido cada vez mais intenso e facilitado pela utilização de recursos tecnológicos.

Ratificando os autores acima, Manoel (2014, p.2) afirma que: “A informação é um ativo da organização, talvez o mais precioso, um bem que deve ser tão protegido quanto os bens físicos, tendo em vista a sua importância para a própria existência da organização”.

A literatura, apresenta os mais diversos conceitos para informação, dentre eles destaca-se: Associação Brasileira de Normas Técnicas NBR ISO/IEC 27002:2013, a informação é um conjunto de dados que representa um ponto de vista, um dado processado é o que gera uma informação.

Albuquerque Junior e Santos (2012), completa que “a informação é um elemento importante no processo de tomada de decisões”, por esse motivo, precisa ser protegida, pois com a expansão da Tecnologia, a informação está exposta a ameaças e vulnerabilidades.

De forma semelhante encontra-se a posição de Alexandria (2009), que afirma que as facilidades trazidas pela tecnologia vieram acompanhadas de ameaças para as informações. Com esse avanço, as empresas enfrentam alguns problemas de segurança, pois quanto mais pessoas acessam as informações, maior poderá ser a probabilidade de imprudência e mau uso. Por esse motivo observa-se o aumento dos problemas de segurança, que levam as empresas a investirem na Segurança da Informação.

2.1.2 Ciclo de Vida da Informação

Nesta era a informação é considerada um ativo importante na tomada de decisões, no entanto, para que ela represente um sinônimo de valor deve ser utilizada de forma efetiva no planejamento de suas estratégias.

Para Manoel (2014, p.2), “Uma organização deve estar segura em relação às informações que trafegam, apoiando todos os seus processos de diversas formas em diversos meios. O autor relata ainda, porque uma organização deve proteger suas informações:

- Pelo seu valor, como já pode ser entendido. No mundo dos negócios, informação é dinheiro;
- Pelo impacto de sua ausência. Se uma organização não produz, nem gera informação, ela não adquire conhecimento;
- Pelo impacto resultante de seu uso por terceiros. A informação preciosa na mão da concorrência pode causar prejuízos significativos;
- Pela importância da existência da informação gerar conhecimento;
- Pela relação de dependência entre todos os processos de negócio da organização. Sem a própria informação, o processo pode ser tornar inútil para atender ao seu objetivo.

Segundo a Norma ABNT NBR ISO/IEC 27002:2013 “[...] a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegida. ”

De acordo com Sêmola (2007), possuir uma visão integrada dos riscos é fundamental para as empresas que buscam o desenvolvimento e a continuidade do negócio, e ainda dependem de uma infraestrutura operacional sob risco controlado.

Toda informação é influenciada por três propriedades principais: Confidencialidade, Integridade e Disponibilidade, além dos aspectos Autenticidade e Legalidade, que complementam esta influência.

De acordo com o autor Manoel (2014, p.4) “Se um desses princípios básicos for desrespeitados em algum momento durante o ciclo de vida das informações, isso significa uma quebra de Segurança da informação, [...]”.

O fator motivacional em proteger as informações, são normalmente identificados como necessário pois subsidiam o funcionamento dos processos de negócio da empresa. Mas na visão de Sêmola (2007), na verdade as Empresas pensam de maneira objetiva: “[...] precisam preservar os atributos de confidencialidade, integridade e disponibilidade das informações com base em três únicos motivos ou fatores motivacionais: ganhar dinheiro, não perder dinheiro e não ser responsabilizado.

Para o Manoel (2014, p.2) as informações devem ser protegidas durante todo o seu ciclo de vida. Para o mesmo autor, o ciclo de vida da informação é representado por: elaboração, manuseio, armazenamento, transporte e descarte.

Vamos seguir o ciclo de vida das informações de acordo com Manoel (2014, p. 2 e 3):

- **Elaboração** – momento em que a informação é produzida;
- **Manuseio** – a informação é manipulada, como por exemplo, ao digitar informações em um site web, ou ainda, ao utilizar sua senha de acesso para autenticação na conta de um banco.
- **Armazenamento** – é onde a informação é guardada; seja em um banco de dados ou em uma mídia de CD-ROM depositada dentro de uma gaveta com chave.
- **Transporte** – a informação é transportada; seja ao encaminhar informações por correio eletrônico ou no diálogo de pessoas, no transporte de envelopes confidenciais, etc.
- **Descarte** – momento onde a informação é descartada; seja ao jogar uma mídia direta na lixeira, seja ao apagar um arquivo eletrônico em seu *desktop* etc.

Ratificando o autor acima, Sêmola (2003), apud Oziro, A.K. (2006), ensina que o ciclo de vida da informação é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Para melhor compreensão o mesmo autor apresenta os quatro momentos do ciclo.

A Figura 1 é ilustra a informação e os princípios de segurança de sistema de informações, bem como o ciclo de vida das informações, podendo concluir que se um dos princípios for desrespeitados durante o ciclo, há uma quebra de segurança da informação. Não basta garantir a segurança de três das quatro fases acima, é necessário que todo o ciclo de vida da informação seja assegurado.

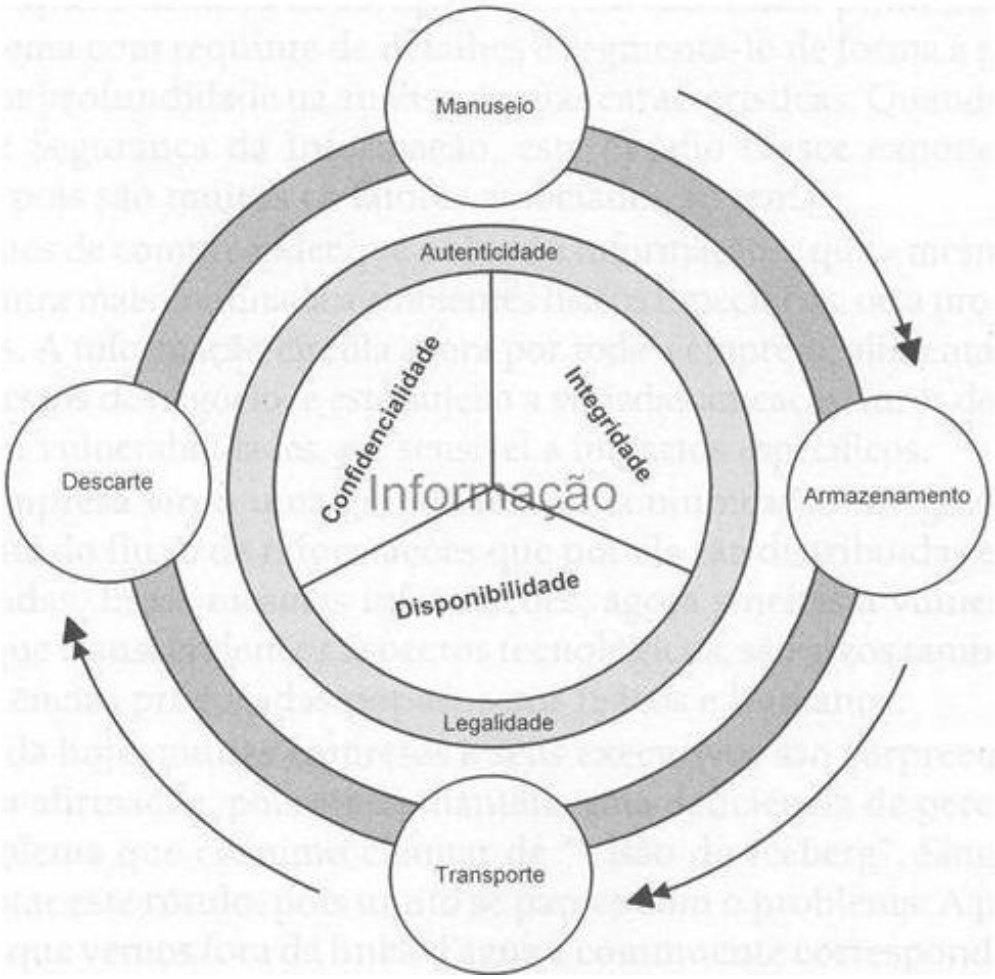

Figura 1 – Os quatro momentos do ciclo de vida da informação

Fonte – SÊMOLA, 2003, *apud* Oziro, A.K.,2006.

2.1.3 A Necessidade da Segurança da informação

O termo Segurança da Informação é definido por Beal (2005) como a proteção dos ativos de informação contra riscos, vulnerabilidades e ameaças à sua integridade, confidencialidade e disponibilidade, o que é semelhante a uma das duas

definições apresentadas pela ABNT NBR ISO/IEC 27002:2013 (2013), na qual é definida: como a preservação da confidencialidade, da integridade e da disponibilidade, seus três pilares; e como a proteção da informação contra ameaças para minimizar o risco e garantir a continuidade do negócio, maximizar as oportunidades e o retorno sobre os investimentos.

Dessa forma, nenhuma organização vai querer que suas informações sejam alteradas ou corrompidas por pessoas não autorizadas, a gestão de segurança da informação vai agir para tentar impedir, evitar ou minimizar que potenciais ameaças comprometam a integridade e a disponibilidade das informações.

Hoje vive-se num ambiente global de muita competitividade, um dos maiores problemas que se pode encontrar para a implantação de uma política de segurança em uma pequena ou média empresa parte justamente daqueles que devem ter o melhor entendimento do quanto isso é importante, ou seja, os proprietários, gerentes, empresários. É o que afirma Campos (2007, p.29; apud OLIVEIRA,2013):

> Em primeiro lugar, muitas vezes é difícil obter o apoio da própria alta administração da organização para realizar os investimentos necessários em segurança da informação. Os custos elevados das soluções contribuem para esse cenário, mas o desconhecimento da importância do tema é provavelmente ainda o maior problema.

Dessa forma, para realizar trabalhos que levam à implementação da prática de Segurança da Informação na organização, deve-se partir da conscientização dos funcionários, colaboradores, prestadores de serviços, fornecedores, principalmente dos gestores, para que possam entender a importância e a necessidade do engajamento de todos com a prática efetiva de Segurança da Informação.

2.2 A IMPORTANCIA DA SEGURANÇA DA INFORMAÇÃO

Entende-se por Segurança da Informação de acordo com a definição de Beal (2005) como a proteção do ativo da informação contra ameaças à sua integridade, confidencialidade e disponibilidade. A norma NBR ISO/IEC 27002:2013 da ABNT diz que, Segurança da Informação apresenta duas definições semelhantes: definida como a preservação da confidencialidade, da integridade e da disponibilidade, seus três pilares; e como a proteção da informação contra ameaças para minimizar os

riscos e garantir a continuidade do negócio, maximizar as oportunidades de negócio e o retorno sobre os investimentos.

O autor Campos (2007, p. 17, apud OLIVEIRA,2013), também afirma que um “sistema de segurança da informação baseia-se em três princípios básicos: confidencialidade, integridade e disponibilidade”. Ao referir-se em Segurança da informação, deve-se levar em consideração estes três princípios básicos, pois toda ação que comprometer qualquer um desses princípios estará contribuindo contra a sua segurança, para tanto abordar-se-á a definição de cada um, de acordo com a ABNT NBR ISO/IEC 27002:2013.

2.2.1 Confidencialidade

De acordo com KIM (2014, p.10) confidencialidade “é um termo comum, que significa proteger informações de todos, exceto daqueles que tenham direito a elas. ”

As informações devem ser conhecidas apenas pelos indivíduos que detém as permissões de acesso, evitando assim o vazamento de informação e dificultando a espionagem.

Manoel (2014, p. 3) ratifica essa mesma ideia, quando escreve: “toda informação deve ser protegida de acordo com o grau de sigilo”. A quebra desse sigilo pode acarretar danos inestimáveis para a empresa ou até mesmo para uma pessoa física.

2.2.2 Integridade

Sobre a integridade Kim (2014, p. 10) esclarece que: “ A integridade lida com a validade e a precisão dos dados”, ou seja, dados não válidos não possuem utilidade.

Quanto a este princípio Manoel (2014, p.3): “Integridade: característica da informação de manter-se na mesma condição em que foi disponibilizada pelo seu proprietário". As informações devem ser mantidas no seu estado original, sem alterações, garantindo a quem as receber, a certeza de que não foram falsificadas, corrompidas ou alteradas.

2.2.3 Disponibilidade

Segundo Manoel (2014, p.3) “Disponibilidade é a qualidade de tornar disponível para usuários, sempre que necessário e para qualquer finalidade, a informação gerada ou adquirida por um indivíduo ou organização”. A disponibilidade

é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Para o autor Kim (2014, p. 9), “[...] a disponibilidade geralmente é expressa como a quantidade de tempo que um usuário pode usar um sistema, aplicativo e dados’”. Dessa forma, a segurança da informação vai agir para evitar que potenciais ameaças venham comprometer a confidencialidade, a integridade e disponibilidade das informações da organização.

2.3 MODELOS PARA A SEGURANÇA DA INFORMAÇÃO: ISO/IEC 27000

Apresenta-se neste capítulo os modelos de normas de segurança da informação que foram utilizados na execução desta pesquisa, para um melhor entendimento das etapas necessárias para se chegar a adequados controles para segurança da informação em uma organização.

2.3.1 ABNT NBR ISO/IEC 17799:2005

Se faz necessário alguns comentários sobre a Norma ISO/IEC 17799:2005 Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação, por se tratar de uma norma voltada a tecnologia da informação que utiliza de técnicas de segurança, o que embasa ainda mais o presente trabalho.

Conforme a ABNT NBR ISO/IEC 17799:2005, para estabelecer adequadamente requisitos de segurança da informação, é de extrema importância que, uma organização busque a partir de uma análise de riscos, conforme seus objetivos e estratégias de negócio, que sejam identificados as possíveis ameaças e vulnerabilidades, verificar a probabilidade de ocorrência dessas ameaças e do seu impacto ao negócio da organização.

Outra forma de identificar ameaças e vulnerabilidade está na legislação vigente, nos estatutos, na regulamentação a nas cláusulas contratuais que a organização, seus parceiros comerciais, contratantes e contratados, provedores de serviço tem que atender.

Também através de princípios particulares da organização, seus objetivos e requisitos do negócio para que haja o processamento da informação que a organização necessita desenvolver para realizar suas operações.

Como principal informação do interesse deste trabalho a ABNT ISO/IEC 17799:2005, esclarece que, um certo número de controles pode ser considerado um bom ponto de partida para a implementação da segurança da informação. Estes controles são baseados tanto em requisitos legais como nas melhores práticas de segurança da informação normalmente usadas.

Os controles considerados essenciais para uma organização, sob o ponto de vista legal, incluem, dependendo da legislação aplicável:

a) Proteção de dados e privacidade de informações pessoais;
b) Proteção de registros organizacionais;
c) Direitos de propriedade intelectual.

Os controles considerados nas práticas para a segurança da informação incluem:

a) Documento da política de segurança da informação;
b) Atribuição de responsabilidades para a segurança da informação;
c) Conscientização, educação e treinamento em segurança da informação;
d) Processamento correto nas aplicações;
e) Gestão de vulnerabilidades técnicas;
f) Gestão da continuidade do negócio;
g) Gestão de incidentes de segurança da informação e melhorias.

Esses controles são aplicáveis na grande maioria das organizações. Embora todos os controles contidos nesta Norma são importantes e devem certamente ser considerados, a importância real dos controles deve ser determinada segundo os riscos específicos que a organização está exposta. Por isto, a consideração de pontos de partida não deve substituir em nenhuma hipótese a seleção de controles, baseado na análise/avaliação de riscos.

Para servir de guia e ajudar na compreensão dos riscos de segurança da informação, objetivo dessa pesquisa, segue breve considerações sobre a família ISO/IEC 27000. O significado da sigla ISO origina-se da palavra isonomia e tem como função desenvolver e promover normas que possam ser utilizadas igualmente em todos os países (ABNT ISO/IEC 27001:2006). No Brasil é representado pela Associação Brasileira de Normas Técnicas – ABNT.

A ISO/IEC 27001:2006 - Sistema de Gestão de Segurança da Informação especifica requerimentos para estabelecer, implementar, monitorar e rever, além de manter e provisionar um sistema de gerenciamento completo.

A Norma ISO/IEC 27002:2013 - Código de Melhores Práticas para a Gestão de Segurança da Informação - apresenta diretrizes para práticas de gestão de segurança da informação e normas de segurança de informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

A parte principal da norma se encontra distribuída em 14 seções, correspondendo a controles de segurança da informação, sendo um total de 35 objetivos de controles e 114 controles.

A pesquisa será limitada seguindo a numeração das seções que se inicia no número 5 e termina no número 18. Importante salientar que a ordem em que a norma está estruturada, não quer induzir a importância de cada seção, pois isso dependerá exclusivamente de cada organização, podendo a empresa definir quais controles serão mais importantes ou aplicáveis em seu ambiente de atuação.

A norma ISO/IEC 27005:2013 - Gestão de Riscos de Segurança da Informação - fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um SGSI de acordo com a ABNT NBR ISO/IEC 27001:2006. Faz-se necessário uma abordagem sistemática de Gestão de Riscos de Segurança da informação, para se identificar as necessidades da organização em relação aos requisitos de segurança da informação, e para criar um sistema de gestão de segurança da informação (SGSI) que seja eficaz (ISO/IEC 27005:2013, p.6).

Dessa forma as normas acima serão abordadas com mais especificidade, sendo estas normas consideradas eficazes no controle de Segurança da Informação, tema escolhido para presente pesquisa.

2.3.2 ABNT NBR ISO/IEC 27002:2013

De acordo com a Norma ABNT NBR ISO/IEC 27002:2013, cada seção principal contém:

a) um objetivo de controle declarando o que se espera que seja alcançado;

b) um ou mais controles que podem ser aplicados para se alcançar o objetivo do controle;

A norma apresenta as descrições do controle estruturadas da seguinte forma:

• Controle - Define a declaração específica do controle, para atender ao objetivo de controle. • Diretrizes para implementação - Apresenta informações mais detalhadas para apoiar a implementação do controle e alcançar o objetivo do controle.

• Informações adicionais - Apresenta mais dados que podem ser considerados, como por exemplo, questões legais e referências normativas, não existindo informações adicionais, esta parte não é mostrada no controle. Abaixo será descrita cada Seção, parafraseando o texto publicado na Norma ABNT NBR ISO/IEC 27002:2013:

SEÇÃO 5 - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O objetivo desta seção é orientar na criação de um documento sobre a política de segurança da informação da organização, contendo, 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 deve ser comunicada à todos, bem como analisada e revisada criticamente, em intervalos regulares ou quando mudanças se fizerem necessárias.

SEÇÃO 6 – ORGANIZANDO A SEGURANÇA DA INFORMAÇÃO

Esta seção tem como objetivo auxiliar na organização estrutural. Para que isso aconteça de forma ideal, as devidas responsabilidades pela segurança da informação devem ser definidas, entendidas e coordenadas pelas partes da organização representadas com funções e papéis importantes dentro da organização.

Deve-se esclarecer e estabelecer acordos de confidencialidade a fim de proteger as informações de caráter sigiloso, bem como as informações que são acessadas, comunicadas, processadas ou gerenciadas por partes externas, tais como terceiros e clientes.

SEÇÃO 7 – SEGURANÇA EM RECURSOS HUMANOS

Os funcionários, fornecedores e terceiros, precisam saber das responsabilidades que cada um tem sobre as informações que manipulam na organização, principalmente se essas informações forem sigilosas. Estar conscientes das ameaças à segurança da informação, podendo assim apoiar a política de segurança de informação da organização. Precisam ser treinados nos procedimentos de segurança da informação e no uso correto dos recursos de processamento da informação.

É de suma importância adotar procedimentos formais neste ponto, para que ocorrendo o término ou mudança na contratação, a saída de funcionários, fornecedores e terceiros deve ser feita de modo ordenado e controlado, e assim a retirada de todos os privilégios a eles outorgados ocorra corretamente e sem maiores problemas.

SEÇÃO 8 – GESTÃO DE ATIVOS

O principal objetivo desta seção é proteger e manter os ativos da organização, devendo estes serem identificados e catalogados, criando um inventário de ativos estruturado. Essas informações devem ser classificadas, conforme o nível de proteção e qual tipo de uso é permitido fazer com esses ativos.

SEÇÃO 9 – CONTROLE DE ACESSO

O acesso à informação, ao seu processamento e aos processos de negócios devem ser controlados, assegurando assim o acesso de usuário autorizado, limitando o não autorizado a sistemas de informação. Devendo assim ser elaborados procedimentos que garantam a segurança desde um simples cadastro de novo usuário, gerenciamento de senhas, aplicativos e equipamentos de usuários nos mais diversos setores da organização.

SEÇÃO 10 – CRIPTOGRAFIA

Assegurar o uso correto de criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação. Levar em consideração as leis ou regulamentações e restrições aplicáveis ao seu uso legal. Convém que algoritmos criptográficos, tamanho de chaves e práticas usuais sejam selecionados de acordo

com as melhores práticas, sendo essas chaves protegidas contra modificação e perda.

SEÇÃO 11 – SEGURANÇA FÍSICA E DO AMBIENTE

Esta seção tem como objetivo prevenir o acesso físico não autorizado das instalações da organização, oferecendo níveis e controles de acesso apropriados, incluindo proteção física. Essa proteção deve estar de acordo com os riscos previamente identificados.

Os equipamentos também devem ser protegidos contra ameaças físicas e ambientais, inclusive os que se encontram fora do local real da organização.

SEÇÃO 12 – SEGURANÇA NAS OPERAÇÕES

O objetivo desta seção é de garantir que as operações tenham procedimentos seguros e documentados e as devidas responsabilidades informadas. As possíveis mudanças na organização sejam controladas, seus recursos monitorados. Orientar para que ambientes de desenvolvimento, teste e produção sejam separados, sejam feitas cópias de segurança das informações.

Quando eventos acontecerem na organização, estes precisam ser registrados e evidenciados, sendo estes registros também protegidos. Ter restrições quanto à instalação de software pelos usuários e o gerenciamento de serviços terceirizados.

SEÇÃO 13 – SEGURANÇA NAS COMUNICAÇÕES

O objetivo desta seção é de assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam, para que estas sejam gerenciadas e controladas afim de proteger as informações nos sistemas e aplicações. Criar mecanismos de segurança que gerenciem e protejam os serviços de rede internos ou de terceiros na organização.

SEÇÃO 14 – AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Seu objetivo é de garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação. Os requisitos de segurança de sistemas de informação devem ser identificados e averiguado antes do seu desenvolvimento e/ou de sua implementação. As informações devem ser

protegidas visando a manutenção de sua confidencialidade, autenticidade ou integridade.

SEÇÃO 15 – RELACIONAMENTO NA CADEIA DE SUPRIMENTO

Tem como objetivo principal garantir a proteção dos ativos da organização que são acessados pelos fornecedores. Criar processos para acertar acordos com os acessos, processos, armazenagem, comunicação que são permitidos aos fornecedores.

Sendo necessário a identificação e documentação dos tipos de fornecedores. Manter níveis de segurança da informação e de entrega de serviços em conformidade com as especificações acertadas anteriormente entre os interessados.

SEÇÃO 16 – GESTÃO DE INCIDENTES DA SEGURANÇA DA INFORMAÇÃO

Seu objetivo principal é garantir que eventos de segurança da informação sejam o mais rapidamente comunicados, tornando possível assim que a ação corretiva seja realizada em tempo hábil.

Para isso, devem ser estabelecidos procedimentos formais de registro principalmente de notificações de fragilidades, avaliação, decisão e respostas a esses eventos danosos ao sistema da organização.

SEÇÃO 17 – ASPECTOS DA SEGURANÇA DA INFORMAÇÃO NA GESTÃO DA CONTINUIDADE DO NEGÓCIO

Esta seção tem como objetivo orientar nas medidas necessárias para impedir a interrupção das atividades do negócio e proteger os processos contra possíveis falhas ou desastres significativos, assegurando sua retomada em tempo hábil. Criar para isso, planos de continuidade do negócio, onde será identificado e reduzido riscos no sistema, visando a verificação, análise crítica e avaliação da continuidade da segurança da informação.

SEÇÃO 18 – CONFORMIDADE

Devendo garantir e evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação, esta seção trata de identificar a legislação aplicável a cada possível

situação dentro do ambiente de negócios da organização. Verificar os direitos de propriedade intelectual, registros, privacidade de informações.

Verificando o texto apresentado, percebe-se que toda a norma tem por principal característica a prevenção contra as ameaças e vulnerabilidades da informação, orientando a todo momento, o uso de mecanismos de ação efetiva contra qualquer perda de informação que uma organização possa ser afetada.

2.3.3 ABNT NRB ISO/IEC 27005:2013

Esta norma descrita por Manoel (2014) estabelece diretrizes para gestão de riscos de Segurança da Informação. Inclui-se nela os conceitos gerais especificados na norma ABNT NBR ISO/IEC 27001:2006 e é projetada para auxiliar a implementação da Segurança da Informação de forma satisfatória numa abordagem de gestão de riscos. De acordo com mesmo autor, o processo de gestão de riscos é composto pelas atividades:

- Definição do contexto
- Análise e avaliação de risco
- Tratamento dos riscos
- Aceitação dos riscos
- Monitoramento e análise dos riscos
- Comunicação dos riscos

A ABNT NBR ISO/IEC 27005:2013 possui regras de como proceder na gestão de riscos de segurança da informação de uma organização, focada nas características de um sistema de gestão de segurança da informação de acordo com a norma ABNT NBR ISO/IEC 27002:2013.

Para relevância da pesquisa, será descrita uma das atividades do processo, sendo esta, um dos pontos mais importante do processo de gestão de risco de segurança da Informação a definição do contexto.

2.4.3.1 Definição do contexto

De acordo com Sampaio (2014), a definição do contexto designa o alvo cujo a gestão de risco vai proceder. Como entrada a atividade recebe todas as informações relevantes sobre a organização para a definição do contexto da gestão de riscos de segurança da informação.

Esta atividade divide em: definição de escopo e a definição dos critérios de riscos.

2.4.3.1.1 Definição do escopo

O escopo é o conjunto de ativos, ameaças e vulnerabilidades que o sistema de gestão de riscos terá sua ação,

A ABNT NBR ISO/IEC 27005:2013 apresenta meios para a definição do escopo de uma organização, conforme descrito abaixo:

> **I – Análise da organização**
>
> **Propósito principal da organização:** O seu propósito pode ser definido como a razão pela qual a organização existe (sua área de atividade, seu segmento de mercado etc.)
>
> **Negócio:** O negócio de uma organização, definido pelas técnicas e know-how de seus funcionários, viabiliza o cumprimento de sua missão. É específico à área de atividade da organização e frequentemente define sua cultura.
>
> **Missão:** A organização atinge seu propósito ao cumprir sua missão. Para bem identifica-la, convém que os serviços prestados e/ou produtos manufaturados sejam relacionados aos seus públicos-alvo.
>
> **Valores:** Valores consistem de princípios fundamentais ou de um código de conduta bem definido, aplicados na rotina de um negócio, podem incluir os recursos humanos, as relações com agentes externos (clientes e outros), a qualidade dos produtos fornecidos ou dos serviços prestados.
>
> **Organograma:** A estrutura da organização é esquematizada em seu organograma. Convém que essa representação deixe claro quem se reporta a quem, destacando também a linha de comando que legitima a delegação de autoridade. Convém que inclua também outros tipos de relacionamentos, os quais, mesmo que não sejam baseados em uma autoridade oficial, criam de qualquer forma caminhos para o fluxo de informação.
>
> **Estratégia:** Ela requer a expressão formalizada dos princípios que norteiam a organização. A estratégia determina a direção e o desenvolvimento necessários para que a organização possa se beneficiar das questões em pauta e das principais mudanças sendo planejadas.
>
> **II – Restrições que afetam a organização:** Convém que todas as restrições que afetam a organização e determinam o direcionamento da segurança da informação sejam consideradas.
>
> **III – Legislações e regulamentações aplicáveis à organização:** Convém que os requisitos regulatórios aplicáveis à organização sejam identificados. Eles consistem nas leis, decretos, regulamentações específicas que dizem respeito à área de atividade da

organização ou regulamentos internos e externos. Englobam também contratos, acordos e, mais genericamente, qualquer obrigação de natureza legal ou regulatória.

IV – Restrições que afetam o escopo: Ao identificar as restrições é possível enumerar aquelas que causam um impacto no escopo e determinar quais são passíveis de intervenção. Elas complementam e talvez venham a corrigir as restrições da organização discutidas mais acima.

V – Identificação de ativos: Para estabelecer o valor de seus ativos, uma organização precisa identifica-los.

Após a coleta de todos os dados, gera como saída:

- Especificação dos critérios básicos, critérios esses que se dividem em critérios para avaliação de riscos, critérios de impacto e critérios para aceitação do risco;
- O escopo e os limites do processo de Gerenciamento de Riscos do Sistema de Informação;
- A organização responsável pelo processo.

2.4 Gerenciamento de Riscos de Segurança da Informação

Segundo Fontes (2000, apud Sampaio,2014) não existe solução certa ou errada. Existe solução mais adequada a cada organização. Independentemente de como se rotule o seu planejamento de segurança, não deixe de fazê-lo. Como qualquer outro planejamento, ele é o rumo a ser seguido com os objetivos definidos.

A implantação de um SGSI envolve primeiramente a análise de riscos na infraestrutura da empresa: a avaliação do ambiente organizacional, a valoração do risco e a análise de incidentes de segurança. Esta análise permite identificar os pontos vulneráveis e as falhas nos sistemas, que deverão ser corrigidos.

A Gestão de Riscos, de acordo com Manoel (2014, p.71) é fundamental para garantir o perfeito funcionamento de toda a estrutura tecnológica da empresa e, engloba a Segurança da Informação, pois hoje conta-se com uma grande quantidade de vulnerabilidades e riscos que podem comprometer as informações da empresa.

Ao se tratar de risco no que se refere a segurança, segundo a ABNT NBR ISO/IEC 27005:2013:

> Riscos de segurança da informação é a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira prejudicando a organização. É medido em função da combinação da probabilidade de um evento e de sua consequência.

Pode-se dizer assim que risco é algo que causa algum tipo de dano, sendo possível calcular a possibilidade de ocorrência de um risco e os danos que ele possa causar.

De acordo com a ABNT NBR ISO/IEC 27002:2013 (apud Sampaio 2014), existem 4 (quatro) elementos para o processo de gestão de riscos:

- Ativo – Qualquer coisa que tenha valor para a organização;
- Ameaça – Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- Vulnerabilidade – Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;
- Consequência – Está relacionada a perdas operacionais relativas à proteção de ativos.

Ainda segundo a ABNT NBR ISO/IEC 27005:2013, a gestão de riscos auxilia na:

- Identificação de riscos;
- Análise/avaliação de risco em função das consequências ao negócio e da probabilidade de sua ocorrência;
- Comunicação e entendimento da probabilidade e das consequências destes riscos;
- Estabelecimento da ordem prioritária para tratamento do risco;
- Priorização das ações para reduzir a ocorrência dos riscos;
- Envolvimento das partes interessadas quando as decisões de gestão de risco são tomadas e mantidas informadas sobre a situação da gestão de riscos;
- Eficácia do monitoramento do tratamento do risco;
- Monitoramento e a análise crítica regular de riscos e do processo de gestão dos mesmos;
- Coleta de informações de forma a melhorar a abordagem da gestão de riscos;
- Treinamento de gestores e pessoal a respeito dos riscos e das ações para mitiga-los.

Os riscos de segurança da informação comprometem ou podem comprometer os ativos de uma organização em sua confidencialidade, integridade e disponibilidade de suas informações. Para Oliveira (apud Sampaio 2014) riscos são uma oportunidade, uma incerteza ou uma ameaça. Sendo a ameaça a maior preocupação, pois é a que pode produzir danos como, por exemplo, indisponibilidade de serviços, perca financeira.

Na gestão de riscos a ABNT NBR ISO/IEC 27005:2013 auxilia com conceitos e práticas para o gerenciamento mais adequado de gestão de riscos

Já ABNT NBR ISO/IEC 27002:2013 caracteriza os processos de gestão de risco como atividades que são coordenadas para orientar e controlar o risco de uma organização (LUND; SOLHAUG; STOLEN, 2010, apud Sampaio 2014).

2.4.1 O processo de Gestão de Riscos

O processo de gestão de riscos contém algumas atividades propostas para implementação conforme pode-se observar na Figura 2 (ABNT NBR ISO/IEC 27005:2013).

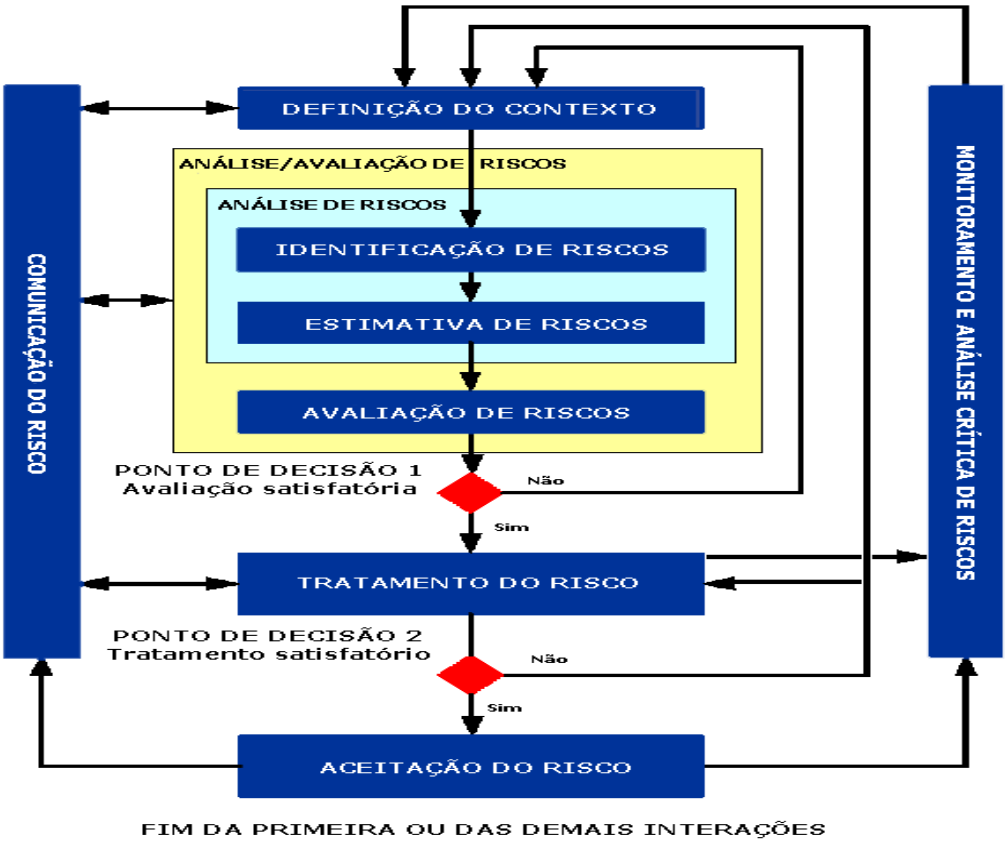

FIGURA 2– Processo de gestão de riscos de segurança da informação.

Fonte: ABNT NBR ISO/IEC 27005:2013.

3. MATERIAL E METODOS

Neste capítulo é descrito os materiais utilizados para a realização desta pesquisa, esclarecendo os processos que são realizados dentro da empresa, analisando os riscos de segurança de informação nesses processos, delimitando o experimento para se elevar o nível de segurança da informação na empresa alvo da pesquisa.

Depois é explicado o método utilizado para analisar a vulnerabilidades e ameaças ao sistema da empresa e as etapas para realizar uma adequada gestão de riscos.

3.1 Material

É indispensável se ter a clareza necessária em todo e qualquer processo realizado dentro de uma empresa, a segurança de informação é uma parte essencial para auxiliar que os processos tenham um bom desempenho, servindo de apoio ao negócio de uma empresa.

É certo que em uma situação de risco, ter a certeza da não ocorrência de falhas é muito importante e mais vantajoso do que ocorrer uma falha de segurança de fato, porém uma falha pode ser algo construtivo, pois ela pode levar a um novo conhecimento que proporcione à presença de um risco de segurança, sabendo da existência desse risco pode-se analisar e avaliar o seu nível de importância e a partir desse ponto, encontrar uma solução que possa mitigar esse risco.

A validade do questionário aplicado foi verificada pelo responsável do setor de TI da empresa moveleira, tendo ele experiência no negócio da empresa e, consciência daquilo que é de maior ou menor pertinência e interesse da empresa para implementar diretrizes de segurança da informação.

A confiabilidade foi estimada aplicando-se o método de questionário, que auxiliou na análise dos pontos mais críticos a ocorrência de riscos de segurança da informação, feito isso, pode-se chegar a uma avaliação correta e precisa sobre o que é necessário e o que se deve fazer para que os processos da empresa sejam mais seguros e organizados.

3.1.1 DELINEAMENTO DO EXPERIMENTO

Buscando contribuir para elevar o nível de segurança de informação da empresa, tendo como objetivo, promover ajustes e orientações através de diretrizes de segurança, para que a empresa desenvolva melhor o seu negócio no ambiente em que ela se situa.

Assim fez-se necessário à aplicação de um questionário, contendo 19 questões (Apêndice A), avaliativo afim de se obter com maior clareza os pontos falhos na política de segurança da informação da empresa. Utilizou-se perguntas diretas para facilitar o entendimento das necessidades reais e para elevar o nível de segurança de informações no ambiente de trabalho da empresa Moveleira.

Participaram do questionário o responsável do setor de TI da empresa, que, com sua experiência e conhecedor do negócio da empresa, possibilitou avaliar os níveis críticos de segurança da informação.

O questionário foi elaborado com base na Norma ABNT NBR ISO/IEC 27002:2013, sendo esta norma a referência principal deste trabalho.

Levou-se em consideração no questionário aquilo que se julgou essencial quanto a Análise de Gestão de Riscos de Segurança da Informação conforme o negócio exercido pela empresa. Não foi dado uma sequência hierárquica nas questões quanto a seu nível de importância pois, chegou-se a um consenso que, as alterações sugeridas pelas diretrizes na segurança da informação para a empresa eram uma necessidade e do interesse da empresa que, busca melhoria constante em seus processos de negócio.

Foi realizada uma reunião informal com o responsável pelo setor de TI da empresa para uma prévia avaliação das necessidades, possibilidades e importância da implementação de diretrizes de segurança da informação.

Após esse primeiro contato, tornou-se claro como funcionavam os processos de negócio dentro empresa e das necessidades de segurança de informação de que a empresa necessitava, assim, elaborou-se um questionário informativo para avaliar e analisar como poderiam ser feitas e organizadas melhorias na segurança de informações da empresa.

Com o questionário (Apêndice A) formulado, novamente uma nova reunião foi realizada com o responsável do setor de TI da Empresa e aplicado o questionário com o objetivo de encontrar na Norma ABNT NBR ISO/IEC 27002:2013 os pontos

de maiores riscos de segurança da informação para que assim a empresa pudesse se tornar mais segura e organizada no que se refere à segurança da informação, seja ela interna ou externamente.

A presença de questões contextualizadas foi um grande desafio, pois há necessidade de se desenvolver no ambiente da empresa, e principalmente conscientizar os diretores da empresa sobre a necessidade de uma política de segurança de informação, pautada em diretrizes que possam guiar a empresa a evitar futuras falhas de segurança e consequentemente prejuízos financeiros, sem que com isso se eleve seu capital de investimento financeiro.

O entrevistado recebeu o questionário e teve um tempo hábil de leitura e entendimento das questões, onde dúvidas e novos questionamentos foram sendo sanadas para que se chegasse a uma conclusão efetiva daquilo que seria necessário implementar por meio das diretrizes de segurança da informação.

Foram elaboradas e discutidas 19 questões buscou-se delimitar os pontos falhos na segurança de informação na empresa, afim de averiguar corretamente a necessidade da aplicação de diretrizes de segurança de informação para diminuir riscos, organizar processos, antecipar mudanças, prevenir falhas, promover melhorias e conscientizar usuários sobre a importância de seguir uma política de segurança de informação.

3.1.2 As empresas no Norte Pioneiro e a Segurança da Informação

A realização de um projeto de segurança em empresas de médio porte só se faz realmente produtivo, se realizado como um dos elementos de um processo de crescimento empresarial, para isso, se faz necessário uma breve descrição do setor empresarial do Norte Pioneiro do Paraná, local onde se situa a Empresa alvo deste estudo de caso.

A empresa de médio porte selecionada para análise e implementação do tema deste estudo de caso, atualmente emprega mais de 400 colaboradores, sendo que dentre esses colaboradores aproximadamente 70 utilizam o sistema da empresa. No Setor de Tecnologia de Informação são em 3 colaboradores.

Quanto a estrutura organizacional da empresa, atualmente:

Presidente, Diretores Administrativo-Financeiro-Comercial e Industrial, Gerentes Comerciais e de Marketing, Supervisores de TI, Financeiro, Compras, Contábil, Comercial, Logística, Recursos Humanos e de Produção, sendo que o supervisor de Produção está abaixo do Industrial, o Comercial abaixo do Gerente Comercial e os restantes abaixo do Diretor Administrativo-Financeiro-Comercial.

O principal negócio da empresa são soluções e inovações em mobiliário, tendo como sua missão: desenvolver, fabricar e comercializar móveis para quarto de forma simples, eficiente e sustentável, maximizando valor para seus clientes. Buscando comportamento ético, inovação, espírito de equipe, compromisso com o resultado, ser implacável no corte de desperdícios, disciplina e simplicidade como seus principais valores, procurando sempre atender as necessidades de seus clientes, que são a razão de sua existência.

3.2 Método

Conforme está descrito na ABNT NBR ISO/IEC 27005:2013, as atividades do processo da gestão de risco iniciam-se com a atividade de definição do contexto, depois análise e avaliação de riscos, tratamento do risco, aceitação do risco, comunicação do risco, e por fim o monitoramento e análise crítica de riscos.

A seguir as atividades do processo de gestão de riscos, conforme a ABNT NBR ISO/IEC 27005:2013:

3.2.1 Definição do contexto

Nesta atividade, todas as informações sobre a organização são recebidas para que seja definido em que contexto a gestão de riscos de segurança da informação vai ser estruturada, gerando critérios para avaliação de riscos, de impacto e de aceitação do risco, o escopo e os limites de gestão de risco de segurança da informação.

3.2.2 Análise e avaliação de riscos de segurança da informação

São executados nesta atividade a identificação dos papéis, a descrição qualitativa dos riscos, a prioridade dos riscos conforme avaliação dos objetivos da organização, é gerada uma lista de riscos, conforme suas prioridades e de acordo com critérios de avaliação de riscos.

3.2.3 Tratamento de risco de segurança da informação

O tratamento de risco tem como objetivo reduzir, reter, evitar ou transferir os riscos, que são selecionados e um plano de tratamento do risco seja definido, gerando um plano de tratamento dos riscos e os residuais que podem ou não ser aceito pelos gestores da organização. A Figura 3 ilustra o processo de Gestão de Riscos de Segurança da Informação:

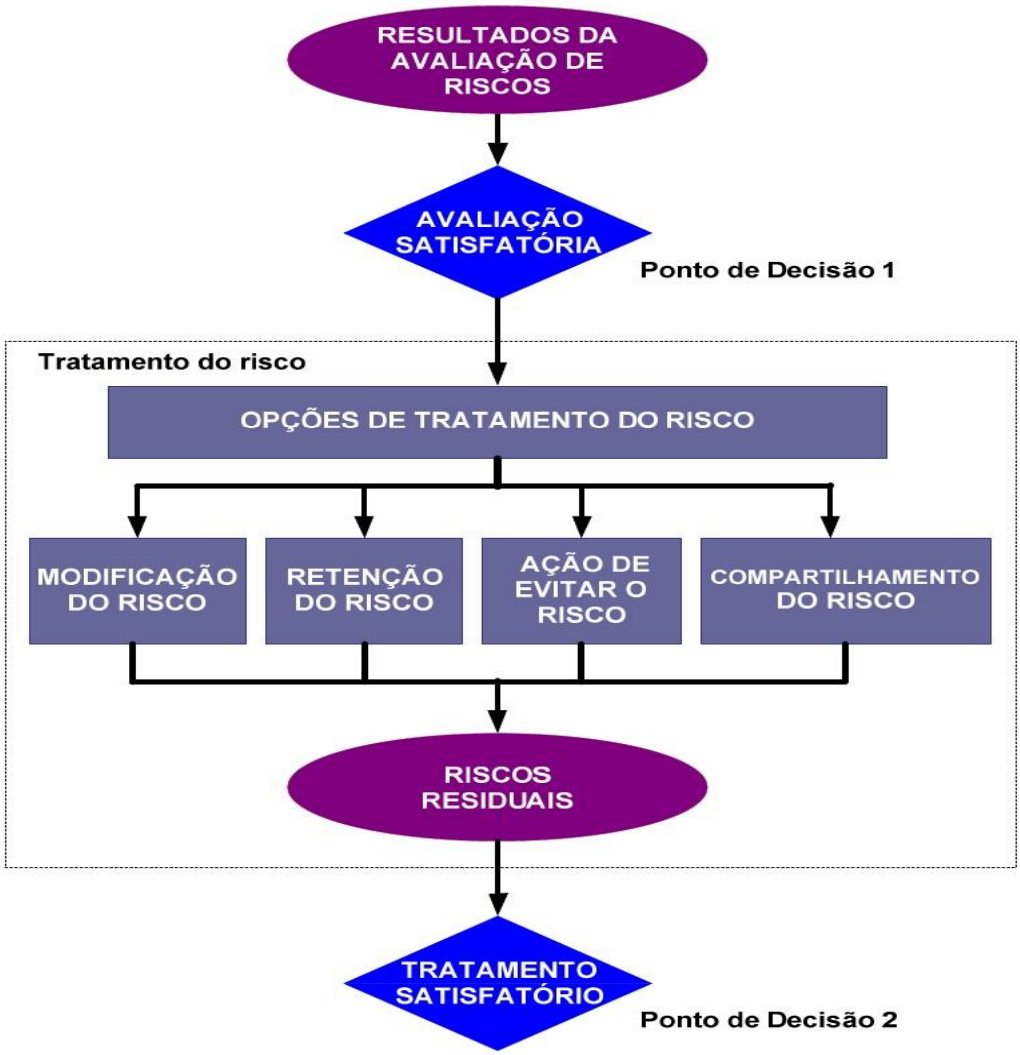

FIGURA 3 – Processo de gestão de riscos de segurança da informação.

Fonte: ABNT NBR ISO/IEC 27005:2013.

3.2.4 A aceitação do risco de segurança da informação

Nesta atividade é tomada a decisão de aceitação dos riscos e responsabilidade pela decisão, sendo adequadamente registrada. É gerada então uma lista de riscos que a organização aceita.

3.2.5 Comunicação do risco de segurança da informação

Esta atividade tem como objetivo o compartilhamento de informações sobre os riscos, entre o responsável pelas decisões e as partes interessadas, gerando o entendimento entre as partes sobre a gestão de risco de segurança da informação.

3.2.6 Monitoramento e análise crítica de riscos de segurança da informação

Esta é a última atividade de todo o processo de gestão de risco de segurança da informação, que tem como objetivo o monitoramento dos riscos para que na ocorrência de possíveis mudanças, os riscos sejam identificados o mais rápido possível, o que gera um nivelamento contínuo da gestão de riscos conforme os negócios da organização e a aceitação do risco.

3.3 Segurança da Informação nos Processos de Negócios Críticos

Nesta etapa realizou-se uma priorização das ações de segurança da informação nos processos críticos de negócios da organização, é necessário identificar quais os processos que necessitam com maior urgência da implementação de uma Política de Segurança de Informação adequada.

De início é preciso identificar qual a missão da organização, sua visão, e seus principais objetivos estratégicos. A partir disso, iniciou o processo de mapeamento dos componentes organizacionais, ou seja, as áreas, seus processos de negócio e seus principais ativos de informação.

3.4 Mapeamento dos componentes organizacionais

Esses componentes organizacionais são utilizados para definir o alcance da Política de Segurança da Informação na organização.

Os três componentes organizacionais são: Área, Processo de Negócio e Ativo de Informação.

Identificados e mapeados esses componentes ao longo do projeto de elaboração das Políticas de Segurança da Informação. Além disso, com essa análise foram definidos o escopo da gestão de riscos e o diagnóstico da situação atual da segurança da informação na organização.

A forma utilizada para a realização desse trabalho está descrita a seguir:

- Foi agendada e realizada entrevistas com o responsável pelo setor de Tecnologia da organização.
- Foi identificado as áreas da organização e seus processos de forma macro, com a descrição de seus atributos e especificações.
- Foi identificado a sensibilidade de cada um dos processos com relação a eventos de quebra dos princípios básicos de segurança da informação.
- Foi pontuado e priorizado os processos de acordo com os critérios de gravidade, urgência e tendência.
- E por fim foi consolidado as informações para obter a relação das áreas e dos processos mais críticos para a organização.

3.5 Mapeamento das áreas e dos processos de negócio da organização

3.5.1 Mapeamento das áreas

Para avaliar e priorizar os riscos foi feito um mapeamento das áreas e dos processos de negócio da organização. Foi utilizado o termo “área” para definir o setor ou departamento da organização.

A organização alvo deste trabalho, está dividida em:

1. Escritório da Qualidade.
2. Departamento Administrativo/Financeiro.
3. Departamento Comercial.
4. Departamento de Marketing.
5. Departamento Industrial.

Segue na Tabela 1 a descrição dos processos de cada departamento da organização:

Tabela 1 – Áreas e seus processos na organização.

Nº	Área	Processo
1	Escritório da Qualidade/Diretoria	Inspeção de qualidade
2	Departamento Administrativo/ Financeiro	Contabilidade
		Contas a receber
		Contas a pagar
		Recursos Humanos
		Informática
		Administração de Vendas
3	Departamento Comercial	Supervisão de exportação
		Supervisão de Mercado
4	Departamento de Marketing	Desenvolvimento de Produtos
		Marketing
5	Departamento Industrial	Fábrica I
		Fábrica II
		Planejamento de Produção
		Engenharia de Processos
		Depósito de Produto Acabado
		Expedição
		Assistência Técnica
		Manutenção Predial
		Compras

Tabela 2 – Relevância da área da organização.

Relevância da área	Valor	Auxílio para interpretações
Muito baixa	1	A interrupção das operações da área causa impactos irrelevantes para a organização.
Baixa	2	A interrupção das operações da área causa impactos apenas consideráveis para a organização.
Média	3	A interrupção das operações da área causa impactos parcialmente significativos para a organização.
Alta	4	A interrupção das operações da área causa impactos muito significativos para a organização.
Muito alta	5	A interrupção das operações da área causa impactos incalculáveis, que comprometem a continuidade da organização.

Fonte – Manoel (2014).

Análise realizada, conforme Tabela 3 a seguir:

Tabela 3 – Análise de relevância das áreas da organização.

Nome da área	Responsável	Relevância
Escritório de Qualidade/Diretoria	Presidente	Muito alta
Departamento Administrativo/Financeiro	Gerentes Administrativo/Financeiro	Muito alta
Departamento Comercial	Gerente Comercial	Muito alta
Departamento de Marketing	Gerente de Marketing	Alta
Departamento Industrial	Gerente e Supervisores industriais	Alta

3.5.2 Mapeamento dos processos de negócio

Nesta etapa foi apresentado, para cada processo de negócio, a identificação da área pertencente, o seu responsável e sua relevância para a organização, bem como os resultados dos estudos de impacto e prioridade dos processos.

3.5.2.1 Relevância dos processos de negócio

Para relevância dos processos (RP), foram consideradas as seguintes escalas:

Tabela 4 – Escala de relevância dos processos da organização.

Relevância do processo	Valor	Auxílio para interpretação
Muito baixa	1	A interrupção do processo causa impactos irrelevantes para a organização.
Baixa	2	A interrupção do processo causa impactos apenas consideráveis para a organização.
Média	3	A interrupção do processo causa impactos pouco significativos para a organização.
Alta	4	A interrupção do processo causa impactos muito significativos para a organização.
Muito alta	5	A interrupção do processo causa impactos incalculáveis para a organização.

Fonte – Manoel (2014).

Tabela 5 – Análise da escala de relevância dos processos da organização.

Área	Responsável	Processo	Relevância
Escritório da Qualidade/Diretoria	Presidente	Inspeção de qualidade	Muito alta
Departamento Administrativo/ Financeiro	Gerente Administrativo/ Financeiro	Contabilidade	Muito alta
		Contas a receber	Alta
		Contas a pagar	Alta
		Recursos Humanos	Baixa
		Informática	Muito Alta
		Administração de Vendas	Alta
Departamento Comercial	Gerente Comercial	Supervisão de exportação	Média
		Supervisão de Mercado	Média
Departamento de	Gerente de	Desenvolvimento de Produtos	Média

Marketing	Marketing	Marketing	Média
Departamento Industrial	Gerente e Supervisores industriais	Fábrica I	Média
		Fábrica II	Média
		Planejamento de Produção	Alta
		Engenharia de Processos	Alta
		Depósito de Produto Acabado	Baixa
		Expedição	Baixa
		Assistência Técnica	Baixa
		Manutenção Predial	Baixa
		Compras	Alta

3.5.2.2 Estudos de impacto

Neste estudo foi apontado a sensibilidade de cada processo em relação a eventos de quebra dos princípios básicos de segurança da informação.

Nesta atividade de análise do impacto nos princípios básicos de segurança da informação, foi utilizado os três critérios básicos que sustentam a segurança de informação, para alcançar o grau de impacto e prioridade: Confidencialidade (C), Integridade (I) e Disponibilidade (D).

Tabela 6 – Escala de estudo de impacto.

Classificação do Impacto	Valor	Auxílio para interpretação
Muito baixo	1	A quebra do critério do processo pode provocar impactos irrelevantes.
Baixo	2	A quebra do critério do processo pode provocar impactos consideráveis.
Médio	3	A quebra do critério do processo pode provocar impactos parcialmente significativos.
Alto	4	A quebra do critério do processo pode provocar

		impactos muito significativos.
Muito alto	5	A quebra do critério do processo pode provocar impactos incalculáveis.

Fonte – Manoel (2014).

Tabela 7 – Análise do estudo de impacto.

	Classificação do impacto		
Nome do processo	Confidencialidade	Integridade	Disponibilidade
Inspeção de qualidade	Muito alto	Muito alto	Muito alto
Contabilidade	Muito alto	Muito alto	Alto
Contas a receber	Muito alto	Muito alto	Muito alto
Conta a pagar	Muito alto	Muito alto	Muito alto
Recursos humanos	Alto	Alto	Alto
Informática	Muito alto	Muito alto	Muito alto
Administração de vendas	Muito alto	Muito alto	Muito alto
Supervisão de exportação	Alto	Alto	Alto
Supervisão de Mercado	Alto	Alto	Alto
Desenvolvimento de Produtos	Muito alto	Muito alto	Alto
Marketing	Muito alto	Muito alto	Alto
Fábrica I	Alto	Muito alto	Alto
Fábrica II	Alto	Muito alto	Alto
Planejamento de Produção	Alto	Muito alto	Alto
Engenharia de Processos	Muito alto	Muito alto	Alto
Depósito de Produto Acabado	Alto	Muito alto	Alto
Expedição	Alto	Muito alto	Alto
Assistência Técnica	Alto	Muito alto	Alto
Manutenção Predial	Médio	Muito alto	Alto
Compras	Muito alto	Muito alto	Muito alto

3.5.2.3 Estudos de prioridade

Segundo Marcos Sêmola, autor do livro “Gestão da Segurança da Informação: uma visão executiva” apud (Manoel 2014), o estudo de prioridade é uma ferramenta que ajuda a apontar a prioridade de cada processo de negócio para a organização, aplicando-se entre eles a matriz GUT: Gravidade, Urgência e Tendência. Utilizando as dimensões do GUT, classificamos da seguinte forma:

- ✓ **Gravidade (G):** seria muito grave para o processo de negócio em análise se algum evento atingisse qualquer um dos critérios, provocando a quebra da segurança da informação?
- ✓ **Urgência (U):** havendo a quebra da Segurança da Informação, qual seria a urgência em solucionar os efeitos do ocorrido e em reduzir os riscos no processo em análise?
- ✓ **Tendência (T):** qual seria a tendência dos riscos de Segurança da Informação caso nenhuma atividade corretiva ou preventiva fosse aplicada?

Tabela 8 – Escala da matriz de GUT.

Classificação da prioridade					
Gravidade		Urgência		Tendência	
1	Sem gravidade	1	Sem pressa	1	Não vai agravar
2	Baixa gravidade	2	Tolerante à espera	2	Vai agravar em longo prazo
3	Média gravidade	3	O mais cedo possível	3	Vai agravar em médio prazo
4	Alta gravidade	4	Com alguma urgência	4	Vai agravar em curto prazo
5	Altíssima gravidade	5	Imediatamente	5	Vai agravar imediatamente

Fonte – Manoel (2014).

Tabela 9 – Análise realizada da matriz de GUT.

	Classificação da prioridade		
Nome do processo	Gravidade	Urgência	Tendência
Inspeção de qualidade	Altíssima gravidade	Com alguma urgência	Vai agravar em curto prazo
Contabilidade	Média gravidade	Com alguma urgência	Vai agravar em curto prazo
Contas a receber	Alta gravidade	Com alguma urgência	Vai agravar em curto prazo
Contas a pagar	Alta gravidade	O mais cedo possível	Vai agravar a curto prazo
Recursos humanos	Média gravidade	O mais cedo possível	Vai agravar em longo prazo
Informática	Altíssima gravidade	Imediatamente	Vai agravar imediatamente
Administração de vendas	Altíssima gravidade	Imediatamente	Vai agravar imediatamente
Supervisão de exportação	Alta gravidade	Imediatamente	Vai agravar imediatamente
Supervisão de Mercado	Alta gravidade	O mais cedo possível	Vai agravar em curto prazo
Desenvolvimento de Produtos	Alta gravidade	O mais cedo possível	Vai agravar em médio prazo
Marketing	Alta gravidade	Com alguma urgência	Vai agravar em curto prazo
Fábrica I	Média gravidade	O mais cedo possível	Vai agravar em longo prazo
Fábrica II	Média gravidade	O mais cedo possível	Vai agravar em longo prazo
Planejamento de Produção	Altíssima gravidade	Imediatamente	Vai agravar imediatamente
Engenharia de Processos	Alta gravidade	Com alguma urgência	Vai agravar em curto prazo

Depósito de Produto Acabado	Média gravidade	O mais cedo possível	Vai agravar em curto prazo
Expedição	Alta gravidade	Com alguma urgência	Vai agravar em curto prazo
Assistência Técnica	Média gravidade	Com alguma urgência	Vai agravar em curto prazo
Manutenção Predial	Baixa gravidade	Com alguma urgência	Vai agravar em curto prazo
Compras	Alta gravidade	Imediatamente	Vai agravar imediatamente

3.6 Consolidação dos resultados

Para se obter uma visão geral da pesquisa os dados coletados, foram consolidados a partir da fórmula a seguir que calcula a pontuação final da criticidade:

Classificação do Impacto (CI) = Confidencialidade X Integridade X Disponibilidade / 3.
Classificação da prioridade (CP) = Gravidade X Urgência X Tendência / 3.
Criticidade = CI X CP X RP.

Fonte – Manoel (2014).

A tabela a seguir apresenta a escala da consolidação dos resultados:

Tabela 10 – Escala de nível de criticidade.

Cor	Nível	Pontuação
Verde	Baixo	O até 2801
Amarelo	Médio	2802 até 5602
Vermelho	Alto	5603 até 8405

Fonte – Manoel (2014).

Nas tabelas seguintes, é apresentado a sequência para o cálculo de maior criticidade para o de menor criticidade da organização analisada, com os seus respectivos valores de pontuação.

Tabela 11 – Relevância dos processos (RP).

Área	Processo	Relevância
Escritório da Qualidade/Diretoria	Inspeção de qualidade	Muito alta(5)
Departamento Administrativo/ Financeiro	Contabilidade	Muito alta(5)
	Contas a receber	Alta(4)
	Contas a pagar	Alta(4)
	Recursos Humanos	Média(3)
	Informática	Muito Alta(5)
	Administração de Vendas	Alta(4)
Departamento Comercial	Supervisão de exportação	Alta(4)
	Supervisão de Mercado	Alta(4)
Departamento de Marketing	Desenvolvimento de Produtos	Média(3)
	Marketing	Média(3)
Departamento Industrial	Fábrica I	Média(3)
	Fábrica II	Média(3)
	Planejamento de Produção	Alta(4)
	Engenharia de Processos	Alta(4)
	Depósito de Produto Acabado	Média(3)
	Expedição	Média(3)
	Assistência Técnica	Média(3)
	Manutenção Predial	Baixa(2)
	Compras	Alta(4)

Tabela 12 - Resultado da Classificação de Impacto (CI).

Processos	**Classificação de impacto (CI)**			**Pontos**
	Confidencialidade	**Integridade**	**Disponibilidade**	
Inspeção de qualidade	Muito alto(5)	Muito alto(5)	Muito alto(5)	42
Contabilidade	Muito alto(5)	Muito alto(5)	Alto(4)	34
Contas a receber	Muito alto(5)	Muito alto(5)	Muito alto(5)	42
Contas a pagar	Muito alto(5)	Muito alto(5)	Muito alto(5)	42
Recursos Humanos	Alto(4)	Muito alto(5)	Alto(4)	27
Informática	Muito alto(5)	Muito alto(5)	Muito alto(5)	42
Administração de Vendas	Muito alto(5)	Muito alto(5)	Muito alto(5)	42
Supervisão de exportação	Alto(4)	Muito alto(5)	Alto(4)	27
Supervisão de Mercado	Alto(4)	Muito alto(5)	Alto(4)	27
Desenvolvimento de Produtos	Muito alto(5)	Muito alto(5)	Alto(4)	34
Marketing	Muito alto(5)	Muito alto(5)	Alto(4)	34
Fábrica I	Alto(4)	Muito alto(5)	Alto(4)	27
Fábrica II	Alto(4)	Muito alto(5)	Alto(4)	27
Planejamento de Produção	Alto(4)	Muito alto(5)	Alto(4)	27
Engenharia de	Muito alto(5)	Muito	Alto(4)	34

Processos		alto(5)		
Depósito de Produto Acabado	Alto(4)	Muito alto(5)	Alto(4)	27
Expedição	Alto(4)	Muito alto(5)	Alto(4)	27
Assistência Técnica	Alto(4)	Muito alto(5)	Alto(4)	27
Manutenção Predial	Alto(4)	Muito alto(5)	Alto(4)	27
Compras	Muito alto(4)	Muito alto(5)	Alto(4)	27

Tabela 13 – Resultado da Classificação de Prioridade.

Processos	**Classificação da Prioridade (CP)**			**Pontos**
	Gravidade	**Urgência**	**Tendência**	
Inspeção de qualidade	Alta gravidade(4)	Com alguma urgência(4)	Vai agravar em curto prazo(4)	22
Contabilidade	Média gravidade(3)	Com alguma urgência(4)	Vai agravar em curto prazo(4)	16
Contas a receber	Alta gravidade(4)	Com alguma urgência(4)	Vai agravar em curto prazo(4)	22
Contas a pagar	Alta gravidade(4)	O mais cedo possível(3)	Vai agravar em curto prazo(4)	16
Recursos Humanos	Média gravidade(3)	O mais cedo possível(3)	Vai agravar em longo prazo(2)	6
Informática	Alta gravidade(4)	Imediatamente (5)	Vai agravar imediatamente(5)	34
Administração de Vendas	Altíssima gravidade(5)	Imediatamente (5)	Vai agravar imediatamente(5)	42
Supervisão de exportação	Alta gravidade(4)	Imediatamente (5)	Vai agravar imediatamente(5)	34
Supervisão de	Alta	O mais cedo	Vai agravar em	16

Mercado	gravidade(4)	possível(3)	curto prazo(4)	
Desenvolvimento de Produtos	Alta gravidade(4)	O mais cedo possível(3)	Vai agravar em médio prazo(3)	12
Marketing	Alta gravidade(4)	Com alguma urgência(4)	Vai agravar em curto prazo(4)	22
Fábrica I	Média gravidade(3)	O mais cedo possível(3)	Vai agravar em longo prazo(2)	6
Fábrica II	Média gravidade(3)	O mais cedo possível(3)	Vai agravar em longo prazo(2)	6
Planejamento de Produção	Altíssima gravidade(5)	Imediatamente (5)	Vai agravar imediatamente(5)	42
Engenharia de Processos	Alta gravidade(4)	Com alguma urgência(4)	Vai agravar em curto prazo(4)	22
Depósito de Produto Acabado	Média gravidade(3)	O mais cedo possível(3)	Vai agravar em curto prazo(4)	12
Expedição	Alta gravidade(4)	Com alguma urgência(4)	Vai agravar em curto prazo(4)	22
Assistência Técnica	Média gravidade(3)	Com alguma urgência(4)	Vai agravar em curto prazo(4)	16
Manutenção Predial	Média gravidade(3)	Com alguma urgência(4)	Vai agravar em curto prazo(4)	16
Compras	Alta gravidade(4)	Imediatamente (5)	Vai agravar imediatamente(5)	27

Tabela 14 – Resultado da Criticidade dos riscos.

Processos	CI	CP	RP	Relevância	Criticidade
Inspeção de qualidade	42	22	5	Médio	4650
Contabilidade	34	16	5	Baixo	2720
Contas a receber	42	22	4	Médio	3696
Contas a pagar	42	16	4	Baixo	2688

Recursos Humanos	27	6	3	Baixo	486
Informática	42	34	5	Alto	7140
Administração de Vendas	42	42	4	Alto	7056
Supervisão de exportação	27	34	4	Médio	3672
Supervisão de Mercado	27	16	4	Baixo	1728
Desenvolvimento de Produtos	34	12	3	Baixo	1224
Marketing	34	22	3	Baixo	2244
Fábrica I	27	6	3	Baixo	486
Fábrica II	27	6	3	Baixo	486
Planejamento de Produção	27	42	4	Médio	4536
Engenharia de Processos	34	22	4	Médio	2992
Depósito de Produto Acabado	27	12	3	Baixo	972
Expedição	27	22	3	Baixo	1782
Assistência Técnica	27	16	3	Baixo	1296
Manutenção Predial	27	16	2	Baixo	864
Compras	27	27	4	Médio	2916

4. RESULTADOS E DISCUSSÃO DOS DADOS

Com consolidação dos dados coletados através da Gestão de Riscos e do questionário (Apêndice A) aplicado no Setor de Informática da empresa, obteve-se uma visão geral dos estudos de impacto e prioridade, com objetivo de apresentar as áreas e os processos mais críticos, ou seja, os que requerem maior atenção quanto às questões de Segurança da Informação.

Tabela 15 – Resultados em conformidade com as Normas

Questões	ABNT NBR ISO/IEC 27002:2013	EMPRESA	DIRETRIZES PARA EMPRESA MÉDIO PORTE	OBJETIVO
Política de Segurança de informação.	Seção 5 - Política de Segurança de Informação	Existe, mas não é utilizada	Seção 1 - Políticas de Segurança da Informação	Orientar a direção, apoiar a segurança
Controle de acesso de usuários	Seção 7 - Segurança em Recursos Humanos	Sim, com alto nível de segurança	Não houve necessidade de implementação	Esclarecer as responsabilidades de cada usuários
Orientações aos usuários	Seção 7 - Segurança em Recursos Humanos	Sim, com alto nível de segurança	Não houve necessidade de implementação	Esclarecer as responsabilidades de cada usuários
Transferência de informações?	Seção 13 - Segurança nas Comunicações	Sim, com alto nível de segurança	Não houve necessidade de implementação	Assegurar proteção das informações
Classificação das informações	Seção 8 - Gestão de Ativos	Não existe	Seção 4 - Classificação da Informação	Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização
Ativos	Seção 8 - Gestão de Ativos	Sim, com alto nível de segurança	Não houve necessidade de implementação	Identificar os ativos e definir devidas proteções
Dispositivos móveis	Seção 6 - Organização da	Sim, mas incompleto	Seção 3 - Dispositivos Móveis e Trabalho	Garantir a segurança das

	Segurança da Informação		Remoto	informações no trabalho remoto e n o uso de dispositivos móveis
Ferramentas contra vírus e outros	Seção 12 - Segurança nas Operações	Sim, com alto nível de segurança	Não houve necessidade de implementação	Garantir a operação segura e correta dos recursos de processamento da informação
Criptografia	Seção 10 - Criptografia	Sim, mas incompleto	Seção 5 - Criptografia	Assegurar o uso efetivo e adequado da criptografia
Registros e monitoração de redes	Seção 12 - Segurança nas Operações	Sim, com alto nível de segurança	Não houve necessidade de implementação	Garantir a operação segura e correta dos recursos de processamento da informação
Planejamento a continuidade da segurança da informação	Seção 17 - Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio	Sim, mas incompleto	Seção 10 - Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio	Continuidade da segurança da informação seja contemplada nos sistemas de gestão da continuidade do negócio da organização
Regulamentos em conformidade com requisitos legais e contratuais	Seção 18 - Conformidade	Não existe	Seção 11 - Conformidade	Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação
Funções e responsabilidades são claramente estabelecidas?	Seção 6 - Organização da Segurança da Informação	Não existe	Seção 2 - Organização da Segurança da Informação	Estabelecer um estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação da organização

Existem informações para assegurar respostas rápidas, efetivas e ordenadas aos incidentes?	Seção 16 - Gestão de Incidentes de Segurança da Informação	Não existe	Seção 9 - Gestão de Incidentes de Segurança da Informação	Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação
Desenvolvimento de software e/ou aplicativos?	Seção 12 - Segurança nas Operações	Sim, mas incompleto	Seção 6 - Segurança nas Operações	Garantir a operação segura e correta dos recursos de processamento da informação
Processo formal nas mudanças de aplicativos e/ou softwares?	Seção 12 - Segurança nas Operações	Sim, mas incompleto	Seção 6 - Segurança nas Operações	Garantir a operação segura e correta dos recursos de processamento da informação
Exigências de segurança quanto a seus fornecedores?	seção 15 - Relacionamento na Cadeia de Suprimento	Sim, mas incompleto	Seção 8 - Relacionamento na Cadeia de Suprimento	Garantir a proteção dos ativos que são acessados pelos fornecedores
Fornecedores são documentados e identificados?	seção 15 - Relacionamento na Cadeia de Suprimento	Sim, mas incompleto	Seção 8 - Relacionamento na Cadeia de Suprimento	Garantir a proteção dos ativos que são acessados pelos fornecedores
Fornecedores podem manipular dados no sistema da empresa?	seção 15 - Relacionamento na Cadeia de Suprimento	Sim, mas incompleto	Seção 8 - Relacionamento na Cadeia de Suprimento	Garantir a proteção dos ativos que são acessados pelos fornecedores

4.1 Análise descritiva dos dados

Na análise dos dados coletados no questionário aplicado ao profissional de informática para verificação da segurança de informação na empresa, após submetidos à análise, apontam em cada questão que:

QUESTÃO 1 - Existe na empresa uma Política de Segurança de informação, com procedimentos que contemplem requisitos da estratégia do negócio, regulamentações, legislação e contrato, bem como se tem conhecimento de ambientes de ameaça da segurança da informação?
R.: Sim, mas não é utilizado.

Foi constatado que existe uma documentação, incompleta e que não era utilizada para padronizar os processos de negócio quanto a segurança de informação o que levou a considerar o documento como não sendo sobre uma Política de Segurança de Informação, mas meramente um documento para se ter arquivado na empresa caso alguma fiscalização/auditoria exigisse uma apresentação documentada sobre algum tipo de segurança de informação. Porém sabe-se que uma Política de Segurança de informação serve para orientar e apoiar o negócio de acordo com as leis e regulamentos relevantes.

Para tornar real a implementação de uma Política de Segurança de Informação na empresa retirou-se da Norma ABNT NBR ISO/IEC 27002:2013, na Seção 5, Políticas de segurança da informação, que tem como objetivo a orientação da direção e apoio para segurança de informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes, que foi inserida nas Diretrizes de Políticas Segurança da Informação para Empresa como Seção 1, Políticas de segurança da informação, separada em dois controles: 1.1 Políticas para segurança da informação e 1.2 Análise crítica da políticas para segurança da informação.

QUESTÃO 2 - Existe na empresa algum controle de acesso de usuários autorizado e não autorizado, seja acesso físico ou virtual?
R.: Sim, com alto nível de segurança virtual, mas baixo nível se segurança físico.

Quanto ao acesso de usuários, foi constatado que, para acessarem o sistema os usuários precisam ter um login e senha, com bloqueios para evitar a utilização de mídias externas no ambiente da empresa, que foi julgado um nível alto de segurança

e neste ponto não havia necessidade de acrescentar melhorias. Quanto a questão do acesso físico, onde estão os servidores, o acesso só aos colaboradores do setor de TI, é uma sala que permanece trancada, mas sem tecnologia avançada de segurança. Conforme consta na Norma ABNT NBR ISO/IEC 27002:2013 Seção 9, Controle de Acesso que tem como objetivo limitar o acesso à informação e aos recursos de processamento da informação.

Constatou-se que não era de interesse da empresa em implementar uma segurança mais consistente, como por exemplo, a utilização de aparelho para acesso com digitais eletrônicas.

QUESTÃO 3 - Existe na empresa orientações para os usuários finais quanto as suas responsabilidades na manipulação das informações?
R.: Sim, alto nível de segurança.

Quando um novo funcionário ingressa na empresa, lhe é passado todas as orientações referente a como deve se comportar com relação as informações que terá acesso diariamente. Tanto nas questões de informações que circulam somente internamente quanto as que transitam através de e-mails, ferramentas como Skype, etc. O usuário fica ciente do que pode e não pode fazer estando dentro da empresa. Também quando um colaborador é desligado, seu login é bloqueado, impedindo dessa forma que consiga acessar a rede através de qualquer computador, assim como sua conta de e-mail, caso o mesmo tenha uma, evitando dessa forma que o mesmo continue utilizando após seu desligamento.

Conforme foi verificado não havia mais o que agregar sobre segurança relacionado com usuários (referentes as perguntas 2 e 3), nem foi do interesse da empresa pois já continha todos os requisitos em conformidade com a Norma ABNT NBR ISO/IEC 27002:2013, na Seção 7, Segurança em recursos humanos que tem como objetivo assegurar que funcionários e partes externas entendam as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.

Porém na parte de segurança física apesar da baixa segurança na empresa, como acessos por impressões digitais a locais específicos, não houve o interesse da empresa em instalar dispositivos eletrônicos de segurança, pois apesar de saber que a segurança não estava de acordo não se achou interessante pelos dirigentes da empresa até o momento desta entrevista.

QUESTÃO 4 - Existe na empresa algum procedimento quanto a transferência de informações internas ou externas?

R.: Sim, alto nível de segurança.

Foi verificado que os arquivos que circulam dentro da rede da empresa são basicamente gerados dentro da própria rede, portanto com um nível alto de confiança. Já com arquivos externos, o processo de monitoramento é maior, visto que não é possível baixar e-mails com anexos e as máquinas tem suas unidades de USB bloqueadas, e se, houver a necessidade de se copiar algum arquivo isso só pode ser feito nas máquinas da TI, são verificados os conteúdos antes de serem colocados na rede da empresa.

Antes de entregar a mensagem, o sistema da empresa faz uma checagem do endereço para validá-lo, e em caso de um retorno negativo, o sistema envia mensagem ao usuário informando que aquele endereço não é válido.

Sendo assim constatado, não houve a necessidade de implementar um novo controle de segurança de informação conforme consta na Norma ABNT NBR ISO/IEC 27002:2013, Seção 13 Segurança nas comunicações, que tem como objetivo assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam.

QUESTÃO 5 - Existe tratamento e classificação das informações que circulam no ambiente interno e externo da empresa? Ou seja, a informação é classificada conforme o seu nível de importância na empresa?

R.: Não.

Não existe uma classificação específica. O que se aplica é o nível de acesso aos arquivos, as permissões dadas a um usuário ou departamento, lhe permite acesso ao conteúdo de todos os documentos que são compartilhados nas pastas que este tem acesso.

Dentro da Seção 8, Gestão de ativos, da Norma ABNT NBR ISO/IEC 27002:2013, que tem como objetivo identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos. Retirou-se desta seção, o controle de Classificação da informação e transformada em uma das Diretrizes de Políticas Segurança da Informação para Empresa Moveleira como Seção 4, Classificação da informação que tem objetivo específico de assegurar que a informação receba um nível adequado de proteção, de acordo com a sua

importância para a organização, separada por dois controles: 4.1 Classificação da informação e 4.2 Rótulos e tratamento da informação.

QUESTÃO 6 - Os ativos são identificados, catalogados e claramente definidos?
R.: Sim, alto nível de segurança.

Existe na empresa um software de inventário que especifica diariamente todos os seus ativos. Dessa forma, a retirada ou o acréscimo de qualquer equipamento é imediatamente identificado por este software.

Como no ambiente da empresa existe o uso de um software de inventário não se fez necessário a implementação de uma diretriz conforme a da Norma ABNT ISO/IEC 27002:2013, Seção 8, Gestão de ativos, que tem por objetivo identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.

QUESTÃO 7 - São utilizados no ambiente de trabalho da empresa o uso de dispositivos móveis, como por exemplo *tablets*, *notebooks* para acesso ao sistema da empresa?
R.: Sim, mas incompleto.

Somente na área interna da empresa, mas existe a possibilidade e necessidade de que num futuro próximo, externamente seja necessário a utilização desses dispositivos. Portanto se viu necessário a incorporação de diretrizes que auxiliem a empresa na segurança de informação também em setores externos.

Portanto foi constatado que havia o interesse da implementação de uma diretriz para uso futuro na empresa, e foi retirado da Norma ABNT ISO/IEC 27002:2013, na Seção 6, Organização da segurança da informação, que tem como objetivo estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização, sendo retirado o controle 6.2, Dispositivos móveis e trabalho remoto, que tem como objetivo principal garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis, sendo inserida nas Diretrizes de Políticas Segurança da Informação para empresa como Seção 3, Dispositivos móveis e trabalho remoto, dividida em dois controles: 3.1 Política para uso de dispositivo móvel e 3.2 Trabalho remoto.

QUESTÃO 8 - São utilizadas ferramentas na empresa contra vírus, *malwares,* etc?
R.: Sim, alto nível de segurança.

Foi verificado a utilização de uma ferramenta de terceiros para esta finalidade. Ferramenta corporativa que é constantemente atualizada no servidor e replicada para todas as estações.

Portanto não foi necessário e implementação de um diretriz conforme a Norma ABNT ISO/IEC 27002:2013, na Seção 12, Segurança nas operações, que tem como objetivo garantir a operação segura e correta dos recursos de processamento da informação.

QUESTÃO 9 - Existem controles de criptografia quanto a informação interna e externa da empresa?
R.: Sim, mas incompleto.

Os controles de criptografia de informações, que circulam interna ou externamente na empresa, é feito somente nas informações que são enviadas para nosso backup na nuvem. Portanto o restante de informações que circulam dentro da rede não existe segurança nenhuma até o momento de realização do backup e envio a nuvem.

Foi verificado então a necessidade e melhoria quanto a criptografia nas informações que circulam dentro e fora da empresa, para isso foi retirada da Norma ABNT ISO/IEC 27002:2013, na Seção 10, Criptografia que tem como objetivo assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação. Para isso foi criada nas Diretrizes de Políticas Segurança da Informação para empresa a Seção 5, Criptografia, com apenas um controle 5.1 Controles criptográficos que foi dividido em dois sub controles: 5.1.1 Políticas para uso de controles criptográficos e 5.1.2 Gerenciamento de chaves.

QUESTÃO 10 - Existem mecanismos de registro e monitoração de rede que assegurem ações que possam afetar a segurança da informação, seja interna ou externa?
R.: Sim, alto nível de segurança.

Foi verificado a emissão de relatórios diários sobre tudo que circula no ambiente de negócio da empresa, tanto através de e-mails quanto nas unidades de

rede, onde os arquivos e programas que não são permitidos são apontados nesses relatórios.

Foi verificado o não interesse de implementar uma diretriz conforme a Norma ABNT ISO/IEC 27002:2013 da Seção 12, controle 12.4 Registros e monitoramento que tem como objetivo registrar eventos e gerar evidências que tem como objetivo registrar eventos e gerar evidências.

QUESTÃO 11 - Existem procedimentos na empresa, de planejamento a continuidade da segurança de informação? Ou seja, em situações adversas, como uma crise ou desastre.
R.: Sim, mas incompleto.

Existe na empresa atualmente apenas um sistema de backups internos e externos, os quais possibilitam a recuperação dessas informações em um curto espaço de tempo.

Então se verificou a necessidade de implementar uma diretriz conforme a Norma ABNT ISO/IEC 27002:2013 da Seção 17 Aspectos da segurança da informação na gestão da continuidade do negócio que tem como objetivo que a continuidade da segurança da informação seja contemplada nos sistemas de gestão da continuidade do negócio da organização. Foi incorporada pelas Diretrizes de Políticas Segurança da Informação para empresa como Seção 10 aspectos da segurança da informação na gestão da continuidade do negócio, com uma subseção 10.1 Continuidade da segurança da informação e dividida em 3 controles: 10.1.1 Planejamento a continuidade da segurança da informação, 10.1.2. Implementando a continuidade da segurança da informação e 10.1.3 Verificação, análise crítica e avaliação da continuidade da segurança da informação.

QUESTÃO 12 - São documentados regulamentos em conformidade com requisitos legais e contratuais, para evitar violações de quaisquer obrigações legais, estatutárias, regulamentares e contratuais relacionadas à segurança da informação?
R.: Não.

Foi constatado que não existe na empresa nenhum documento que informa a legalidade de ações feitas dentro da empresa, além daquele que informa aos usuários de suas responsabilidades, somente é feito uma orientação informal aos

colaboradores. Quanto a utilização de softwares não existe nada além daquilo que se é conhecido popularmente.

Conforme verificação é necessário implementar um controle conforme a Norma ABNT ISO/IEC 27002:2013 da Seção 18 Conformidade, que tem como objetivo evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança. Com isso foi adicionada nas Diretrizes de Políticas Segurança da Informação para empresa como Seção 11, Conformidade, sendo dividida em duas sub diretrizes: 11.1 Conformidade com requisitos legais e contratuais que é dividido em cinco controles: 11.1.1 Identificação da legislação aplicável e de requisitos contratuais, 11.1.2 Direitos de propriedade intelectual, 11.1.3 Proteção de registros, 11.1.4 Proteção e privacidade de informações de identificação pessoal e 11.1.5 Regulamentação de controle de criptografia; 11.2 Análise crítica da segurança da informação que é dividida em três controles: 11.2.1 análise crítica independente da segurança da informação, 11.2.2 Conformidade com as políticas e procedimentos de segurança da informação e 12.2.3 Análise crítica de conformidade técnica.

QUESTÃO 13 - As funções dentro da empresa são claramente estabelecidas para evitar conflitos de responsabilidades e assim reduzir oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da empresa?
R.: Não.

Existe apenas uma hierarquia estabelecida, orientações informais sobre as responsabilidades de cada departamento e estes seguem essas recomendações.

Conforme foi verificado não existe nenhum documento esclarecendo as responsabilidades reais dos usuários dentro da empresa, somente as que são apresentadas numa eventual contratação ou desligamento de um colaborador. Fez-se assim necessário a implementação de uma diretriz conforme a Norma ABNT ISO/IEC 27002:2013 da Seção 6, Organização da segurança da informação, que tem como objetivo estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização, sendo incorporada nas Diretrizes de Políticas Segurança da Informação para empresa como Seção 2, Organização da segurança da informação com uma subdiretriz 2.1 Organização interna que é dividida em 4 controles: 2.1.1

responsabilidades e papéis pela segurança da informação, 2.1.2 Segregação de funções, 2.1.3 Contato com autoridades e 2.1.4 Contato com grupos especiais.

QUESTÃO 14 - Existem na empresa troca de informações quanto a responsabilidade e procedimentos quanto a fragilidade e eventos de segurança da informação, para assegurar respostas rápidas, efetivas e ordenadas aos incidentes?
R.: Não.

Foi verificado que quanto a confidencialidade de procedimentos a serem tomados no caso de falha ou quebra de segurança referentes informações que circulam no ambiente de trabalho, é inexistente no caso de ocorrer algum incidente de segurança de informação na empresa, não existe mecanismos para informar aos responsáveis sobre o ocorrido e de como proceder para evitar futuros problemas similares ao ocorrido.

Portanto foi necessário implementar uma diretriz de segurança da informação conforme a Norma ABNT ISO/IEC 27002:2013 da Seção 16, Gestão de incidentes de segurança da informação, que tem como objetivo assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre a fragilidade e eventos de segurança da informação. Foi então adicionada nas Diretrizes de Políticas Segurança da Informação para empresa como Seção 9, Gestão de incidentes de segurança da informação, com uma subseção: 9.1 Gestão de incidentes de segurança da informação, que é dividida em 6 controles; 9.1.1 Responsabilidades e procedimento, 9.1.2 Notificação de eventos de segurança da informação, 9.1.3 Notificando fragilidades de segurança da informação, 9.1.4 Avaliação e decisão dos eventos de segurança da informação, 9.1.5 Respostas aos incidentes de segurança da informação e 9.1.6 Aprendendo com os incidentes de segurança da informação.

QUESTÃO 15 - Existem na empresa o desenvolvimento particular de sistemas e/ou aplicativos?
R.: Sim, bom nível de segurança.

No ambiente da empresa existem alguns programas foram desenvolvidos pela equipe de TI, mas não consta nenhum tipo de procedimento ou documentação que serve de orientação nos procedimentos para o desenvolvimento ou implantação de sistemas e/ou aplicativos.

QUESTÃO 16 - Quanto a possíveis mudanças nestes sistemas e/ou aplicativos existe algum processo formal de documentação, especificação, teste, controle de qualidade e gestão da implementação?
R.: Não.

Foi verificado que não existe uma documentação orientando como proceder na implementação ou desenvolvimento de sistemas e/ou aplicativos, no caso de existir alguma atualização ou modificação, existe um ambiente de teste antes de colocar em produção.

Verificou-se então, conforme as questões 15 e 16 a necessidade de se implementar também uma diretriz conforme Norma ABNT ISO/IEC 27002:2013 da Seção 12, Segurança nas operações, tem como objetivo garantir a operação segura e correta dos recursos de processamento da informação, sendo adicionada nas Diretrizes de Políticas Segurança da Informação para empresa como Seção 6 Segurança nas operações, com uma subseção: 6.1 Responsabilidades e procedimentos operacionais, que está dividida em 4 controles: 6.1.1 Documentação dos procedimentos de operação, 6.1.2 Gestão de mudanças, 6.1.3 Gestão de capacidade e 6.1.4 Separação dos ambientes de desenvolvimento, teste e produção.

QUESTÃO 17 - Existe na empresa exigências, quanto a seus fornecedores, controles de segurança por eles implementados ou a empresa faz alguma recomendação quanto a níveis de segurança dentro dos sistemas dos fornecedores?
R.: Não.

Nenhuma exigência deste tipo foi colocada aos fornecedores.

QUESTÃO 18 - Fornecedores são documentados e identificados?
R.: Sim, bom nível de segurança.

Pela necessidade de se ter garantias sobre os serviços prestados e/ou produtos comercializados, os fornecedores são devidamente identificados e documentados na empresa.

QUESTÃO 19 - Fornecedores possuem autorização para manipulação de dados no sistema da empresa?

R.: Sim.

Foi verificado que, os fornecedores, não podem manipular os dados do sistema da empresa, fora aqueles em que ele é o responsável e isso é feito mediante monitoramento de alguém responsável do lado da empresa.

Conforme verificou-se nas perguntas 17, 18 e 19, viu-se necessário a inclusão de uma diretriz para os fornecedores, pois não existe algo realmente eficaz para auxiliar no processo de riscos com os fornecedores da empresa apesar de existir alguns pontos já feitos. Conforme a Norma ABNT ISO/IEC 27002:2013 da Seção 15 Relacionamento na cadeia de suprimento que tem como objetivo garantir a proteção dos ativos que são acessados pelos fornecedores, foi adicionada nas Diretrizes de Políticas Segurança da Informação para empresa como Seção 8, Relacionamento na cadeia de suprimento, contendo uma subseção 8.1 Segurança de informação na cadeia de suprimento e dividida em dois controles: 8.1.1 Política de segurança da informação no relacionamento com os fornecedores e 8.1.2 Identificando a segurança da informação nos acordos com os fornecedores.

Para melhor visualização dos dados consolidados para a implementação de Controles de Segurança da Informação da empresa alvo desta pesquisa, a Tabela 15 ilustra os controles utilizados com base na norma ABNT NBR ISO/IEC 2700:2013:

Tabela 16 – Controles de Segurança implementados

ABNT 27002:2013	**Diretriz para empresa**	**Objetivo**	**Controles para implementação**
Seção 5 – Política de Segurança da Informação	Seção 1 – Política de Segurança da Informação	Orientar a direção e apoiar a segurança	1.1 Orientação da direção para segurança da informação e 1.2 Análise crítica das políticas para segurança da informação
Seção 7 –	Já existia tal	Esclarecer as	

Segurança em Recursos Humanos	controle na empresa	responsabilidades de cada usuário	
Seção 7 – Segurança em Recursos Humanos	Já existia tal controle na empresa	Esclarecer as responsabilidades de cada usuário	
Seção 13 – Segurança nas Comunicações	Já existia tal controle na empresa	Assegurar a proteção das informações	
Seção 8 – Gestão de Ativos	Seção 4 – Classificação da Informação	Assegurar que a informação receba um nível adequado de proteção	4.1 Classificação da Informação e 4.2 Rótulos e tratamento da informação
Seção 8 – Gestão de Ativos	Já existia tal controle na empresa	Identificar ativos e definir proteções	
Seção 6 – Organização da Segurança da Informação	Seção 3 – Dispositivos Móveis	Garantir a segurança no trabalho remoto e no uso de dispositivos móveis	3.1 Política para uso de dispositivo móvel e 3.2 Trabalho remoto
Seção 12 – Segurança nas operações	Já existia tal controle na empresa	Garantir operações seguras e corretas dos recursos	
Seção 10 – Criptografia	Seção 5 – Criptografia	Assegurar uso efetivo e adequado de criptografia	5.1.1 Política para uso de controles criptográficos e 5.1.2 Gerenciamento de

			chaves
Seção 12 – Segurança nas operações	Já existia tal controle na empresa	Garantir operações seguras e corretas dos recursos	
Seção 17 – Aspectos da segurança da informação na gestão da continuidade do negócio	Seção 10 – Aspectos da segurança da informação na gestão da continuidade do negócio	Contemplar a continuidade da segurança da informação	10.1.1 Planejamento da continuidade da Segurança da informação, 10.1.2 Implementando a continuidade da segurança da informação e 10.1.3 Verificação, análise crítica e avaliação da continuidade da segurança da informação
Seção 18 – Conformidade	Seção 11 – Conformidade		11.1.1 Identificação da legislação aplicável e de requisitos contratuais, 11.1.2 Direitos de propriedade intelectual, 11.1.3 proteção de registros, 11.1.4 Proteção e privacidade de informações de identificação pessoal, 11.1.5 Regulamentação de controle de

			criptografia, 11.2.1 Análise crítica independente da segurança da informação, 11.2.2 Conformidade com as políticas e procedimentos de segurança da informação e 11.2.3 Análise crítica de conformidade técnica
Seção 6 – Organização da Segurança da informação	Seção 2 – Organização da Segurança da informação	Estabelecer uma estrutura de gerenciamento para controlar a implementação e operação da segurança da informação	2.1.1 Responsabilidades e papéis pela segurança da informação, 2.1.2 Segregação de funções, 2.1.3 Contato com autoridades, 2.1.4 Contato com grupos especiais e 2.1.5 Segurança da informação no gerenciamento de projetos
Seção 16 – Gestão de incidentes de segurança da informação	Seção 9 – Gestão de incidentes de segurança da informação	Gerenciar incidentes de segurança da informação	9.1.1 Responsabilidades e procedimentos, 9.1.2 Notificação de eventos de segurança de informação, 9.1.3 Notificando fragilidades de segurança da

			informação, 9.1.4 Avaliação e decisão dos eventos de segurança da informação, 9.1.5 Respostas aos incidentes de segurança da informação, 9.1.6 Aprendendo com os incidentes de segurança da informação e 9.1.7 Coleta de evidências
Seção 12 – Segurança nas operações	Seção 6 – Segurança nas operações	Garantir a operação segura dos recursos de processamento da informação	6.1.1 Documentação dos procedimentos de operação, 6.1.2 Gestão de mudanças, 6.1.3 Gestão de capacidade e 6.1.4 Separação dos ambientes de desenvolvimento, teste e produção
Seção 12 – Segurança nas operações	Seção 6 – Segurança nas operações	Garantir a operação segura dos recursos de processamento da informação	6.1.1 Documentação dos procedimentos de operação, 6.1.2 Gestão de mudanças, 6.1.3 Gestão de capacidade e 6.1.4 Separação dos ambientes de desenvolvimento, teste e produção
Seção 15 – Relacionamento na	Seção 8 – Relacionamento	Garantir a proteção dos	8.1.1 Política de segurança da

cadeia de suprimento	na cadeia de suprimento	ativos acessados pelos fornecedores	informação no relacionamento com os fornecedores e 8.1.2 Identificando segurança da informação nos acordos com fornecedores
Seção 15 – Relacionamento na cadeia de suprimento	Seção 8 – Relacionamento na cadeia de suprimento	Garantir a proteção dos ativos acessados pelos fornecedores	8.1.1 Política de segurança da informação no relacionamento com os fornecedores e 8.1.2 Identificando segurança da informação nos acordos com fornecedores
Seção 15 – Relacionamento na cadeia de suprimento	Seção 8 – Relacionamento na cadeia de suprimento	Garantir a proteção dos ativos acessados pelos fornecedores	8.1.1 Política de segurança da informação no relacionamento com os fornecedores e 8.1.2 Identificando segurança da informação nos acordos com fornecedores

5. CONCLUSÃO

A presente pesquisa apresentou alguns conceitos feitos por diversos autores e também uma visão geral sobre a Segurança da Informação. No cenário atual, em que as empresas dependem cada vez mais da tecnologia e da informação, é vital garantir a segurança adequada deste ativo, assim como a implementação da prática de Segurança da Informação no âmbito da organização compreende uma sequência de ações importantes e indispensáveis. Com essas ações, as empresas de todos os ramos de atuação evitam perda de qualidade, tempo e dinheiro.

Para o desenvolvimento desta pesquisa foi constatado a empresa dificuldades como: falta de procedimentos documentados, a falta de diretriz de trabalho com segurança, dentre outros. Tornou-se visível durante a pesquisa a dificuldade em modificar a cultura organizacional da empresa, pois encontra-se da parte de alguns funcionários mais antigos resistência às mudanças.

Durante a elaboração da pesquisa, considerou-se todas as falhas, que deverão ser sanadas de forma gradual, para alcançar um bom nível de segurança.

O ponto positivo é que a Empresa e seus gestores compreendem que o Setor de Tecnologia da Informação tem papel importante, e necessita de um perfeito funcionamento para atingir mais clientes e mais lucros.

Com a elaboração da versão inicial das Diretrizes para implementação de políticas de segurança da informação, será possível definir mais responsabilidades e limites, devendo este documento estar sempre atualizado.

Outro ponto importante é que os funcionários do setor de tecnologia da informação se comprometeram a reunir com a alta direção para discutir as mudanças que precisam ser feitas, e os procedimentos que devem ser adotados com máxima urgência para não expor mais a organização a tantos riscos desnecessários.

Em Suma, a Administração da Empresa, e os funcionários do departamento de informática, declararam estar cientes que é preciso investir em segurança da Informação para manter sua competitividade no mercado, declararam ser este trabalho de pesquisa um passo inicial.

Como sugestão de trabalhos futuros acredita-se que tem muito ainda a estudar e analisar, quanto aos conceitos apresentados e a implementação e acompanhamento das Diretrizes propostas na Política de Segurança na empresa.

Mapear e modelar os processos do setor de TI, bem como a atualização desta pesquisa para a Norma ABNT NBR ISO/IEC 27002:2013, que foi o foco principal.

A segurança da informação nas empresas em geral é um tema que abrange todo ambiente estrutural, organizacional e financeiro de uma empresa, levando-se em consideração ao aumento das negociações empresariais de hoje envolverem de alguma forma algum tipo de tecnologia e com isso nem sempre é possível se ter organização e controle dos negócios.

Com a evolução tecnológica é preciso também estar em constante atualização na segurança da informação no âmbito empresarial, contudo é normal não haver uma preocupação quanto a isso na maioria das pequenas e médias empresas, principalmente se adequar a algum tipo de padrão ou norma de segurança de informação.

Este trabalho alerta e informa que a segurança da informação é tão importante que, se ela não for levada a sério, uma organização pode estar caminhando para o seu fim a passos largos.

Observou-se que, com Controles adequados de segurança, pode-se organizar, melhorar sistemas, mitigar riscos, reparar falhas, evitar perdas financeiras consideráveis sem investimento financeiro alto.

Com a aplicação dos controles de segurança da informação, conforme a Norma ABNT NBR ISO/IEC 27002:2013, possibilitou-se melhorias na segurança de informação da empresa alvo desta pesquisa. Inclusive, já no presente orientar a mesma na proteção de serviços futuros, como por exemplo, o uso de dispositivos móveis para negociações financeiras mais dinâmicas.

Foi possível conscientizar mais adequadamente os colaboradores da empresa quanto a importância de se proteger os ativos da empresa e, ainda mais, conscientizar os diretores e gestores sobre a necessidade de se implantar uma política de segurança da informação baseada em normas e regras atestadas por órgãos competentes.

Sendo assim, pode-se concluir, conforme o objetivo deste trabalho que, após realizada uma análise dos aspectos relacionados à riscos de segurança da informação em uma empresa de médio porte, em seguida a implementação de controles de segurança apresentadas conforme a Norma ABNT NBR ISO/IEC 27002:2013, demonstrou-se a importância em se adotar políticas de segurança da informação.

6. REFERÊNCIAS

ALBUQUERQUE JUNIOR, Antônio E. de; SANTOS, Ernani M. dos. Segurança da Informação em Hospitais: A Percepção da Importância de Controles para Gestores e Profissionais de TI. Revista Gestão & Saúde, v.4, n.2, p. 1-14, 2012.

ALEXANDRIA, João C. S de. Gestão de Segurança da Informação – Uma Proposta para potencializar a Efetividade da Segurança da Informação em Ambiente de Pesquisa Científica. São Paulo, 2009. 193f. Tese (Doutorado em Tecnologia Nuclear) – Universidade de São Paulo, São Paulo, 2009. Disponível em http://www.teses.usp.br/teses/disponiveis/85/85131publico< acesso em 19 de dez. de 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799:2005: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da Segurança da informação. Rio de Janeiro: ABNT, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2006: Sistemas de Gestão de Segurança da informação. Requisito,2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2013: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da Segurança da informação. Rio de Janeiro: ABNT, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27005:2013: Tecnologia da Informação – Técnicas de segurança – Gestão de Riscos de Segurança da informação. Rio de Janeiro: ABNT, 2013.

BARRETO, Aldo de Albuquerque. A QUESTÃO DA INFORMAÇÃO. São Paulo em Perspectiva, São Paulo, v. 8, n. 4, p.1-11, 1994. In: Alves, Allan Ricardo. Política de Segurança da Informação: Análise ergonômica da difusão das normas em uma organização pública e seu impacto nos comportamentos inseguros. Monografia (especialização) Universidade de Brasília. Instituto de Ciências Exatas. Departamento de Ciência da Computação, 2011. 61 p.; Disponível em< http://dsic.planalto.gov.br/documentos/cegsic/monografias> Acesso em 20 de dez. de 2016.

BEAL, Adriana. Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. São Paulo: Atlas, 2005, 180p.

CAMPOS, André; Sistemas de segurança da informação Controlando Riscos; Editora Visual Books,2007. In: OLIVEIRA, Paulo Cesar. Política de Segurança da Informação: Definição, Importância, Elaboração e Implementação. 5 de junho de 2013. Disponível em < https://www.profissionaisti.com.br/2013> acesso em 19 de dez.de 2016.

KIM, David. Fundamentos de segurança de sistemas de informação; Tradução Daniel Vieira; revisão Técnica Jorge Duarte Pires Valério. 1. Ed.- Rio de Janeiro: LTC, 2014.

MANOEL, Sérgio da Silva. Governança de Segurança da Informação: Como criar oportunidades para seu negócio. Ed. Brasnorte, 2014.

NETO, Gonçalo Manoel da Silva; ALENCAR, Gliner Dias; QUEIROZ, Anderson Apolônio Lira. Proposal for Simplified Security Model for Small and Medium Business. In: Proceedings of the XI Brazilian Symposium on Information Systems (SBSI), 05 -2015. Disponível em, < http://aisel.aisnet.org/sbis2015> Acesso em 20 de junho de 2017.

NOBRE, Anna C. dos S.; RAMOS, Anatália S. M.; NASCIMENTO, Thiago C. Fatores que Influenciam a Aceitação de Práticas Avançadas de Gestão de Segurança da Informação: um estudo com gestores públicos estaduais no Brasil. In: XXXIV Encontro da ANPAD – EnANPAD. Rio de Janeiro, 2010. Anais. Rio de Janeiro: ANPAD, set.2010.Disponível em http://www.anpad.org.br/diversos/trabalhos/2013, Acesso em 19 de dez.2016.

OSIRO, A. K. (2006). Estudo de Segurança da Informação com enfoque nas Normas ABNT NBR ISO/IEC 17799:2005 e NBR ISO/IEC 27001:2006, para aplicação no Senado Federal. Monografia de Especialização, Publicação agosto/2006, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 114p.

SAMPAIO, Dhiêgo Rhubens Lima. Um estudo sobre riscos de segurança da informação no campus da UFC em Quixadá com base na norma ISO/IEC 27005:2013. – 2014. 51 f.: il. color. enc.; 30 cm.

SÊMOLA, Marcos. Segurança da Informação: Visão e compilação. 2007. Disponível em: http://www.semola.com.br/disco/InformationSecurityHotLInks2007.pdf. Acesso em 18 de maio de 2017.

APÊNDICE A - QUESTIONÁRIO APLICADO AO PROFISSIONAL DE INFORMÁTICA NA EMPRESA.

1 – Existe na empresa uma Política de Segurança de informação, com procedimentos que contemplem requisitos da estratégia do negócio, regulamentações, legislação e contrato, bem como se tem conhecimento de ambientes de ameaça da segurança da informação?
1- Não. 2-Não sei. 3--Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

2 – Existe na empresa algum controle de acesso de usuários autorizado e não autorizado, seja acesso físico ou virtual?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

3 – Existe tratamento e classificação das informações que circulam no ambienteinterno e externo da empresa? Ou seja, a informação é classificada conforme o seunível de importância na empresa?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4- Sim, mas não é utilizado. 5-Sim.

4 – Existe na empresa orientações para os usuários finais quanto as suas responsabilidades na manipulação das informações?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

5 – Os ativos são identificados, catalogados e claramente definidos?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

6 – Existe na empresa algum procedimento quanto a transferência de informações internas ou externas?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

7 - Existe algum aplicativo de comunicação interna?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

8 – São utilizadas ferramentas na empresa contra vírus, malwares, etc?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

9 – Existem controles de criptografia quanto a informação interna e externa da empresa?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

10 – Existem mecanismos de registro e monitoração de rede que assegurem ações que possam afetar a segurança da informação, seja interna ou externa?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

11 – Existem procedimentos na empresa, de planejamento a continuidade da segurança de informação? Ou seja, em situações adversas, como uma crise ou desastre.
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

12 – São documentados regulamentos em conformidade com requisitos legais econtratuais, para evitar violações de quaisquer obrigações legais, estatutárias,regulamentares e contratuais relacionadas à segurança da informação?

1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

13 – Existem na empresa troca de informações quanto a responsabilidade e procedimentos quanto a fragilidade e eventos de segurança da informação, para assegurar respostas rápidas, efetivas e aos incidentes?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

14 – Existem na empresa o desenvolvimento particular de sistemas e/ou aplicativos?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

15 - Quanto a possíveis mudanças nestes sistemas e/ou aplicativos existe algum processo formal de documentação, especificação, teste, controle de qualidade e gestão da implementação?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

16 – As funções dentro da empresa são claramente estabelecidas para evitar conflitos de responsabilidades e assim reduzir oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da empresa?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

17 – Existe na empresa exigências, quanto a seus fornecedores, controles de segurança por eles implementados?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

18 - Fornecedores são documentados e identificados?
1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

19 – Fornecedores possuem autorização para manipulação de dados no sistema da empresa?

1-Não. 2-Não sei. 3-Sim, mas não entendo. 4-Sim, mas não é utilizado. 5-Sim.

ANEXO A - DIRETRIZES PARA IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NA EMPRESA CONFORME ABNT ISO/IEC 27002:2013.

As diretrizes abaixo são indicações para se estabelecer a implementação da Política de segurança da informação, na Empresa analisada nesta pesquisa. Todos os itens abaixo foram compilados da norma ISO/IEC 27002:2013, de acordo com a análise dos dados coletados.

Toda norma tem por principal característica a prevenção contra as ameaças e vulnerabilidades da informação. O uso desse mecanismo tem por objetivo auxiliar na orientação da direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

A implementação da prática destas diretrizes no âmbito da organização compreende uma sequência de ações importantes para minimizar os impactos dos incidentes relacionados à segurança da informação, garantindo a segurança e continuidade dos negócios.

1. Políticas para segurança da informação

Objetivo: Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

1.1 Orientação da direção para segurança da informação

Controle

Convém que, no mais alto nível, a organização defina uma política de segurança da informação, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança da informação.

Convém que as políticas de segurança da informação contemplem requisitos oriundos de:

a) Estratégia de negócio;
b) Regulamentações, legislações e contratos;
c) Ambiente de ameaça da segurança da informação, atual e futuro.

Convém que a política de segurança da informação contenha declarações relativas a:

a) Definição de segurança da informação, objetivos e princípios para orientar todas as atividades relativas à segurança da informação;
b) Atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos;
c) Processos para o tratamento dos desvios e exceções.

No nível mais baixo, convém que a política de segurança da informação seja apoiada por políticas específicas do tema, que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos.

Convém que estas políticas sejam comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação”.

Informações adicionais

A necessidade de políticas internas de segurança da informação varia entre organizações. Políticas de segurança da informação podem ser emitidas em um único documento, “política de segurança da informação” ou como um conjunto de documentos individuais, relacionados.

Se qualquer uma das políticas de segurança de informação for distribuída fora da organização, convém que cuidados sejam tomados para não divulgar informações confidenciais.

1.2 Análise crítica das políticas para segurança da informação

Controle

Convém que as políticas de segurança da informação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Diretrizes para implementação

Convém que cada política de segurança da informação tenha um gestor que tenha aprovado a responsabilidade pelo desenvolvimento, análise crítica e avaliação das políticas de segurança da informação. Convém que a análise crítica inclua a

avaliação de oportunidades para melhoria da política de segurança da informação da organização e tenha um enfoque para gerenciar a segurança da informação em resposta às mudanças ao ambiente organizacional, às circunstâncias de negócio, às condições legais ou ao ambiente de tecnologia.

Convém que a análise crítica das políticas de segurança da informação leve em consideração os resultados da análise crítica pela direção.

Convém que seja obtida a aprovação da direção para a política revisada.

2. Organização da segurança da informação

2.1 Organização interna

Objetivo: Estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização.

2.1.1 Responsabilidades e papéis pela segurança da informação

Controle

Convém que todas as responsabilidades pela segurança da informação sejam definidas e atribuídas.

Diretrizes para implementação

Convém que a atribuição das responsabilidades pela segurança da informação seja feita em conformidade com as políticas de segurança da informação. Convém que as responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de segurança da informação específicos sejam claramente definidas. Convém que as responsabilidades pelas atividades do gerenciamento dos riscos de segurança da informação e, em particular, pela aceitação dos riscos residuais sejam definidas. Convém que as responsabilidades sejam complementadas, onde necessário, com orientações mais detalhadas para locais específicos e recursos de procedimento da informação. Convém que as responsabilidades locais para a proteção dos ativos e para realizar processos de segurança da informação específicos sejam definidas.

Indivíduos que receberam responsabilidades de segurança da informação podem delegar tarefas de segurança da informação para outros. Todavia, convém que eles

permaneçam responsáveis e determinem se quaisquer tarefas delegadas tenham sido corretamente executadas.

Convém que as áreas pelas quais as pessoas sejam responsáveis estejam claramente definidas; em particular, recomenda-se que os seguintes itens sejam cumpridos:

a) Convém que os ativos e os processos de segurança da informação sejam identificados e claramente definidos;
b) Convém que a entidade responsável por cada ativo ou processo de segurança da informação seja determinada e os detalhes dessa responsabilidade sejam documentados;
c) Convém que os níveis de autorização sejam claramente definidos e documentados;
d) Convém que pessoas indicadas sejam competentes e capazes de cumprir com as responsabilidades pela segurança da informação e a elas seja dada a oportunidade de manter-se atualizada com os desenvolvimentos;
e) Convém que a coordenação e a visão global dos aspectos de segurança da informação na cadeia de suprimento sejam identificadas e documentadas.

Informações adicionais

Muitas organizações atribuem a um gestor de segurança da informação a responsabilidade global pelo desenvolvimento e implementação da segurança da informação, e para apoiar a identificação de controles.

Entretanto, a responsabilidade por pesquisar e implementar os controles frequentemente permanecerá com os gestores individuais. Uma prática comum é a nomeação de um proprietário para cada ativo que, então, se torna responsável por sua proteção no dia a dia.

2.1.2 Segregação de funções

Controle

Convém que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização.

Diretrizes para implementação

Convém que sejam tomados certos cuidados para impedir que uma única pessoa possa acessar, modificar ou usar ativos sem a devida autorização ou detecção. Convém que o início de um evento seja separado de sua autorização. Convém que a possibilidade de existência de conjuntos seja considerada no projeto dos controles.

Pequenas organizações podem achar difícil realizar segregação de funções, mas convém que o princípio seja aplicado tanto quanto possível e praticável. Convém que sempre que seja difícil segregar, outros controles como monitoração das atividades, trilha de auditoria e supervisão da gestão sejam considerados.

Informações adicionais

Segregação de funções é um método para reduzir o risco de mau uso, acidental ou deliberado, dos ativos de uma organização.

2.1.3 Contato com autoridades

Controle

Convém que contatos com autoridades relevantes sejam mantidos.

Diretrizes para implementação

Convém que a organização tenha procedimentos implementados que especifiquem quando e quais autoridades (por exemplo, obrigações legais, corpo de bombeiros, autoridades fiscalizadoras, organismos regulatórios) serão contatadas e como os incidentes de segurança da informação identificados serão reportados em tempo hábil (por exemplo, no caso de suspeita de que a lei foi violada).

Informações adicionais

Organizações sob ataque da internet podem vir a necessitar que autoridades tomem providências contra a origem dos ataques.

Manter tais contatos pode ser um requisito para apoiar a gestão de incidentes de segurança da informação ou do processo de planejamento da contingência e da continuidade de negócio. Contatos com organismos regulatórios também são úteis para antecipar-se e preparar-se para futuras alterações em leis ou regulamentos, que terão que ser implementados pela organização. Contatos com outras

autoridades incluem serviços de infraestrutura serviços de emergência, fornecedores de energia, saúde e segurança, por exemplo, corpo de bombeiros (juntamente com continuidade de negócios), fornecedores de telecomunicações (juntamente com rotas de linha e disponibilidade) e fornecedores de água (juntamente com instalação de refrigeração para os equipamentos).

2.1.4 Contato com grupos especiais

Controle

Convém que contatos apropriados com grupos especiais associações profissionais ou outros fóruns especializados em segurança da informação sejam mantidos.

Diretrizes para implementação

Convém que a associação a grupos especiais ou fóruns sejam considerados como forma de:

a) Ampliar o conhecimento sobre as melhores práticas e manter-se atualizado com as informações relevantes sobre segurança da informação;
b) Assegurar que o entendimento do ambiente de segurança da informação esteja atual e completo;
c) Receber previamente advertências de alertas, aconselhamentos e correções relativos a ataques e vulnerabilidades;
d) Conseguir acesso à consulta especializada em segurança da informação;
e) Compartilhar e trocar informações sobre novas tecnologias, produtos, ameaças ou vulnerabilidades;
f) Prover relacionamentos adequados quando tratar com incidentes de segurança da informação.

Informações adicionais

Acordos de compartilhamentos de informações podem ser estabelecidos para melhorar a cooperação e coordenação de assuntos de segurança da informação. Convém que tais acordos identifiquem requisitos para a proteção de informação confidencial.

2.1.5 Segurança da informação no gerenciamento de projetos

Controle

Convém que a segurança da informação seja considerada no gerenciamento de projetos, independentemente do tipo de projeto.

Diretrizes para implementação

Convém que a segurança da informação seja integrada nos métodos de gerenciamentos de projeto da organização para assegurar que os riscos de segurança da informação estejam identificados e considerados como parte de um projeto. Isto se aplica, de um modo geral, a qualquer projeto, independentemente do se propósito, por exemplo, se é um projeto para u processo crítico do negócio, um processo de TI, de gerenciamento de recursos ou outro processo de apoio.

Convém que os métodos de gerenciamento de projetos usados requeiram que:

a) Os objetivos de segurança da informação sejam contemplados nos objetivos do projeto;
b) Uma avaliação dos riscos de segurança da informação seja conduzida em estágios iniciais do projeto para identificar os controles que são necessários;
c) A segurança da informação seja parte integrante de todas as fases da metodologia do projeto.

Convém que as questões de segurança de informação sejam consideradas e analisadas criticamente a intervalos planejados, em todos os projetos. Convém que as responsabilidades pela segurança da informação sejam definidas e alocadas para papéis específicos definidos dos métodos de gerenciamento de projeto.

3. Dispositivos móveis e trabalho Remoto

Objetivo: garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis.

3.1 Política para o uso de dispositivo móvel

Controle

Convém que uma política e medidas que apoiam a segurança da informação sejam adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis.

Diretrizes para implementação

Convém que, quando se utilizam dispositivos móveis, cuidados especiais sejam tomados para assegurar que as informações do negócio não sejam comprometidas. Convém que a política de dispositivos móveis leve em consideração os riscos de se trabalhar com esses dispositivos móveis em ambientes desprotegidos.

Convém que a política para uso de dispositivos móveis considere:

a) Registro dos dispositivos móveis;
b) Requisitos para a proteção física;
c) Restrições quanto à instalação de software;
d) Requisitos para as versões dos softwares e aplicações de patches;
e) Restrições para conexão aos serviços de informação;
f) Controle de acesso;
g) Técnicas criptográficas;
h) Proteção contra malware;
i) Desativação, bloqueio e exclusão de forma remota;
j) Backups;
k) Uso dos serviços web e aplicações web;

Convém que cuidados sejam tomados ao se utilizarem dispositivos móveis em locais públicos, sala de reuniões e outras áreas desprotegidas. Convém que sejam estabelecidas proteções para evitar o acesso não autorizado ou a divulgação de informações armazenadas e processadas nesses dispositivos, por exemplo, usando técnicas de criptografia e obrigando o uso de autenticação por informação secreta.

Convém que os dispositivos móveis sejam também protegidos fisicamente contra roubo, especialmente quando deixados, por exemplo, em carros ou em outros meios de transporte, quartos de hotéis, centros de conferência e locais de reunião. Convém que seja estabelecido um procedimento específico que leve em consideração requisitos legais, securitários e outros requisitos de segurança da organização para casos de furto, roubo ou perda de dispositivos móveis. Convém que os dispositivos móveis que contém informações importantes, sensíveis e/ou críticas para o negócio, não sejam deixados sem observação e, quando possível estejam fisicamente trancados com o uso de travas especiais, para proteger esses dispositivos móveis.

Convém que seja programado treinamento para as pessoas que usam dispositivos móveis como forma de aumentar a conscientização quanto aos riscos adicionais decorrentes desta forma de trabalho, e quanto aos controles que recomenda-se implementar.

Onde a política de dispositivos móveis permita o uso de dispositivos pessoais, convém que esta política e os controles de segurança relacionados também considerem:

a) Separação do uso do dispositivo para negócio e para fins pessoais, incluindo os softwares para apoiar esta separação e proteger os dados do negócio em um dispositivo privado;
b) Prover acesso às informações do negócio somente depois que os usuários assinarem o acordo de conhecimento das suas responsabilidades (quanto a proteção física, atualização do software, entre outros), renunciando direitos autorais dos dados do negócio, permitindo a exclusão remota dos dados pela organização no caso de furto, roubo ou perda do dispositivo móvel ou, ainda, quando não mais houver autorização para o uso dos serviços. Esta política precisa levar em consideração a legislação sobre privacidade.

Informações adicionais

Conexões de dispositivos móveis sem fio são similares a outros tipos de conexões de rede, mas possuem diferenças importantes, as quais recomenda-se considerar na identificação dos controles. As diferenças típicas são;

a) Alguns protocolos de segurança sem fio são imaturos e possuem fraquezas conhecidas;
b) Informações armazenadas em dispositivos móveis podem não ser passíveis de cópia de segurança por conta de limitações da largura de banda da rede ou porque dispositivos móveis podem não estar conectados no momento em que a cópia de segurança for agendada.

Dispositivos móveis geralmente compartilham funções comuns, por exemplo: rede, acesso à internet, e-mail e manuseio de arquivos, com uso de dispositivos fixos. Controles de segurança da informação para os dispositivos móveis geralmente

consistem naqueles adotados para o uso de dispositivos fixos e naqueles para endereçar ameaças levantadas pelo seu uso fora das instalações da organização.

3.2 Trabalho remoto

Controle

Convém que uma política e medidas que apoiam a segurança da informação sejam implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.

Diretrizes para implementação

Convém que a organização que permita a atividade de trabalho remoto publique uma política que defina as condições e restrições para o uso do trabalho remoto. Onde considerados aplicáveis e permitidos por lei, convém que os seguintes pontos sejam considerados:

a) A segurança física existente no local do trabalho remoto, levando-se em consideração a segurança física do prédio e o ambiente local;
b) O ambiente físico proposto para o trabalho remoto;
c) Os requisitos de segurança nas comunicações, levando em consideração a necessidade do acesso remoto aos sistemas internos da organização, a sensibilidade da informação que será acessada e trafegada na linha de comunicação e a sensibilidade do sistema interno;
d) O fornecimento de acesso virtual às estações de trabalho dos usuários, para prevenir o processamento e o armazenamento da informação em um equipamento de propriedade particular;
e) A ameaça de acesso não autorizado à informação ou aos recursos de processamento da informação por outras pessoas que utilizam o local, por exemplo familiares e amigos;
f) O uso de redes domésticas e requisitos ou restrições na configuração de serviços de rede sem fio;
g) Políticas e procedimentos para prevenir disputas relativas a direitos de propriedade intelectual desenvolvidas em equipamentos de propriedade particular;

h) Acesso a equipamentos de propriedade particular (para verificar a segurança da máquina ou durante uma investigação), o qual pode ser restringido por lei;
i) Acordos de licenciamento de software que podem tornar as organizações responsáveis pelo licenciamento do software cliente em estações de trabalho particulares de propriedade de funcionários, fornecedores ou partes externas;
j) Requisitos de firewall e proteção antivírus.

Convém que as diretrizes e providências considerem:

a) A provisão de equipamento e mobília apropriados às atividades de trabalho remoto, onde o uso de equipamentos de propriedade particular que não esteja sob controle da organização não seja permitido;
b) Uma definição do trabalho permitido, a classificação da informação que pode ser tratada e os sistemas internos e serviços que o usuário do trabalho remoto está autorizado a acessar;
c) Provisão de equipamento de comunicação apropriado, incluindo métodos para acesso remoto seguro;
d) Segurança física;
e) Regras e diretrizes sobre o acesso de familiares e visitantes ao equipamento e à informação;
f) A provisão de suporte e manutenção de hardware e software;
g) A provisão de seguro;
h) Os procedimentos para cópias de segurança e continuidade do negócio;
i) Auditoria e monitoramento da segurança;
j) Revogação de autoridade e direitos de acesso, e devolução do equipamento quando as atividades de trabalho remoto encerrarem.

Informações adicionais

Trabalho remoto refere-se a todas as formas de trabalho fora do escritório, incluindo ambientes de trabalho não tradicionais, como aqueles referidos como: ambientes de telecommuting, local de trabalho flexível, trabalho remoto e trabalho virtual.

4. Classificação da informação

Objetivo: Assegurar que a informação receba um nível adequado de proteção, de acordo com sua importância para a organização.

4.1 Classificação da informação

Controle

Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

Diretrizes para implementação

Convém que a classificação e os controles de proteção, associados à informação, levem em consideração as necessidades do negócio para compartilhar ou restringir a informação bem como os requisitos legais. Convém que outros ativos, além dos ativos de informação, também sejam classificados de acordo com a classificação da informação armazenada, processada, manuseada ou protegida pelo ativo.

Convém que os proprietários de ativos de informação sejam responsáveis por sua classificação.

Convém que o esquema de classificação inclua convenções para classificação e critérios para análise crítica da classificação ao longo do tempo. Convém que o nível de proteção seja avaliado por meio da análise da confidencialidade, integridade e disponibilidade, e quaisquer requisitos considerados para a informação. Convém que o esquema esteja alinhado com a política de controle de acesso.

Convém que a cada nível seja dado um nome que faça sentido no contexto do esquema de classificação.

Convém que o esquema seja consistente em toda a organização, de forma que cada pessoa possa classificar a informação e os ativos relacionados da mesma forma, e tenha um entendimento comum dos requisitos de proteção e aplique a proteção apropriada.

Convém que a classificação seja incluída nos processos da organização e seja consistente e coerente em toda a organização. Convém que os resultados da classificação indiquem o valor dos ativos em função da sua sensibilidade e criticidade para a organização, em termos da confidencialidade, integridade e disponibilidade. Convém que os resultados da classificação sejam atualizados de

acordo com as mudanças do seu valor, sensibilidade e criticidade ao longo do seu ciclo de vida.

Informações adicionais

A classificação fornece às pessoas que lidam com informações uma indicação concisa de como tratar e proteger a informação. A criação de grupos de informação com necessidades de proteção semelhantes e especificação dos procedimentos de segurança da informação que se aplicam a todas as informações de cada grupo é um facilitador. Esta abordagem reduz a necessidade de avaliação de risco e a customização personalizada de controles caso a caso.

A informação pode deixar de ser sensível ou crítica após certo período de tempo, por exemplo, quando a informação se torna pública. Convém que estes aspectos sejam levados em consideração, pois uma classificação superestimada pode levar à implementação de controles desnecessários, resultando em despesas adicionais ou, pelo contrário, classificações subestimadas podem colocar em perigo o alcance dos objetivos do negócio.

Um exemplo de um esquema de classificação de confidencialidade da informação poderia ser baseado em quatro níveis, como a seguir;

a) Quando sua divulgação não causa qualquer dano;
b) Quando a divulgação causa constrangimento menor ou inconveniência operacional menor;
c) Quando a divulgação tem um pequeno impacto significativo nas operações ou objetivos táticos;
d) Quando a divulgação tem um sério impacto sobre os objetivos estratégicos de longo prazo, ou coloca a sobrevivência da organização em risco.

4.2 Rótulos e tratamento da informação

Controle

Convém que um conjunto apropriado de procedimentos para rotular e tratar a informação seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização.

Diretrizes de implementação

Convém que procedimentos para a rotulagem da informação abranjam a informação e os seus ativos relacionados, nos formatos físico e eletrônico. A rotulagem pode refletir o esquema de classificação estabelecido em 4.1. convém que os rótulos sejam facilmente reconhecidos. Convém que o procedimento oriente sobre onde e como os rótulos devem ser colocados, levando-se em conta como a informação é acessada ou os ativos são manuseados, em função dos tipos de mídias. O procedimento pode definir uma situação onde a rotulagem é omitida, por exemplo, rotulagem de informação não confidencial, para reduzir a carga de trabalho. Convém que os funcionários e partes externas estejam conscientes do procedimento de classificação.

Convém que os resultados de sistemas que contém informações classificados como críticas ou sensíveis tenham um nível de classificação apropriado.

Informações adicionais

A rotulagem de informações classificadas é um requisito-chave para acordos de compartilhamento de informações. Rótulos físicos e metadados são uma forma comum de rotulagem.

A rotulagem de informação e de ativos relacionados pode às vezes ter efeitos negativos. Ativos classificados são mais fáceis de identificar e, consequentemente, roubados por pessoas internas ou externas.

5. Criptografia

5.1 Controle Criptográficos

Objetivo: Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

5.1.1 Política para o uso de controles criptográficos

Controle

Convém que seja desenvolvida e implementada uma política sobre o uso de controles criptográficos para a proteção da informação.

Diretrizes para implementação

Quando do desenvolvimento de uma política para criptografia, convém que sejam considerados:

a) A abordagem da Direção quanto ao isso de controles criptográficos em toda a organização, incluindo os princípios gerais sob os quais as informações de negócio sejam protegidas;
b) A identificação do nível requerido de proteção com base em uma avaliação de risco, levando em consideração o tipo, a força e a qualidade do algoritmo de criptografia requerido;
c) O uso de criptografia para proteção de informações sensíveis transportadas em dispositivos móveis, mídias removíveis ou através de linhas de comunicação;
d) A abordagem do gerenciamento de chaves, incluindo métodos para lidar com a proteção das chaves criptográficas e a recuperação de informações cifradas, no caso de chaves perdidas, comprometidas ou danificadas;
e) Papéis e responsabilidades, por exemplo, de quem for responsável:
    1) Pela implementação da política;
    2) Pelo gerenciamento de chaves, incluindo sua geração;
f) Os padrões a serem adotados para a eficaz implementação ao longo de toda a organização (qual solução é usada para quais processos de negócios);
g) O impacto do uso de informações cifradas em controles que dependem da inspeção de conteúdo (por exemplo, detecção de malware).

Convém que sejam consideradas na implementação da política criptográfica da organização as leis ou regulamentações e restrições nacionais aplicáveis ao uso de técnicas criptográficas, nas diferentes partes do mundo, e as questões relativas ao fluxo transfronteiras de informações cifradas.

Controles criptográficos podem ser usados para alcanças diferentes objetivos de segurança da informação, como, por exemplo:

a) Confidencialidade: usando a criptografia da informação para proteger informações sensíveis ou críticas, armazenadas ou transmitidas;

b) Integridade/autenticidade: usando assinaturas digitais ou códigos de autenticação de mensagens para verificar a autenticidade ou integridade de informações sensíveis ou críticas, armazenadas ou transmitidas;
c) Não repúdio: usando técnicas de criptografia para obter evidência da ocorrência ou não ocorrência de um evento ou ação;
d) Autenticação: usando técnicas criptográficas para autenticas usuários e outras camadas sistêmicas que requeiram acesso para transações com usuários de sistemas, entidades e recursos.

Informações adicionais

Convém que a tomada de decisão quanto a uma solução de criptografia ser apropriada seja vista como parte de processos mais amplos de avaliação de riscos e seleção de controles. Essa avaliação pode, então, ser usada para determinar se um controle criptográfico é apropriado, que tipo de controle convém ser aplicado e para qual propósito e processos de negócio.

Uma política sobre o uso de controles criptográficos é necessária para maximizar os benefícios, minimizar os riscos do uso de técnicas criptográficas e para evitar o uso incorreto ou inapropriado.

Convém que seja buscada a opinião de um especialista para identificar os controles criptográficos adequados para atender aos objetivos da política de segurança da informação.

5.1.2 Gerenciamento de chaves

Controle

Convém que uma política sobre o uso, proteção e tempo de vida das chaves criptográficas seja desenvolvida e implementada ao longo de todo o seu ciclo de vida.

Diretrizes para implementação

Convém que a política inclua requisitos para o gerenciamento de chaves criptográficas ao longo de todo o seu ciclo de vida, incluindo a geração, armazenamento, arquivo, recuperação, distribuição, retirada e destruição das chaves.

Convém que algoritmos criptográficos, tamanho de chaves e práticas de chaves e práticas usuais sejam selecionados de acordo com as melhores práticas. A gestão de chaves apropriada requer processos seguros para a geração, armazenamento, arquivo, recuperação, distribuição, retirada e destruição das chaves.

Convém que todas as chaves criptográficas sejam protegidas contra modificação e perda. Adicionalmente, chaves secretas e privadas necessitam de proteção contra o uso ou a divulgação não autorizada. É recomendável que os equipamentos utilizados para gerar, armazenar e guardar as chaves sejam fisicamente protegidos.

Convém que um sistema de gerenciamento de chaves seja baseado em um conjunto estabelecido de normas, procedimentos e métodos seguros para:

a) Gerar chaves para diferentes sistemas criptográficos e diferentes aplicações;
b) Gerar e obter certificados de chaves públicas;
c) Distribuir chaves para os usuários devidos, incluindo a forma como as chaves são ativadas, quando recebidas;
d) Armazenar chaves, incluindo a forma como os usuários autorizados obtêm acesso a elas;
e) Mudar ou atualizar chaves, incluindo regras quando as chaves são mudadas e como isto deve ser conduzido;
f) Lidar com chaves comprometidas;
g) Revogar chaves, incluindo regras de como elas são retiradas ou desativadas, por exemplo, quando chaves tiverem sido comprometidas ou quando um usuário deixa a organização (é recomendável também, neste caso, que as chaves sejam arquivadas);
h) Recuperar chaves perdidas ou corrompidas;
i) Realizar cópias de segurança ou arquivas as chaves;
j) Destruir chaves;
k) Manter registro e auditoria das atividades relacionadas ao gerenciamento de chaves;

Para reduzir a probabilidade de comprometimento, convém que as datas de ativação e desativação de chaves sejam definidas de forma que possam ser utilizadas apenas por um período de tempo definido na política de gerenciamento de chaves.

Além do gerenciamento seguro de chaves secretas e privadas, convém que a autenticidade de chaves públicas seja considerada. Este processo de autenticação pode ser conduzido utilizando-se certificados de chaves públicas que são normalmente emitidos por uma autoridade certificadora, a qual recomenda-se que seja uma organização reconhecida, com controles adequados e procedimentos implantados com o objetivo de garantir o requerido nível de confiança.

Convém que os conteúdos dos acordos de nível de serviço ou dos contratos com fornecedores externos de serviços criptográficos, como, por exemplo, com uma autoridade certificadora, cubra aspectos como responsabilidades, confiabilidade dos serviços e tempo s de resposta para a execução dos serviços contratados.

Informações adicionais

As técnicas criptográficas podem ser também utilizadas para proteger chaves criptográficas. Pode ser necessário o estabelecimento de procedimentos para o manuseio de solicitações legais para acesso a chaves criptográficas, por exemplo, a disponibilização de informação cifrada pode ser requerida em sua forma decifrada para uso como evidência em um processo judicial.

6. Segurança nas operações

6.1 Responsabilidades e procedimentos operacionais

Objetivo: Garantir a operação segura e correta dos recursos de processamento da informação.

6.1.1 Documentação dos procedimentos de operação

Controle

Convém que os procedimentos de operação sejam documentados e disponibilizados para todos os usuários que necessitem deles.

Diretrizes para implementação

Convém que os procedimentos documentados sejam preparados para as atividades operacionais associadas a recursos de processamento de comunicação e informações, como procedimentos de inicialização e desligamento de computadores, geração de cópias de segurança, manutenção de equipamentos, tratamento de

mídias, segurança e gestão do tratamento das correspondências e das salas de computadores.

Convém que os procedimentos de operação especifiquem as instruções, incluindo:

a) A instalação e configuração de sistemas;
b) Processamento e tratamento da informação, tanto automática como manual;
c) Cópias de segurança;
d) Requisitos de agendamento, incluindo interdependências com outros sistemas, a primeira hora para início da tarefa e a última hora para o término da tarefa;
e) Instruções para tratamento de erros ou outras condições excepcionais, que possam ocorrer durante a execução de uma tarefa, incluindo restrições de uso utilitários do sistema;
f) Contatos para suporte e escalação, incluindo contatos de suporte externos, para o caso de eventos operacionais inesperados ou dificuldades técnicas;
g) Instruções quanto ao manuseio de mídias e saídas especiais, como o uso de formulários especiais ou o gerenciamento de dados confidenciais, incluindo procedimentos para o descarte seguro de resultados provenientes de rotinas com falhas;
h) Procedimento para o reinício e recuperação em caso de falha do sistema;
i) Gerenciamento de trilhas de auditoria e informações de registros (logs) de sistemas;
j) Procedimentos de monitoramento.

Convém que os procedimentos operacionais e os procedimentos documentados para atividades de sistemas sejam tratados como documentos formais e as mudanças sejam autorizadas pela direção. Quando tecnicamente possível, convém que sistemas de informação sejam gerenciados uniformemente, usando os mesmos procedimentos, ferramentas e utilitários.

6.1.2 Gestão de mudanças

Controles

Convém que mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação sejam controladas.

Diretrizes para implementação

Convém que os seguintes itens, em particular, sejam considerados:

a) Identificação e registro das mudanças significativas;
b) Planejamento e testes das mudanças;
c) Avaliação de impactos potenciais, incluindo impactos de segurança da informação de tais mudanças;
d) Procedimento formal de aprovação das mudanças propostas;
e) Verificação de que os requisitos de segurança da informação foram atendidos;
f) Comunicação dos detalhes das mudanças para todas as pessoas relevantes;
g) Procedimentos de recuperação, incluindo procedimentos e responsabilidades para interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados;
h) Provisão de um processo emergencial de mudança para permitir uma implementação rápida e controlada de mudanças, necessárias para resolver um incidente.

Convém que sejam estabelecidos procedimentos e responsabilidades de gestão formais para garantir que haja um controle satisfatório de todas as mudanças. Quando mudanças forem realizadas, é conveniente manter um registro de auditoria contendo todas as informações relevantes.

Informações adicionais

O controle inadequado de modificações nos sistemas e nos recursos de processamentos das informações é uma causa comum de falhas de segurança ou de sistema. Mudanças em ambientes operacionais, especialmente quando da

transferência de um sistema em desenvolvimento para o estágio operacional, podem trazer impactos à confiabilidade de aplicações.

6.1.3 Gestão de capacidade

Controle

Convém que a utilização dos recursos seja monitorada e ajustada, e que as projeções sejam feitas para necessidade de capacidade futura para garantir o desempenho requerido do sistema.

Diretrizes para implementação

Convém que requisitos de capacidade sejam identificados levando-se em conta a criticidade do negócio do sistema em questão. Convém que o ajuste e o monitoramento dos sistemas sejam aplicados para garantir e, quando necessário, melhorar a disponibilidade e eficiência dos sistemas. É recomendável que os controles detectivos sejam implantados para identificar problemas em tempo hábil. É conveniente que projeções de capacidade futura levem em consideração os requisitos de novos negócios e sistemas e as tendências atuais e projetadas de capacidade de processamento de informação da organização.

Atenção particular precisa ser dada a qualquer recurso que possua um ciclo de renovação longo ou custo alto, sendo responsabilidade dos gestores monitorar a utilização dos recursos-chave dos sistemas. Convém que eles identifiquem as tendências de utilização dos recursos em relação às aplicações do negócio ou às ferramentas de gestão de sistemas de informação.

Convém que os gestores utilizem essas informações para identificar e evitar os potenciais gargalos e a dependência em pessoas-chave que possam representar ameaças à segurança dos sistemas ou aos serviços, e planejar ação apropriada.

O fornecimento de capacidade suficiente pode ser obtido por meio do aumento de capacidade ou pela redução da demanda. Exemplos de gerenciamento da demanda de capacidade incluem:

a) Exclusão de dados obsoletos (espaço em disco);
b) Desativação de aplicações, sistemas, bases de dados ou ambientes;
c) Otimização das programações e dos processos de lote;

d) Otimização da lógica de aplicação ou das consultas à base de dados;
e) Negar ou restringir a largura da banda para serviços que demandam muitos recursos, se estes não forem críticos ao negócio.

Convém que um plano documentado de gestão de capacidade seja considerado para os sistemas de missão crítica.

Informações adicionais

Este controle também considera a capacidade dos recursos humanos, bem como dos escritórios e instalações.

6.1.4 Separação dos ambientes de desenvolvimento, teste e produção

Controle

Convém que ambientes de desenvolvimento, teste e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.

Diretrizes para implementação

Convém que o nível de separação dos ambientes de produção, testes e desenvolvimento, que é necessário para prevenir problemas operacionais, seja identificado e os controles apropriados sejam implementados.

Convém que os seguintes itens sejam considerados:

a) Convém que as regras para a transferência de software do ambiente de desenvolvimento para o de produção sejam definidas e documentadas;
b) Convém que o software em desenvolvimento e o software em produção sejam, sempre que possível, executados em diferentes sistemas ou processadores e em diferentes domínios ou diretórios;
c) Convém que as mudanças nas aplicações e nos sistemas operacionais sejam testadas em um ambiente de teste ou projeto-piloto, antes de serem aplicadas aos sistemas operacionais;
d) Convém que os testes não sejam realizados nos sistemas operacionais, exceto em circunstâncias excepcionais;

e) Convém que os compiladores, editores e outras ferramentas de desenvolvimento ou utilitários de sistemas não sejam acessíveis aos sistemas operacionais, quando não for necessário;
f) Convém que os utilitários tenham diferentes perfis para sistemas em testes e em produção, e que os menus mostrem mensagens apropriadas de identificação para reduzir o risco de erro;
g) Convém que os dados sensíveis não sejam copiados para os ambientes de testes, a menos que controles equivalentes sejam fornecidos para o sistema de teste.

Informações adicionais

As atividades de desenvolvimento e teste podem causar sérios problemas, como, por exemplo, modificações inesperadas em arquivos ou no ambiente dos sistemas, ou falhas de sistemas. Nesse caso, é necessária a manutenção de um ambiente conhecido e estável, no qual possam ser executados testes significativos e que seja capaz de prevenir o acesso indevido do pessoal de desenvolvimento ao ambiente operacional.

Quando o pessoal de desenvolvimento e teste possui acesso ao sistema operacional e suas informações, estes podem introduzir códigos não autorizados e não testados, ou mesmo alterar os dados de produção. Em alguns sistemas essa capacidade pode ser mal utilizada para a execução de fraudes ou introdução de códigos maliciosos ou não testados, que podem causar sérios problemas operacionais.

O pessoal de desenvolvimento e teste também representa uma ameaça à confidencialidade das informações de produção. As atividades de desenvolvimento e teste podem causar modificações não intencionais no software ou nas informações, se eles compartilharem o mesmo ambiente computacional. A separação dos ambientes de desenvolvimento, teste e produção é, portanto, desejável para reduzir o risco de modificações acidentais ou acessos não autorizados aos sistemas operacionais e aos dados do negócio.

7. Registros e monitoramento

Objetivo: Registrar eventos e gerar evidências.

7.1 Registro de eventos

Controle

Convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares.

Diretrizes para implementação

Convém que os registros (log) de eventos incluam, quando relevante:

a) Identificação dos usuários;
b) Atividades do sistema;
c) Datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (log-on) e saída (log-off) no sistema;
d) Identidade do dispositivo ou sua localização, quando possível, e o identificador do sistema;
e) Registro das tentativas de acesso ao sistema, aceitas e rejeitadas;
f) Registros das tentativas de acesso a outros recursos e dados, aceitas e rejeitadas;
g) Alterações na configuração do sistema;
h) Uso de privilégios;
i) Uso de aplicações e utilitários do sistema;
j) Arquivos acessados e o tipo de acesso;
k) Endereços e protocolos de rede;
l) Alarmes provocados pelo sistema de controle de acesso;
m) Ativação e desativação dos sistemas de proteção, como sistemas de antivírus e sistemas de detecção de intrusos;
n) Registros de transações executadas pelos usuários nas aplicações.

Os registros de eventos estabelecem o fundamento para os sistemas de monitoramento automáticos, os quais são capazes de gerar relatórios consolidados e alertas na segurança do sistema.

Informações adicionais

Os registros (log) de eventos podem conter dados confidenciais e informações de identificação pessoal. Convém que medidas apropriadas de proteção de privacidade sejam tomadas.

Quando possível, convém que os administradores de sistemas não tenham permissões de exclusão ou desativação dos registros (log0 de suas próprias atividades.

7.2 Instalação de software nos sistemas operacionais

Controle

Convém que procedimentos para controlar a instalação de software em sistemas operacionais sejam implementados.

Diretrizes para implementação

Convém que as seguintes diretrizes sejam consideradas para controlar as mudanças de software em sistemas operacionais:

a) Convém que as atualizações do software operacional, aplicativos e bibliotecas de programas sejam executadas por administradores treinados e com autorização gerencial apropriada;
b) Convém que os sistemas operacionais somente contenham código executável e aprovado, e não contenham código em desenvolvimento ou compiladores;
c) Convém que sistemas operacionais e aplicativos somente sejam implementados após testes extensivos e bem-sucedidos: é recomendável que os testes incluam sobre uso, segurança, efeitos sobre outros sistemas, como também sobre uso amigável, e sejam realizados em sistemas separados; convém que seja assegurado que todas as bibliotecas de código-fonte dos programas correspondentes tenham sido atualizadas;
d) Convém que um sistemas de controle de configuração seja utilizado para manter o controle da implementação do software, assim como da documentação do sistema;
e) Convém que uma estratégia de retorno às condições anteriores seja disponibilizada antes que mudanças sejam implementadas no sistema;

f) Convém que um registro de auditoria seja mantido para todas as atualizações das bibliotecas dos programas operacionais;
g) Convém que versões anteriores dos softwares aplicativos sejam mantidas como medida de contingência;
h) Convém que versões antigas dos softwares arquivadas, junto com todas as informações e parâmetros requeridos, procedimentos, detalhes de configurações, e software de suporte durante um prazo igual ao prazo de retenção dos dados.

É recomendável que software adquirido de fornecedores e utilizado em sistemas operacionais seja mantida em um nível apoiado pelo fornecedor. Ao transcorrer o tempo, fornecedores de software cessam o apoio às versões antigas do software. É recomendado que a organização considere os riscos associados à dependência de software sem suporte.

Convém que qualquer decisão de atualização para uma nova versão considere os requisitos do negócio para a mudança, e da segurança associada, por exemplo, à introdução de uma nova funcionalidade de segurança da informação ou à quantidade e à gravidade dos problemas de segurança associados a esta versão. Convém que os pacotes de correções de software sejam aplicados quando puderem remover ou reduzir as vulnerabilidades de segurança da informação.

É recomendado que acessos físicos e lógicos sejam concedidos a fornecedores, somente quando necessário, com a finalidade de suporte e com aprovação gerencial. Convém que as atividades do fornecedor sejam monitoradas.

Software para computadores podem depender de outros softwares e módulos fornecidos externamente, os quais convém que sejam monitorados e controlados para evitar mudanças não autorizadas, que podem introduzir fragilidades na segurança.

7.3 Considerações quanto à auditoria de sistemas da informação

Objetivo: Minimizar o impacto das atividades de auditoria nos sistemas operacionais.

7.3.1 Controles de auditoria de sistemas de informação

Controle

Convém que as atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio.

Diretrizes para implementação

Convém que as seguintes diretrizes sejam observadas:

a) Convém que os requisitos de auditoria para acesso aos sistemas e dados sejam acordados com o nível apropriado da gerência;
b) Convém que o escopo dos testes técnicos da auditoria seja acordado e controlado;
c) Convém que os testes de auditoria sejam limitados ao acesso somente para leitura de software e dados;
d) Convém que os outros acessos diferentes de apenas leitura sejam permitidos somente através de cópias isoladas dos arquivos do sistema, as quais recomenda-se que sejam apagadas ao final da auditoria, ou dada proteção apropriada quando existir uma obrigação para guardar tais arquivos como requisitos da documentação da auditoria;
e) Convém que os requisitos para processamento adicional ou especial sejam identificados e acordados;
f) Convém que os testes de auditoria que possam afetar a disponibilidade do sistema sejam realizados fora do horário de trabalho;
g) Convém que todo o acesso seja monitorado de forma a produzir uma trilha de referência.

8. Relacionamento na cadeia de suprimento

8.1 Segurança da informação na cadeia de suprimento

Objetivo: Garantir a proteção dos ativos da organização que são acessados pelos fornecedores.

8.1.1 Política de segurança da informação no relacionamento com os fornecedores.

Controle

Convém que os requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização sejam acordados com o fornecedor e documentados.

Diretrizes para implementação

Convém que a organização identifique e exija os controles de segurança da informação para tratar, especificamente, do acesso do fornecedor às informações da organização, através de uma política. Convém que estes controles considerem os procedimentos e processos a serem implementados pela organização, bem como aqueles processos e procedimentos que a organização requeira do fornecedor a sua implementação, incluindo:

a) Identificação e documentação dos tipos de fornecedores, por exemplo, serviços de TI, utilidades, serviços financeiros, componentes de infraestrutura de TI, aos quais a organização permitirá acessar suas informações;
b) Um processo padronizado e o ciclo de vida para gerenciar as relações com o fornecedor;
c) Definição dos tipos de acesso à informação que diferentes tipos de fornecedores terão permissão, o monitoramento e o controle do acesso;
d) Requisitos mínimos de segurança da informação para cada tipo de acesso e tipo de informação, para servir como base para acordos individuais com o fornecedor, baseados nos perfis de risco, requisitos e necessidades de negócio;
e) Procedimentos e processos para monitorar a aderência dos requisitos de segurança da informação estabelecidos para cada tipo de acesso e tipo de fornecedor, incluindo análise crítica da parte externa e validação do produto;
f) Completeza e exatidão dos controles para assegurar a integridade da informação ou o processamento da informação provido pelas partes;
g) Tipos de obrigações aplicáveis aos fornecedores para proteger as informações da organização;

h) Tratamentos de incidentes e contingências associados ao acesso do fornecedor, incluindo responsabilidades, tanto da organização como dos fornecedores;
i) Resiliência e, quando necessário, acordos de contingência e recuperação para assegurar a disponibilidade da informação ou o processamento da informação fornecido pelas partes;
j) Treinamento de conscientização para o pessoal da organização envolvido com aquisição, relativo aos procedimentos, processos e políticas aplicáveis;
k) Treinamento de conscientização para o pessoal da organização que interage com o pessoal do fornecedor, relativo às regras apropriadas de interação e comportamento baseados no tipo do fornecedor e no nível de acesso do fornecedor às informações e sistemas da organização;
l) Condições sob as quais os controles e requisitos de segurança da informação serão documentados em um acordo, assinado por ambas as partes;
m) O gerenciamento da transição necessária da informação, dos recursos de processamento da informação e de qualquer coisa que necessite ser transferida, e a garantia de que a segurança da informação esteja mantida ao longo de todo o período de transição.

Informações adicionais

As informações podem ser colocadas em risco por fornecedores com a gestão da segurança da informação inadequada. Convém que controles sejam identificados e aplicados para administrar os acessos dos fornecedores aos recursos de processamento da informação. Por exemplo, se existir uma necessidade especial de confidencialidade da informação, acordos de não divulgação podem ser utilizados. Outro exemplo são os riscos de proteção dos dados quando os acordos com fornecedores envolvem a transferência ou acesso à informação além das fronteiras. A organização precisa estar ciente de que as responsabilidades contratuais e legais para proteger a informação permanecem com a organização.

8.1.2. Identificando segurança da informação nos acordos com fornecedores

Controle

Convém que todos os requisitos de segurança da informação relevantes sejam estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar ou prover componentes de infraestrutura de TI para as informações da organização.

Diretrizes para implementação

Convém que os acordos com fornecedores sejam estabelecidos e documentados para assegurar que não existam desentendimentos entre a organização e o fornecedor, com relação à obrigação de ambas as partes com o cumprimento dos requisitos de segurança da informação relevantes.

Convém que os seguintes termos sejam considerados para inclusão nos acordos, visando atender aos requisitos da segurança da informação identificados:

a) Descrição da informação a ser fornecida ou acessada e os métodos de acesso à informação;
b) Classificação da informação de acordo com o esquema de classificação da organização; quando necessário, mapeamento do esquema de classificação da organização com o esquema de classificação do fornecedor;
c) Requisitos regulatórios e legais, incluindo a proteção de dados, os direitos de propriedade intelectual e os direitos autorais, e uma descrição de como isto será assegurado que os fornecedores cumprirão;
d) Obrigação de cada parte contratual para implementar o conjunto de controles acordados, incluindo o controle de acesso, a análise crítica do desempenho, o monitoramento, o reporte e a auditoria;
e) Regras de uso aceitável da informação, incluindo o uso inaceitável, se necessário;
f) Uma lista explícita do pessoal do fornecedor autorizado a cessar ou receber as informações da organização ou as condições e procedimentos para autorização e remoção do pessoal do fornecedor para acessar ou receber as informações da organização;
g) Políticas de segurança da informação relevantes para o contrato específico;

h) Procedimentos e requisitos de gestão de incidentes (especialmente para notificação e colaboração durante a correção de um incidente);
i) Requisitos de treinamento e conscientização para procedimentos específicos e requisitos de segurança da informação, por exemplo, resposta a incidentes, procedimentos de autorização;
j) Regulamentações relevantes para subcontratação, incluindo os controles que precisam ser implementados;
k) Acordos relevantes com parceiros, incluindo um contato pessoal para as questões de segurança da informação;
l) Requisitos de seleção, se necessário, para o pessoal do fornecedor, incluindo responsabilidades por realizar a verificação e procedimentos de notificação, caso a verificação não tenha sido concluída ou se os resultados apresentados causarem dúvidas ou preocupações;
m) Direito de auditar os processos do fornecedor e os controles relacionados ao acordo;
n) Processos para resolução de defeitos e de conflitos;
o) Obrigações do fornecedor para, periodicamente, apresentar um relatório independente da eficácia dos controles e um acordo das correções em tempo hábil, das questões relevantes apresentadas no relatório;
p) Obrigações do fornecedor de cumprir com os requisitos de segurança da informação da organização.

Informações adicionais

Os acordos podem variar consideravelmente para diferentes organizações e entre diferentes tipos de fornecedores. Por este motivo, convém tomar cuidados para incluir todos os requisitos e riscos de segurança da informação relevantes. Acordos com fornecedores podem também envolver outras partes (por exemplo, subfornecedores).

Convém que sejam considerados nos acordos os procedimentos para continuidade nos casos em que o fornecedor se torne incapaz de fornecer seus produtos ou serviços, para evitar qualquer atraso nos acordos de substituição de produtos ou serviços.

9. Gestão de incidentes de segurança da informação

9.1 Gestão de incidentes de segurança da informação e melhorias

Objetivo: Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre a fragilidade e eventos de segurança da informação.

9.1.1 Responsabilidades e procedimentos

Controle

Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação.

Diretrizes para implementação

Convém que as seguintes diretrizes para o gerenciamento de responsabilidade e procedimentos com relação à gestão de incidentes de segurança da informação sejam consideradas:

a) Convém que responsabilidades pelo gerenciamento sejam estabelecidas para assegurar que os seguintes procedimentos sejam desenvolvidos e comunicados, adequadamente, dentro da organização:
   1) Procedimentos para preparação e planejamento a resposta a incidente;
   2) Procedimento para monitoramento, detecção, análise e notificação de incidentes e eventos de segurança da informação;
   3) Procedimentos para registros das atividades de gerenciamento de incidentes;
   4) Procedimentos para manuseio de evidências forenses;
   5) Procedimentos para avaliação e decisão dos eventos de segurança da informação e avaliação de fragilidades de segurança da informação;
   6) Procedimentos para resposta, incluindo aquelas relativas à escalação, recuperação controlada de um incidente e comunicação as pessoas ou organizações, internas e externas;

b) Convém que procedimentos estabelecidos assegurem que:
    1) Pessoal competente trate as questões relativas a incidentes de segurança dentro da organização;
    2) Um ponto de contato para notificação e detecção de incidentes de segurança esteja implementado;
    3) Contatos apropriados sejam mantidos com autoridades, grupos de interesses externos ou fóruns que tratem de questões relativas a incidentes de segurança da informação;
c) Convém que procedimentos de notificação incluam:
    1) Preparação de formulários de notificação de evento de segurança da informação para apoiar as ações de notificações e ajudar a pessoa que está notificando, lembrando de todas as ações necessárias no caso de um evento de segurança da informação;
    2) O procedimento a ser realizado no caso de um evento de segurança de informação, por exemplo, relatar todos os detalhes imediatamente, como tipo de não conformidade ou violação, ocorrências de mau funcionamento, mensagens na tela; e imediatamente notificar ao ponto de contato, tomando apenas ações coordenadas;
    3) Referência a um processo disciplinar formal estabelecido para tratar com funcionários que cometam violações de segurança da informação;
    4) Processo de realimentação adequado para assegurar que aquelas pessoas que notificaram um evento de segurança da informação sejam informadas de os resultados após o assunto ter sido tratado e encerrado.

Convém que os objetivos para a gestão de incidentes de segurança da informação sejam acordados com a direção e garantam que as pessoas responsáveis pela gestão dos incidentes de segurança da informação entendem as prioridades da organização para tratar com os incidentes de segurança da informação.

Informações adicionais

Incidentes de segurança da informação podem transcender os limites organizacionais e nacionais. Para responder a tais incidentes, existe uma crescente necessidade de coordenar resposta e compartilhar informação sobre esses incidentes com organizações externas, quando apropriado.

9.1.2 Notificação de eventos de segurança de informação

Controle

Convém que os eventos de segurança da informação sejam relatados por meio dos canais de gestão, o mais rápido possível.

Diretrizes para implementação

Convém que todos os funcionários e partes externas sejam alertados sobre sua responsabilidade de notificar qualquer evento de segurança da informação o mais rapidamente possível. Convém que eles também estejam cientes do procedimento para notificar os eventos de segurança da informação e do ponto de contato, ao qual os eventos devem ser notificados.

Situações a serem consideradas para notificar um evento de segurança da informação incluem:

a) Controle de segurança ineficaz;
b) Violação da disponibilidade, confidencialidade e integridade da informação;
c) Erros humanos;
d) Não conformidade com políticas ou diretrizes;
e) Violações de procedimentos de segurança física;
f) Mudanças descontroladas de sistemas;
g) Mau funcionamento de software ou hardware;
h) Violação de acesso;

Informações adicionais

Mau funcionamento ou outro comportamento anómalo do sistema pode ser um indicador de um ataque de segurança ou violação na segurança atual e, portanto, convém que sempre seja reportado como um evento de segurança da informação.

9.1.3 Notificando fragilidades de segurança da informação

Controle

Convém que os funcionários e partes externas que usam os sistemas e serviços de informação da organização sejam instruídos a notificar e registrar quaisquer

fragilidades de segurança de informação observada ou suspeita, nos sistemas ou serviços.

Diretrizes para implementação

Convém que todos os funcionários e partes externas notifiquem essas questões para o ponto de contato, o mais rápido possível, de forma a prevenir incidentes de segurança da informação. O mecanismo de notificação deve ser fácil, acessível e disponível, sempre que possível.

Informações adicionais

Convém que funcionários e fornecedores sejam avisados a não tentar provar fragilidades de segurança da informação suspeitas. Testar fraquezas pode ser interpretado como potencial mau uso do sistema e pode também causar danos ao serviço ou sistema de informação e resultar em responsabilidade legal para o indivíduo que executou o teste.

9.1.4 Avaliação e decisão dos eventos de segurança da informação

Controle

Convém que os eventos de segurança da informação sejam avaliados e seja decidido se eles são classificados como incidentes de segurança da informação.

Diretrizes para implementação

Convém que o ponto de contato avalie cada evento de segurança da informação, usando a escala acordada de classificação de incidentes e eventos de segurança da informação, para decidir se é recomendado que o evento seja classificado como um incidente de segurança da informação. A priorização e a classificação de incidentes podem ajudar a identificar o impacto e a abrangência de um incidente.

Em casos onde a organização tenha uma equipe de resposta a incidentes de segurança da informação, a avaliação e decisão podem ser encaminhadas para a equipe, para confirmação ou reavaliação.

Convém que os resultados da avaliação e decisão sejam registrados em detalhes, para o propósito de verificação e referência futura.

9.1.5 Respostas aos incidentes de segurança da informação

Controle

Convém que incidentes de segurança da informação sejam reportados de acordo com procedimentos documentados.

Diretrizes para implementação

Convém que incidentes de segurança da informação sejam reportados para um ponto de contato definido e outras pessoas relevantes da organização, ou ainda, partes externas.

Convém que a notificação inclua os seguintes itens:

a) Coleta de evidências, tão rápido quanto possível, logo após a ocorrência;
b) Condução de análise forense de segurança da informação, conforme requerido (ver 9.1.7);
c) Escalação, conforme requerido;
d) Garantia de que todas as atividades de respostas envolvidas sejam adequadamente registradas para análise futura;
e) Comunicação da existência de incidente de segurança da informação ou qualquer detalhe relevante para pessoas internas ou externas, ou organizações que precisam tomar conhecimento;
f) Tratamento com as fragilidades de segurança da informação encontradas que causem ou contribuam para o incidente;
g) Uma vez que o incidente foi tratado de forma bem-sucedida, encerrá-lo o incidente e registrá-lo formalmente;

Convém que análises pós-incidente sejam realizadas, quando necessário, para identificar a fonte do incidente.

Informações adicionais

O primeiro objetivo de resposta a incidente é “voltar ao nível de segurança normal” e então iniciar a recuperação necessária.

9.1.6 Aprendendo com os incidentes de segurança da informação

Controle

Convém que os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação sejam usados para reduzir a probabilidade ou o impacto de incidentes futuros.

Diretrizes para implementação

Convém que haja mecanismos implementados para permitir monitorar e quantificar os tipos, volumes e custos de incidentes de segurança da informação. Convém que a informação resultante da análise de incidentes de segurança da informação seja usada para identificar incidentes recorrentes ou de alto impacto.

Informações adicionais

A avaliação de incidentes de segurança da informação pode indicar a necessidade de melhoria ou controles adicionais para diminuir a frequência, dano e custo de futuras ocorrências, ou ser levada em conta no processo de análise crítica da política de segurança.

Com o devido cuidado aos aspectos de confidencialidade, estórias de incidentes atuais de segurança da informação podem ser usadas em treinamentos de conscientizações de usuários como exemplos do que pode acontecer, como responder a tais incidentes e como evita-los no futuro.

9.1.7 Coleta de evidências

Controle

Convém que a organização defina e aplique procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências.

Diretrizes para implementação

Convém que procedimentos internos sejam desenvolvidos e seguidos quando lidando com evidência, para o propósito de ação legal ou disciplinar.

Em geral, convém que esses procedimentos para evidência fornecem processos de identificação, coleta, aquisição e preservação de evidências, de acordo com

diferentes tipos de mídia, dispositivos e situação dos dispositivos, por exemplo, se estão ligados ou desligados. Convém que os procedimentos levem em conta:

a) Cadeia de custódia;
b) Segurança de evidência;
c) Segurança das pessoas;
d) Papéis e responsabilidades das pessoas envolvidas;
e) Competência do pessoal;
f) Documentação;
g) Resumo do incidente.

Convém que, onde disponível, certificação ou outros meios relevantes de qualificação de pessoal e ferramentas sejam buscados, para reforçar o valor de evidência preservada.

Evidência forense pode ir além dos limites da organização ou da jurisdição. Em tais casos, convém que seja assegurado que a organização tem direito de coletar as informações requeridas como evidência forense. Convém que os resultados de diferentes jurisdições também sejam considerados para maximizar as chances de aceitação em jurisdições relevantes.

Informações adicionais

Identificação é o processo envolvendo a busca, reconhecimento e documentação de potencial evidência. Coleta é o processo de levantamento de itens físicos que pode conter potencial evidência. Aquisição é o processo de criação de uma cópia dos dados dentro de um cenário definido. Preservação é o processo para manter e proteger a integridade e condição original da potencial evidência.

Logo quando um evento de segurança da informação é detectado, pode não ser óbvio se o evento resultará em uma ação judicial ou não. Portanto, existe o perigo que esta evidência necessária seja destruída intencionalmente ou acidentalmente antes que a gravidade do incidente seja percebida. É aconselhável envolver um advogado ou a polícia o quanto antes em qualquer ação legal e receber aconselhamento sobre e evidência requerida.

10. Aspectos da segurança da informação na gestão da continuidade do negócio

10.1 Continuidade da segurança da informação

Objetivo: Convém que a continuidade da segurança da informação seja contemplada nos sistemas de gestão da continuidade do negócio da organização.

10.1.1 Planejamento a continuidade da segurança da informação

Controle

Convém que a organização determine seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre.

Diretrizes para implementação

Convém que uma organização avalie se a continuidade da segurança da informação está contida dentro do processo de gestão da continuidade do negócio ou no processo de gestão de recuperação de desastre. Requisitos de segurança da informação podem ser determinados quando do planejamento da continuidade do negócio e da recuperação de desastre.

Na ausência de um planejamento formal de continuidade do negócio e de recuperação de desastre, convém que a gestão da segurança da informação assuma que os requisitos de segurança da informação permanecem os mesmos, em situações adversas, comparadas com as condições de operação normal. Alternativamente, uma organização pode realizar uma análise de impacto do negócio relativa aos aspectos de segurança da informação, para determinar os requisitos de segurança da informação que são aplicáveis nas situações adversas.

Informações adicionais

Para reduzir o tempo e o esforço de uma análise de impacto do negócio adicional, da segurança da informação, é recomendado capturar os aspectos da segurança da informação no gerenciamento da continuidade normal dos negócios ou na análise do impacto ao negócio no gerenciamento da recuperação de um desastre. Isto implica que os requisitos de continuidade da segurança da informação estejam

explicitamente contemplados na gestão da continuidade do negócio ou nos processos de gerenciamento da recuperação de desastre.

10.1.2 Implementando a continuidade da segurança da informação

Controle

Convém que a organização estabeleça, documente, implemente e mantenha processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa.

Diretrizes para implementação

Convém que uma organização se assegure de que:

a) Uma estrutura de gerenciamento adequada esteja implementada para mitigar e responder a um evento de interrupção, usando pessoal com a necessária autoridade, experiência e competência;
b) O pessoal de resposta a incidente com a necessária responsabilidade, autoridade e competência para gerenciar um incidente e garantir a segurança da informação esteja designado;
c) Planos documentados, procedimentos de recuperação e resposta estejam desenvolvidos e aprovados, detalhando como a organização irá gerenciar um evento de interrupção e como manterá a sua segurança da informação aprovado pela direção.

Em função dos requisitos de continuidade de segurança da informação, convém que a organização estabeleça, documente, implemente e mantenha:

a) Controles de segurança da informação dentro dos processos de recuperação de desastre ou de continuidade do negócio, procedimentos e ferramentas e sistemas de suporte;
b) Processos, procedimentos e mudança de implementação para manter os controles de segurança da informação existentes durante uma situação adversa;
c) Controles compensatórios para os controles de segurança da informação que não possam ser mantidos durante uma situação adversa.

Informações adicionais

Dentro do contexto da continuidade do negócio ou da recuperação de desastre, pode ser necessário que procedimentos e processos específicos sejam definidos. Convém que informações que sejam tratadas nestes processos e procedimentos ou em sistemas de informação dedicados para apoiá-los sejam protegidas. Desta forma, convém que a organização envolva especialistas em segurança da informação, quando do estabelecimentos, implementação e manutenção dos procedimentos e processos de recuperação de desastres ou da continuidade dos negócios.

Convém que os controles de segurança da informação a serem implementados continuem a operar durante uma condição de situação adversa. Se os controles de segurança não forem capazes de manter a informação segura, convém que outros controles sejam estabelecidos, implementados e mantidos para garantir um nível aceitável da segurança da informação.

10.1.3 Verificação, análise crítica e avaliação da continuidade da segurança da informação

Controle

Convém que a organização verifique os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles sejam válidos e eficazes em situações adversas.

Diretrizes para implementação

Mudanças organizacionais, técnicas, procedimentos e processos, quando em um contexto operacional ou de continuidade, podem conduzir a mudanças nos requisitos de continuidade da segurança da informação. Em tais casos, convém que a continuidade dos processos, procedimentos e controles para segurança da informação sejam analisados criticamente com base nesses requisitos alterados.

Convém que a organização verifique se a sua continuidade da gestão da segurança da informação através de:

a) Teste e verificação da funcionalidade dos processos, procedimentos e controles da continuidade da segurança da informação, de modo a assegurar

que o seu desempenho esteja consistente com os objetivos da continuidade da segurança da informação;

b) Teste e verificação do conhecimento e rotina para operar os procedimentos, processos e controles de continuidade da segurança da informação, de modo a assegurar que o seu desempenho esteja consistente com os objetivos da continuidade da segurança da informação;

c) Análise crítica quanto à validade e eficácia dos controles de continuidade da segurança da informação quanto aos sistemas de informação, processos de segurança da informação, procedimentos e controles ou gestão da continuidade do negócio/gestão de recuperação de desastre e soluções de mudança.

Informações adicionais

A verificação dos controles da continuidade da segurança da informação é diferente das verificações e testes da segurança da informação normal, e convém que seja realizada fora do âmbito dos testes de mudanças. Quando possível é recomendável integrar a verificação dos controles da continuidade da segurança da informação com os testes de recuperação de desastre ou da continuidade dos negócios da organização.

11. Conformidade

11.1 Conformidade com requisitos legais e contratuais

Objetivo: Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança.

11.1.1 Identificação da legislação aplicável e de requisitos contratuais

Controle

Convém que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes e o enfoque da organização para atender a esses requisitos sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização.

Diretrizes para implementação

Convém que os controles específicos e as responsabilidades individuais para atender a estes requisitos sejam definidos e documentados.

Convém que os gestores identifiquem toda a legislação aplicável à sua organização, para atender aos requisitos relativos ao seu tipo de negócio. Caso a organização realize negócios em outros países, convém que os gestores considerem a conformidade em todos esses países.

11.1.2 Direitos de propriedade intelectual

Controle

Convém que procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados aos direitos de propriedade intelectual, e sobre o uso de produtos de softwares proprietários.

Diretrizes para implementação

Convém que as seguintes diretrizes sejam consideradas para proteger qualquer material que possa ser considerado propriedade intelectual:

a) Divulgar uma política de conformidade com os direitos de propriedade intelectual que defina o uso legal de software e de informação;
b) Adquirir software somente por meio de fontes conhecidas e de reputação, para assegurar que o direito autoral não esteja sendo violado;
c) Manter conscientização das políticas para proteger os direitos de propriedade intelectual e notificar a intenção de tornar ações disciplinares contra as pessoas que violarem essas políticas;
d) Manter, de forma adequada, os registros de ativos, e identificar todos os ativos com requisitos para proteger os direitos de propriedade intelectual;
e) Manter provas e evidências da propriedade de licenças, discos-mestres, manuais, etc;
f) Implementar controles para assegurar que o número máximo de usuários permitidos, dentro da licença concedida, não esteja excedido;
g) Conduzir verificações para que somente produtos de software autorizados e licenciados sejam instalados;

h) Estabelecer uma política para a manutenção das condições adequadas de licenças;
i) Estabelecer uma política para disposição ou transferência de software para outros;
j) Cumprir termos e condições para software e informação obtidos a partir de redes públicas;
k) Não duplicar, converter para outro formato ou extrair de registros comerciais (filme, áudio) outros que não os permitidos pela lei de direito autoral;
l) Não copiar, no todo ou em partes, livros, artigos, relatórios ou outros documentos, além daqueles permitidos pela lei de direito autoral;

Informações adicionais

Direitos de propriedade intelectual incluem direitos autorais de software ou documento, direitos de projetos, marcas, patentes e licenças de código-fonte.

Produtos de softwares proprietários são normalmente fornecidos sob um contrato de licenciamento que especifica os termos e condições de licença, por exemplo, limitar o uso dos produtos em máquinas especificadas ou limitar a reprodução apenas para a criação de cópias de backup. Convém que a importância e a conscientização dos direitos de propriedade intelectual de software sejam comunicadas aos responsáveis pelo desenvolvimento de software na organização.

Requisitos legais, regulamentares e contratuais podem colocar restrições sobre a cópia de material proprietário. Em particular, eles podem exigir que apenas o material que é desenvolvido pela organização ou que está licenciado ou fornecido pelo desenvolvedor para a organização possa ser utilizado. Violação de direitos autorais pode levar à ação judicial e pode envolver multas e processos criminais.

11.1.3 Proteção de registros

Controle

Convém que registros sejam protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.

Diretrizes para implementação

Convém que, quando a organização decidir proteger os registros específicos, a classificação correspondente seja baseada no esquema de classificação da organização. Convém que os registros sejam categorizados em tipos de registros, como registros contábeis, registros de base de dados, registros de transações, registros de auditoria e procedimentos operacionais, cada qual com detalhes do período de retenção e do tipo de mídia de armazenamento, como, por exemplo, papel, microficha, meio magnético ou ótico. Convém que quaisquer chaves de criptografia relacionadas com arquivos cifrados ou assinaturas digitais sejam armazenadas para permitir a decifração de registros pelo período de tempo que os registros são mantidos.

Convém que cuidados sejam tomados a respeito da possibilidade de deterioração das mídias usadas no armazenamento dos registros. Convém que os procedimentos de armazenamento e manuseio sejam implementados de acordo com as recomendações dos fabricantes.

Onde mídias eletrônicas armazenadas forem escolhidas, convém que sejam incluídos procedimentos para assegurar a capacidade de acesso aos dados (leitura tanto nas mídias como no formato utilizado) durante o período de retenção, para proteger contra perdas ocasionadas pelas futuras mudanças na tecnologia.

Convém que sistemas de armazenamento e manuseio sejam escolhidos de modo que o dado solicitado possa ser recuperado de forma aceitável, dependendo dos requisitos a serem atendidos.

Convém que o sistema de armazenamento e manuseio assegure a clara identificação dos registros e dos seus períodos de retenção, conforme definido pela legislação nacional ou regional ou por regulamentações, se aplicável. Convém que este sistema permita a destruição apropriada dos registros após esse período, caso não sejam mais necessários à organização.

Para atender aos objetivos de proteção dos registros, convém que os seguintes passos sejam tomados pela organização:

a) Emitir diretrizes gerais para retenção, armazenamento, tratamento e disposição de registros e informações;

b) Elaborar uma programação para retenção, identificação os registros essenciais e o período recomendado para que cada um seja mantido;
c) Manter um inventário das fontes de informações-chave.

Informações adicionais

Alguns registros podem precisar ser retidos de forma segura para atender a requisitos estatutários, regulamentares ou contratuais, bem como para apoiar as atividades essenciais do negócio. Exemplos incluem os registros, que podem ser exigidos como prova de que uma organização opera dentro de normas estatutárias ou regulamentares, para assegurar a defesa contra potencial ação civil ou criminal, ou para confirmar a situação financeira de uma organização perante os acionistas, partes externas e auditores. A legislação nacional ou a regulamentação pode definir conteúdo de dados e o período de tempo para a retenção de informações.

11.1.4 Proteção e privacidade de informações de identificação pessoal

Controle

Convém que a privacidade e a proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.

Diretrizes para implementação

Convém que uma política de dados da organização para proteção e privacidade da informação de identificação pessoal seja desenvolvida e implementada. Esta política desse comunicada a todas as pessoas envolvidas no processamento de informação de identificação pessoal.

A conformidade com esta política e todas as regulamentações e legislação relevantes, relativas a proteção da privacidade das pessoas e da proteção da informação de identificação pessoal, requer um controle e uma estrutura de gerenciamento apropriada. Quase sempre isto é melhor conseguido indicando uma pessoa responsável, como, por exemplo, um privacy officer, que tem a função de fornecer orientações aos gestores, usuários e provedores de serviços sobre as suas responsabilidades individuais e procedimentos específicos que devem ser seguidos. Convém que a responsabilidade pelo manuseio da informação de identificação

pessoal e a garantia da conscientização sobre os princípios da privacidade, sejam tratadas de acordo com as regulamentações e legislações pertinentes. Convém que técnicas apropriadas e medidas da organização para proteger a informação de identificação pessoal sejam implementadas.

11.1.5 Regulamentação de controle de criptografia

Controle

Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.

Diretrizes para implementação

Convém que os seguintes itens sejam considerados para conformidade com leis, acordos e regulamentações relevantes:

a) Restrições à importação/exportação de hardware e software de computador para execução de funções criptográficas;
b) Restrições à importação e/ou exportação de hardware e software de computador que foi projetado para ter funções criptográficas embutidas;
c) Restrições no uso de criptografia;
d) Métodos mandatários ou discricionários de acesso pelas autoridade dos países à informação cifrada por hardware ou software para fornecer confidencialidade ao conteúdo.

Convém que a assessoria jurídica garanta a conformidade com as legislações e regulamentações vigentes. Convém que seja obtida assessoria jurídica antes de se transferir informações cifradas ou controles de criptografia para além das fronteiras jurisdicionais.

11.2 Análise crítica da segurança da informação

Objetivo: Assegurar que a segurança da informação esteja implementada e operada de acordo com as políticas e procedimentos da organização.

11.2.1 Análise crítica independente da segurança da informação

Controle

Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, objetivo dos controles, políticas, processos e procedimentos para a segurança da informação) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas.

Diretrizes para implementação

Convém que a análise crítica independente seja iniciada pela direção. Tal análise crítica independente é necessária para assegurar a contínua pertinência, adequação e eficácia do enfoque da organização para gerenciar a segurança da informação. Convém que a análise crítica inclua a avaliação de oportunidades para melhoria e a necessidade de mudanças para o enfoque da segurança da informação, incluindo a política e os objetivos de controle.

Convém que análise crítica seja executada por pessoas independentes da área avaliada, como, por exemplo, uma função de auditoria interna, um gerente independente ou uma organização externa especializada em tais análises críticas. Convém que as pessoas que realizem estas análises críticas possuam habilidade e experiência apropriadas.

Convém que os resultados da análise crítica independente sejam registrados e relatados para a direção que iniciou a análise crítica e que estes registros sejam mantidos.

Se a análise crítica independente identificar que o enfoque da organização e a implementação para gerenciar a segurança da informação são inadequados ou não conforme com as orientações estabelecidas pela segurança da informação, convém que, nas políticas de segurança da informação, a direção considera a tomada de ações corretivas.

11.2.2 Conformidade com as políticas e procedimentos de segurança da informação

Controle

Convém que os gestores analisem criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das áreas de responsabilidade, com as normas políticas de segurança e quaisquer outros requisitos de segurança da informação.

Diretrizes para implementação

Convém que os gestores identifiquem como analisar criticamente se os requisitos da segurança da informação estabelecidos nas políticas, procedimentos, normas e outras regulamentações aplicáveis estão sendo atendidos. Ferramentas de notificação e medições automáticas podem ser consideradas para alcançar uma análise crítica regular de forma eficaz.

Se qualquer não conformidade for encontrada com um resultado da análise crítica, convém que os gestores:

a) Identifiquem as causas da não conformidade;
b) Avaliem a necessidade de ações para atender à conformidade;
c) Implementem ação corretiva apropriada;
d) Analisem criticamente a ação corretiva tomada, para verificar a sua eficácia e identificar quaisquer deficiências ou fragilidades.

Convém que os resultados das análises críticas e das ações corretivas realizadas sejam registrados e esses registros sejam mantidos. Convém que os gestores relatem os resultados para as pessoas que estão realizando a análise crítica independente, quando a análise crítica independente, quando a análise crítica independente for realizada na área de sua responsabilidade.

11.2.3 Análise crítica de conformidade técnica

Controle

Convém que os sistemas de informação sejam analisados criticamente, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da organização.

Diretrizes para implementação

Convém que a verificação de conformidade técnica seja analisada criticamente, preferencialmente com o apoio de uma ferramenta automática, a qual gera relatórios técnicos para a interpretação dos especialistas técnicos. Alternativamente, análises críticas manuais (auxiliadas por ferramentas de software apropriadas, se necessário) podem ser realizadas por um engenheiro de sistemas experiente.

Se forem usados testes de invasão ou avaliações de vulnerabilidades, convém que sejam tomadas precauções, uma vez que tais atividades podem conduzir a um comprometimento da segurança do sistema. Convém que tais testes sejam planejados, documentados e repetidos.

Convém que qualquer verificação de conformidade técnica somente seja executada por pessoas autorizadas e competentes, ou sob a supervisão de tais pessoas.

Informações adicionais

A verificação da conformidade técnica envolve a análise dos sistemas operacionais para garantir que controles de hardware e software foram corretamente implementados. Este tipo de análise crítica de conformidade exige conhecimentos técnicos especializados.

Análise de conformidade também engloba, por exemplo, testes de invasão e avaliações de vulnerabilidades, que podem ser realizadas por peritos independentes, contratados especificamente para esta finalidade. Isto pode ser útil na detecção de vulnerabilidades no sistema e na verificação do quanto os controles são eficientes na prevenção de acessos não autorizados devido a estas vulnerabilidades.

Os testes de invasão e avaliação de vulnerabilidades fornecem um snapshot de um sistema em um estado específico para um tempo específico. O snapshot está limitado àquelas partes do sistema realmente testadas durante a etapa da invasão. O teste de invasão e as avaliações de vulnerabilidades não são um substituto da avalição de risco.

ANEXO B – TERMO DE CONFIDENCIALIDADE

TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Pelo presente instrumento e na melhor forma de direito, de um lado EMERSON TURIM CARVALHO, GRADUANDO EM SISTEMAS DE INFORMAÇÃO, BRASILEIRO, SOLTEIRO, Estudante da UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ - UENP CAMPUS LUÍS MENEGHEL, e de outro (nome completo), BRASILEIRO (qualificação de empresa), residente e domiciliado na (ENDEREÇO)

Considerando que para bom e fiel desempenho das atividades da UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ, faz-se necessária a disponibilização de informações técnicas e confidenciais, incluídas as de projeto, especificação, funcionamento, organização e desempenho da referida empresa para uso em seu Trabalho de Conclusão de Curso (TCC).

CLÁUSULA PRIMEIRA – DO OBJETO

O objeto do presente termo é a proteção das INFORMAÇÕES CONFIDENCIAIS disponibilizadas pelo Trabalho de Conclusão de Curso (TCC), em razão da relação de confiabilidade desenvolvida pelas partes.

CLÁUSULA SEGUNDA – DAS DEFINIÇÕES

Todas as informações técnicas obtidas através da relação de confiabilidade com o graduando Emerson Turim Carvalho relacionadas a projeto, especificação,

funcionamento, organização ou desempenho da referida empresa serão tidas como CONFIDENCIAIS E SIGILOSAS.

PARÁGRAFO ÚNICO: Serão consideradas para efeito deste termo toda e qualquer informação, patenteada ou não, de natureza técnica, operacional, comercial, jurídica, Know-how, invenções, processos, fórmulas e *designs*, patenteáveis ou não, planos de negócios (*business plans*), métodos de contabilidade, técnicas e experiências acumuladas, documentos, contratos, papéis, estudos, pareceres e pesquisas a que o funcionário tenha acesso:

a) Por qualquer meio físico (*v.g.* documentos expressos, manuscritos, fac-símile, mensagens eletrônicas (e-mail), fotografias etc.;
b) Por qualquer forma registrada em mídia eletrônica (fitas, disquetes etc.);
c) Oralmente.

CLÁUSULA TERCEIRA - DA RESPONSABILIDADE

O graduando Emerson Turim Carvalho compromete-se a manter sigilo não utilizando tais informações confidenciais em proveito próprio ou alheio.

PARÁGRAFO PRIMEIRO: As informações confidenciais confiadas ao graduando Emerson Turim Carvalho somente poderão ser abertas a terceiro mediante consentimento prévio do responsável pelo setor de TI da Empresa.

CLÁUSULA QUARTA – DAS INFORMAÇÕES NÃO CONFIDENICAIS

Não configuram informações confidenciais aquelas:

a) Já disponíveis ao público em geral sem culpa do funcionário;
b) Que já eram do conhecimento do funcionário antes de sua do ingresso na empresa e que não foram adquiridas direta ou indiretamente da empresa;
c) Que não são mais tratadas como confidenciais pela empresa.

PARÁGRAFO PRIMEIRO: O GRADUANDO fica desde já proibido de produzir cópias ou *backup*, por qualquer meio ou forma, de qualquer dos documentos a ele fornecidos ou documentos que tenham chegado ao seu conhecimento em virtude da relação de emprego.

CLÁUSULA QUINTA - DAS DISPOSIÇÕES ESPECIAIS

Ao assinar o presente instrumento, o graduando manifesta sua concordância no seguinte sentido:

I) Todas as condições, termos e obrigações ora constituídas serão regidas pelo presente Termo, bem como pela legislação e regulamentação brasileiras pertinentes;
II) O presente termo só poderá ser alterado mediante a celebração de novo termo, posterior e aditivo;
III) As alterações do número, natureza e quantidade das informações confidenciais disponibilizadas pela empresa não descaracterizarão ou reduzirão o compromisso ou as obrigações pactuadas neste Termo de Confidencialidade e Sigilo, que permanecerá válido e com todos os seus efeitos legais em qualquer das situações tipificadas neste instrumento;
IV) O acréscimo, complementação, substituição ou esclarecimento de qualquer das informações confidenciais disponibilizadas para o funcionário, em razão do presente objetivo, serão incorporadas a este Termo, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as

informações iniciais disponibilizadas, não sendo necessário, nessas hipóteses, a assinatura ou formalização de Termo aditivo.

CLÁUSULA SEXTA – DA VALIDADE

Este termo tornar-se-á válido a partir da data de sua efetiva assinatura pelas partes.

Parágrafo Único: As disposições deste instrumento devem, contudo, ser aplicadas retroativamente a qualquer informação confidencial que possa já ter sido divulgada, antes da data de sua assinatura.

CLÁUSULA SÉTIMA – DAS PENALIDADES

A não-observância de quaisquer das disposições de confidencialidade estabelecidas neste instrumento, sujeitará ao GRADUANDO infrator, como também ao agente causador ou facilitador, por ação ou omissão de qualquer um daqueles relacionados neste termo, ao pagamento, ou recomposição, de todas as perdas e danos comprovadas pela empresa, bem como as de responsabilidade civil e criminal respectivas, as quais serão apuradas em regul
ar processo judicial ou administrativo.

CLÁUSULA OITAVA – DO FORO

Por força do disposto no art. 109, inciso I, da Constituição Federal, o foro competente para dirimir quaisquer dúvidas ou controvérsias resultantes da execução deste Instrumento de Contrato é o da Justiça Federal, Subseção Judiciária de Lavras, Estado de Minas Gerais, caso não sejam solucionadas administrativamente.

E por estarem assim justas e acordadas, as Partes assinam o presente Termo em 02 (duas) vias de igual teor e forma, na presença de duas testemunhas.

Andirá, maio de 2017.

_____

Pelo Graduando em Sistemas de Informação

Emerso Turim Carvalho

_____

Nome do funcionário

TESTEMUNHAS:

Nome: _____

CPF:

Nome: _____

CPF: