UNIVERSIDADE DE CAXIAS DO SUL
ÁREA DO CONHECIMENTO DE CIÊNCIAS EXATAS E ENGENHARIAS

ALEXANDRE TAGLIARI

ANÁLISE DA APLICAÇÃO E AVALIAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EM *CALL CENTER*: UM ESTUDO DE CASO

CAXIAS DO SUL
2018

ALEXANDRE TAGLIARI

ANÁLISE DA APLICAÇÃO E AVALIAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EM *CALL CENTER*: UM ESTUDO DE CASO

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação da Universidade de Caxias do Sul.

Orientadora: Profa. Dra. Maria de Fátima Webber do Prado Lima

CAXIAS DO SUL

2018

ALEXANDRE TAGLIARI

ANÁLISE DA APLICAÇÃO E AVALIAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EM *CALL CENTER*: UM ESTUDO DE CASO

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação da Universidade de Caxias do Sul.

Aprovado em ___/___/___

Banca Examinadora

_____

Profa. Dra. Maria de Fátima Webber do Prado Lima

Universidade de Caxias do Sul – UCS

_____

Prof. Me. Giovanni Ely Rocco

Universidade de Caxias do Sul – UCS

_____

Profa. Ma. Iraci Cristina da Silveira

Universidade de Caxias do Sul – UCS

Dedico este trabalho à minha família e aos amigos; meus sinceros agradecimentos e gratidão.

AGRADECIMENTOS

Primeiramente, agradeço a Deus por ter me dado a oportunidade de chegar até esta etapa da minha vida, e que, em todos os momentos de fraqueza, deu-me forças para seguir em frente.

Agradeço aos meus pais que, acima de tudo, sempre me apoiaram e me deram todas as condições para que fosse possível eu ter oportunidades ímpares na minha vida, pois foram os pilares que deram suporte e sustento aos sonhos que estou realizando.

Agradeço à minha irmã, Bárbara, que, mesmo distante fisicamente, esteve sempre presente comigo, me apoiando, me ajudando, me dando forças e sendo o meu maior incentivo de como ser enquanto pessoa.

Agradeço a meu irmão, Felipe, por me mostrar que a vida é feita de altos e baixos, e que nos momentos em que estive nos baixos, me tirou destes e me incentivou a tirar o melhor de mim e mostrou que sou melhor de uma maneira que nem eu mesmo acreditava.

Agradeço à minha orientadora, Profa. Dra. Maria de Fátima, que me proporcionou, com todo seu conhecimento, seja durante as conversas nos corredores, seja nas diversas aulas, as correções do trabalho desenvolvido e o devido suporte para apresentar da melhor forma possível um trabalho digno de um estudante bacharel em Sistemas de Informação.

“Se você tivesse uma chance, ou uma oportunidade,

para ter tudo o que você sempre quis, um momento,

Você pegaria, ou deixaria escapar?”

Eminem

RESUMO

Nos dias atuais, as informações são consideradas ativos e um diferencial competitivo. As organizações não estão preparadas para lidar com os riscos que seus ativos possam sofrer. A solução para a redução de fraudes nas organizações é a implementação de uma política de segurança de informação. A política de segurança da informação é um mecanismo de segurança essencial para as organizações. A política tem por objetivo garantir a continuidade do negócio por meio da redução dos riscos pelos quais as organizações podem vir a sofrer. Por meio de um estudo de caso em um *call center*, com foco na operação, setor que lida com informações pessoais de clientes, o presente trabalho tem como intuito auxiliar na implementação de diretrizes da segurança da informação e medição de eficiência dos controles implementados. Abordam-se neste trabalho a análise de risco, o método de avaliação da política de informação e a aplicabilidade do uso das normas da série ABNT/NBR 27000 para a organização em questão.

Palavras-chave: Segurança da informação. Organização. *Call center*. Políticas de segurança.

ABSTRACT

Nowadays, information is considered asset and a competitive differential. Organizations are not prepared to deal with the risks their assets may suffer. The solution to reduce fraud in the organization is the implementation of an information security policy. Information security policy is an essential security mechanism for organizations. The policy aims to ensure business continuity by reducing the risk that organizations may suffer. Through a case study in a call center, focused on the operation, which deals with personal information of clients, the present coursework aims to help in the implementation of information security guidelines and efficiency measurement of the implemented controls. This paper discusses the risk analysis, the information policy evaluation method and the applicability of the ABNT / NBR 27000 series standards for the organization in question.

Keywords: Information security. Organization. *Call center*. Security policies.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CRM	*Customer Relationship Management*
HD	*Hard Disc*
ID	Identificação de Usuário
GRSI	Gestão de Riscos de Segurança da Informação
IEC	*International Eletrotechnical Comission*
ISO	*International Organization for Standardization*
NBR	Norma Brasileira
NIST-SP	*National Institute of Standards and Technology - Special Publication*
PDCA	*Plan – Do – Check – Act*
SGSI	Sistema de Gestão da Segurança da Informação
TI	Tecnologia da Informação
USB	*Universal Serial Bus*

SUMÁRIO

1 INTRODUÇÃO

Atualmente, as empresas investem em novas tecnologias para garantir a segurança da informação, porém esquecem de treinar seus colaboradores quando se trata de engenharia social. A engenharia social age de forma a persuadir e influenciar as pessoas a revelarem informações, ou liberar acessos não autorizados à rede da organização.

Segundo Canepa (2013), o problema mais comum na maioria das organizações é a questão da engenharia social. As empresas não estão devidamente orientadas para evitar que seus colaboradores copiem dados confidenciais. Canepa ainda aponta um levantamento da Symantec, organização especializada em segurança da informação, a qual identificou que, no Brasil, 62% dos colaboradores levam consigo informações confidenciais da empresa em que trabalhavam no momento em que trocam de emprego. O principal motivo pelo qual os entrevistados admitiram quebrar o sigilo da empresa era o de usar os dados e informações em uma nova organização. Mesmo sabendo dos riscos que correm em relação ao furto de informações, apenas 33% das organizações possuem diretrizes de como agir quando as políticas internas de sigilo não são seguidas.

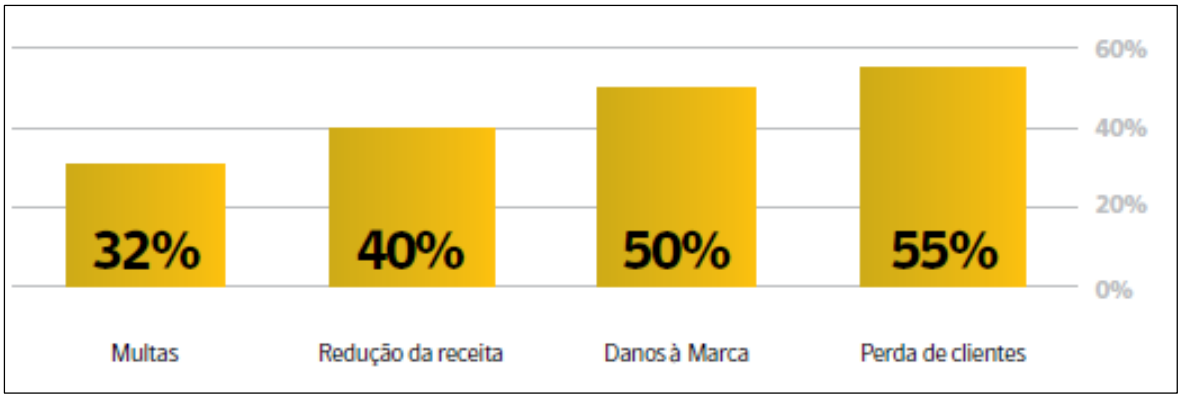
A redação da revista *CIO* (2017) divulgou avaliações do Gartner, nas quais é apresentado que: a) até 2020, 60% das empresas sofrerão falhas em seus principais serviços devido à incapacidade das equipes de segurança; b) até 2020, 60% dos orçamentos das organizações serão voltados à segurança da informação, com o objetivo de detectar e dar respostas mais rápidas às ameaças; c) até 2018, 25% do tráfego de dados corporativos partirá diretamente de dispositivos móveis para a nuvem, ignorando os controles de segurança da empresa; d) em 2018, mais de 50% dos fabricantes de dispositivos IoT (*Internet of Things*) não serão capazes de conter as ameaças devido ao fraco método de autenticação.

Rohr e Simões Gomes (2016) relataram que dois vazamentos expuseram na *Internet* milhões de gravações de um *call center* que continham informações como RG e CPF. Os mesmos autores relataram que, também em 2016, outra ação por parte de *hackers* expôs 9,5 milhões de arquivos de áudio, supostamente copiados de um *call center.*

Pesquisa desenvolvida pela empresa Symantec sobre custo e gestão da informação, realizada no ano de 2012, na América Latina, informou que as organizações estão gerando dados cada vez mais rápido em repositórios como *data centers, desktops, laptops* e *smartphones*. Segundo os entrevistados, o valor da informação corresponde a 50% do valor

de mercado das organizações e, para eles, a perda dessas informações resultaria em perda de clientes (55%), danos à marca (50%), redução na receita (40%) e/ou multas (32%) (Figura 1).

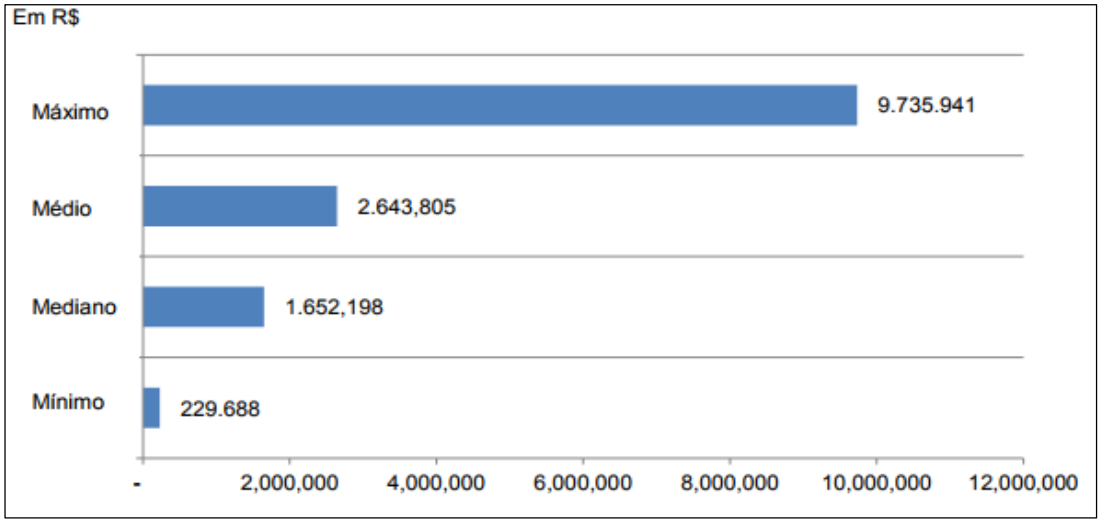
Figura 1 - Consequências da perda de informações de negócios



Fonte: Symantec (2012).

A mesma empresa, em novo relatório do ano de 2013, analisou os custos de violações em 31 empresas brasileiras e concluiu que o custo das violações de dados resulta em uma média global de US$ 136 por registro, sendo que, no Brasil (Figura 2), o custo máximo do vazamento de dados entre as 31 foi de aproximadamente R$ 9,74 milhões e o custo mínimo foi de aproximadamente R$ 230 mil.

Figura 2 – Custos do vazamento de dados de 31 empresas brasileiras

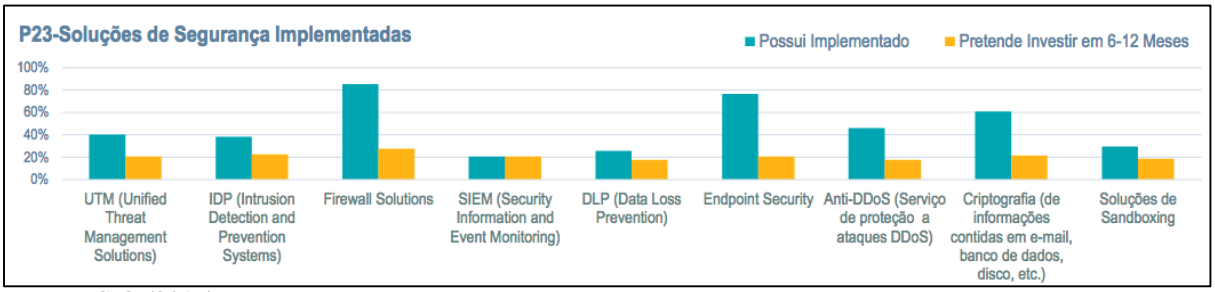


Fonte: Symantec (2012).

Segundo a redação da revista *CIO* (2017), uma pesquisa conduzida pela IDC Brasil indicou que a maioria das organizações é incapaz de lidar com as novas e crescentes ameaças à segurança da informação.

Em termos de mecanismos de segurança, a maioria das empresas brasileiras tem investido em *firewall* e soluções de *endpoint security* (Figura 3), que são *softwares* que protegem a rede corporativa de dispositivos móveis conectados a ela. Estas tecnologias são consideradas de nível inferior às necessárias para servir como solução de ataques DDoS (*Distributed Denial of Service*) ou prevenir vazamentos de dados.

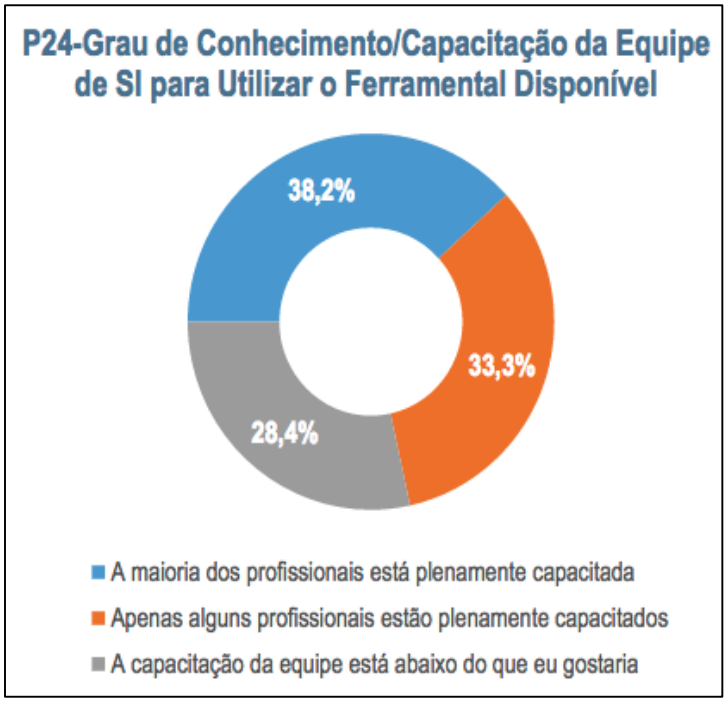
Figura 3 – Soluções de segurança implementadas



Fonte: CIO (2017).

A mesma pesquisa informa que a capacitação de 61,7% dos profissionais de segurança da informação das organizações (Figura 4) está abaixo do desejável para o uso das ferramentas disponíveis.

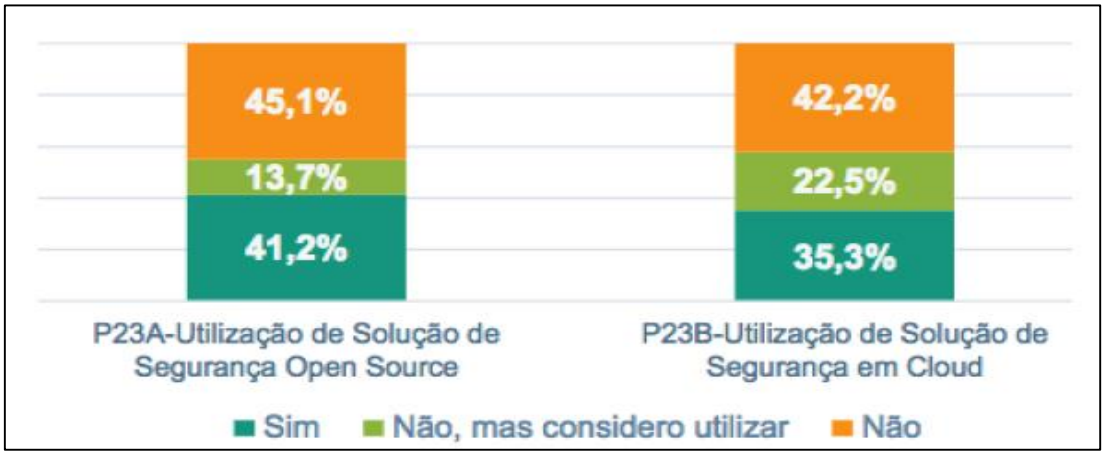
Figura 4 – Grau de conhecimento/capacitação da equipe de SI para utilizar o ferramental disponível



Fonte: CIO (2017).

A pesquisa indicou que 54,9% das organizações usam ou consideram utilizar soluções de segurança no modelo *Open Source,* por ser uma alternativa para quem não quer efetuar um investimento inicial mais elevado (Figura 5).

Figura 5 – Aderência ao *Open Source* pelas organizações

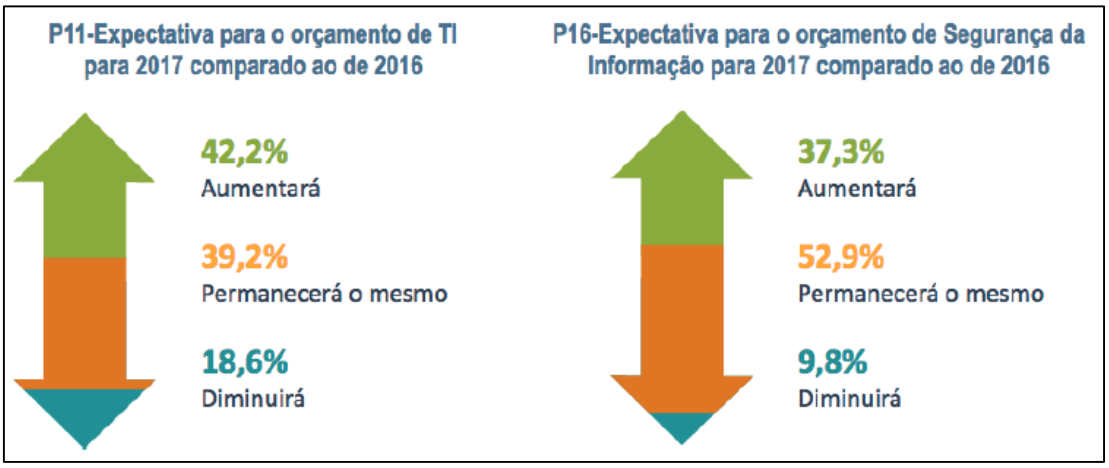


Fonte: CIO (2017).

A pesquisa apresenta uma perspectiva mais positiva para a segurança da informação em 2017, pelo fato de que, dentre as empresas pesquisadas, 52,9% pretendem manter e 37,3% pretendem aumentar seu orçamento de tecnologia da informação (TI), em comparação a 2016. A mesma visão positiva se dá para os investimentos em TI, em que,

das empresas pesquisadas, 42,2% aumentará o investimento em TI e 39,2% manterá o investimento (Figura 6).

Figura 6 – Expectativa de investimentos em TI e em segurança de TI para 2017



Fonte: CIO (2017).

1.1 PROBLEMA DE PESQUISA E QUESTÃO DE PESQUISA

A exposição de informações que circulam nas empresas pode gerar prejuízos relacionados à perda de clientes, impacto negativo na imagem e ações judiciais.

Em virtude dos riscos de mau uso das informações, as empresas necessitam de mecanismos que forneçam diretrizes para lidar com a informação, entre eles a Política de Segurança da Informação (PSI).

A PSI é um documento formal, com validade jurídica, e é o principal item da segurança da informação. Serve para dar ciência aos colaboradores das diretrizes e normas criadas pela organização que devem ser seguidas e respeitadas.

As normas da família ISO/IEC 27000 são reconhecidas mundialmente e fornecem diversas diretrizes para o desenvolvimento de um Sistema de Gestão de Segurança da Informação (SGSI). O SGSI apresenta um conjunto de procedimentos que visam prover a segurança no uso de todos os tipos de dados, informações e ativos tecnológicos. Um desses procedimentos é a implementação da PSI.

Em relação ao *call center*, ambiente onde a rotatividade de pessoas é elevada e onde há circulação de informações confidenciais, é relevante a existência de controles para evitar e prevenir que as informações sejam expostas aos riscos.

Diante do exposto acima, questiona-se como as diretrizes das normas da série ABNT/NBR 27000 podem ser aplicadas no ambiente corporativo de um *call center,* de modo que seja possível a elaboração de uma PSI.

1.2 OBJETIVOS GERAL E ESPECÍFICOS

Este trabalho tem por objetivo desenvolver, implantar e avaliar uma Política de Segurança de Informação, seguindo as normas da série ABNT/NBR 27000, em um *call center* situado na cidade de Caxias do Sul-RS.

Para atingir o objetivo geral apresentado, foram eleitos os seguintes objetivos específicos:

a) Verificar quais são os tipos de ameaça mais frequentes em empresas do setor de *call center*;
b) identificar quais itens da norma 27002 podem ser aplicados em empresas de *call center*;
c) desenvolver um estudo de caso em um *call center*, criando uma PSI de acordo com as normas 27000;
d) avaliar a PSI.

1.3 METODOLOGIA

Para adquirir os dados e informações que serviram como subsídios para a pesquisa bibliográfica, foram utilizados obras e artigos relacionados ao assunto.

A primeira etapa desenvolvida no TCC foi a pesquisa bibliográfica, iniciada pelo estudo das normas da série 27000 que tratam de segurança da informação. A norma 27001 (ABNT, 2013) auxiliou na definição das condições de como um SGSI deve ser desenvolvido.

A norma ABNT NBR ISO/IEC 27002 (ABNT, 2005) teve por objetivo fornecer as informações sobre como selecionar, implementar e gerenciar os controles na organização.

A norma 27003 (ABNT, 2011) contribuiu na informação sobre as diretrizes para implementar o SGSI que, diferentemente da 27001, disponibiliza apenas requisitos.

Foram utilizados artigos científicos atuais para estudar a melhor forma de realizar a avaliação da utilização da PSI, entre eles o de Malin (2006), Flowerday e Tuyikeze (2016), Tarnes (2012), Abdyli (2014), Nyangira e Ngome (2016), e a norma 27004 (ABNT, 2009).

Por sua vez, a norma 27005 (ABNT, 2013) forneceu informações sobre o levantamento de riscos, pré-requisito para o desenvolvimento de uma PSI.

A seguir, foi realizado um estudo sobre o funcionamento, funções e principais serviços prestados por um *call center*, além da identificação dos principais riscos a que estas empresas estão sujeitas.

Para verificar como as normas da série ABNT/NBR 27000 podem ser aplicadas no ambiente corporativo de um *call center*, de modo que seja possível a elaboração de uma PSI, foi realizado um estudo de caso com o objetivo de que a organização em questão pudesse alcançar um nível de conformidade com a norma e, por consequência, corrigir os problemas de segurança da informação existentes.

A segunda etapa do trabalho consistiu no desenvolvimento do estudo de caso, no qual a empresa em questão passou por uma análise de levantamento de riscos, que teve por objetivo identificar os riscos que a empresa possuía, para, posteriormente, tratá-los de maneira adequada.

Com base nos riscos identificados no processo de levantamento, foi desenvolvida a PSI e, posteriormente, apresentados à direção os riscos encontrados. Com o auxílio dos gestores da operação, foi efetuado um refinamento na PSI desenvolvida para adequá-la ao negócio sem impactar as áreas sem necessidade. Com a PSI pronta, definiu-se a melhor maneira de avaliá-la e mensurá-la, de acordo com os estudos teóricos realizados.

Por fim, a terceira e última etapa do trabalho consistiu na implantação e avaliação da eficácia da PSI.

1.4 ESTRUTURA DO TRABALHO

No capítulo 2 deste trabalho são abordados os conceitos sobre os princípios básicos da informação, ciclo de vida da informação, política de segurança da informação e normas ABNT NBR ISO da série 27000, além de diretrizes e conceitos sobre a estrutura de documentos, arquitetura e elaboração da política de segurança da informação. Também são apresentados os métodos para efetuar uma avaliação da eficácia de uma PSI e para coletar dados que auxiliam no desenvolvimento da avaliação.

O capítulo 3 descreve os conceitos básicos sobre *call center*, tais como estrutura e os serviços prestados, além da forma de classificá-lo e os principais riscos de segurança da informação voltadas a organizações do tipo.

O capítulo 4 apresenta a proposta de solução baseada em um estudo de caso, além da análise de riscos desenvolvida na organização e o método de avaliação da PSI.

No capítulo 5 são apresentadas as atividades a serem desenvolvidas no TCC 2 com o cronograma das atividades.

2 REFERENCIAL TEÓRICO

A segurança da informação é baseada em técnicas, conceitos e procedimentos que organizam as informações e que visam ao planejamento estratégico, visto que o sucesso de uma empresa depende da integridade e segurança da informação (GALVÃO, 2015).

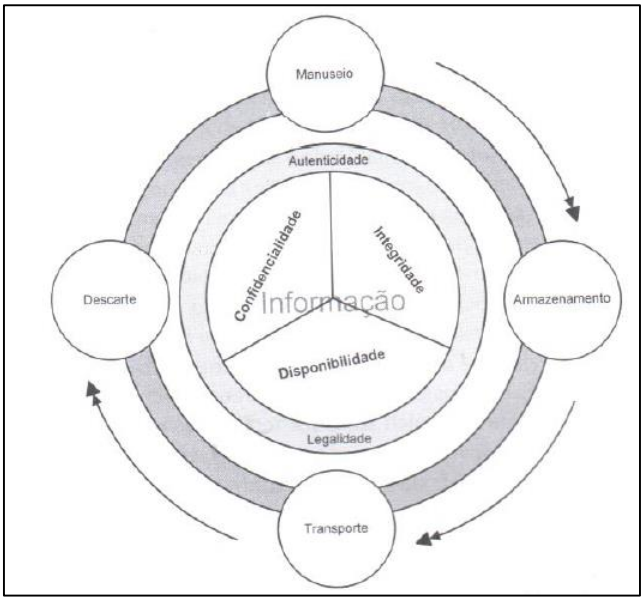
Segundo Sêmola (2014), para a proteção das informações, alguns princípios básicos devem ser seguidos, tais como: a) **confidencialidade**: somente pessoas autorizadas devem ter acesso à informação; b) **integridade**: garantir que a informação disponibilizada pelo autor não sofreu nenhuma alteração, ou seja, manteve-se íntegra; c) **disponibilidade**: a informação tem que estar disponível a qualquer momento, sempre que for solicitada, e para o funcionamento da organização.

Para manter o negócio, a informação precisa circular livremente para não engessar o processo, logo é exposta a riscos que podem influenciar na sua integridade e segurança (SÊMOLA, 2014).

Segundo a ABNT NBR ISO/IEC 27002 (2013), a informação possui um ciclo de vida natural, desde sua criação até sua destruição ou obsolescência. A Figura 7 apresenta as etapas do ciclo de vida da informação: **manuseio** (criação e utilização da informação), **armazenamento** (conservação/manutenção da informação como, por exemplo, em HD externo), **transporte** (condução da informação, como, por exemplo, via *e-mail*) e **descarte** (exclusão/rejeição da informação, como depositar na lixeira da empresa um material impresso, por exemplo).

De acordo com Galvão (2015), cada etapa do ciclo de vida da informação deve garantir os princípios básicos da informação (confidencialidade, integridade e disponibilidade).

Figura 7 – Os quatro momentos do ciclo de vida da informação



Fonte: Sêmola (2014).

As próximas seções apresentam o conceito de PSI, as normas da série ABNT NBR ISO/IEC 27000 associadas à construção de uma PSI, e, por fim, os métodos de avaliação de uma PSI.

2.1 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Para Galvão (2015), a PSI é definida como um documento que contém todos os riscos organizados de maneira hierárquica, com métodos que devem ser seguidos para atingir as metas de segurança. O autor sugere que a leitura desse documento deve ser obrigatória a todos os colaboradores da organização. O autor apresenta três tipos de políticas: a) **regulatória**: deve-se assegurar que o documento não sairá da empresa, pois contém informações exclusivas da organização referentes às necessidades legais impostas na empresa e na execução das suas atividades; b) **consultiva**: é opcional, pois tem como objetivo indicar quais ações devem ser tomadas para determinada atividade de maneira objetiva; e c) **informativa**: apenas de caráter informativo, pelo fato de que especifica o que é desejado pelos funcionários, porém não é requerida nenhuma atividade e não existem riscos, caso não seja cumprida.

Segundo a ABNT NBR ISO/IEC 27002 (2013), o objetivo da PSI é fornecer orientações à gestão de segurança da informação sobre os requisitos de negócios. A PSI deve elaborada para ser clara e alinhada aos objetivos do negócio e apoiada pela direção da empresa.

Para Fontes (2015), na elaboração das políticas, normas e procedimentos de segurança, deve-se atentar às seguintes características: a) entendimento e leitura fáceis, com palavras comuns para todos os usuários; b) regras e controles que possam ser cumpridos; c) aplicabilidade à organização; d) desenvolvimento de modo que os usuários possam cumprir os controles definidos; e) instruções sobre o que fazer em casos de exceções que não estejam previstas no documento; f) possibilidade de acesso por parte de todos os colaboradores; g) caráter positivo, para que os usuários vejam-nas como algo importante e não apenas como regulamentos proibitivos; h) foco em um único macroassunto, com informações que contenham apenas o necessário; e i) objetividade e eficácia na comunicação.

Além disso, o autor lista os elementos que compõem a PSI:

a) **objetivo:** expõe o que é tratado no documento, o motivo de sua existência;

b) **escopo:** delimita a abrangência da política, podendo ser relacionado a diversos aspectos que venham a definir a sua limitação, seja de usuário da informação, ambiente físico, entre outros;

c) **definições:** detalham todas as siglas, abreviaturas, explicações, detalhamento de termos e siglas organizacionais;

d) **regras:** expõem os controles a serem seguidos pelos usuários e informa o que é obrigatório ser feito, o que é proibido de se fazer, entre outros tipos de regras;

e) **responsabilidades:** indicam as incumbências das pessoas ou das áreas em relação ao documento. Definem-se atribuições em relação à gestão de manutenção da política, à garantia do entendimento e do conhecimento por todas as pessoas e à realização de revisões do documento quando necessário, dando ciência a cada usuário;

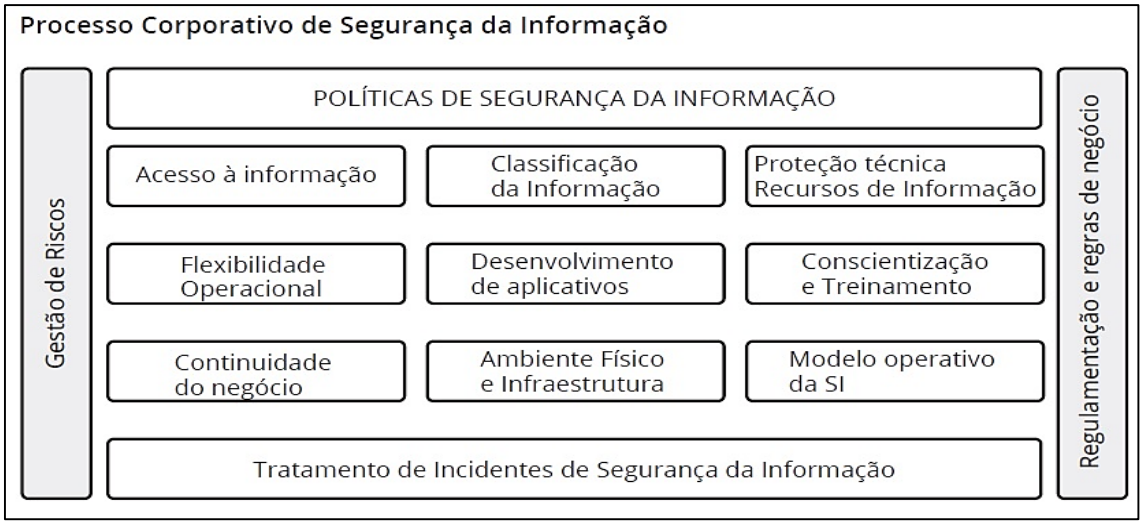
f) **cumprimento:** apresenta as penalidades do não cumprimento dos controles descritos na política. Deve considerar situações de erro/exceção e instruir o usuário sobre o que deve ser feito em cada situação. É importante atribuir um responsável pelo monitoramento do cumprimento desse documento.

Fontes (2015) ainda cita que alguns aspectos devem ser considerados em um processo de segurança da informação, e tais aspectos são denominados dimensões da

segurança da informação. Cada dimensão tem sua devida importância no processo organizacional de segurança da informação, e todas possuem o mesmo grau de relevância. A classificação da organização quanto à maturidade da segurança da informação depende da eficácia do conjunto das dimensões.

A Figura 8 apresenta as dimensões da segurança da informação, estruturadas conforme orientações da norma ABNT NBR ISO/IEC 27002.

Figura 8 – Dimensões da segurança da informação

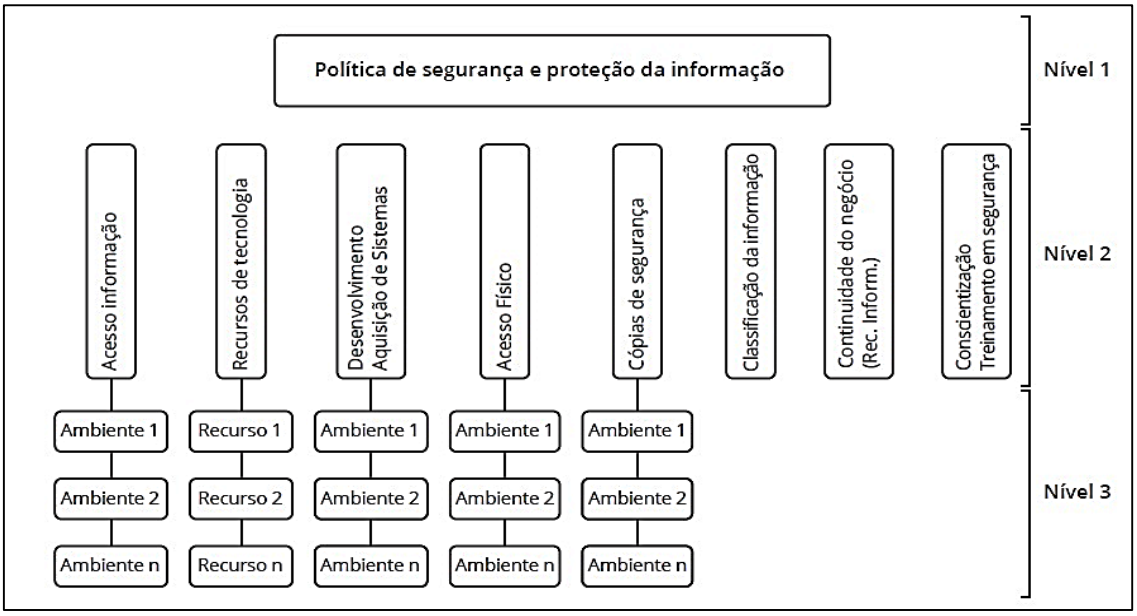


Fonte: Fontes (2015).

2.1.1 Arquitetura da política de segurança da informação

De acordo com Fontes (2015), para diretrizes da segurança da informação serem desenvolvidas e planejadas, deve-se utilizar uma arquitetura que defina os diversos documentos que se relacionam entre si, com o objetivo de compor a PSI principal. Sem o uso de uma estrutura para desenvolvê-la, o risco de se obterem documentos confusos, repetidos e de difícil compreensão é elevado. A arquitetura deve permitir que toda a organização siga suas diretrizes. A Figura 9 apresenta a estrutura da arquitetura da PSI.

Figura 9 – Estrutura da arquitetura da PSI



Fonte: Fontes (2015).

O autor explica que o nível 1 corresponde à política principal e deve ser desenvolvida de modo que não haja necessidade de alteração nos próximos cinco a dez anos. O documento contém toda a filosofia da empresa em relação à segurança da informação e deve ser assinado pela direção da empresa. Neste documento são encontrados os princípios de segurança da informação que a organização deseja que seus colaboradores sigam.

Os documentos pelo qual o nível 2 da estrutura da PSI da organização é formado deve conter as regras e controles básicos para cada dimensão da segurança da informação. Os controles básicos devem estar relacionados com os controles estruturais definidos pela política principal.

A política da dimensão é composta pelos seguintes documentos de políticas/normas:

a) **Acesso lógico**: documento que detalha controles e regras de acesso aos ambientes da organização.
b) **Ambiente físico**: documento que contém os controles e regras comuns a todos os ambientes físicos que possuam acesso aos recursos de informação.
c) **Correio eletrônico**: detalha os controles e regras aos colaboradores que utilizam correio eletrônico na organização.
d) ***Internet***: documento que especifica todos os controles e regras básicas que devem ser seguidos por todos os usuários no acesso à *Internet*;
e) **Equipamentos de TI**: descreve os controles e regras que são comuns a todos os equipamentos de TI da organização.

f) **Classificação da informação**: documento que define os princípios básicos em segurança referente à classificação da informação e também aos padrões de confidencialidade ou sigilo da informação.
g) **Desenvolvimento/aquisição de sistemas aplicativos**: detalha os princípios de segurança que se referem ao desenvolvimento, implantação e manutenção de sistemas aplicativos. Devem-se especificar os controles e regras comuns a todos os tipos de sistemas aplicativos desenvolvidos e implantados na organização.
h) **Plano de continuidade**: deve detalhar princípios básicos de segurança relacionados ao plano de continuidade do negócio, quando houver indisponibilidade de recursos de informação.
i) **Cópias de segurança**: especifica as regras e controles das cópias de segurança utilizadas pela organização.

O nível 3 é denominado documento procedimento de ação e detalha as ações a serem tomadas para que os controles definidos na norma de dimensão possam ser desenvolvidos e implantados na organização.

2.2 NORMAS DA ABNT

A série das normas NBR ISO/IEC 27000 fornecem diretrizes e incluem padrões que definem os requisitos para um SGSI. As normas auxiliam diretamente sobre aspectos dos processos e requisitos do ciclo *Plan – Do – Check – Act* (PDCA).

2.2.1 ABNT NBR ISO/IEC 27001

Esta norma tem por princípio especificar as diretrizes para estabelecer, implementar, manter e melhorar de maneira contínua um SGSI, incluindo também os requisitos para a avaliação e tratamento de riscos.

A direção da empresa deve apoiar o SGSI a partir dos seguintes meios: a) estabelecer uma PSI que seja voltada à estratégia da organização; b) integrar o SGSI nos processos da organização; c) disponibilizar os recursos para o SGSI; d) comunicar a importância de um SGSI; e) assegurar que o SGSI atinja seus objetivos; f) orientar e apoiar para que as pessoas contribuam para a eficácia do SGSI; g) promover sua melhoria contínua; h) apoiar os gestores com o objetivo de provar que sua liderança se aplica às áreas sob sua responsabilidade.

Em relação à operacionalidade do SGSI, a ABNT NBR ISO/IEC 27001 (2013) orienta que a organização deve planejar, implementar e controlar os processos necessários para atender os requisitos de segurança da informação. Outro fator importante para o desenvolvimento de um SGSI é que a organização deve manter documentada a abrangência do SGSI, para que se possa gerar a confiança de que os processos da organização sejam realizados conforme o planejado.

Quanto à questão de desempenho e eficácia do SGSI, a organização deve manter métodos de avaliação, para que, quando ocorrer uma não conformidade, a organização possa tomar atitudes para controlá-la e corrigi-la. O Quadro 1 apresenta as principais fases e objetivos de criação de um SGSI.

Quadro 1 – Fases e principais objetivos de cada fase da criação de um SGSI

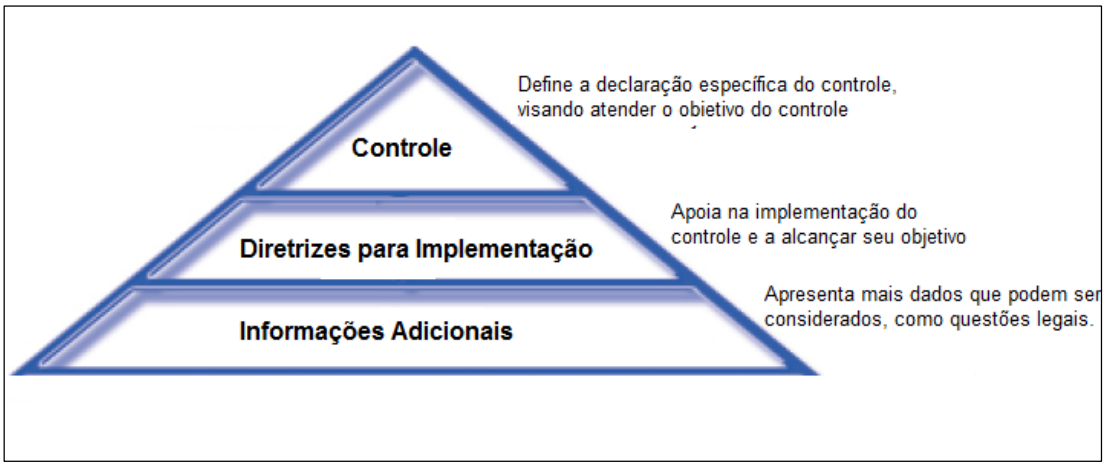
Liderança	• Assegura que a PSI é compatível com a estratégia da organização; • assegura que o SGSI alcançará os resultados pretendidos; • assegura que as pessoas contribuam para a eficácia do SGSI.
Planejamento	• Previne ou reduz os efeitos indesejados; • define e aplica um processo de avaliação de riscos de segurança da informação; • define e aplica um processo de tratamento dos riscos de segurança da informação; • estabelece os objetivos de segurança da informação para as funções e níveis relevantes.
Apoio	• Determina a competência necessária das pessoas que realizam trabalho; • retém informação documentada apropriada como evidência da competência.
Operação	• Mantém a informação documentada; • assegura que os processos terceirizados estão determinados e são controlados.
Avaliação do desempenho	• Realiza a realimentação sobre o desempenho da segurança da informação; • realiza realimentação das partes interessadas; • assegura que os resultados das auditorias são relatados para a direção.
Melhoria	Assegura continuamente a melhoria, adequação e eficácia do sistema de gestão da segurança da informação.

Fonte: elaborado pelo autor (2017).

2.2.2 ABNT NBR ISO/IEC 27002

A norma ABNT NBR ISO/IEC 27002 (2013) apresenta diretrizes para as práticas de gestão de segurança da informação. Ela inclui as diretrizes para a seleção, a implementação e o gerenciamento de controles de segurança da informação da organização. A norma foi estruturada em 14 seções de controles de segurança da informação, 35 objetivos de controles e 114 controles. Para cada um dos controles foram definidas diretrizes para implementação e informações adicionais (Figura 10).

Figura 10 – Estrutura dos controles



Fonte: elaborada pelo autor (2017).

Segundo a ABNT NBR ISO/IEC 27002 (2013), a ordem dos controles não significa o seu grau de importância. Dependendo das circunstâncias, todas as seções podem ter relevância em um mesmo grau. Portanto, cada organização deve identificar quais são os itens aplicáveis e deve adaptar os controles à realidade do negócio.

O Quadro 2 apresenta as 14 seções de controle da norma ABNT ISO/IEC 27002 com seus respectivos objetivos:

Quadro 2 – Seção de controle de acessos

(continua)

Seções de controle	Objetivos
Políticas de segurança da informação	Prover orientação e apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

(continuação)

Seções de controle	Objetivos
Organização da segurança da informação	• Estabelecer uma estrutura de gerenciamento, para iniciar e controlar a implementação da segurança da informação dentro da organização; • garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis.
Segurança em recursos humanos	• Assegurar que funcionários e partes externas entendam suas responsabilidades e estejam em conformidade com os papéis para os quais eles foram selecionados; • assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação; • proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.
Gestão de ativos	• Identificar os ativos da organização e definir as responsabilidades apropriadas para sua proteção; • assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização; • prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.
Controle de acesso	• Limitar o acesso à informação e aos recursos de processamento da informação; • assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços; • tornar os usuários responsáveis pela proteção das suas informações de autenticação; • prevenir o acesso não autorizado aos sistemas e aplicações.
Criptografia	Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.
Segurança física e do ambiente	• Prevenir o acesso físico não autorizado, danos e interferências aos recursos de processamento das informações e às informações da organização; • impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das operações da organização.
Segurança nas operações	• Garantir a operação segura e correta dos recursos de processamento da informação; • proteger contra a perda de dados; • registrar eventos e gerar evidências; • assegurar a integridade dos sistemas operacionais; • prevenir a exploração de vulnerabilidades técnicas;

(conclusão)

Seções de controle	Objetivos
Segurança nas operações	• minimizar o impacto das atividades de auditoria nos sistemas operacionais.
Aquisição, desenvolvimento e manutenção de sistemas	• Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação, o que inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas; • garantir que a segurança da informação está projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação; • assegurar a proteção dos dados usados para teste; • garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores; • manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.
Relacionamento na cadeia de suprimento	
Gestão de incidentes de segurança da informação	Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.
Aspectos da segurança da informação na gestão da continuidade do negócio	• É recomendado que a continuidade da segurança da informação seja considerada nos sistemas de gestão da continuidade do negócio da organização; • assegurar a disponibilidade dos recursos de processamento da informação.
Conformidade	• Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança; • garantir que a segurança da informação está implementada e operada de acordo com as políticas e procedimentos da organização.

Fonte: ABNT NBR ISO/IEC 27002 (2005).

2.2.3 ABNT NBR ISO/IEC 27003

Esta norma tem o objetivo de fornecer diretrizes para a implantação do SGSI, desde a idealização do projeto até a criação dos planos de aplicação. O que a diferencia da norma ABNT NBR ISO/IEC 27001 é que, enquanto a 27001 informa apenas os requisitos, a norma 27003 apresenta uma orientação detalhada para a implementação do SGSI. A norma fornece subsídios para a preparação de um plano para a implantação do SGSI, auxilia na

definição da estrutura organizacional do projeto, na aprovação da sua direção e suas atividades críticas.

Figura 11 – Fases do projeto de SGSI

Fonte: ABNT NBR ISO/IEC 27003 (2011).

A norma define que o processo de planejamento da implantação de um SGSI contém cinco fases. A Figura 11 ilustra as 5 fases do planejamento do SGSI e os principais documentos produzidos em cada fase. A numeração 5 a 9 da Figura 11 relaciona cada uma das fases à seção em que está descrita na norma.

As fases do planejamento do SGSI são: a) aprovação da direção: a organização deve criar os motivos que justifiquem a implantação. O documento deve incluir os objetivos e as prioridades para a implementação de um SGSI; b) definição do escopo do SGSI: compõe-se da abrangência do SGSI. A definição da política do SGSI, a aceitação e o apoio por parte da direção são os fatores-chave para a implementação bem-sucedida do SGSI. Deve ser escrita de forma simples e ter uma abordagem sistemática para identificar os ativos de informação e avaliar mecanismos de segurança viáveis; c) condução da análise dos requisitos de segurança: as informações aqui coletadas devem fornecer uma direção como ponto de partida, identificar condições para a implementação, situações particulares na organização e o nível desejado de proteção para a informação; d) condução da

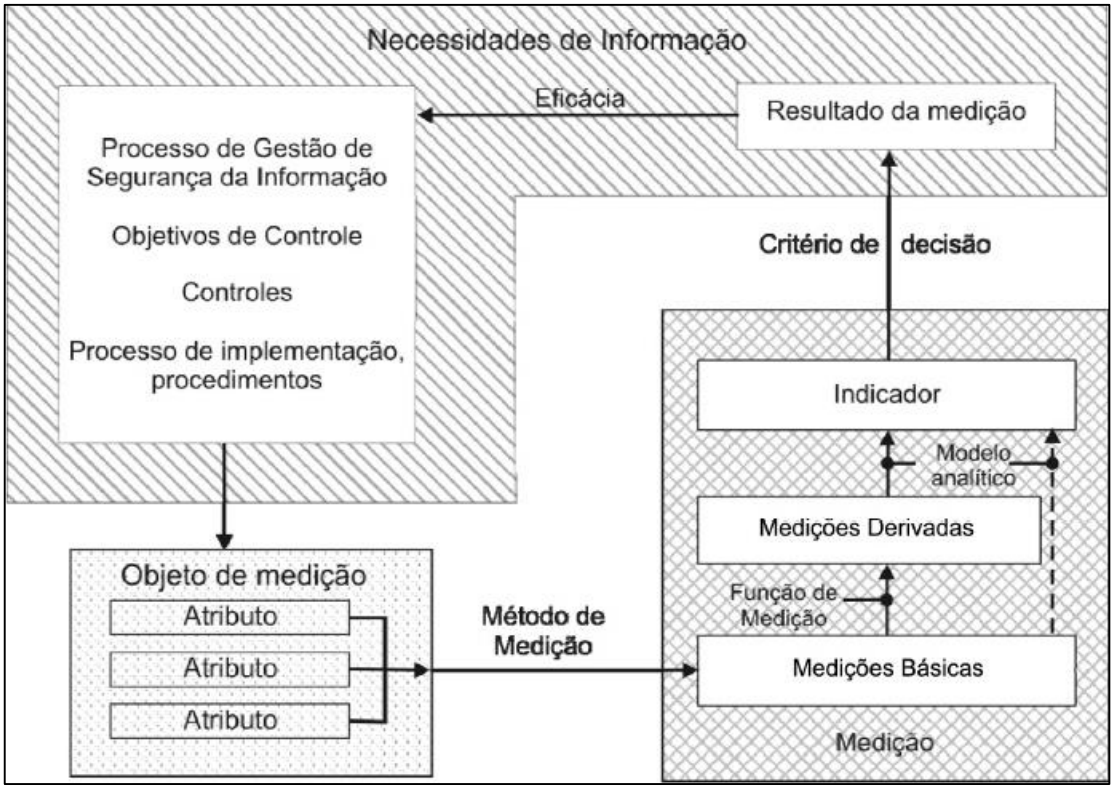
análise/avaliação de riscos e planejamento do risco: etapa na qual é realizada a avaliação dos riscos a partir dos ativos identificados. Devem-se identificar as ameaças e suas fontes, os controles existentes e planejados, as vulnerabilidades, os impactos, a probabilidade de incidente e a estimativa de níveis de riscos; e) definição do SGSI: define no SGSI os papéis e responsabilidades de cada colaborador para a segurança de informação, com o tratamento de risco.

2.2.4 ABNT NBR ISO/IEC 27004

Essa norma fornece instruções para o desenvolvimento e utilização de medidas e medições para avaliar a eficácia de um SGSI. A PSI, a gestão de riscos e os controles, por fazerem parte do SGSI, são incluídos no processo de avaliação de eficácia, com o objetivo de identificar se é necessária a modificação ou otimização dos seus processos. Tal norma parte do princípio de que, para desenvolver as medidas e medições, é necessário que a análise e o levantamento dos riscos sejam executados corretamente, possibilitando aos interessados a utilização das medidas na tarefa da melhoria contínua da segurança da informação.

Segundo a ABNT NBR ISO/IEC 27004 (2009), as medições podem ser integradas às atividades operacionais ou executadas a intervalos regulares. Uma estrutura denominada modelo de medição de segurança da informação (Figura 12) é responsável por relacionar uma necessidade de informação com os objetos relevantes da medição e seus atributos. O modelo também mostra como os atributos são quantificados e convertidos em indicadores que fornecem uma base para a tomada de decisão.

Figura 12 – Modelo de Medição de Segurança da Informação



Fonte: ABNT NBR ISO/IEC 27004 (2010).

O Quadro 3 apresenta um padrão para um modelo de medição em segurança da informação, conforme norma ABNT NBR ISO/IEC 27004, com suas respectivas definições.

Quadro 3 – Identificação do modelo de medição

(continua)

Identificação do modelo de medição	
Nome do modelo de medição	Nome da medição
Identificador numérico	Identificador numérico único específico da organização
Propósito do modelo da medição	Descreve as razões para introduzir a medição
Objetivo de controle/processo	Objetivos de controle sob medição
Controle(1)/Processo(1)	Controle/processo sob medição
Controle(2)/Processo(2)	Opcional: controle/processo adicional
Objeto de medição e atributos	
Objeto de medição	Caracterizado a partir da medição de seus atributos. Um objeto pode incluir processos, planos, projetos, recursos e sistemas, ou componente de sistemas.

(continuação)

Atributo	Propriedade ou característica de um objeto de medição que pode ser distinguida quantitativamente ou qualitativamente por meios manuais ou automatizados.
Especificação da Medida Básica (medida para cada base [1...n])	
Medida Básica	Definida em termos de um atributo e o método de medição especificado para quantificá-lo.
Método de medição	Sequência lógica de operações usada na quantificação de um atributo em relação a uma escala especificada.
Tipo do método de medição	Dependendo da natureza das operações usadas para quantificar um atributo, dois tipos de método podem ser distinguidos: • Subjetivo: quantificação envolvendo julgamento humano; • Objetivo: quantificação baseada em regras numéricas, tais como a contagem.
Escala	Conjunto ordenado de valores ou categorias a partir do qual o atributo da medida básica é mapeado
Tipo da escala	Dependendo da natureza do relacionamento entre os valores na escala, quatro tipos de escala são comumente definidos: Nominal, Ordinal, Intervalo e Razão.
Unidade de Medição	Quantidade específica, definida e adotada por convenção, com a qual outra quantidade qualquer do mesmo tipo pode ser comparada para expressar por um número a razão das duas quantidades.
Especificação de medida derivada	
Medida derivada	Uma medida que é derivada como uma função de duas ou mais “medidas básicas”.
Função de medição	Algoritmo ou cálculo realizado para combinar duas ou mais “medidas básicas”. A escala e a unidade da medida derivada dependem das escalas e unidades das “medidas básicas”, das quais ela é composta e como ela é combinada pela função.
Especificação de Indicador	
Indicador	Medida que fornece uma estimativa ou avaliação dos atributos especificados, derivados de um modelo analítico relacionado a uma determinada necessidade de informação. São a base para a análise e a tomada de decisão.
Modelo Analítico	Algoritmo ou cálculo combinando uma ou mais “medidas básicas” ou derivadas relacionadas ao critério de decisão associado. Baseado no entendimento de, ou suposição sobre, a relação esperada entra a medida básica e/ou derivada e o seu comportamento ao longo do tempo. Produz estimativas ou avaliações relevantes para uma determinada necessidade de informação.
Especificação do Critério de Decisão	

(conclusão)

Critério de decisão	Metas ou padrões usados para determinar a necessidade de ação ou investigação, ou para descrever o nível de confiança em um dado resultado.
	em um dado resultado.
Resultado da Medição	
Interpretação do indicador	Descrição de como convém que seja interpretado o indicador.
Formatos de relatórios	Convém que os formatos de relatórios sejam identificados e documentados. Descreve as observações que a organização ou proprietário da informação pode querer no registro. Descreve visualmente as medidas e fornece uma explanação verbal dos indicadores.
Partes interessadas	
Cliente da medição	Direção ou outra parte interessada que solicita ou exige informações sobre a eficácia do SGSI, controle ou grupos de controles.
Revisor da medição	Pessoa ou unidade organizacional que afere se os modelos de medição desenvolvidos são apropriados para avaliar a eficácia de um SGSI, controles ou grupo de controles.
Proprietário da informação	Pessoa ou unidade organizacional que possui a informação de um objeto de medição e atributos, e é responsável pela medição.
Coletor da Informação	Pessoa ou unidade organizacional responsável pela coleta, registro e armazenamento dos dados.
Comunicador da informação	Pessoa ou unidade organizacional responsável pela análise dos dados e comunicação dos resultados da medição.
Frequência / Período	
Frequência de coleta dos dados	Frequência com que os dados são coletados.
Frequência de Análise dos dados	Frequência com que os dados são analisados.
Frequência de relato dos resultados da medição	Frequência com que os resultados da medição são reportados.
Revisão de medição	Data da revisão da medição.
Período de medição	Define o período sendo medido.

Fonte: ABNT NBR ISO/IEC 27004 (2010).

Conforme a norma ABNT NBR ISO/IEC 27004, um método de medição pode usar objetos de medição e atributos de variadas fontes como, por exemplo, questionários, pesquisas e entrevistas pessoais.

O Quadro 4 apresenta um exemplo do modelo de medição que trata da proteção contra *software* malicioso e tem como objetivo demonstrar a aplicabilidade dessa norma usando o padrão fornecido no apêndice D.

Quadro 4 – Modelo de medição

(continua)

Identificação do modelo de medição	
Nome do modelo de medição	Proteção contra *software* malicioso.
Identificador numérico	Específico da organização.
Identificação do modelo de medição	
Propósito do modelo da medição	Avaliar a eficácia do sistema de proteção contra ataques de *softwares* maliciosos.
Objetivo de controle/processo	Proteger a integridade do *software* e da informação, contra *softwares* maliciosos.
Controle(1)/Processo(1)	Controle de detecção, prevenção, e recuperação para proteger contra código malicioso e procedimentos apropriados de conscientização do usuário que devem ser implementados.
Objeto de medição e atributos	
Objeto de medição	1. Relatório de incidentes de segurança da informação. 2. *Logs* de *software* de contramedida para *software* malicioso.
Atributo	Incidentes de segurança de informações causadas por *software* malicioso
Especificação da Medida Básica (medida para cada base [1…n])	
Medida Básica	1. Número de incidentes de segurança da informação causadas por *software* malicioso. 2. Total de ataques bloqueados causados por *software* malicioso
Método de medição	1. Contar o número de incidentes de segurança causados por *software* malicioso nos relatórios de incidentes de segurança da informação. 2. Contar o número de registros de ataques bloqueados.
Tipo do método de medição	1. Objetivo 2. Objetivo
Escala	1. Inteiros de zero até infinito 2. Inteiros de zero até infinito
Tipo da escala	1. Ordinal 2. Ordinal
Unidade de medição	1. Incidente de segurança da informação 2. Registros
Especificação de medida derivada	
Medida derivada	Força da proteção de *software* malicioso
Função de medição	Número de incidentes de segurança causados por *software* / número de ataques detectados e bloqueados causados por *software* malicioso
Especificação de Indicador	
Indicador	Tendência de ataques detectados que não foram bloqueados sobre múltiplos períodos do relatório.
Modelo Analítico	Comparar a razão com a porcentagem anterior.

(conclusão)

Especificação do Critério de Decisão	
Critério de decisão	Convém que as linhas de tendência se mantenham abaixo do número especificado e que a tendência resultante seja decrescente ou constante.
Resultado da Medição	
Interpretação do indicador	Tendência ascendente indica não-conformidade e descendente indica melhoria da conformidade. Quando uma tendência aumenta consideravelmente, a investigação da causa e oportu-
Interpretação do indicador	nidades para futuras contramedidas tornam-se necessárias.
Formatos de relatórios	Linha de tendência que descreve a proporção da detecção de código malicioso e linhas de prevenção produzidas durante períodos de relatórios anteriores.
Partes interessadas	
Cliente da medição	Gestor de segurança da informação.
Revisor da medição	Gestor de segurança da informação.
Proprietário da informação	Administrador do sistema.
Coletor da informação	Gestor de segurança da informação.
Comunicador da informação	Coordenação de serviço.
Frequência / Período	
Frequência de coleta dos dados	Diariamente.
Frequência de análise dos dados	Mensalmente.
Frequência de relato dos resultados da medição	Mensalmente.
Revisão de medição	Anualmente.
Período de medição	Aplicável por 1 ano.

Fonte: ABNT NBR ISO/IEC 27004 (2010).

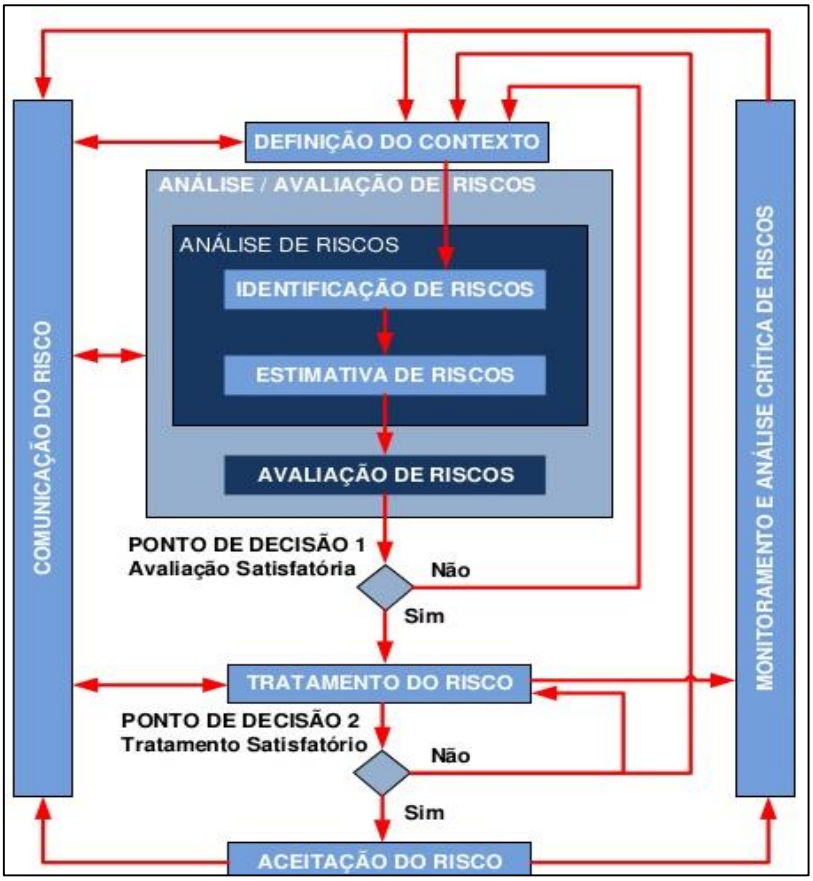
2.2.5 ABNT NBR ISO/IEC 27005

Esta norma apresenta diretrizes para o processo de gestão de riscos de segurança da informação (GRSI). Segundo a norma ABNT NBR ISO/IEC 27005 (2013), para uma gestão de riscos ser eficiente, a organização deve, em todos os níveis, seguir os seguintes princípios:

a) Criar e proteger valor: a gestão de risco contribui para a melhoria do desempenho, a saúde das pessoas, as conformidades legais, a qualidade de produto, entre outros processos;
b) ser parte integrante de todos os processos organizacionais: a gestão de riscos não é autônoma, separada das principais atividades da organização e, sim, integra todos os processos organizacionais;
c) ser parte da tomada de decisões, auxiliando na priorização de ações;
d) levar em consideração a incerteza e como ela deve ser tratada;
e) ser sistemática, estruturada e oportuna, contribuindo para a eficiência e resultados consistentes e confiáveis;
f) basear-se nas melhores informações disponíveis;
g) estar alinhada ao contexto interno e externo da organização, voltada ao negócio da empresa e com o perfil do risco;
h) considerar fatores humanos e culturais que facilitam ou dificultam a realização dos objetivos da organização;
i) ser transparente, inclusiva, pertinente e atualizada, permitindo considerações das partes interessadas à determinação dos critérios de risco;
j) ser dinâmica, interativa e capaz de reagir a mudanças;
k) facilitar a melhoria contínua da organização.

Como é possível observar na Figura 13, as atividades do processo de um SGSI iniciam com a definição do contexto, seguidas de análise/avaliação de riscos, tratamento do risco, aceitação do risco, comunicação do risco e, por fim, o monitoramento e a análise crítica de riscos.

Figura 13 – Processo do SGSI



Fonte: ABNT NBR ISO/IEC 27005 (2013).

A definição do contexto é responsável por estabelecer o escopo, critérios de avaliação, entre outras definições. Os critérios básicos para avaliação de riscos são os a) critérios de impacto, que servem para mensurar o montante dos danos ou custos à organização, causados por algum evento de segurança da informação; e b) critérios para aceitação de riscos, a partir dos quais a organização define o nível de aceitação dos riscos.

O processo de análise de riscos tem como objetivo identificar os riscos e o que deve ser feito para reduzi-lo a um nível aceitável.

O plano de tratamento de risco estabelece controles para as ameaças levantadas na etapa anterior. Com o plano de tratamento de risco e a análise do risco elabora-se uma lista dos que são aceitos e uma justificativa para os que não foram aceitos.

Para o processo de comunicação, as informações sobre riscos são divulgadas para todas as áreas operacionais e seus gestores. Todos os colaboradores devem ter consciência sobre os riscos e os controles a serem adotados.

Por fim, a atividade de monitoramento é responsável por acompanhar os resultados obtidos e desenvolver uma análise crítica para a melhoria contínua do processo.

O Quadro 5 resume as principais atividades de GRSI para as quatro fases do processo do SGSI, de acordo com aplicação do modelo PDCA.

Quadro 5 – Alinhamento do processo de SGSI e do processo de GRSI

Processo do SGSI	Processo de SGSI
Planejar	• Definir o contexto; • definir o processo de avaliação de riscos; • definir o plano de tratamento de riscos; • definir o plano de aceitação de riscos.
Executar	Implementar o plano de tratamento do risco.
Verificar	Efetuar o monitoramento contínuo e a análise dos riscos.
Agir	Manter a melhoria do processo de gestão de riscos da Segurança da Informação.

Fonte: elaborada pelo autor (2017).

2.3 MÉTODOS DE COLETA DE DADOS

Para auxiliar na coleta de dados para avaliar a PSI, deve-se identificar quais são as técnicas mais apropriadas para a atividade. Os métodos qualitativos e quantitativos de pesquisa, questionários e entrevistas são os métodos mais conhecidos.

Segundo Bell (2015), a pesquisa quantitativa é induzida a produzir resultados genéricos, por isso é considerada como um método formalizado e controlado. Quem desenvolve pesquisas a partir desse método coleta os dados e estuda como o conjunto das respostas se relaciona. Ela é muito utilizada quando se conhece a natureza das variáveis utilizadas na área da investigação, e também pelo fato de que ela apresenta em números padrões de comportamentos dos indivíduos pesquisados e, por consequência, gera resultados precisos.

Lima (2001) afirma que a pesquisa qualitativa surgiu em função da insatisfação da concepção de mundo da visão positivista, que desconsiderava qualquer conhecimento que não pudesse ser comprovado cientificamente, como, por exemplo, conhecimentos voltados à engenharia social, ética ou crenças.

Para Dantas e Cavalcante (2006), a pesquisa qualitativa faz com que os entrevistados respondam livremente sobre o tema abordado, e é usada quando se busca entendimento sobre determinado assunto, abrindo espaço para interpretações diversificadas. A Figura 14 apresenta as diferenças entre a pesquisa qualitativa e quantitativa.

Figura 14 – Diferença entre pesquisa qualitativa e quantitativa

PESQUISA QUALITATIVA	PESQUISA QUANTITATIVA
Percepção do fenômeno	Percepção do fenômeno
Isolar casos	Identificar propriedades
Observar seqüências, testemunhos, contexto	Medir, correlacionar escalas
Selecionar casos	Conceituar população e amostras
Observar, entrevistar, registrar	Selecionar situações p/ estudo
Determinar padrões, selecionar e classificar	Medir, comparar, explicar variância
Triangular, validar, interpretar	Interpretar
Fazer estudos de caso ou relatórios	Preparar tabelas, quadros, relatórios
Produto: compreensão com ênfase em generalidades	Produto: explicações enfatizando propriedades, população
Realçar valores, opiniões e atitudes	Atua em níveis de realidade

Fonte: Dantas e Cavalcante (2006).

Bell (2005) afirma que, ao se elaborar um questionário, é necessária uma elaboração e seleção criteriosa das perguntas, tanto da questão em si quanto das opções de resposta. Deve-se ter rigor nos critérios, desde a idealização do questionário, bem como seus processos de entrega e devolução, até a etapa de análise dos resultados. Ele tem como finalidade obter informações sobre determinadas opiniões ou, ainda, medir determinadas variáveis. A vantagem dos questionários em relação às entrevistas é sua abrangência, pelo fato de que questionários o*n-line* atingem mais pessoas do que entrevistas individuais.

Dantas e Cavalcante (2006) apresentam dois modelos de questionários: os qualitativos, cuja fonte das informações é por meio de um roteiro, e no qual o processo é gravado e depois analisado; e os quantitativos, em que há um questionário padronizado e uniformizado, com perguntas claras e objetivas.

Ainda segundo os autores, as entrevistas também podem ser qualitativas ou quantitativas. Na primeira, discussões em grupos são elaboradas e entrevistas são aplicadas com os entrevistados de forma individual. Na entrevista quantitativa, os entrevistados são caracterizados por alguns critérios como sexo, idade, ramo de atividade, localização geográfica, entre outros. As entrevistas têm por objetivo fornecer uma quantidade muito grande de dados e informações que possibilitam um trabalho rico em informações.

Bell (2005) cita que uma das principais vantagens das entrevistas em relação aos demais métodos de coleta de dados é a sua adaptabilidade. Outra vantagem é que as entrevistas oferecem algum conhecimento extra, em virtude da linguagem corporal do entrevistado. Durante a entrevista, a forma de questionar deve ser clara para que não haja contradições por parte do entrevistado.

2.4 CONSIDERAÇÕES FINAIS

Nos últimos anos, a preocupação com a forma pela qual as informações circulam nas organizações têm aumentado significativamente. Em virtude dessa preocupação, tornou-se fundamental o desenvolvimento de estratégias que visam garantir a integridade dos dados durante todo o seu ciclo de vida.

Por isso, as normas da série ISO/IEC 27000 entraram em vigor, isto é, para que as empresas, de alguma maneira, possam se prevenir e manter uma gestão da segurança da informação nas organizações.

O presente trabalho utiliza-se da norma ABNT NBR ISO/IEC 27001 para definição de requisitos de uma política de segurança de informação e a norma ABNT NBR ISO/IEC 27003 para obter um aprofundamento teórico sobre a implementação do SGSI.

A norma ABNT NBR ISO/IEC 27002 fornece orientação em relação à seleção dos controles.

A norma ABNT NBR ISO/IEC 27004 foi utilizada na elaboração do método de medição da eficácia da PSI, e, para obter as informações necessárias para esta medição, fontes externas de informações foram utilizadas, baseadas nos métodos de coleta de informações.

Por sua vez, a norma ABNT NBR ISO/IEC 27005 foi utilizada para auxiliar no levantamento dos principais riscos da organização, requisito para poder desenvolver uma PSI.

3 EMPRESAS DE *CALL CENTER*

Para Mancini (2006), o conceito de *call center* consiste em centralizar o gerenciamento das relações da organização com a sociedade, independentemente do meio utilizado, seja ele por telefone ou correio. O elevado nível de adaptabilidade aos variados tipos de serviços e flexibilidade são algumas das vantagens deste modelo de negócio.

Nesta seção serão apresentados os conceitos básicos sobre *call center*, os profissionais envolvidos, os tipos de serviços prestados, como são classificados, bem como sua estrutura tecnológica.

3.1 PROFISSIONAIS ENVOLVIDOS

Segundo Mancini (2006), deve ser efetuada uma análise para identificar quais são os profissionais chave para o negócio, pelo fato de que nem todos são necessários para se obter resultados positivos. Alguns dos setores podem ser inclusive terceirizados, e uma equipe ideal é composta por múltiplas funções. Os profissionais da área atuam nas seguintes funções:

a) **Atendente**: recebe ou realiza as chamadas, estando diretamente em contato com o público;
b) **psicólogo**: responsável em reduzir o estresse e a tensão gerados pelo ambiente de trabalho e pelos clientes;
c) **roteirista**: cria o *script* que será seguido pelos atendentes;
d) **técnico de *database***: alimenta o sistema de *call center* com dados dos clientes;
e) **analista de suporte**: deve manter maior disponibilidade do serviço, superando eventuais problemas;
f) ***controller***: monitora os resultados;
g) **assessor de logística**: mantém integradas as áreas da organização, com o objetivo de evitar procedimentos conflitantes;
h) **gerente de projetos**: conhece o negócio e deve atingir os objetivos estabelecidos dentro do prazo e custo estabelecidos junto com a direção;
i) **facilitador**: deve manter os funcionários motivados, evitar ruídos na comunicação permitindo que todos os procedimentos da operação fluam de forma harmônica.

3.2 CLASSIFICAÇÃO

Segundo Mancini (2006), o *call center*, por estar presente nos mais diversos segmentos econômicos, pode ser classificado por diversos critérios, tais como:

a) **Setor econômico**: pode ser setor público ou privado. No setor privado, usam-se as centrais de atendimento para solidificar a imagem da empresa, enquanto no setor público, por exemplo, usa-se para comunicar uma emergência policial ou médica;
b) **ponto de origem do contato**: ligações efetuadas a partir da empresa são consideradas ativas e ligações realizadas pelo cliente são consideradas receptivas; ligações ativas geralmente são efetuadas por cobrança e ações de pós-vendas, enquanto ligações receptivas são, geralmente, de quem busca informações.
c) **serviços oferecidos**;
d) **constituição da empresa**: a classificação é realizada em função do porte, faturamento ou pelo número de postos de atendimentos.
e) **sistema adotado**: é classificado como "*in house*" se o *call center* for um setor da organização, que presta serviços e atende as demandas da organização. Se a organização terceiriza o serviço, ela pode ser classificada como terceirização total, parcial ou mista. Cada uma tem suas particularidades, vantagens e desvantagens, porém a melhor opção é aquela que se adapta ao negócio.

3.3 SERVIÇOS

Segundo ITIL V3 (Information Technology Infrastructure Library) (2011), um serviço é uma forma de criar valor aos clientes, facilitando o alcance dos objetivos, sem ter que assumir custos e riscos indesejados.

Mancini (2006) indica que os principais serviços realizados por um *call center* são:

a) **SAC**: tem a missão de funcionar como ponte entre a empresa e o público e auxiliar na fidelização do cliente;

b) **0800**: são disponibilizados de forma gratuita, para, geralmente, responder a perguntas frequentes por um sistema já automatizado;
c) **pesquisa**: por meio das ligações, realiza pesquisas mais rápidas e baratas, pois não é necessária uma equipe em campo coletando dados;
d) **pré-agendamento**: auxilia na administração do tempo, minimizando transtornos de horas em ligações para agendamentos. Confirmando algumas informações básicas, agenda-se uma visita com determinada pessoa, reduzindo o desgaste da equipe e melhorando o desempenho no fechamento de negócios;
e) **ações promocionais *one-to-one***: são realizadas ligações para uma lista de possíveis clientes com um código chamado "*key number*". Este é utilizado para uma conversação personalizada facilitando e otimizando o fechamento do negócio;
f) **propaganda**: utilizada para motivar um cliente em potencial a experimentar um produto ou serviço.

3.4 ESTRUTURA TECNOLÓGICA

Segundo Mancini (2006), CRM (*Customer Relationship Management*) é a ferramenta que fornece velocidade e qualidade às informações, integrando todas as áreas da empresa e suas bases de dados. O CRM é utilizado para administrar os contatos com o público-alvo, mantendo-o sempre fiel às informações, com o intuito de tornar a operação lucrativa.

Com essa ferramenta, é possível atender de forma personalizada os clientes da organização, aumentando a probabilidade de um retorno positivo.

Por fim, os objetivos são melhorar o relacionamento com o público, otimizar os serviços prestados, reduzir o tempo de espera em filas, proporcionar, por telefone, um atendimento sem risco, com segurança e que faça parte do dia a dia do público.

3.5 RISCOS EM *CALL CENTER*

Riscos em *call center* vão muito além das vulnerabilidades tecnológicas. Segundo Silva (2015), também afetam a saúde e a integridade física do operador de *call center,* como, por exemplo, os riscos físicos (consequência da digitação repetida e pela mobília desconfortável, que abrange também distúrbios osteomusculares. Há também riscos de

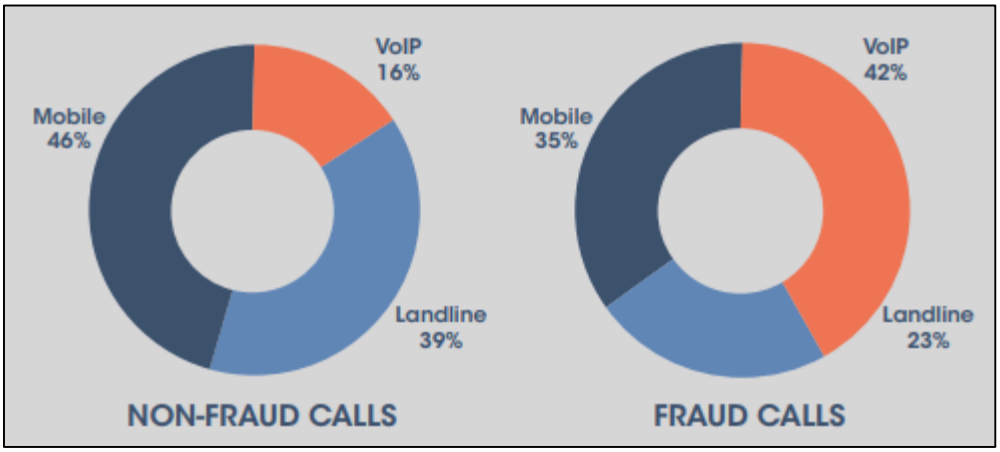
acúmulo de gordura no abdômen, devido à má postura do operador e à proibição de saída do posto de trabalho) e emocionais (estão relacionados às cargas emocionais e mentais que são superiores ao normal. Ansiedade e insegurança são alguns dos males que o operador pode vir a adquirir, bem como síndrome do pânico e depressão).

Não desprezando os riscos à saúde dos operadores, deve-se considerar que os riscos em função da vulnerabilidade tecnológica também impactam no negócio da organização.

Segundo pesquisa da Pindrop (2016), no ano de 2015, uma a cada 2000 ligações eram fraude, o que corresponde a um aumento de 45% em relação a 2013, em que tais ligações correspondiam a uma de cada 2.900.

A mesma pesquisa informa que, das ligações analisadas como fraude, 42% tinham origem em VoIP, 35% em celulares e 23% em telefones fixos. Das ligações não fraudulentas, 46% eram originadas de celulares, 39% de telefones fixos, e 16% de VoIP (Figura 15).

Figura 15 – Armas dos fraudadores



Fonte: Pindrop (2016).

A pesquisa também informa que os *call centers* possuem diversas vulnerabilidades que atraem o fraudador, tais como:

a) **IVR (Resposta Iterativa de Voz)**: foram identificadas repetições de PIN (*Personal Identification Number*) e chamadas extremamente longas que sugerem uma fraude de IVR;

b) **Elemento humano**: *call centers* nos quais o atendimento é feito por operadores reais correm alto risco de ataques em virtude da engenharia social;

c) **ID do chamador**: fraudadores conseguem alterar o número de origem da chamada com facilidade, o que pode ser um requisito para a fraude;

Autenticação baseada no conhecimento: devido à grande quantidade de informações disponíveis no mercado negro, fraudadores podem facilmente encontrar a resposta correta para a autenticação.

Conforme outra pesquisa, desta vez elaborada pela Dtex Systems (2016), os maiores riscos em um *call center* são os internos, os quais são compreendidos por:

a) **Acesso dos colaboradores às informações pessoais dos clientes**: colaboradores do *call center* têm acesso direto a informações confidenciais do cliente. Em virtude disso, os gestores devem estar cientes do que acontece nesse ramo do negócio para se precaver de furtos de tais informações;

b) **Colaboradores são de baixa renda ou é o primeiro emprego**: por não verem o *call center* como uma carreira de longo prazo e serem de renda mais baixa, são mais propensos a venderem ou usarem informações dos clientes;

c) **Elevada taxa de rotatividade**: esse fator faz com que a organização esteja constantemente exposta ao risco de furto de informações.

Segundo Upton e Creese (2014), os funcionários, em virtude da facilidade de acesso à informação, causam maiores riscos à organização do que ataques externos. Empregados que utilizam dispositivos pessoais para o trabalho aumentam consideravelmente o risco de exposição da informação. Os autores citam, em pesquisa desenvolvida pela Alcatel-Lucent, que cerca de 11,6 milhões de dispositivos móveis em todo o mundo podem ser infectados a qualquer momento, e as infecções por *malware* em celulares aumentaram 20% em 2013.

Ainda para Upton e Creese (2014), outra vulnerabilidade é decorrente do acesso às redes e mídias sociais, que, se não usadas adequadamente pelos colaboradores, podem expor informações, muitas vezes sem o conhecimento da empresa.

Kitten (2013) ressalta que, em serviços bancários, o atendimento via telefone é o meio mais fácil de causar uma fraude, e, por este motivo, é esperado um aumento na fraude de *call center* dos bancos. O autor cita também que o modo de ataque é DDoS [*denial-of-service*], em que os fraudadores fazem séries de ligações fingindo ser o cliente, causando interrupções no serviço e, usando números não identificáveis, solicitam informações de saldo de contas.

Para Urrico (2015), a fraude de *call center* está ligada à engenharia social. Isso ocorre pelo fato de que os fraudadores são melhores do que os operadores de *call center*

em identificar a fraude, ou seja, estes conseguem manipular as pessoas para que executem atividades tais como divulgar informações confidenciais.

Para Papanicolaou (2016), as organizações estão buscando terceirizar o serviço de *call center,* porém esse modelo as preocupa em relação à exposição de dados e informações, visto que muitas delas são confidenciais. Os riscos de terceirização incluem a engenharia social, em que os colaboradores podem querer se beneficiar com o uso das informações com as quais lidam diariamente. O autor apresenta algumas sugestões de como um *call center* pode proteger as informações dos clientes, como, por exemplo, seguir um protocolo de perguntas de segurança, restringir o acesso a pessoas autorizadas, possuir diversas camadas de proteção antes de chegar ao arquivo e aplicar políticas de senhas fortes.

Por fim, Bryars (2015) faz uma observação importante sobre as ligações gravadas pelos *call centers.* Como as gravações podem conter informações confidenciais, existe o risco de acesso e divulgação das informações em todo o ciclo de vida da informação, desde o período em que ela é gravada até o momento de seu descarte. O autor informa que uma forma de mitigar o risco é trancar fisicamente todas as gravações arquivadas. No entanto, considera que esta não é uma solução prática. Outra saída é fazer cópia das ligações e armazenar os arquivos em nuvem privada, descartando as mídias físicas originais.

3.6 CONSIDERAÇÕES FINAIS

De acordo com as informações coletadas e apresentadas nesse capítulo, é possível afirmar que o *call center* é um modelo de negócio que apresenta diversas vantagens, pois é adaptável a diversos tipos de serviços, em virtude de todas as atividades que ele pode exercer. Pelo fato de estar nos diversos segmentos de negócio, pode ser classificado por diversos critérios.

O *call center* apresenta uma flexibilidade em relação aos profissionais envolvidos, visto que não é necessária a utilização de todos profissionais citados para se obter resultados positivos, e sim montar uma equipe que seja mais produtiva para negócio.

O CRM é o *software* que controla todas as informações dos clientes, o que mantém a precisão da informação. Dessa forma, é a principal ferramenta de trabalho de um *call center*.

Neste capítulo foi evidenciado que os riscos envolvidos são tanto físicos e mentais quanto tecnológicos. Uma das principais fontes de ameaças é a engenharia social, cujos próprios colaboradores da organização, por serem usuários com acessos privilegiados às

informações da organização, podem se aproveitar delas de alguma forma para obter benefícios. Em virtude dessa situação, qualquer pessoa que tiver contato direto com as informações da organização apresenta risco para a mesma.

Visto que ameaças internas são o principal risco, alguns autores citam como modo de prevenção manter o acesso restrito a conteúdos confidenciais, o que dificulta ataques internos. Outro modo de prevenção é a utilização de antivírus e *firewall* para evitar ataques cibernéticos derivados do crescimento da *IoT.* Muitas organizações permitem a utilização de dispositivos móveis para exercer funções corporativas e estes, por sua vez, não apresentam segurança alguma, já que a maioria não tem *software* de antivírus.

A falta de controle do que trafega na rede expõe a empresa a ataques externos, tais como roubo de propriedade intelectual e de informações de clientes, bem como vazamento de informações confidenciais. A falta de conscientização dos usuários é outro fator que pode causar riscos à organização. Por exemplo, se o usuário não é instruído a alterar a senha com frequência, a organização ficará vulnerável a ataques cibernéticos.

Para reduzir as vulnerabilidades, utiliza-se como referência a norma ABNT NBR ISO/IEC 27002 (2013). A norma auxilia as organizações a identificar, analisar e controlar os riscos, para que, quando um incidente de segurança ocorrer, ele seja percebido imediatamente e uma ação seja elaborada para contornar a situação de risco. A implementação de uma PSI não inibe todos os riscos das organizações, mas, com a aplicação dessa política, as organizações se tornam menos vulneráveis.

Foi elaborada uma tabela genérica para identificar como os itens da norma 27002 podem ser aplicados em empresas de *call center.* Por ser uma tabela genérica, não é descartada nenhuma seção de controle, mas sim, apresentado onde cada seção pode ser aplicada em um *call center*. Com essa relação, foi possível identificar de que forma as seções de controle servirão de base para montar as normas de dimensão.

O Quadro 6 apresenta as normas de dimensões e sua aplicabilidade em um *call center*.

Quadro 6 – Aderência do *call center* à norma 27002

(continua)

Controle 27002	Call center
Políticas de segurança da informação	A direção do call center deve apoiar a segurança da informação, visando sempre ao bem do negócio.
Organização da segurança da informação	O Call center deve definir as responsabilidades de cada colaborador responsável pela política, com o objetivo de estabelecer uma estrutura de gerenciamento, seja na implementação da PSI ou dos controles.

(continua)

Segurança em recursos humanos	O RH da organização deve avaliar o histórico dos candidatos à vaga, visto que as informações a serem acessadas no call center são confidenciais.
Gestão de ativos	Deve ser aplicada em um call center, com a intenção de identificar os ativos da organização e métodos para proteção dos ativos, assegurando que os estes recebam níveis adequados de proteção, prevenindo a divulgação não autorizada, modificação e/ou remoção das informações.
Controle de acesso	Devido ao fato da alta rotatividade em um call center, o limite de acesso deve ser mantido, garantindo, assim, maior segurança nos dados e informações da organização.
Criptografia	Pelo fato de se lidar com informações pessoais de clientes, a criptografia em um call center tem o objetivo de assegurar e proteger a confidencialidade, autenticidade e/ou a integridade da informação.
Segurança física e do ambiente	Deve oferecer prevenção do acesso não autorizado em locais onde as informações são criadas e manipuladas, além de perdas, danos, furto ou roubo dos ativos, bem como de toda atividade que possa causar interrupção das operações.
Segurança nas operações	operacionais, como, por exemplo, de que forma manipular as informações, manter cópias de segurança e configurar sistemas.
Segurança nas comunicações	Deve garantir a proteção das informações em redes, além de instruir os colaboradores a transferir informações seguindo as diretrizes da política de segurança da organização.
Aquisição, desenvolvimento e manutenção de sistemas	Deve assegurar que os *softwares* utilizados preservem os dados. Se terceirizado, definir um bom acordo de nível de serviço para manter sempre a alta disponibilidade e contratos de confidencialidade.
Relacionamento na cadeia de suprimento	O *call center* tem como foco a cobrança, por isso, normalmente, fazem *outsourcing* de impressão, ou do setor de TI. Em virtude das terceirizações, uma política deve ser desenvolvida para tratar somente do acesso do fornecedor às informações da organização.
Gestão de incidentes de segurança da informação	O *call center* deve manter procedimentos rápidos e efetivos para os incidentes de segurança de informação. Um exemplo são os *softwares* de monitoramento que auxiliam a gerenciar a rede. Constatada alguma irregularidade, procedimentos de detecção e análise são efetuados na hora.

(Conclusão)

Aspectos da segurança da informação na gestão da continuidade do negócio	Como o *call center* é um negócio que funciona de forma 24x7, ou seja, 24 horas, 7 dias por semana, a disponibilidade das informações deve ser assegurada, principalmente no CRM do *call center*, mantendo a sua operacionalidade.
Conformidade	Garantir que tudo que envolve a segurança de informação não seja violado.

Fonte: elaborado pelo autor (2017). (conclusão)

4 PROPOSTA DE SOLUÇÃO

Baseado na análise de riscos efetuada na empresa BETA, o presente capítulo apresenta a proposta de uma Política de Segurança da Informação (PSI) a ser implantada na empresa e como essa política é avaliada. Para desenvolver a PSI, foram analisadas as normas da série 27000 (Quadro 7) e os documentos referentes à análise de risco efetuada.

Quadro 7 – Normas da família 27000 utilizadas

Norma	**Utilizada para**
27001	Compreender e ter uma visão geral de como é possível elaborar um SGSI em uma organização.
27002	Compreender como é efetuada a seleção e implementação dos controles.
27003	Compreender detalhadamente cada etapa da implantação de um SGSI e os documentos gerados em cada uma dessas etapas.
27004	Elaborar os modelos de medição de eficácia dos controles implantados na organização.
27005	Servir como guia para a realização da gestão de riscos da organização.

Fonte: Elaborado pelo Autor (2018).

A seção 4.1 apresenta a Empresa BETA, informando o modelo de organograma utilizado pela organização, seu tempo de mercado e a classificação da organização perante seu faturamento.

A seção 4.2 apresenta todo o processo de análise de riscos e como o mesmo foi elaborado para a empresa BETA, desde a concepção da ideia, passando pela definição do escopo, a análise a ser efetuada, assim como todas identificações necessárias para uma boa gestão de riscos da empresa.

A subseção 4.2.1 teve por objetivo dar início a gestão de riscos da organização e apresenta como foi efetuado o processo de identificação dos ativos, a forma de divisão dos mesmo e como cada um se enquadra em cada categoria na organização, no escopo abrangido.

A subseção 4.2.2 apresenta a etapa de identificação das ameaças, como foi elaborada a coleta de dados, como foi classificada toda a informação obtida nesta etapa, desde o tipo de ameaça, sua fonte e a qual ativo essa ameaça estava relacionada. É apresentado um quadro-exemplo para uma melhor compreensão dos dados obtidos e como ficou a distribuição da origem e dos tipos de ameaças por grupos de ativos.

A subseção 4.2.3 informa como foi desenvolvido o processo de identificação dos controles da organização, ou seja, quais os mecanismos de segurança que a empresa já tinha, para evitar os riscos. Apresenta, também, um quadro para melhor compreensão de como foram coletados os dados para apresentação aos interessados. Além disso, há um quadro para melhor entendimento de como estão divididos os controles pelos grupos de ativos desenvolvidos na subseção 4.2.1.

A subseção 4.2.4 apresenta o processo de identificação de vulnerabilidades, para o qual foram necessárias as três etapas anteriores a fim de relacioná-los entre si e elaborar um cenário de incidentes prováveis na organização. Um quadro foi elaborado para auxiliar na compreensão de como essa seção serviu para a organização se precaver durante o processo de gestão de riscos e das vulnerabilidades que estão sujeitas a serem exploradas pelas ameaças.

A subseção 4.2.5 salienta como foi elaborado o processo de identificar as consequências, além de apresentar qual diretriz foi utilizada para avaliar a probabilidade de uma ameaça acontecer e suas consequências. É apresentado um quadro-exemplo para facilitar a compreensão de como foi preenchido o quadro para esta atividade e como se deu a análise de riscos da organização em relação a todos os dados coletados nas etapas anteriores.

A seção 4.3 demonstra a estrutura da PSI e correlaciona os riscos identificados durante a pesquisa efetuada em *call center* às normas de dimensões utilizadas para controlá-los antes de refinar a política ao negócio e aos riscos encontrados na pesquisa.

A seção 4.4 evidencia os controles a serem utilizados para efetuar a medição e avaliação da eficácia da PSI na organização, além de apresentar o método de coleta de dados, em virtude de que cada controle tem suas métricas específicas para auxiliar no processo de medição. Apresenta, também, um quadro para auxiliar na compreensão do uso de cada métrica e função da medição em relação ao seu controle.

A seção 4.5 apresenta as considerações finais do capítulo, resumindo todos os assuntos abordados.

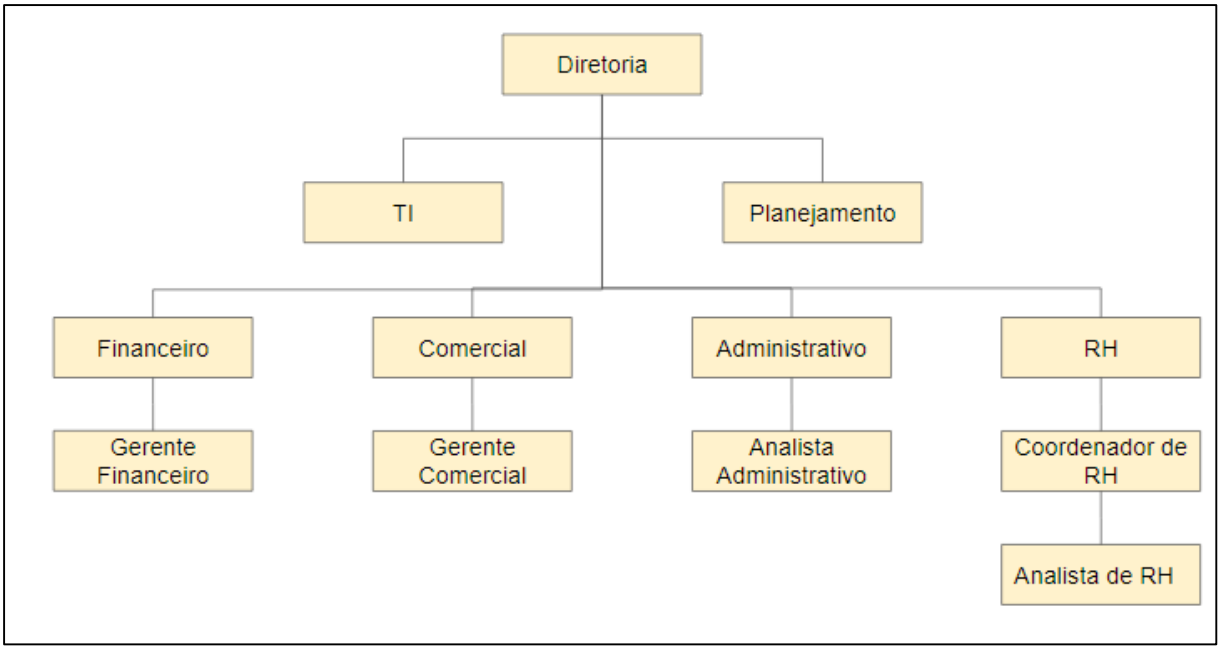
4.1 A EMPRESA BETA

A realização do estudo de caso ocorreu em uma empresa de médio porte[1] que atua no ramo de cobrança há mais de 30 anos. A empresa que, por motivos de confidencialidade, é denominada BETA, presta serviços no setor de cobranças.

Os negócios da empresa são baseados na cobrança de crédito e na venda de cursos para seus clientes. Entretanto, em 2016, a empresa identificou falhas de segurança em seu ambiente corporativo e também possíveis riscos, os quais, se não tratados, causariam problemas à organização.

Atualmente, a empresa possui um organograma linear *staff* (Figura 16), no qual o setor de TI está vinculado de forma direta à direção. A TI é responsável pela segurança da informação, infraestrutura, gerenciamento de rede e dos sistemas.

Figura 16 – Organograma da empresa BETA



Fonte: elaborada pelo autor (2017).

4.2 ANÁLISE DE RISCOS DA EMPRESA BETA

Para realizar a análise de risco da organização, o escopo dessa análise foi selecionado. Definiu-se que, inicialmente, o processo de operação do *call center* seria analisado, sendo esse processo um dos mais críticos da organização. Todas as informações

[1] Conforme classificação do BNDES, trata-se de uma organização com receita operacional bruta ou renda anual maior que R$ 3,6 milhões e menor ou igual a R$ 300 milhões.

de clientes são manipuladas, e *softwares* e *hardwares* que possibilitam disponibilidade integral do negócio são utilizados no processo de operação. Os demais processos da organização, tais como o de compras ou o de implantação de novos clientes, não foram selecionados por não serem o foco do negócio da empresa. É importante salientar que a implementação da Política de Segurança da Informação é um processo interativo e incremental. Após o processo de operação de *call center* ter sido implantado e estabilizado, novos processos poderão ser definidos e aplicados.

A análise de riscos realizada seguiu as boas práticas estabelecidas na norma 27005. Segundo a norma ABNT NBR ISO/IEC 27005 (2013), o processo de avaliação de riscos é o primeiro macroprocesso da gestão de riscos, e é composto pelas etapas de sua identificação, análise e avaliação (Figura 17).

Figura 17 – Processo de avaliação de risco

Fonte: ABNT NBR ISO/IEC 27005 (2013).

Para Stoneburner (2002), o processo de análise de riscos determina a abrangência das ameaças que envolvem a infraestrutura de TI. A norma ABNT NBR ISO/IEC 27005 (2013) informa que o processo de identificar o risco pode ser realizado pelas seguintes atividades (Figura 18):

a) **Identificação de ativos**: define os ativos de um processo da organização;

b) **identificação de ameaças**: detecta riscos que podem ser naturais (enchentes, terremotos, tempestades de raios, entre outros), intencionais (atos dolosos, negligentes, imprudentes, de uso de programas maliciosos, de acesso a dados sigilosos, de mau uso dos sistemas, entre outros) ou acidentais (falta de treinamento, entre outros);

c) **identificação dos controles**: define os controles que podem ser utilizados para reduzir ou eliminar riscos. Tem a função de avaliar os controles existentes ou planejados, com o objetivo de minimizar chances de uma ameaça explorar alguma vulnerabilidade;

d) **identificação de vulnerabilidades**: verifica as falhas nos processos de segurança;

e) **identificação de consequências**: identifica as consequências decorrentes de diversos cenários de incidentes, fruto das vulnerabilidades para a organização.

Figura 18 – Processo de identificação de risco

Fonte: ABNT NBR ISO/IEC 27005 (2013).

4.2.1 Identificação de ativos

O primeiro passo realizado, com o auxílio dos gestores da operação e da direção, foi a identificação e a classificação dos ativos tangíveis e intangíveis. Para realizar a identificação de ativos tangíveis, foi percorrido o ambiente em que se encontra a operação

de *call center*, bem como toda a infraestrutura que sustenta a atividade do escopo abrangido. Após percorrer esses ambientes, foi elaborado um inventário para quantificar os ativos de forma única, independentemente da quantidade. Para coletar informações referentes aos ativos intangíveis, foi realizada uma reunião com os diretores da organização, a fim de quantificar os processos e procedimentos chave que fazem o negócio ser rentável e que, se divulgados, prejudicariam a organização. Foram identificados vinte e um ativos que foram classificados e agrupados em cinco grupos: humano, *hardware, software*, intangíveis/inteligência e instalações físicas.

Os ativos humanos são representados pelos colaboradores que fazem o processo ter continuidade. Os de *hardware* e *software*, são compostos, respectivamente, pelos equipamentos ou elementos que sustentam os processos, e os que tratam das informações essenciais. Os ativos identificados como intangíveis/inteligência são representados por procedimentos secretos ou que, se interrompidos, causam prejuízo a organização. Por fim, os classificados em instalações físicas representam a infraestrutura na qual estão dispostos os ativos identificados.

A Tabela 1 apresenta um exemplo de como as informações coletadas foram construídas e preenchidas, no qual o ativo colaborador, por ser uma pessoa física, é contabilizado na coluna de ativos humanos. Computador e demais dispositivos, por serem *hardware*, encontram-se na coluna de *hardware*. A coluna de *software* é contabilizada a partir dos programas de computador que se fazem necessário para a operação de *call center* funcionar. O processo de cobrança, por ser um processo-chave do negócio, está listado na coluna de intangível/inteligência. Por sua vez, a parte de infraestrutura é contabilizada na coluna de instalações físicas.

Tabela 1 – Exemplo do quadro de identificação de ativo

Ativo	**Humanos**	***Hardware***	***Software***	**Intangível/ Inteligência**	**Instalações físicas**
Negociador de pessoa física	1				
Computador		1			
Software CRM			1		
Processo de cobrança				1	
Sala de servidores					1
Total	**1**	**1**	**1**	**1**	**1**

Fonte: elaborado pelo autor (2018).

4.2.2 Identificação de ameaças

Em conjunto com a direção e os gestores da operação, foi percorrido o setor da empresa onde foi definido o ambiente em análise da gestão de riscos, no qual as ameaças, que são eventos que se aproveitam das vulnerabilidades, com o objetivo de afetar os ativos da organização, foram identificadas e registradas.

Os tipos de ameaças foram classificados de acordo com sua fonte, podendo ser de origem interna (tais como colaboradores) e/ou externa (terceiros, por exemplo), e pela sua origem, podendo ser acidental (por falta de instrução para determinada tarefa), intencional (má fé de colaboradores), ou natural (sendo causadas por forças da natureza).

O exemplo apresentado na Tabela 1 explana como foram organizadas as informações coletadas nesta etapa. Os dados da coluna representada pelos ativos foram coletados na etapa de identificação dos mesmos. A coluna de ameaça representa ações que podem explorar as vulnerabilidades. Por fim, há uma coluna que representa o tipo e outra, a fonte da ameaça.

No exemplo do Quadro 8, para o ativo servidores, foi definido um cenário de incidente: o furto de dados como ameaça, que, por sua vez, ocorre de forma intencional e pode ser praticado tanto pelos colaboradores quanto por terceiros.

Quadro 8 – Exemplo do quadro de identificação de ameaça

Ativo	**Ameaça**	**Tipo**	**Fonte da ameaça**
Servidores	Furto de dados	Intencional	Interna/externa

Fonte: elaborado pelo autor (2018).

Após realizar o levantamento dos ativos na organização e da sua respectiva fonte de ameaças, foi elaborada uma tabela (Tabela 2) que expõe como ficou a distribuição destas em relação ao grupo de ativos. Contabilizando, é possível concluir que foram encontradas vinte e sete ameaças na organização. É possível destacar o grupo de ativos de *hardware* como o que obteve a maior quantidade de ameaças.

Tabela 2 – Distribuição das ameaças por grupos de ativos

Tipo de ameaça/ativo	**Humanos**	***Hardware***	***Software***	**Intangível/ Inteligência**	**Instalações físicas**
Interna/externa	1	1	1	2	2
Interna	3	7	6	2	1
Externa	-	1	-	-	-
Total	**4**	**9**	**7**	**4**	**3**

Fonte: elaborada pelo autor (2017).

Em relação às origens das ameaças, os ativos do grupo *Hardware* apresentam, na sua totalidade, a maior quantidade de ameaças, sendo a origem acidental o maior agravante, conforme apresentado na Tabela 3.

Tabela 3 – Distribuição da origem das ameaças por grupos de ativos

Origem da ameaça/ativo	**Humanos**	***Hardware***	***Software***	**Intangível/ Inteligência**	**Instalações Físicas**
Acidental	3	6	-	2	2
Acidental/Natural	-	-	-	-	1
Acidental/Intencional	-	-	-	-	-
Acidental/Intencional/Natural	-	-	-	-	-
Intencional	2	-	1	2	-
Intencional/Natural	-	-	-	-	-
Natural	-	1	1	-	-
Total	**5**	**7**	**2**	**4**	**3**

Fonte: elaborada pelo autor (2017).

4.2.3 Identificação de controles

Ao adentrar a terceira etapa do processo de identificação de risco, foi verificado quais mecanismos de segurança já estão implementados para cada grupo de ativos. Os controles foram classificados entre: existentes, se já estão em atividade na organização; planejados, se têm prazo para a implantação do controle, e; que necessitam revisão, se devem ser melhorados ou atualizados. Com os dados encontrados, foi elaborado um quadro, semelhante ao exemplo apresentado na Tabela 4.

Foi criada uma coluna com os ativos encontrados no processo de identificação de ativos, e, para tal, os mecanismos que auxiliam a diminuir ou eliminar a probabilidade de uma ameaça explorar uma vulnerabilidade vinculada a esse ativo.

Tabela 4 – Exemplo do quadro de identificação de distribuição de controles

Ativos	Controle	Existente	Planejado	Necessita revisão
Desktop	Antivírus	X		Atualizar antivírus
Sala de servidores	Câmera de segurança	X		
	Piso elevado		X	Em andamento
	Controle de acesso		X	Projeção para o ano de 2019
Servidor	*Firewall*	X		
Total	**5**	**3**	**2**	

Fonte: elaborado pelo autor (2018).

Como é possível observar no exemplo da Tabela 4, para o ativo *desktop*, utiliza-se um antivírus como forma de diminuir a probabilidade de determinada ameaça explorar alguma vulnerabilidade. Nesse caso, é possível destacar que o antivírus é um controle que tem o objetivo de diminuir ameaças de que *malwares* furtem dados da empresa. A mesma lógica se aplica aos demais ativos, sempre visando eliminar ou reduzir os riscos à organização. Essa tarefa teve por objetivo identificar se os controles existentes estão funcionando, ou se é necessária alguma ação para sua melhor utilização.

A Tabela 5 apresenta o resultado do levantamento de dados.

Tabela 5 – Distribuição de controles por grupos de ativos

Ativos/Controles	Existente	Planejado	Necessita revisão
Humano	3	3	-
Hardware	7	2	-
Software	5	11	3
Intangível/Inteligência	1	7	-
Instalações Físicas	3	-	-
Total	**19**	**23**	**-**

Fonte: elaborada pelo autor (2017).

Foram encontrados dezenove controles existentes, sendo a maior parte para o grupo de *hardware*, e vinte e três planejados, sendo a sua maioria para o grupo *software*. Dessa

forma, com o somatório dos controles existentes e planejados para cada vulnerabilidade encontrada, é possível concluir que foram identificadas quarenta e duas vulnerabilidades.

4.2.4 Identificação das vulnerabilidades

Para fazer o levantamento das vulnerabilidades na empresa BETA, foi percorrido o escopo da análise da gestão de riscos, mapeando e catalogando as falhas encontradas e reportando os resultados obtidos nessa análise em um relatório. Com as informações obtidas, foi possível criar uma lista de cenários de incidentes, que relaciona os ativos identificados, as ameaças encontradas e controles existentes na organização, para detectar as vulnerabilidades e como elas podem afetar os ativos, caso sejam exploradas. Essa lista permitiu construir uma imagem do estado real de exposição dos ativos aos riscos, a fim de que estes sejam tratados, com o objetivo de garantir maior segurança à organização.

O Quadro 9 exemplifica como foram distribuídas as informações coletadas nessa etapa. A coluna representada pelos ativos é responsável por apresentar os ativos coletados na etapa de identificação destes. Uma coluna denominada vulnerabilidade representa as fraquezas que possam ser exploradas e comprometer os ativos da organização. A coluna de ameaça apresenta a possibilidade de algum agente, proposital ou não, se beneficiar de uma vulnerabilidade, que, nesse caso é representada pelo furto de dados. Por fim, a coluna controles, representa os controles existentes na organização para reduzir ou evitar as ameaças referente ao ativo em análise.

Quadro 9 – Exemplo do quadro de identificação de vulnerabilidades

Ativo	Vulnerabilidade	Ameaça	Controles
Servidores	Invasão remota e acesso indevido por atribuição incorreta de direitos e permissões.	Furto de dados.	*Firewall* e política de classificação da informação.
Estrutura elétrica	Rede elétrica instável.	Interrupção do suprimento de energia.	*No-breaks*.

Fonte: elaborado pelo autor (2018).

Como é possível analisar no exemplo do Quadro 9, para o ativo *servidores* foram definidos, a partir de uma lista de cenários de incidente, a invasão remota e o acesso

indevido por atribuição incorreta de direitos e permissões, sendo ambas fragilidades a serem exploradas. Além disso, foi determinado qual (ou quais) ameaça(s) pode(m) explorar essas vulnerabilidades. Nesse caso, foi estipulado o furto de dados. No presente exemplo, para evitar que essas ameaças afetem o ativo para esta vulnerabilidade, um *firewall* e uma política de classificação de informação são formas de controles existentes que visam evitar ou reduzir as ameaças.

O mesmo vale para o segundo ativo, representado pela estrutura elétrica, já que a interrupção do suprimento de energia pode ser uma fragilidade a ser explorada. Como controle, a utilização de *no-breaks* pode evitar ou reduzir essa ameaça. Vale ressaltar que uma mesma ameaça pode afetar mais de um ativo de diferentes formas. Se, por acaso, não existe controle para um determinado risco, ações devem ser tomadas para evitá-la ou reduzi-la.

A Tabela 6 apresenta os totais de vulnerabilidades e ameaças encontradas.

Tabela 6 – Totais de vulnerabilidades e ameaças encontradas

Ativos	Vulnerabilidades	Ameaças
Humano	6	4
Hardware	9	9
Software	16	7
Intangível/Inteligência	8	4º
Instalações Físicas	3	3
Total	**42**	**27**

Fonte: elaborado pelo autor (2018).

4.2.5 Identificação de consequências

Esta atividade teve por objetivo identificar os prejuízos que a organização pode sofrer. Para avaliar as consequências, foi utilizada a lista de cenários de incidentes. Como resultado desta atividade, foi construído o Quadro 10.

No exemplo, para o ativo de infraestrutura, foram elencados diversos cenários de incidentes tais como: falha no sistema de refrigeração, tentativas não autorizadas de acesso à sala de infraestrutura, entre outros incidentes, e, para cada um, a consequência correspondente. Dessa forma, obteve-se, para o primeiro exemplo, perda de equipamentos devido ao aquecimento e, para o segundo, furto de dados, divulgação indevida de informação, entre outros. Um incidente pode apresentar diversas consequências, conforme

apresentado no primeiro ativo do Quadro 10. Cada incidente recebeu um valor qualitativo para as informações de probabilidade e impacto, e baseado nas diretrizes da NIST SP 800-30, o valor quantitativo do risco foi definido.

Quadro 10 – Exemplo do quadro de identificação de consequências

Ativos afetados	**Incidente**	**Consequência**	**Probabilidade**	**Impacto**	**Risco**
Operadores	Utilização da informação por má fé	Divulgação indevida	Baixa	Alto	4
		Comprometimento da informação	Média	Médio	4
Servidores	Inexistência de backup	Perda de informações	Baixa	Alto	4
	Invasão remota	Comprometimento da informação	Baixa	Alto	4
Software CRM	Falta de versionamento	Desorganização do histórico de mudanças	Média	Alto	5
Infraestrutura	Falha no sistema de refrigeração	Perda de equipamentos devido ao aquecimento	Baixa	Alto	4

Fonte: elaborado pelo autor (2018).

No levantamento de dados para esta etapa, foram identificadas trinta e três consequências e dezessete incidentes. A maior parte está concentrada nos grupos de ativos humanos, *hardware* e *software*. As principais consequências causadas pelos ativos humanos estão relacionadas à perda de dados e informações, em virtude da engenharia social. Já as que estão relacionadas aos ativos de *hardware e software* são voltadas à questão financeira, por falta de operacionalidade e, também, perdas de informação.

Para avaliar a probabilidade de uma ameaça ocorrer e suas consequências (impactos), foram utilizadas as diretrizes da NIST SP 800-30 (NIST SP 800-30, 2002), já que a ABNT NBR 27005 não estabelece como esses itens devem ser medidos. A NIST SP 800-30 utiliza como critérios de probabilidade e impacto os valores qualitativos alto, médio e baixo (Quadro 11).

Quadro 11 – Matriz de probabilidade *versus* impacto

Probabilidade/ impacto	**Alto**	**Médio**	**Baixo**
Alto	Alto	Alto	Médio
Médio	Alto	Médio	Baixo
Baixo	Médio	Baixo	Baixo

Fonte: NIST SP 800-30 (2002).

Pela NIST SP 800-30, as probabilidades são classificadas como: a) alta: ameaça altamente capaz de explorar uma vulnerabilidade para a qual os controles forem eficazes; b) média: ameaça suficiente para explorar uma vulnerabilidade, mas os controles podem impedir sua ação com sucesso; e c) baixa: ameaça incapaz de explorar uma vulnerabilidade para a qual os controles forem eficazes. O impacto, por sua vez, é classificado como: a) alto: gera perdas de recursos ou ativos, com custo bastante elevado; prejudica ou impede a missão da organização, ou; causa danos a pessoas; b) médio: gera perda do recurso ou ativo, apresentando custo elevado; prejudica ou impede a missão da organização, ou; causa danos físicos a pessoas; c) baixo: perda do recurso ou ativo gera um custo razoável e afeta a missão da organização.

Após o desenvolvimento de todas as etapas do processo de identificação dos riscos, é possível estimar o nível de riscos da organização BETA. Para desenvolver essa estimativa, foi utilizada uma abordagem qualitativa definida na norma ABNT NBR 27005. Essa abordagem faz uso de uma matriz que relaciona a probabilidade de um incidente ao impacto relacionado, utilizando valores pré-definidos que variam de 0 a 8 (Figura 19). Cabe ressaltar que, dependendo da necessidade da organização, as classificações podem ser mais detalhadas.

Figura 19 – Matriz de riscos com valores pré-definidos

	Probabilidade do cenário de incidente	Muito baixa (Muito improvável)	Baixa (Improvável)	Média (Possível)	Alta (Provável)	Muito Alta (Freqüente)
Impacto ao Negócio	Muito Baixo	0	1	2	3	4
	Baixo	1	2	3	4	5
	Médio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muito Alto	4	5	6	7	8

Fonte: ABNT NBR ISO/IEC 27005 (2013).

Para a empresa BETA foi encontrada uma média de aproximadamente nove vulnerabilidades para cada grupo de ativos. A maior quantidade foi encontrada no grupo *software*, entretanto, proporcionalmente, foi o grupo humano apresentou vulnerabilidades maior medida. A Tabela 7 apresenta o resultado da estimativa de risco. A empresa BETA

definiu que os riscos de valores entre 0 a 3 são de menor risco e os de 4 a 6 são de maior de risco.

Tabela 7 – Resultado da análise de riscos da empresa BETA

Ativo	Número de ativos analisados	Número de vulnerabilidades	Nível de risco	
			Maior	Menor
Humano	1	7	6	1
Hardware	9	9	4	5
Software	7	16	11	5
Intangível/Inteligência	1	8	6	2
Instalações físicas	3	3	3	-

Fonte: elaborada pelo autor (2017).

Com base nos dados coletados, é possível identificar que a concentração de ameaças está grupo de ativos de *hardware* e são do tipo interna e de origem acidental.

A partir das informações coletadas, é notável que a organização precisa implementar normas internas para conscientizar e instruir todos os colaboradores a respeito de como lidar com as situações do trabalho que exercem, com a finalidade de manter os ativos da organização seguros. Vale ressaltar que os dados coletados estão apresentados de forma quantitativa, para não expor a organização na qual foi realizado o estudo de caso.

4.3 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A gestão de riscos realizada foi utilizada como subsídio para a criação da PSI. Para o desenvolvimento da PSI, foram criados o documento da política principal e as normas de dimensão. No documento de nível 1 da PSI, foram definidos os objetivos, o escopo, as definições, as regras, as responsabilidades e o cumprimento da PSI. Vale ressaltar que esse documento deve ter o apoio da direção e o comprometimento de todos colaboradores. A política principal elaborada para a empresa BETA tem a finalidade de nortear os seus colaboradores quanto ao uso dos ativos que a empresa disponibiliza para a execução do trabalho, além de instruir condutas que auxiliam na redução de riscos e ameaças, sendo um documento formal, que possui a contribuição direta da direção. O documento da política principal encontra-se no Apêndice A.

As normas de dimensão, por sua vez, complementam a política principal e definem regras e procedimentos para os colaboradores, referentes ao uso das ferramentas disponibilizadas pela organização, visando sempre à segurança da informação, além de ditar as responsabilidades dos gestores e colaboradores quanto ao uso dessas ferramentas. As normas de dimensão da empresa BETA foram criadas e basearam-se no estudo da norma ABNT NBR 27002, nos incidentes pesquisados e identificados no Capítulo 3 e na gestão de riscos realizada na empresa (Tabela 5). As normas de dimensão elaboradas foram:

a) **Controle dos contatos telefônicos**: tem por finalidade instruir o colaborador a não passar informações confidenciais da organização para terceiros via telefone;
b) **Política de senhas**: tem por objetivo orientar o colaborador a não compartilhar suas senhas nos sistemas da empresa, visto que cada colaborador tem acessos diferentes a informações diferentes. Política desenvolvida visando à integridade, disponibilidade e confidencialidade dos dados;
c) **Segurança nas operações**: trata das atitudes dos colaboradores na operação da sua atividade, bem como instruções sobre como lidar com a infraestrutura que a empresa fornece, a fim de manter a integridade, a disponibilidade e a confidencialidade das informações;
d) **Política de uso da *Internet***: tem a finalidade de instruir o colaborador a utilizar a *Internet* somente para fins corporativos, evitando divulgação indevida dos dados;
e) **Política de uso de *e-mail***: tem o intuito de orientar os colaboradores quanto às melhores maneiras de usar a ferramenta disponibilizada pela organização, evitando que sejam enviadas informações indevidas para terceiros;
f) **Política de classificação da informação**: tem por objetivo manter as informações disponíveis somente para quem deve ter acesso a elas.

O texto completo das normas de dimensão desenvolvidas para a empresa BETA encontra-se no Apêndice B. O Quadro 12 resume as normas de dimensão desenvolvidas, relacionando-as com os incidentes de segurança levantados na análise de riscos da empresa.

Quadro 12 – Relação das pesquisas *versus* normas da dimensão

(continua)

Incidente	Normas da dimensão
Perda de informações confidenciais	Política de Segurança nas Operações
Roubo de propriedade intelectual	Política de Controle de Acesso Físico
Vírus ou ataques cibernéticos	Política de Segurança nas Operações

(conclusão)

Dispositivos pessoais	Política para uso de Dispositivos Portáteis e Dispositivos Móveis
Comprometimento de registros de clientes	Política de Segurança da Informação
Falta de normas internas	Política Norma de Segurança Física
Senhas	Política de Controle de Acesso Lógico
Redes Sociais	Política de uso da *Internet*
Furtos	Política de Controle de Acesso Físico
VOIP	Política de Segurança da Informação
Terceirização	Política de Controle de Acesso Físico
Vazamento de informações confidenciais	Política de Segurança nas Operações
Perda de propriedade intelectual	Política de Controle de Acesso Físico

Fonte: elaborado pelo autor (2017).

A análise de riscos, a política principal e as normas de dimensão foram apresentadas aos gestores da empresa BETA, com a finalidade de definir quais itens das normas de dimensão seriam aplicadas na organização. A direção da empresa decidiu inicialmente tratar, na PSI, os riscos que julgou prioritários. Os gestores sugeriram algumas alterações e melhorias na PSI, com o objetivo de adequá-la à realidade do negócio e torná-la mais eficiente e prática. Também foi levado em consideração, na decisão, quais controles a empresa tem a real capacidade de implementar, em virtude de sua maturidade no quesito segurança de informação. Novos documentos foram gerados, baseados na decisão da direção. Esses documentos encontram-se nos Apêndices D (política principal) e E (normas de dimensão).

Algumas alterações se fizeram necessárias nas propostas dos controles para dar maior viabilidade de implementação. Para todos os controles, a frequência de coleta da informação foi alterada. Para os controles de processamento ilegal de dados via *e-mail* e *Internet*, a forma de coleta dos dados se dá por um *software* terceirizado denominado NAC 3.

4.4 AVALIAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Durante o processo de aprovação da PSI, foi estruturado o modelo de avaliar e medir a eficácia da política, portanto, durante sua implementação na organização, o processo de avaliação dos controles ocorria simultaneamente. As medições foram definidas de acordo com a norma NBR ISO/IEC 27004 (2010) e toda sua estrutura está definida no Apêndice F.

Os controles desenvolvidos serviram para medir a eficiência da PSI. Para tanto, foi desenvolvido um controle que se baseia na escuta das ligações pelo setor de monitoria. Esse setor já era responsável por acompanhar as ligações para fins de treinamento e auditoria. Quatro monitoras efetuam 15 escutas por dia, totalizando 60. Essas monitoras foram orientadas a registrar sempre que identificassem, nestas escutas, divulgação indevida de informação. Para tal, foi criado um indicador, que é a razão entre o número de ligações sem irregularidades e o número total de ligações escutadas. Se esse indicador estiver abaixo da meta estipulada serão tomadas medidas para reverter o quadro. Esse controle está diretamente relacionado ao risco de vazamento de informações confidenciais e é o único controle cuja medição não é feita pela equipe de TI ou por *software*.

Os controles de processamento de informações via *e-mail* e/ou *Internet* e a conscientização quanto à segurança nas operações também serviram como forma de avaliar a eficácia da PSI. O controle relacionado à conscientização de segurança nas operações está diretamente relacionado a todos os riscos causados pelas pessoas. Os demais controles citados estão diretamente relacionados aos riscos de vazamento de informações confidenciais, vírus ou ataques cibernéticos, falta de normas internas, riscos que as redes sociais podem causar, bem como aqueles referentes aos dispositivos móveis e aos terceiros que circulam na operação.

Para medir a eficiência da PSI por meio dos controles de processamento ilegal de informação via *e-mail* e *Internet*, se fez necessária a aquisição de um software, o NAC 3, e seus módulos complementares, para fazer a coleta dados, em virtude da sua complexidade e quantidade de informação. Com o software, foi possível coletar os dados necessários para avaliar a PSI. Ele foi responsável por contabilizar a quantidade irregularidades encontradas nos controles em que foi utilizado.

O controle de processamento ilegal de dados via *e-mail* funciona de forma que o *software* NAC 3 é parametrizado para que somente arquivos de determinada extensão em anexo possa ser encaminhado e, caso haja tentativa de envio de *e-mail* com demais extensões em anexo, o *e-mail* é encaminhado ao gestor da operação, para que sejam tomadas as devidas providências. O *software* NAC 3 contabiliza a quantidade de *e-mails* totais e barrados e, baseado no resultado da divisão dos primeiros pelos últimos, decisões são tomadas, caso não esteja no percentual de aceitação da direção.

Tratando-se do controle de processamentos ilegais de dados via *Internet*, o *software* NAC 3 busca analisar quais *sites* os colaboradores tentam acessar e barra o acesso àqueles que não sejam permitidos pela empresa. O registro do *site* tentado acessar pelo colaborador

é encaminhado ao gestor que tomará atitudes cabíveis. O *software* contabiliza a quantidade de *sites* totais e barrados, e baseado no resultado da divisão dos *sites* totais pelos barrados, ações serão tomadas, caso não entre no percentual de aceitação da direção.

O controle responsável pela conscientização dos operadores tem por objetivo treinar e instruir os colaboradores a respeito da importância de manter um ambiente seguro quando se trata das informações da empresa, com o objetivo de reduzir o risco de erro humano, instruindo quanto ao cumprimento das normas. Os colaboradores presentes devem assinar o documento de ciência da existência da PSI. Um cronograma foi montado em conjunto com o RH para não prejudicar o negócio.

O controle que é responsável pela classificação da informação tem por objetivo controlar os acessos aos arquivos da organização na rede, de modo que cada colaborador deve estar somente com as permissões referentes ao que é necessário para a execução do seu trabalho. Como a organização faz os controles de permissões e acessos pelo servidor *active directory* (AD), o colaborador só terá acesso a determinada pasta da rede, caso seu usuário esteja vinculado diretamente a esta pasta no AD. Esse controle se justifica em virtude de diversos remanejamentos entre os colaboradores, assim, deve-se atualizar suas permissões removendo as antigas e mantendo somente as atuais.

O controle de políticas de senha visa instruir os colaboradores a não compartilharem suas senhas nos sistemas da organização, além de dificultar acessos indevidos de terceiros. Definiu-se com a direção que, nas datas de avaliação, o setor do desenvolvimento do sistema buscasse as senhas dos operadores diretamente do banco de dados deste e rodaria um algoritmo sobre da consulta, para confirmar se as senhas cumpriam os requisitos de segurança. Após isso, os dados seriam passados ao avaliador. O resultado da divisão do total de senhas pelas regulares forneceria o percentual que indicaria se está satisfatória ao nível de aceitação definido pela direção ou não. Caso não estivesse, providências seriam tomadas para reverter a situação.

O Apêndice F detalha como foi realizada a medição da eficiência dos controles implantados na empresa BETA, apresentando todas as métricas e dados utilizados para montar o critério de aceitação do controle. O campo de controle e processos faz parte do nível 3 da arquitetura da PSI, pelo fato de que identifica as ações a serem tomadas a fim de que os controles definidos possam ser desenvolvidos.

O Quadro 13 relaciona as métricas e medições à sua respectiva norma de dimensão.

Quadro 13 – Relação das medições e métricas utilizadas *versus* normas da dimensão

Métricas e medições	Normas da dimensão
1. Número de senhas existentes. 2. Número de senhas que satisfazem à política de senhas. 3. Divisão do número total de senhas em conformidade pelo número de senhas registradas.	Política de Controle de Acesso Lógico – Políticas de Senhas.
1. Número de colaboradores presentes para treinamento. 2. Número de colaboradores que assinaram termo de responsabilidade. 3. Divisão dos colaboradores que assinaram pelos que estavam estipulados a assinar o termo.	Política de Conscientização de Segurança nas Operações.
1. Número de *logs* analisados. 2. Número de *logs* sem irregularidades. 3. Razão entre os arquivos de *logs* analisados e os sem irregularidades, vezes 100.	Política de Uso da *Internet.*
1. Número de *e-mails* analisados. 2. Número de *e-mails* sem irregularidades. 3. Razão entre os *e-mails* analisados e os sem irregularidades, vezes 100.	Política de Utilização de *E-mail.*
1. Número de usuários com indevido acesso a informações com acesso restrito. 2. Número de usuários com devido acesso a informações restritas. 3. Razão entre o número total de usuários analisados e o total de usuários que estão em conformidade com sua classificação.	Política de Classificação da Informação.
1. Número de ligações analisadas. 2. Número de ligações efetuadas sem irregularidades. 3. Razão entre os arquivos de ligações analisadas e os sem irregularidades, vezes 100.	Política de Controle de Divulgação de Informação nas Ligações.

Fonte: elaborado pelo autor (2018).

4.5 CONSIDERAÇÕES FINAIS

Após a seleção dos controles definidos pela direção e gestores, foi desenvolvido um trabalho para mostrar a avaliação dos controles que a direção escolheu e, assim, foi possível verificar e identificar como se encontram, na organização, os aspectos de segurança de informação dos controles que serão implementados.

A política de segurança da informação e seus documentos complementares têm por objetivo atender aos princípios básicos de segurança da informação, sendo eles: confidencialidade, integridade e disponibilidade.

A direção da organização apoia a implementação dos controles e da PSI, e incentivou a aplicação da política de segurança na organização inteira, e não apenas no processo pelo qual o trabalho foi desenvolvido, a fim de que haja uma constante de conscientização de todos os colaboradores e outros que se relacionem diretamente com os ativos da empresa.

5 IMPLEMENTAÇÃO E AVALIAÇÃO DA PSI

Após a aprovação da PSI e controles por parte da direção, no dia 01/12/2017 iniciou-se a implementação da política e efetuada a aquisição e parametrização do *software* NAC 3, que auxiliou na coleta dos dados para alguns dos controles implementados.

Foi implementada a PSI baseando-se nas normas da família 27000 e utilizado as medições propostas no apêndice E, que seguiram as diretrizes da norma 27004, a fim de medir a eficiência e eficácia das políticas por meio dos controles implementados na organização

As próximas seções detalham as medições realizadas de acordo com cada um dos controles propostos, como foram realizadas, quais as métricas utilizadas e resultados obtidos.

5.1 IMPLEMENTAÇÃO DA PSI

Conforme solicitado pela direção, foi desenvolvido um cronograma de implementação dos controles e das coletas dos dados dos mesmos. Uma correção foi necessária, para ajuste de cronograma. O planejamento foi desenvolvido para definir as datas das coletas dos dados e de treinamentos, bem como ações a serem tomadas para reverter possíveis quadros negativos.

As atividades definidas pela direção da empresa foram:

a) Primeiro contato para comprometimento gerencial da implementação da PSI;

b) planejamento de implementação da PSI;

c) medição e monitoramento do controle dos contatos telefônicos;

d) medição e monitoramento do controle de política de senhas;

e) medição e monitoramento do controle de conscientização de segurança nas operações;

f) medição e monitoramento do controle de uso da *Internet*;

g) medição e monitoramento do controle do uso de *e-mail*;

h) medição e monitoramento do controle de classificação da informação;

i) correções e ajustes dos métodos de avaliação dos controles;

j) apresentação do resultado da eficácia da PSI parcial;

k) conclusão e apresentação dos resultados da avaliação da PSI.

O Quadro 14 mostra o cronograma das atividades definidas pela direção da empresa.

Quadro 14 – Cronograma geral

		Dez.		**Jan.**		**Fev.**		**Mar.**		**Abr.**		**Maio**		**Jun.**	
Atividade	**Quinzena**	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°	1°	2°
1		X													
2		X													
3		X	X	X	X	X	X	X	X	X	X	X	X	X	
4		X		X		X		X		X		X		X	
5		X		X		X		X		X		X		X	
6		X	X	X	X	X	X	X	X	X	X	X	X	X	
7		X	X	X	X	X	X	X	X	X	X	X	X	X	
8		X	X	X	X	X	X	X	X	X	X	X	X	X	
9		X													
10		X											X	X	
11															X

Fonte: elaborado pelo autor (2018).

A política e os controles implementados foram divulgados a todos os funcionários da empresa. Para tal, realizou-se um treinamento prático e reforçado teoricamente em relação ao controle de conscientização da segurança na operação e *e-mail*. Após a divulgação da política aos colaboradores, uma declaração de comprometimento dos funcionários foi elaborada para que ocorresse sua assinatura ao fim do treinamento. Essa declaração fica armazenada no setor de RH, com a assinatura de cada funcionário. O termo de ciência encontra-se no Apêndice G.

As medições foram realizadas de acordo com o estabelecido nas métricas definidas (Apêndice F). Dessa forma, em virtude da disponibilidade do tempo e complexidade do controle, algumas coletas de dados foram feitas de forma quinzenal e algumas de forma mensal.

5.2 AVALIAÇÃO DA PSI

Durante a implementação da PSI na organização, foi elaborado o processo de avaliação dos controles à medida em que fossem implementados, com o objetivo de mensurar sua eficácia para a empresa e apresentar os resultados obtidos durante o processo da avaliação. Para isso, foi definido o indicador, que dita o que se quer medir, bem como o índice do indicador, que determina a expressão numérica do indicador, correlacionando as medidas, o resultado e a meta do indicador.

5.2.1 Política de controle de acesso lógico – políticas de senhas

A política de senhas foi um controle desenvolvido, cujo objetivo é avaliar a qualidade de senhas usadas pelos colaboradores da organização no CRM. Para validar esse controle, é verificado, do total de senhas, quantas estão de acordo com os padrões definidos para tal. O detalhamento da medição de eficiência da política de senhas é apresentada no Apêndice F.

Para contabilizar se as métricas desse controle estavam sendo atingidas, o setor de desenvolvimento buscava as senhas dos colaboradores diretamente do banco do sistema, e as descriptografava. Com o resultado da consulta no banco e com as senhas descriptografadas, era executado um algoritmo que realiza todas as validações exigidas pela política e, em seguida, contabilizava quantas senhas foram analisadas, e quantas cumpriam as exigências. Esse algoritmo é executado na mesma interface onde o código do sistema é produzido. Essa informação era exportada em um arquivo PDF e encaminhada ao responsável pela coleta dos dados, feita mensalmente.

Com o resultado obtido durante a primeira coleta de dados, foi identificado que apenas aproximadamente 29% das senhas seguiam o padrão estipulado pelo controle, logo, não estavam seguindo as diretrizes da política. Como ação, a importância de uma senha segura no ambiente corporativo foi reforçada nos treinamentos do controle de conscientização de segurança nas operações. Essa intensificação e reforço da importância, resultou numa melhora significativa dos resultados, não atingindo ainda, porém, o mínimo da meta exigido pela direção.

Durante o mês de fevereiro, surgiu a ideia de conversar com o setor de desenvolvimento do CRM, para que o método de autenticação ao sistema usasse a mesma senha de *login* no computador. A justificativa dessa mudança vem do fato de que o *login* no computador é gerenciado pelo AD, e os parâmetros setados nas suas configurações

exigem que a senha cumpra todos os requisitos da política de senhas elaborada. Com esta alteração no sistema, as demais coletas dos dados resultaram em 100% de aprovação.

A Tabela 8 apresenta os dias em que foram efetuadas as coletas dos dados, o total de senhas analisadas, a quantidade de senhas que cumprem o que a política exige, o percentual mínimo de aceitação definido pela direção e o percentual de senhas que cumprem o que é exigido pela política.

- Indicador: quantidade de senhas que atendem o requisito de segurança.
- Índice do indicador: razão entre as senhas analisadas e as que atendem ao requisito de segurança, vezes 100.
- Resultado do indicador: apresentado na coluna resultado.
- Meta do indicador: 90% de senhas que atendem o requisito do sistema.

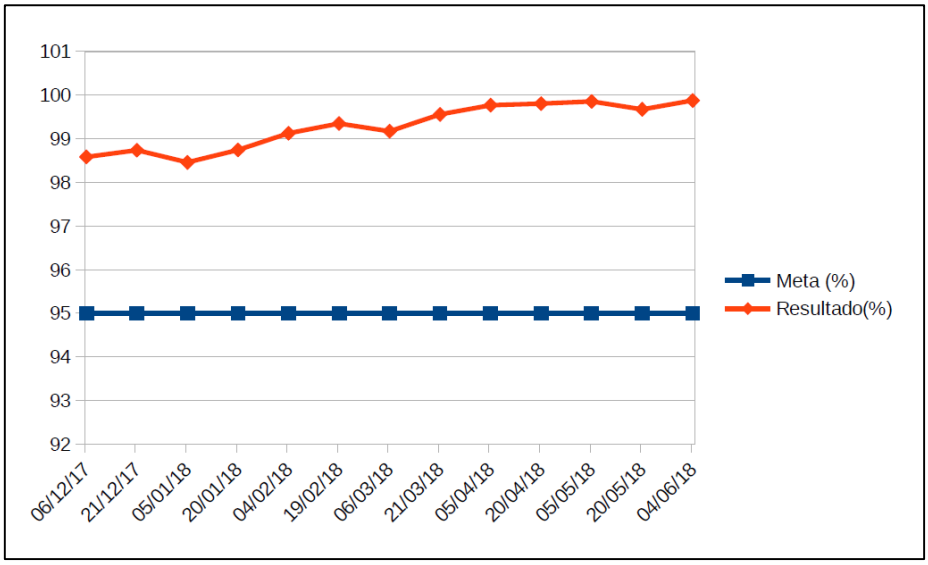
Tabela 8 – Relação de cronograma e dados coletados do controle de política de senhas

Datas	**Senhas analisadas**	**Senhas OK**	**Meta (%)**	**Resultado(%)**
05/12/17	104	30	90	28,84
05/01/18	98	52	90	53,06
05/02/18	90	60	90	66,66
05/03/18	112	112	90	100
05/04/18	119	119	90	100
05/05/18	109	109	90	100
05/06/18	120	120	90	100

Fonte: elaborada pelo autor (2018).

A partir da Tabela 8, foi possível elaborar um gráfico para apresentar os resultados aos gestores:

Figura 20 – Gráfico de resultados



Fonte: elaborado pelo autor (2018).

O gráfico apresenta o resultado das avaliações no período em que foi efetuado o trabalho. A linha em azul corresponde à meta, ou seja, o nível de satisfação mínimo exigido pela direção da organização. A linha com tendência ascendente corresponde a um resultado satisfatório em relação à medição anterior. Pode-se concluir que o objetivo foi atingido com sucesso.

5.2.2 Política de conscientização de segurança nas operações

A avaliação da política de conscientização de segurança nas operações tem por objetivo treinar e conscientizar os colaboradores referente à segurança da informação na organização, além de instruir sobre como funciona a PSI, os demais controles e métodos para atingir a meta definida pela direção. Tem a função de conscientizar os colaboradores sobre todos os riscos encontrados na operação para auxiliar na redução do erro humano. De modo geral, esse controle visa evitar o uso de periféricos, instalações de *softwares*, falta de monitoramento de terceiros, divulgação de informação via *e-mail* ou telefone, armazenamento local de arquivos, falta de normas internas e cópia de arquivos.

A métrica utilizada para validar a eficácia desse controle contou com a quantidade de colaboradores presentes nos treinamentos e os que efetivamente assinaram o documento. Com isso, era possível aumentar a taxa de colaboradores treinados e cientes da existência da PSI. Por consequência, houve um impacto indireto positivo nos demais controles

implementados. Vale ressaltar que a assinatura do colaborador garante a ciência da existência, e não que o mesmo esteja seguindo as normas.

O conteúdo do treinamento era alterado conforme a necessidade, ou seja, caso algum controle não atingisse a meta, era abordado o tema da importância de tal.

O setor do RH foi responsável por dividir as turmas no período do treinamento, a fim de não impactar no negócio da empresa.

A direção definiu como meta que todos colaboradores devessem assinar o termo. Caso o colaborador não concordasse com algo apresentado e exigido pelos controles, uma atitude cabível seria tomada. O detalhamento da medição de eficiência da política de conscientização nas operações é apresentado no Apêndice F.

A Tabela 9 apresenta os dias em que foram efetuadas as coletas dos dados e a quantidade de pessoas presentes e que efetivamente assinaram o termo de ciência no treinamento. Para satisfazer este controle, deve-se ter 100% de assinaturas por treinamento, conforme definido pela direção.

- Indicador: quantidade de pessoas que assinaram o termo de ciência da PSI na organização.
- Índice do indicador: razão entre os colaboradores que assinaram o termo e os presentes, vezes 100.
- Resultado do indicador: apresentado na coluna resultado.
- Meta do indicador: 100% – todos os colaboradores devem assinar.

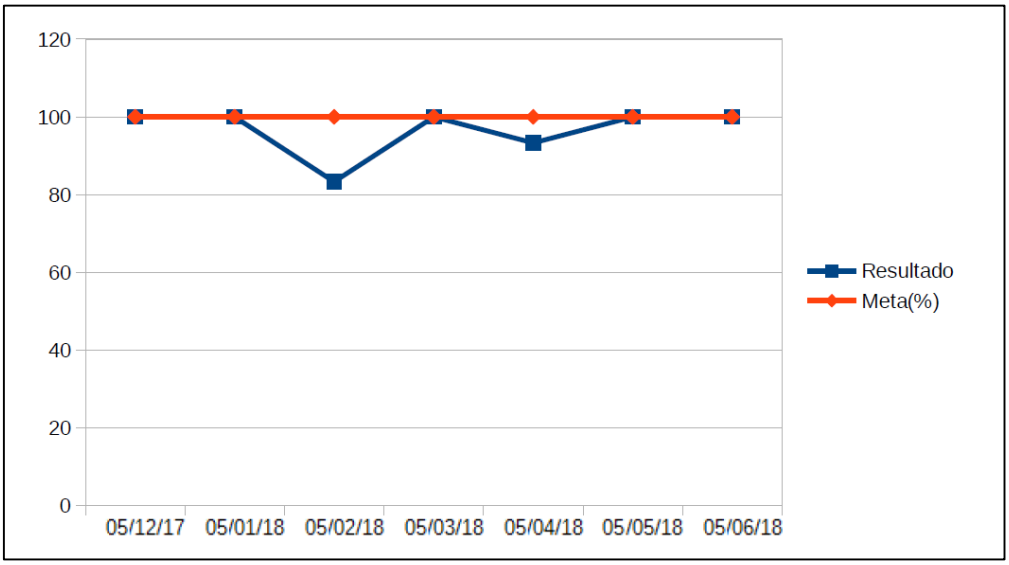
Tabela 9 – Relação de cronograma e dados coletados do controle de conscientização de segurança nas operações

Data	Pessoas presentes	Pessoas que assinaram	Resultado	Meta (%)
05/12/2017	13	13	100	100
05/01/2018	10	10	100	100
05/02/2018	12	10	83,33	100
05/03/2018	12	12	100	100
05/04/2018	15	14	93,33	100
05/05/2018	13	13	100	100
05/06/2018	12	12	100	100

Fonte: elaborada pelo autor (2018).

A partir da Tabela 9, foi possível elaborar um gráfico para apresentar a meta e os resultados aos gestores:

Figura 21 – Gráfico de resultados 2



Fonte: elaborado pelo autor (2018).

O gráfico apresenta que, em duas avaliações, o resultado não atingiu a meta exigida. No entanto, justifica-se pelo fato de que foram casos de saídas antecipadas ou desligamentos dos colaboradores. Durante a coleta das assinaturas, nenhum colaborador se negou a assinar. A linha com tendência ascendente ou estabilizada em 100% corresponde a um resultado satisfatório. Pode-se concluir que o objetivo foi atingido com sucesso, em virtude de que os demais controles também foram bem-sucedidos.

5.2.3 Política de uso da *Internet*

Para elaborar a avaliação da política de uso da *Internet*, que tem por objetivo detectar atividades de processamento ilegal de dados e acessos não autorizados, foi necessária a aquisição do *software* NAC 3. Esse controle está relacionado aos riscos de vazamento de informações confidenciais, vírus ou ataques cibernéticos e acessos indevidos.

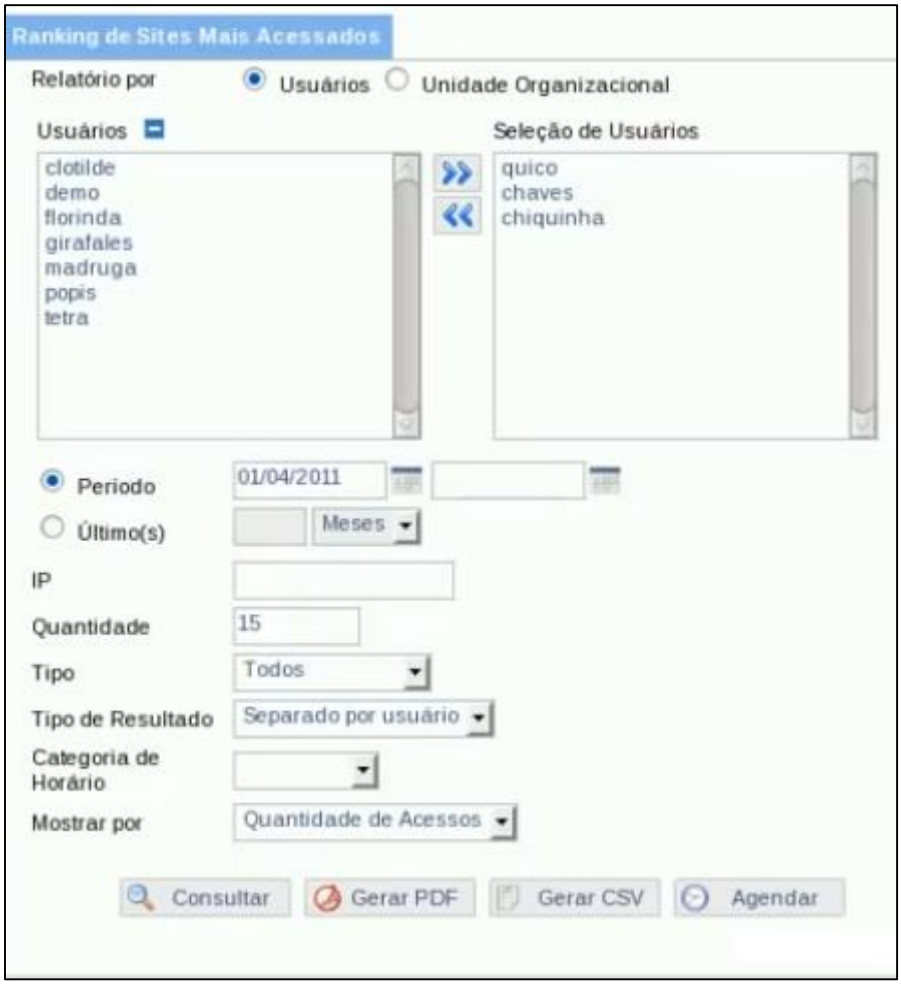
O módulo *proxy* deste *software*, que é responsável por gerenciar os acessos à *Internet*, funciona bloqueando os *sites* não permitidos pela organização, contabilizando o total de endereços eletrônicos analisados, bloqueados e permitidos, e guardando os *logs* de acesso.

O *software*, além de contabilizar os *sites* analisados totais, irregulares e regulares, permite fazer a exportação de diversas informações, tais como os endereços mais acessados e o colaborador que mais utiliza banda de *Internet*, entre outros.

A coleta dos dados foi efetuada de forma quinzenal, para onde os *logs* gerados pelo *software* são exportados. Dessa forma, para validar esse controle, é verificado, do total de *sites* acessados, quantos estão de acordo com os padrões definidos para tal. O detalhamento da medição de eficiência da política de senhas é apresentado no Apêndice F.

Na Figura 22 é apresentado um modelo de filtro que o *software* permite fazer, no qual encontra-se o *ranking* de *sites* mais acessados por determinados usuários do software.

Figura 22 – Interface modelo de filtros

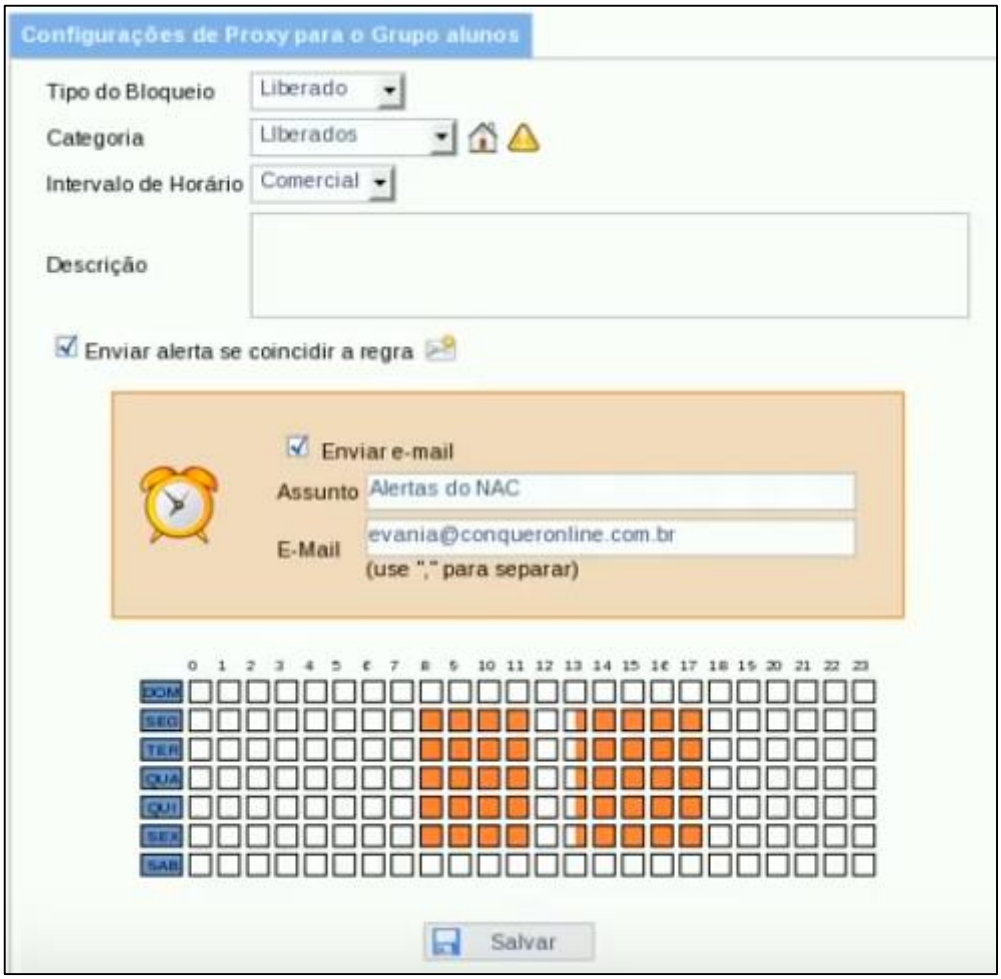


Fonte: acervo pessoal (2018).

Conforme os colaboradores forem acessando *sites* irregulares, foi configurado para que o gestor do colaborador receba um *e-mail* informando o *site* que o funcionário está tentando acessar.

A Figura 23 apresenta um exemplo de como é setada a opção para habilitar esta funcionalidade, onde o *e-mail* é enviado, caso a regra de acesso coincida com o que foi bloqueado.

Figura 23 – Interface modelo de alertas



Fonte: acervo pessoal (2018).

A Tabela 10 apresenta os dias em que foram efetuadas as coletas dos dados, os *logs* totais, regulares, irregulares e a meta. Para satisfazer esse controle, deve-se ter 95% de regularidade na análise.

- Indicador: quantidade de *sites* analisados regulares.
- Índice do indicador: razão entre os *sites* analisados e os regulares, vezes 100.

- Resultado do indicador: apresentado na coluna resultado.
- Meta do indicador: 95%.

Tabela 10 – Relação de cronograma e dados coletados do controle sobre uso da *Internet*

(continua)

Data	Meta (%)	Logs analisados	Regulares	Irregulares	Resultado (%)
06/12/2017	90	426	394	32	92,48
21/12/2017	90	483	454	29	93,99
05/01/2018	90	326	301	25	92,33

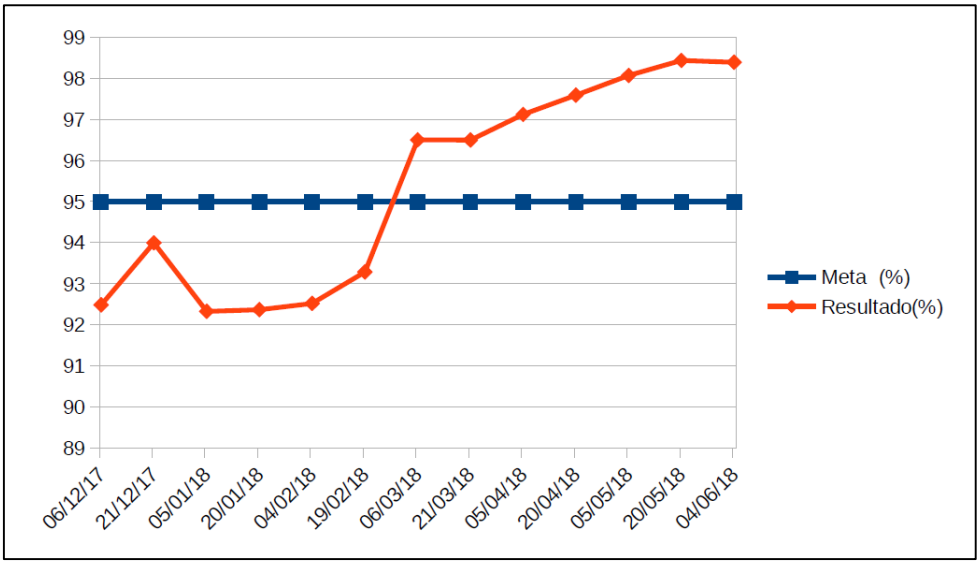
(conclusão)

Data	Meta (%)	Logs analisados	Regulares	Irregulares	Resultado (%)
20/01/2018	90	367	339	28	92,37
04/02/2018	90	321	297	24	92,52
19/02/2018	90	298	278	20	93,28
06/03/2018	90	486	469	17	96,50
21/03/2018	90	514	496	18	96,49
05/04/2018	90	521	506	15	97,12
20/04/2018	90	539	526	13	97,58
05/05/2018	90	518	508	10	98,06
20/05/2018	90	447	440	7	98,43
04/06/2018	90	497	489	8	98,39

Fonte: elaborada pelo autor (2018).

A partir da Tabela 10, foi possível elaborar um gráfico para apresentar a meta e os resultados aos gestores:

Figura 24 – Gráfico de resultados 3



Fonte: elaborado pelo autor (2018).

O gráfico mostra que na terceira medição houve uma queda na linha que tinha por objetivo chegar na meta de 95%. Essa queda se deu em virtude de uma reestruturação no quadro de funcionários e afetou esse controle em particular. Como medida para contornar essa situação e atingir a meta exigida pela direção, foi reforçada nos treinamentos de conscientização na operação a importância de usufruir corretamente da *Internet* corporativa. Em virtude das diversas medidas administrativas, treinamentos e desligamentos, houve uma pressão para a operação seguir mais rigidamente as normas, o que causou aumento das regularidades em 3,21% na medição do dia 06/03/2018. Nas demais avaliações e com o devido treinamento aos colaboradores, os resultados apareceram e houve uma tendência ascendente em direção a 100%, o que corresponde ao sucesso na medição e implantação do controle.

5.2.4 Política de utilização de *e-mail*

A política de utilização de *e-mail* tem por objetivo detectar as atividades de divulgação ilegal de dados não autorizada por meio dos *e-mails* e, para executar essa atividade, foi necessária a aquisição do módulo de *e-mail* do *software* NAC 3. Este controle busca evitar que *e-mails* de cunho pessoal, anexos não permitidos e divulgação indevida de informação partam da empresa, bem como a ocorrência da falta de monitoramento de tais *e-mails*.

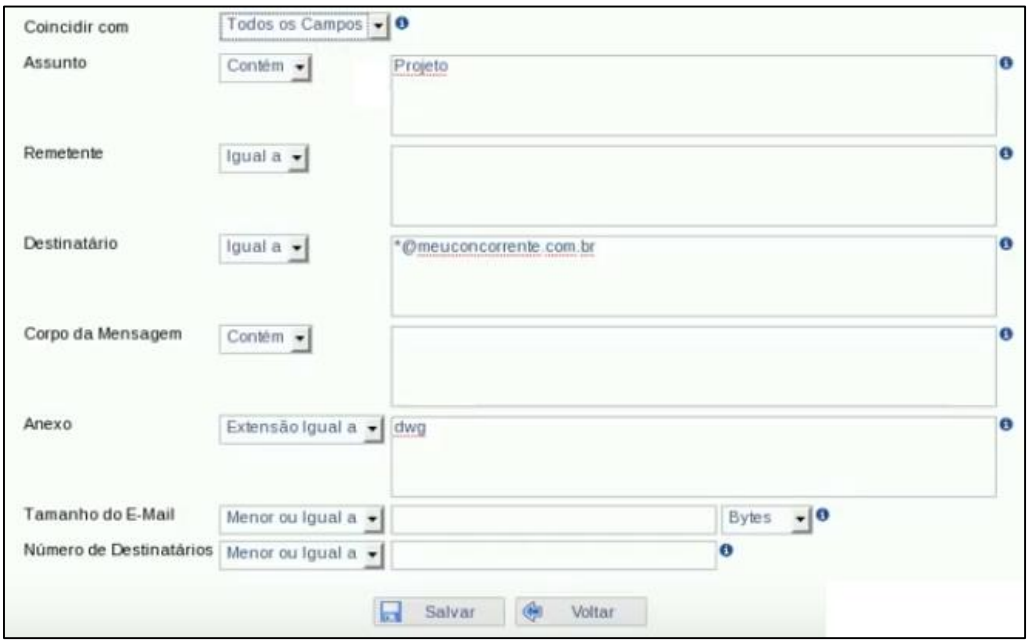
O módulo de *e-mail* desse *software*, que é responsável por gerenciar o que é enviado por tal canal pelos colaboradores, funciona de forma que quando *e-mails* com tamanho

maior do que permitido ou extensões diferentes das autorizadas após a parametrização do *software* sejam bloqueados e encaminhados para o gestor da área, para que seja tomada alguma atitude cabível.

Para validar este controle, é verificado, do total de *e-mails* analisados, quantos estão de acordo com os padrões definidos. O detalhamento da medição de eficiência da política de senhas é apresentado no Apêndice F.

A Figura 25 apresenta a tela de configuração do *software* do que se deseja bloquear.

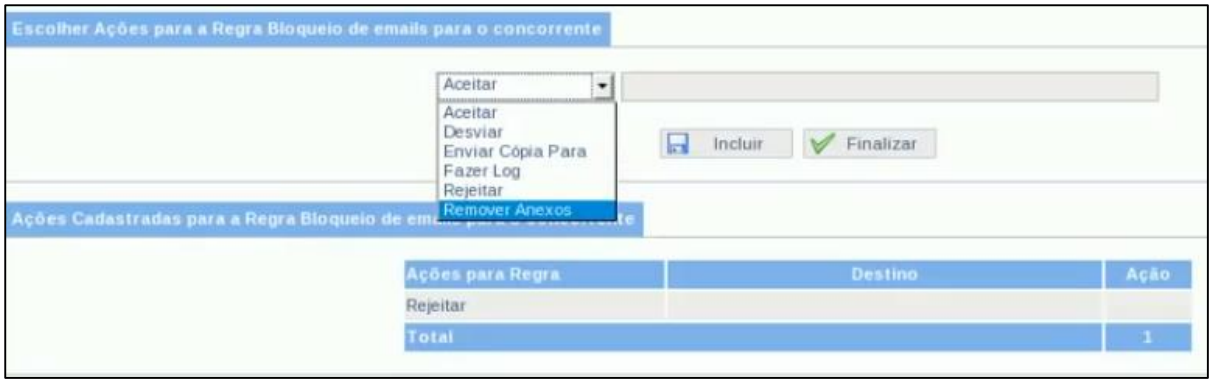
Figura 25 – Interface modelo de bloqueios de *e-mail*



Fonte: acervo pessoal (2018).

Além de ser possível bloquear o *e-mail*, é possível tomar atitudes em relação ao *e-mail* bloqueado. Para a empresa BETA, foi decidido enviar uma cópia para ao gestor e rejeitar o *e-mail*. A Figura 26 apresenta o que se deseja fazer com o *e-mail* bloqueado.

Figura 26 – Interface modelo de consequência de *e-mail* bloqueado



Fonte: acervo pessoal (2018).

A direção definiu como meta que o resultado do indicador deve ser superior a 95%. As ações a serem tomadas caso a meta não fosse atingida ou em caso de tentativa de vazamento de alguma informação, era relativo ao conteúdo do *e-mail*, e poderia causar advertências ou o desligamento do funcionário.

Este controle funciona por meio da utilização do *software*, que contabiliza a quantidade de *e-mails* bloqueados, dentre todos os analisados.

A Tabela 11 apresenta os dias em que foram efetuadas as coletas dos dados, o total de *e-mails* analisados, regulares e os com irregularidades no seu conteúdo, além da meta.

Para satisfazer este controle, deve-se ter 95% de regularidade na análise.

- Indicador: quantidade de *e-mails* analisados regulares.
- Índice do indicador: razão entre os *e-mail* analisados e os regulares, vezes 100.
- Resultado do indicador: apresentado na coluna resultado.
- Meta do indicador: 95%.

Tabela 11 - Relação de cronograma e dados coletados do controle de política de uso de *e-mails*

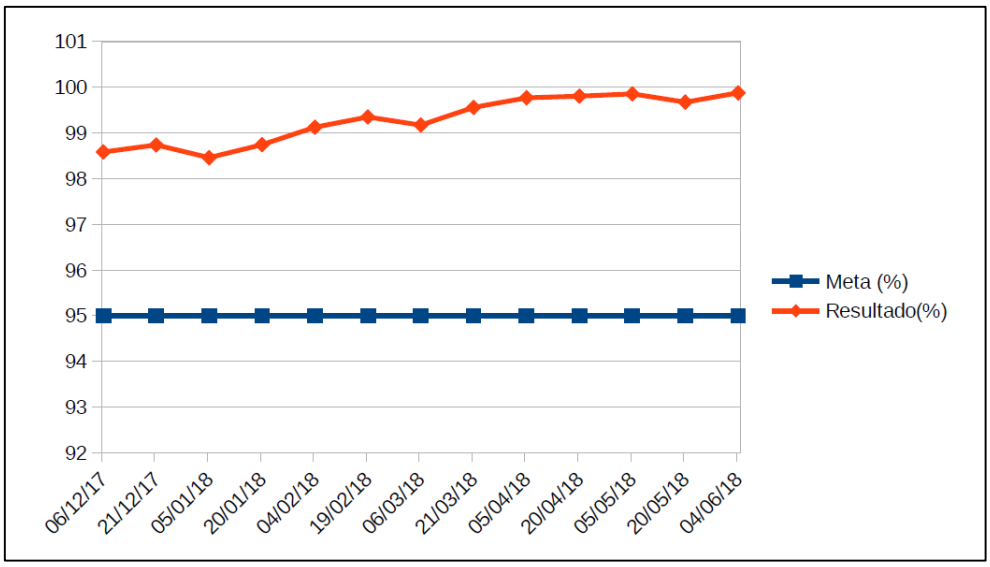
Data	Meta (%)	E-mails analisados	Regulares	Irregulares	Resultado
06/12/2017	95	1129	1113	16	98,58
21/12/2017	95	1030	1017	13	98,73
05/01/2018	95	973	958	15	98,45
20/01/2018	95	954	942	12	98,74
04/02/2018	95	1028	1019	9	99,12
19/02/2018	95	1073	1066	7	99,34
06/03/2018	95	1208	1198	10	99,17
21/03/2018	95	1354	1348	6	99,55
05/04/2018	95	1306	1303	3	99,77

20/04/2018	95	1532	1529	3	99,80
05/05/2018	95	1385	1383	2	99,85
20/05/2018	95	1228	1224	4	99,67
04/06/2018	95	1613	1611	2	99,87

Fonte: elaborada pelo autor (2018).

A partir dessa tabela, foi possível elaborar um gráfico para apresentar a meta e os resultados aos gestores:

Figura 27 – Gráfico de resultados 4



Fonte: elaborado pelo autor (2018).

O gráfico mostra que em nenhum momento da análise a meta deixou de ser atingida, e sim, apresentou uma tendência ascendente em direção a 100%. Essa tendência positiva se deu, também, pelos treinamentos realizados no controle de conscientização da operação, ação que que foi muito bem recebida pelos gestores e demais colaboradores. A partir disso, pode-se concluir que foi obtido sucesso na medição e implantação do controle.

Vale ressaltar que o conteúdo que o *software* bloqueia não resolve a questão do envio de dados não autorizados, pois isso depende dos colaboradores, mas ameniza o vazamento dessas informações com as funcionalidades e parâmetros configurados no *software*.

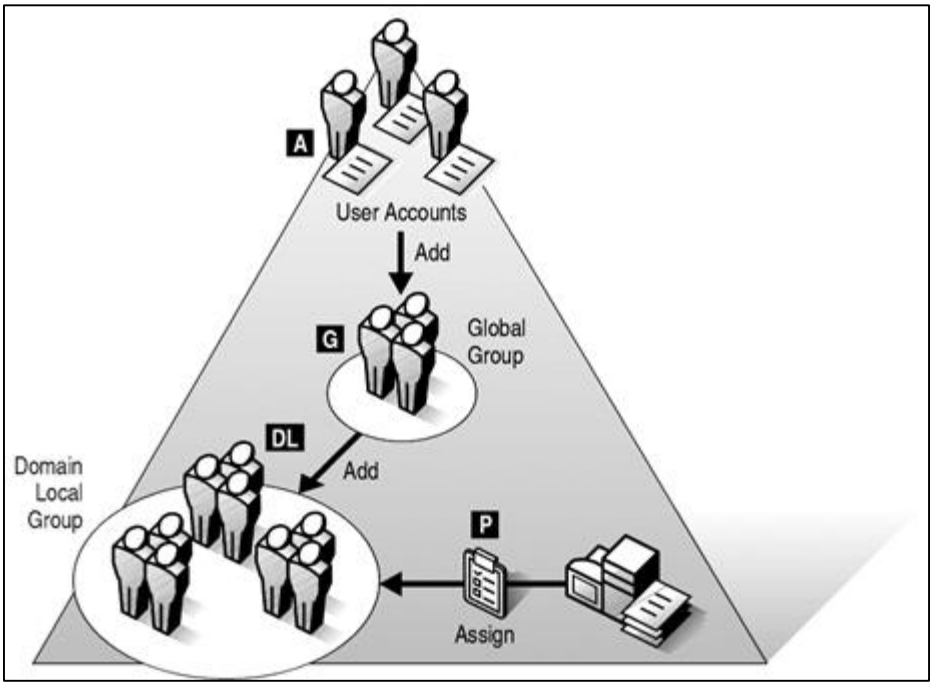
5.2.5 Política de classificação da informação

O método de classificar a informação para a empresa BETA foi projetado a partir da estrutura de compartilhamento de arquivos da organização, visando sempre os princípios da segurança da informação, que são a confidencialidade, disponibilidade e integridade. Esse controle tem por objetivo garantir que a informação não seja disponibilizada de forma equivocada. Se não bem planejado, pode por em risco toda informação disponibilizada na organização, pois, permitindo acessos indevidos, pode haver divulgação indevida, furto, entre outras ameaças que podem prejudicar a organização. Esse controle visa, portanto, reduzir riscos de exposição e/ou divulgação indevida, perda e/ou roubo de informações confidenciais, comprometimento de registros de clientes, bem como roubo de propriedade intelectual.

O modo de compartilhamento de arquivos da organização segue as melhores práticas da Microsoft, a recomendação A (contas) G (grupo) DL (domínio local) P (permissões).

A Figura 28 exemplifica como a recomendação funciona, fazendo com que as contas dos usuários sejam adicionadas em um grupo global, que é membro de um grupo domínio local com permissão nos recursos, tornando, assim a administração das permissões eficiente.

Figura 28 – Recomendação AGDLP



Fonte: Yen (2012).

Por seguir esse modelo de gerenciamento de permissões, é possível identificar se os colaboradores da organização estão tendo acesso somente ao que é permitido. Logo, esse controle é baseado na análise das contas de usuários e suas permissões. Se a conta de usuário de determinado colaborador está somente com as permissões que ele necessita, a conta é contabilizada como regular; se não, como irregular. A direção definiu que o resultado do indicador deve ser igual ou maior que 90%. As atitudes a serem tomadas caso não fosse atingida a meta era o ajuste da conta do colaborador.

O detalhamento da medição de eficiência da política de classificação da informação é apresentado no Apêndice F.

Foi efetuada uma razão entre o total de colaboradores e dias disponíveis para a coleta de dados, que resultou em 15 colaboradores por análise em cada data de coleta, para que fosse, assim, possível analisar o usuário de todos colaboradores no período de coleta de dados.

A Tabela 12 apresenta os dias em que foram efetuadas as coletas, a quantidade de contas de usuários analisados, quantas estavam em conformidade, o resultado e meta.

- Indicador: quantidade de contas de usuários regulares.
- Índice do indicador: razão entre o total de contas de usuários e as que estavam em conformidade, vezes 100.
- Resultado do indicador: apresentado na coluna resultado.
- Meta do indicador: 90%.

Tabela 12 – Relação de cronograma e dados coletados do controle de classificação da informação

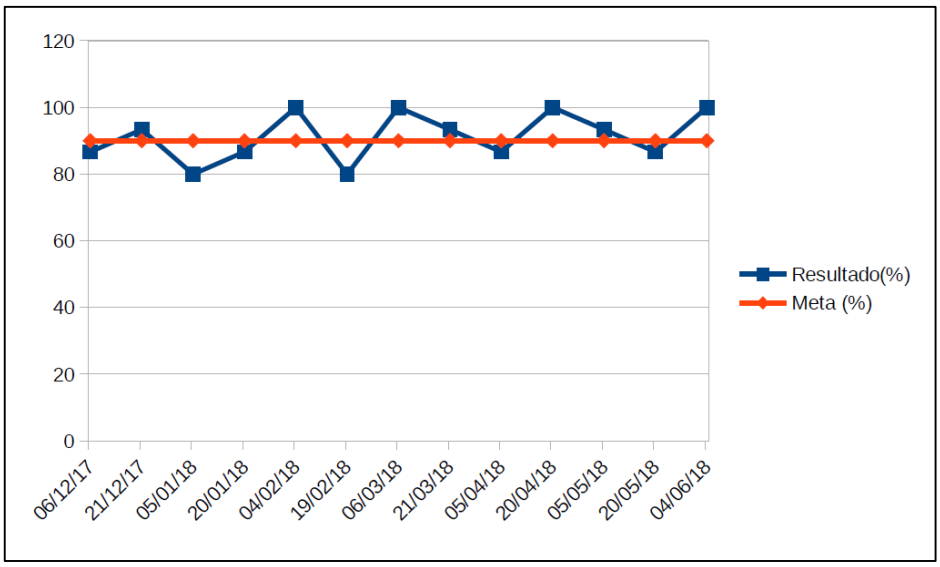
Data	Usuários analisados	Em conformidade	Resultado (%)	Meta (%)
06/12/2017	15	13	86,66	90
21/12/2017	15	14	93,33	90
05/01/2018	15	12	80	90
20/01/2018	15	13	86,66	90
04/02/2018	15	15	100	90
19/02/2018	15	12	80	90
06/03/2018	15	15	100	90
21/03/2018	15	14	93,33	90

05/04/2018	15	13	86,66	90
20/04/2018	15	15	100	90
05/05/2018	15	14	93,33	90
20/05/2018	15	13	86,66	90
04/06/2018	15	15	100	90

Fonte: elaborada pelo autor (2018).

A partir da Tabela 12, foi possível elaborar um gráfico para apresentar a meta e os resultados aos gestores:

Figura 29 – Gráfico de resultados 5



Fonte: elaborado pelo autor (2018).

A partir dos resultados obtidos, foi possível concluir que a variação ocorre pelo fato de que a organização realoca seus colaboradores para gerenciar diferentes clientes e essa informação não é passada para o setor de TI, que consegue somente fazer os ajustes nas datas dos controles. Está sendo efetuada uma mudança cultural na organização, que orienta que quando o colaborador migra de setor, um *e-mail* seja encaminhado ao gestor de TI, a fim de que seja feito o ajuste no ato da mudança, para que as informações mantenham os princípios básicos de segurança.

5.2.6 Política de controle de divulgação indevida de informação nas ligações

A política de divulgação indevida de informação nas ligações, cujo objetivo é detectar atividades de divulgação ilegal de dados não autorizados por meio de escutas de ligações, é o único que não tem as informações coletadas pelos *softwares* e pela TI, e sim, por um setor da organização responsável pelas escutas de ligações, denominado monitoria. O setor de monitoria tem a responsabilidade de fazer as escutas das ligações dos colaboradores e contabilizar quantas foram ouvidas por monitor e, destas, quantas tiveram irregularidades.

Para validar este controle, é verificado, do total de escutas efetuadas, quantas estão de acordo com os padrões definidos. O detalhamento da medição de eficiência da política de senhas é apresentado no Apêndice F.

De modo geral, esse controle é aplicado para evitar a divulgação indevida da informação via contato telefônico e controlar o uso do *script* de atendimentos.

O setor responsável por passar essas informações conta com quatro colaboradores, os quais fazem uma média de quinze escutas de ligações diárias cada um, resultando em aproximadamente 60 escutas por dia. Após fazer as escutas e registrar os resultados, os monitores, foram instruídos que toda escuta irregular deve ser repassada ao gestor, e o colaborador que efetuou a irregularidade deve receber um *feedback.*

No dia da coleta de informações, os dados são passados ao responsável para quem está coletando os dados, que ficará encarregado de contabilizar novamente os dados para validar as informações passadas, fazendo uma revisão no documento.

A Tabela 13 apresenta os dias em que foram efetuadas as coletas dos dados, a quantidade de contas de usuários analisados, quantas estavam em conformidade, o resultado e meta.

- Indicador: quantidade de ligações regulares.
- Índice do indicador: razão entre as ligações escutadas e as regulares, vezes 100.
- Resultado do indicador: apresentado na coluna resultado.
- Meta do indicador: 90%.

Tabela 13 – Relação de cronograma e dados coletados do controle de divulgação indevida via contato telefônico

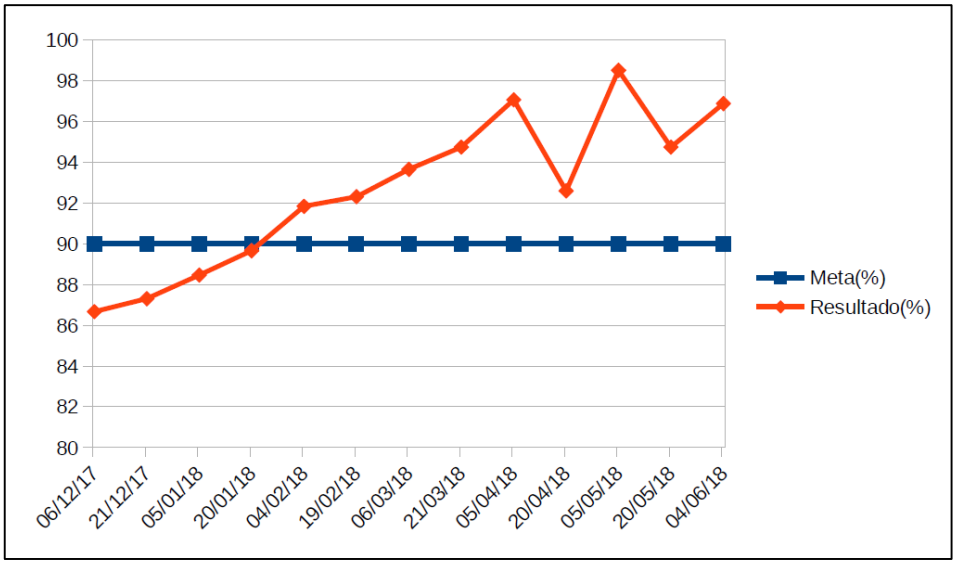
Data	**Total de ligações analisadas**	**Ligações com divulgação**	**Ligações sem divulgação**	**Meta (%)**	**Resultado (%)**

		indevida de ligações	indevida de ligações		
06/12/2017	60	8	52	90	86,66
21/12/2017	63	8	55	90	87,30
05/01/2018	52	6	46	90	88,46
20/01/2018	58	6	52	90	89,65
04/02/2018	49	4	45	90	91,83
19/02/2018	65	5	60	90	92,30
06/03/2018	63	4	59	90	93,65
21/03/2018	76	4	72	90	94,73
05/04/2018	68	2	66	90	97,05
20/04/2018	54	4	50	90	92,59
05/05/2018	67	1	66	90	98,50
20/05/2018	57	3	54	90	94,73
04/06/2018	64	2	62	90	96,87

Fonte: elaborada pelo autor (2018).

A partir da Tabela 13, foi possível elaborar um gráfico para apresentar a meta e os resultados aos gestores:

Figura 30 – Gráfico de resultados 6



Fonte: elaborado pelo autor (2018).

Em análise do gráfico, é possível identificar que a partir da quinta medição, a meta foi atingida e, até o fim da coleta dos dados, não houve caso em que a meta não tenha sido atingida. Para obter resultados positivos, após a segunda medição foi dado um foco especial no treinamento referente a esse controle, o que provocou uma melhora considerável nos

resultados. A medida para contornar a situação negativa que o gráfico apresentava inicialmente foi dar um *feedback* para o colaborador e explicar onde ele errou e o porquê de não poder haver a comunicação de tal informação. O gráfico apresentou uma tendência ascendente em direção a 100%, o que corresponde ao sucesso na medição e implantação do controle.

5.3 CONSIDERAÇÕES FINAIS

Com a apresentação dos resultados aos gestores e à direção, foram feitas sugestões de implementação de novos controles. Além disso, foi notável o apoio da direção da organização em relação a implementação da PSI e seus controles em todos setores, visto que os resultados apresentados foram positivos.

A principal dificuldade encontrada no estudo de caso foi a falta de interesse demonstrada no início do projeto e, para que houvesse maior envolvimento, o gestor de TI teve que intervir para a compreensão da segurança da informação por parte dos diretores. Após a intervenção do gestor de TI, a direção reconheceu a importância de uma PSI. A mudança na cultura da organização foi outro problema enfrentado, pois os colaboradores inicialmente não levaram a sério o projeto. Por essa razão, o apoio e a intervenção da direção foram necessárias.

Em virtude de a organização onde foi efetuado o estudo ser relativamente pequena e a maioria dos controles estarem relacionadas à área de TI, o responsável desse setor assumiu o papel de gestor de TI. Porém é importante que este trabalho não esteja vinculado somente a esse profissional e sim, de acordo com o setor da atuação dos controles, assim, caso o controle esteja vinculado ao setor de vendas, o responsável deve ser o coordenador do setor de vendas, e assim por diante.

Esse trabalho não pretende encerrar a implementação da PSI, uma vez que, por ser um processo incremental, deverá ser desenvolvido nas demais áreas da organização. Além disso, a conscientização de todos os colaboradores é um trabalho contínuo.

6 CONCLUSÕES

Este trabalho teve por objetivo desenvolver uma Política de Segurança da Informação que fosse aplicável a empresas de *call center*. Para desenvolver essa política, foi fundamental realizar um estudo sobre a segurança e os princípios básicos da informação, ciclo de vida da informação e as normas ISO/IEC da família 27000.

Ao longo deste trabalho, foi elaborada uma pesquisa sobre os riscos de segurança da informação em *call centers*. Na pesquisa, constatou-se que nesse modelo de negócio a informação está exposta a diferentes vulnerabilidades e ameaças, principalmente àquelas voltadas a engenharia social. Além disso, o estudo desses riscos ficou diretamente relacionado com o resultado da gestão riscos efetuado na organização.

O processo de gestão de riscos efetuado na empresa apontou as principais fontes de ameaças internas e externas. Entre as fontes internas, estão os colaboradores e terceiros. Já entre as externas estão os vírus, *malwares* e o aumento considerável da *IoT*. A gestão de riscos elaborada na empresa BETA indicou que ela está mais vulnerável internamente. Sendo assim, foram implementados controles definidos pela direção e gestores da empresa. Foi notável que a falta de controles é um dos fatores que deixam a empresa vulnerável.

Após a realização da pesquisa, e em conjunto da gestão de riscos, foi estudada a arquitetura dos documentos da PSI e formas de aplicar do uso das normas da série ABNT/NBR 27000 para a organização em questão. Assim, foi elaborada uma política de segurança da informação, bem como seus documentos complementares com as dimensões da segurança da informação.

A partir deste ponto, ficou evidente que todas organizações devem ter uma PSI para fornecer diretrizes e condutas que os colaboradores devem ter em relação às informações da empresa. Contudo, nenhuma empresa deve implementar normas que não consiga controlar.

Na proposta de solução, foi desenvolvida a gestão de riscos da empresa, que serviu como base para elaborar a PSI e os controles da organização, além de apresentar os métodos de medição dos controles para validar a eficácia da política. A PSI teve por objetivo auxiliar a manter os princípios básicos de segurança da informação na organização.

Após a avaliação dos controles implementados e apresentação dos resultados para a direção, foi possível identificar a importância que os gestores deram à segurança da informação na empresa, além de ter sido possível demonstrar que os riscos realmente

existem na organização. Os gestores conseguiram compreender a importância da segurança da informação dentro das organizações.

O sucesso na implementação da segurança da informação se deu, também, pela compreensão dos colaboradores, visto que os ativos humanos representam a maior parte dos riscos na empresa.

Por fim, é possível afirmar que a segurança da informação é uma área não muito explorada nas organizações de pequeno porte pois, muitas vezes, sua implementação é vista apenas como um gasto. Porém, nos últimos anos, a informação tem sido valorizada e vem recebendo seu real valor. Sendo assim, os gastos em segurança da informação justificam-se como investimentos.

A proposta de continuação deste trabalho, seria a implementação da Política de Segurança da Informação nas demais áreas da organização visto que este é um processo interativo e incremental. Apesar dos resultados das avaliações serem positivos, é necessário que ocorra também em outros ambientes da organização.

O presente trabalho pode se estender contribuindo para a realização de uma avaliação das atividades das organizações antes e depois da implementação de uma Política de Segurança da Informação, a fim de confirmar se a política e controles implementados trouxeram um retorno positivo no andamento das atividades da organização. Também é possível afirmar que contribui para o desenvolvimento de um comparativo dos resultados obtidos na organização onde o estudo de caso foi efetuado, com os resultados das organizações em demais segmentos.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001: *Tecnologia da informação*: Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos. 2. ed. Rio de Janeiro: ABNT, 2013.

ABNT NBR ISO/IEC 27002. (2005). *Tecnologia da informação* – Código de prática para a gestão da segurança da informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

ABNT NBR ISO/IEC 27003. (2011). *Tecnologia da informação* – Diretrizes para Implantação de um Sistema de Gestão da Segurança da Informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

ABNT NBR ISO/IEC 27004. (2010). *Tecnologia da informação* – Gerenciamento de Métricas e Relatórios para um Sistema de Gestão de Segurança da Informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

ABNT NBR ISO/IEC 27005: *Tecnologia de informação*: Técnicas de segurança - Gestão de riscos de segurança da informação. 2. ed. Rio de Janeiro: ABNT, 2013.

ABDYLI, Flamur. *How Ready Are Banks In The Republic Of Kosovo To Implement An Informantion Security Policy?*. Disponível em: <http://www.cek.ef.uni-lj.si/magister/abdyli1329-B.pdf>. Acesso em: 21 ago. 2017.

BELL, Judith. *Doing your research project*. Berkshire: Open University Press, 2015. Disponível em: <http://elearning.ufl.udn.vn/home/esp/pluginfile.php/3274/mod_resource/content/1/Judith%20Bell%20-%20Doing_Your_Research_Project.pdf>. Acesso em: 09 out. 2017.

BRYARS, Matthew. *Are you in the dark about the risk from call centre legacy data?*. 2015. Disponível em: <http://www.information-age.com/are-you-dark-about-risk-call-centre-legacy-data-123459929/>. Acesso em: 09 out. 2017.

CANEPA, Lana. 62% dos profissionais vazam dados sigilosos das empresas. 2013. Disponível em: <http://www.gazetadopovo.com.br/economia/62-dos-profissionais-vazam-dados-sigilosos-das-empresas-bgpop4f9gqwm4xpi0qc6299ou>. Acesso em: 21 ago. 2017.

CIO (São Paulo). Redação (Ed.). Maturidade das empresas brasileiras em Segurança da Informação ainda é baixa. 2017. Disponível em: <http://cio.com.br/noticias/2017/02/03/maturidade-das-empresas-brasileiras-em-seguranca-da-informacao-ainda-e-baixa//>. Acesso em: 21 ago. 2017.

_____. _____. Cinco tecnologias corporativas que podem abalar 2017. 2017. Disponível em: <http://cio.com.br/tecnologia/2017/01/02/cinco-tecnologias-corporativas-que-podem-abalar-2017/?utm_campaign=website&utm_source=sendgrid.com&utm_medium=email&cm_mc_uid=08713946772814890921129&cm_mc_sid_50200000=1489092112/>. Acesso em: 21 ago. 2017.

DANTAS, M.; CAVALCANTE, V. *Pesquisa qualitativa e Pesquisa quantitativa*. Recife, PE: Universidade Federal de Pernambuco, 2006. (Trabalho de Graduação da Disciplina Métodos e Técnicas de Pesquisa). Disponível em: <http://pt.scribd.com/doc/14344653/Pesquisa-qualitativa-e-quantitativa>. Acesso em: 27 nov. 2017.

DTEX SYSTEMS. *The Most Dangerous Call Center Security Threat*: The Why and How of Stopping the Insider Threat. 2016. Disponível em: <https://dtexsystems.com/the-most-dangerous-call-center-security-threat/>. Acesso em: 28 nov. 2017.

FLOWERDAY, Stephen V.; TUYIKEZE, Tite . *Information security policy development and implementation*: The what, how and who. Disponível em: <https://www.passeidireto.com/arquivo/31785653/information-security-policy-development-and-implementation-the-what-how-and-who->. Acesso em: 21 ago. 2017.

FONTES, Edison. *Segurança da Informação*: o usuário faz a diferença. 1. ed. São Paulo: Saraiva, 2006.

_____. *Políticas de Segurança da Informação*. Rio de Janeiro: Escola Superior de Redes - Rnp, 2015.

GALVÃO, Michele da Costa. *Fundamentos em segurança da informação*. São Paulo: Pearson, 2015.

UPTON, David M.; CREESE, Sadie. *The Danger from Within*. 2014. Disponível em: <https://hbr.org/2014/09/the-danger-from-within>. Acesso em: 20 out. 2017.

ITIL V3. *Estratégia de Serviço*, 2011.

KITTEN, Tracy. *New Wave of Call Center Fraud*. 2013. Disponível em: <http://www.bankinfosecurity.com/call-center-fraud-gets-stealthier-a-5660>. Acesso em: 09 maio 2017.

MALIN, Ana Maria Barcelos. *Gestão da Informação Governamental*: em direção a uma metodologia de avaliação. Disponível em: <http://www.brapci.ufpr.br/brapci/_repositorio/2010/01/pdf_4826614d3f_0007610.pdf>. Acesso em: 21 ago. 2017.

MANCINI, Lucas. *Call center*: estratégia para vencer. 2. ed. [S.l.]: Summus, 2006. 152 p.

NIST. NIST SP 800-30. *Risk Management Guide for Information Technology Systems*. 2002. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. Acesso em: 20 jun. 2017.

NYANGIRA, Faustine; NGOMA, Marvin T. *Methodologies and Approaches to Measure Security*. Disponível em: <http://publications.lib.chalmers.se/records/fulltext/246053/246053.pdf>. Acesso em: 21 ago. 2017.

LIMA, P. G. *Tendências paradigmáticas na pesquisa educacional.* 2001. 317f. Dissertação (Mestrado em Educação). Universidade Estadual de Campinas, Faculdade de Educação, Campinas, SP, 2001. Disponível em: <http://www.do.ufgd.edu.br/paulolima/arquivo/mestrado.pdf>. Acesso em: 21 ago. 2017.

PACHECO DA SILVA, Watson. *A saúde do operador de telesserviços*. 2015. Disponível em: <http://www.callcenter.inf.br/artigos/57123/a-saude-do-operador-de-telesservicos/ler.aspx>. Acesso em: 03 abr. 2017.

PAPANICOLAOU, Mia. *Call Center Security Tips For Protecting Customer Data and Preventing Breaches5*. Disponível em: <http://www.tmcnet.com/sectors/security/articles/419851-5-call-center-security-tips-protecting-customer-data.htm>. Acesso em: 09 out. 2017.

PINDROPLABS. The 2016 *Call Center* Fraud Report. Disponível em: <http://www.pindrop.com/wp-content/uploads/2016/05/2016-Call-Center-Fraud-Report-1.pdf>. Acesso em: 03 out. 2017.

QUERESHI, Muhammad Sohail. *Measuring Efficacy of Information Security Policies.* Disponível em <https://www.diva-portal.org/smash/get/diva2:560266/FULLTEXT01.pdf>. Acesso em: 21 ago. 2017.

ROHR, Altieres; SIMÕES GOMES, Gomes. G1 (São Paulo). Vazamentos expõem milhões de chamadas de *call center*. 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/03/vazamentos-expoem-milhoes-de-chamadas-de-call-center.html>. Acesso em: 21 ago. 2017.

SÊMOLA, Marcos. *Gestão da segurança da informação*: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. *Risk Management Guide for Information Technology Systems.* Gaithersburg: NIST - National Institute of Standards and Technology**,** July 2002. 54 p. (Special Publication 800-30). Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. Acesso em: 21 ago. 2017.

SYMANTEC. Estudo da Symantec e Ponemon Institute Revela que Negligência Humana e Erros de Sistema são Responsáveis por Dois Terços dos Vazamentos de Dados. São Paulo, 05 jun. 2013. Disponível em: <http://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20130605_01>. Acesso em: 09 mai. 2017.

_____. Pesquisa sobre Custo e Gestão da Informação: resultados da América Latina. Disponível em: <http://www.symantec.com/content/pt/br/enterprise/images/theme/state-of-information/2012-SOI-PDF-LAM-PORT-v2.pdf>. Acesso em: 21 ago. 2017.

TARNES, Marte.Information Security Metrics An Empirical Study of Current Practice. Disponível em: <https://infosec.sintef.no/wp-content/uploads/2012/12/20121217-Marte-Taarnes-prosjekt-maaling-av-infosikkerhet.pdf>. Acesso em: 21 ago. 2017.

URRICO, Roy. *Call Center Threats Grow*. 2015. Disponível em: <http://www.cutimes.com/2015/04/17/call-center-threats-grow?page=1>. Acesso em: 09 out. 2017.
YEN, Josué Chin, Cuidados ao usar Domain Local groups para dar permissões a objetos no Active Directory.Disponível em: <https://blogs.technet.microsoft.com/latam/2012/01/09/cuidados-ao-usar-domain-local-groups-para-dar-permisses-a-objetos-no-active-directory/> Acesso em: 20 abr. 2018.

APÊNDICE A – DIRETRIZ OU POLÍTICA PRINCIPAL

Introdução

A PSI é o documento que estabelece condutas corporativas de um *call center* genérico para a proteção de ativos.

É baseada na norma ABNT NBR ISO/IEC 27002 e tem a intenção de aumentar a segurança da infraestrutura tecnológica direcionada à prestação de serviços de cobrança e na melhor utilização dos ativos disponibilizados pela empresa.

Escopo

Seu propósito é direcionar o *call center* por meio de diretrizes que auxiliem na redução riscos e manter a segurança da informação para garantir a continuidade dos negócios da organização.

Objetivo

A PSI tem por objetivo assegurar a integridade da informação durante todo seu ciclo e visa reduzir riscos e ameaças, a fim de preservar os ativos. Além disso, estabelece o comprometimento da direção em manter um ambiente seguro, proporcionando melhor qualidade nos processos da organização e dos controles dentro das melhores práticas da segurança da informação.

Abrangência e vigência

A PSI aplica-se a toda a organização, todos os colaboradores, terceiros e todos que acessam as informações da organização.

A PSI tem prazo de validade determinada pela direção.

Conceitos e definições

Os conceitos aplicam-se de forma a auxiliar na interpretação da PSI:

- Usuário – todo colaborador ou contratado que acessa as informações da organização;
- PA – Posição de Atendimento;
- TI – Tecnologia da Informação;
- PSI – Política de Segurança da Informação.

Princípios

- Disponibilidade: garantia de que a informação esteja acessível.
- Confidencialidade: garantia de que a informação esteja disponível somente às pessoas autorizadas pela organização.
- Integridade: garantia de que a informação não foi modificada.

Órgão Responsável

A TI é responsável por manter e atualizar esta política.

Documentos Relacionados

Esta política é complementada pelas normas de dimensões.

Penalidades

A violação da política pode acarretar em advertências e demissões.

APÊNDICE B – DIMENSÕES DE SEGURANÇA

Objetivo

Servir de complemento à norma principal e determinar o nível de segurança necessário para cada informação utilizada na organização.

Abrangência

Esta política é aplicada a todos que circulam e acessam informações no âmbito da organização.

Diretrizes

Todas as informações geradas pelos sistemas ou usuários devem ser classificadas em relação ao seu nível de exposição e risco que podem causar, podendo ser:

- Pública: informação que pode ser divulgada para todos;
- restrita ou interna: informação exclusiva a colaboradores da organização;
- confidencial: limitada ao mínimo necessário de usuários, geralmente direção.

Papéis e responsabilidades

Usuário: preservar a segurança da informação. Informar falhas.

Gestor: classificar e rotular todas as informações, conforme necessidade.

Monitoramento

Essa norma será monitorada por alguém definido pela direção da organização.

Penalidades

A violação à política pode acarretar em advertência, desligamento da empresa e, se necessário, ações jurídicas.

POLÍTICA DE CONTROLE DE ACESSO FÍSICO

Objetivo

Esta política tem por objetivo definir regras e procedimentos para acesso físico às informações e recursos da organização.

Abrangência

As regras aqui apresentadas aplicam-se a todos que acessam o interior da organização.

Diretrizes

- O acesso físico só poderá ocorrer após o cadastro na recepção da empresa;
- áreas de acesso restrito só podem ser acessadas por pessoas autorizadas;
- não é permitido o cadastro de pessoas sem apresentação de documento de identificação;
- para o cadastro, é necessário documento com foto;
- todo colaborador deve utilizar as catracas para acesso às dependências da empresa e jamais emprestar seu cartão de acesso;
- visitantes e prestadores de serviço deverão ser acompanhados por um responsável.

Papéis e responsabilidades

Todos devem verificar irregularidades na questão de acesso físico.

Monitoramento

Os gestores podem solicitar identificação para monitoria do controle de acesso físico.

Penalidades

Caso identificada a tentativa de violação de acesso físico, penalidades serão aplicadas.

POLÍTICA DE CONTROLE DE ACESSO LÓGICO

Objetivo

Esta política tem por objetivo definir apresentar a devida conduta para acesso lógico às informações, serviços e recursos de TI da organização.

Abrangência

As regras aplicam-se a todos os funcionários que utilizam os serviços ou recursos de TI da organização.

Diretrizes

- Um *login* e uma senha de acesso devem ser utilizados para cada sistema;
- não serão criados *logins* compartilhados;
- as senhas terão um tempo de vida útil pré-determinado (60 dias);
- uma senha forte (segura) deverá atender aos requisitos definidos pelo setor de TI;
- os *logins* e senhas serão bloqueados nos desligamentos dos colaboradores.

Papéis e responsabilidades

- Usuários: as senhas de acesso são de uso pessoal e intransferível e o usuário tem total responsabilidade por qualquer ação realizada por sua senha.
- TI: controle de cadastro e gerenciamento das senhas.

Monitoramento

As regras serão monitoradas pela pessoa ou setor definido(a) pela direção.

Penalidades

A tentativa de violação desta política acarretará em ação disciplinar.

POLÍTICA DE SEGURANÇA NAS OPERAÇÕES

Objetivo

Esta política tem por objetivo definir regras e procedimentos voltados à segurança nas operações na organização.

Abrangência

Aplicada a todos os colaboradores e equipamentos de processamento de informação da organização.

Diretrizes

- É proibida a instalação de qualquer *software* nas estações de trabalho;
- não é permitido guardar arquivos de cunho pessoal na estação de trabalho;
- é proibido o uso de *pen-drives*, mp3 *players*, aparelhos celulares etc.;
- não são permitidos jogos nas estações de trabalhos, sejam eles por meio da *Internet* ou instalados na própria máquina;
- a estação de trabalho pode ser monitorada remotamente;
- o acesso às informações da empresa só pode ocorrer em ambiente de trabalho;
- é proibida a cópia de qualquer informação da empresa por meio de dispositivos portáteis, mídias digitais, *e-mail* e outros.

Papéis e responsabilidades

É de responsabilidade do setor que a direção definir a verificação da procedência de *softwares*.

Monitoramento

O setor determinado pela organização deve auditar estações de trabalho.

POLÍTICA PARA USO DE DISPOSITIVOS PORTÁTEIS E DISPOSITIVOS MÓVEIS

Objetivo

Esta política tem por objetivo definir regras e procedimentos para uso de dispositivos portáteis e dispositivos móveis.

Abrangência

Esta norma aplica-se a todos que utilizam dispositivos móveis na rede de dados da organização.

Diretrizes

- É proibido o uso de dispositivos pessoais ou de terceiros na rede da empresa;
- todo equipamento ligado à rede deve ser autorizado pela equipe de segurança da empresa.

Papéis e responsabilidades

O usuário deve manter sigilo de suas credenciais de acesso ao dispositivo móvel e aos recursos disponibilizados.

Monitoramento

A rede corporativa é monitorada pelo setor de TI da organização.

Penalidades

O não cumprimento desta política pode resultar em sanções que vão desde a desativação de acesso até ações disciplinares verbais ou por escrito.

POLÍTICA DE USO DA *INTERNET*

Objetivo

Esta política tem por objetivo definir regras e procedimentos para acesso à *Internet* na organização.

Abrangência

As regras aplicam-se a todos os colaboradores, estagiários e prestadores de serviço que utilizem a *Internet* da organização.

Diretrizes

- É proibido o acesso a conteúdo considerado ofensivo, ilegal ou impróprio como pornografia, pedofilia ou recreativo;
- o acesso à *Internet* é monitorado pelos *logs* de acesso;
- *downloads* de músicas, jogos, filmes e programas são proibidos;
- o acesso a redes sociais é proibido;
- é proibido o acesso a *sites* de bate-papo, *e-mail* particular, *streaming media*, jogos e apostas;
- a liberação da *Internet* ocorre conforme perfil do usuário.

Papéis e responsabilidades

O usuário é responsável por seus acessos.

Monitoramento

Os gestores podem solicitar acesso aos *logs* de acessos de cada usuário na rede.

Penalidades

O usuário é legalmente responsabilizado pelos danos causados por ações contrárias a esta norma.

POLÍTICA DE UTILIZAÇÃO DE *E-MAIL* E MENSAGENS INSTANTÂNEAS

Objetivos

Esta política tem por objetivo definir regras e procedimentos para uso de *e-mails* na organização.

Abrangência

Aplicada a todos que usam *e-mail* na organização.

Diretrizes

- É proibido o uso do *e-mail* para assuntos pessoais;
- deve ser evitado o envio de anexos por *e-mail* sempre que possível. Existemformas mais adequadas para o compartilhamento de arquivos;
- é proibido o uso de *e-mails* pessoais para assuntos profissionais relacionados à empresa;
- sempre que houver desconfiaça quando a um *e-mail* recebido, deve-se acionar a equipe de TI para que seja realizada uma verificação;
- é proibido enviar qualquer *e-mail* que faça uma corrente, ou seja, arquivos que possuem uma mensagem e, no final, pedem para que as pessoas a encaminhem para outros. Nesse caso, estão inclusos alertas de segurança, aviso de vírus, promoções de qualquer empresa (sempre fictícias, pois não há como monitorar para quem o e-mail é enviado), alerta quanto a criança desaparecida ou doente, promoção que envolva termos como “pague menos/não pague por determinado produto/serviço”, piadas, entre outros;
- deve-se evitar o envio de *e-mails* para mais de 10 destinatários de uma única vez;
- relatórios devem ser evitados, pois existem sistemas próprios;
- comunicação interna deve passar pelo departamento competente, que avaliará e decidirá a melhor forma de realizar a comunicação;
- todos os e-mails são monitorados.

Papéis e responsabilidades

O usuário deve respeitar as diretrizes da norma. Ele é o único responsável pelo conteúdo das transmissões feitas por meio do serviço a partir de sua senha ou conta.

Monitoramento

- Gestores: podem solicitar acesso aos *e-mails* dos seus subordinados sempre que houver a necessidade.
- TI: deve analisar *logs* dos *e-mails* enviados.

Penalidades

A utilização do *e-mail* corporativo deve ter finalidade única e exclusiva ao negócio e pode acarretar em advertências, suspensões e até demissão por justa causa se não seguidas as diretrizes de uso.

POLÍTICA DE USO DAS IMPRESSORAS

Objetivos

Esta política tem por objetivo definir regras e procedimentos para o uso da impressora na organização.

Abrangência

As regras aqui dispostas aplicam-se a todos os colaboradores que utilizam as impressoras da organização.

Diretrizes

- A impressão de documentos deve ser somente para atividades da empresa;
- não é permitido imprimir documentos pessoais ou de interesse pessoal;
- é proibido sair da empresa com documento impresso;
- o descarte deve ser efetuado corretamente.

Papéis e responsabilidades

O usuário deve respeitar todas as diretrizes e orientações em relação à impressão.

Monitoramento

Os gestores podem solicitar acessos aos *logs* de impressão para auditorias.

Penalidades

A utilização das impressoras corporativas para fins pessoais pode resultar em advertências ou demissões.

POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

Objetivos

Esta política tem por objetivo definir regras e procedimentos para a classificação da informação na organização.

Abrangência

Esta norma aplica-se aos usuários que desenvolvem atividades de criação, processamento, comunicação, descarte e armazenamento de informações na organização.

Diretrizes

- Todas as informações geradas por sistemas ou usuários deverão ser classificadas em relação ao seu grau de exposição, podendo ser:

  a) Pública: pode ser distribuída sem restrição, inclusive exposta na *Internet*;

  b) interna: limitada ao público interno da organização;

  c) restrita: limitada ao grupo de usuários envolvidos com o assunto;

  d) confidencial: limitada ao mínimo necessário de usuários.
- Toda informação gerada por sistemas ou usuários é considerada de uso confidencial da organização por padrão;
- toda informação pode ser reclassificada conforme a necessidade do negócio;
- informações confidenciais devem ser descartadas de forma qualificada.

Papéis e responsabilidades

- Usuário: preservar o grau de exposição da informação.
- Gestor: classificar ou reclassificar as informações que são de sua responsabilidade, além de conscientizar os colaboradores do risco da exposição da informação.

Monitoramento

Os gestores podem auditar as normas de classificação da informação.

Penalidades

O não cumprimento desta política pode acarretar advertências, suspensões e até demissão por justa causa.

APÊNDICE C – PADRÃO PARA UM MODELO DE MEDIÇÃO EM SEGURANÇA DA INFORMAÇÃO

(continua)

Identificação do modelo de medição	
Nome do modelo de medição	
Identificador numérico Propósito do modelo da medição Objetivo de controle/processo Controle(1)/Processo(1) Controle(2)/Processo(2)	
Objeto de medição e atributos	
Objeto de medição Atributo	
Especificação da Medida Básica (medida para cada base [1...n])	
Medida Básica	
Método de medição	
Tipo do método de medição	
Escala	
Tipo da escala	
Unidade de medição	
Especificação de medida derivada	
Medida derivada	
Função de medição	
Especificação de indicador	
Indicador Modelo Analítico	
Especificação do critério de decisão	
Critério de decisão	
Resultado da medição	
Interpretação do indicador	
Formatos de relatórios	
Partes interessadas	
Cliente da medição Revisor da medição	
Proprietário da informação	

(conclusão)

Partes interessadas	
Coletor da informação	
Comunicador da informação	
Frequência / período	
Frequência de coleta dos dados	
Frequência de análise dos dados	
Frequência de relato dos resultados da medição	
Revisão de medição	
Período de medição	

APÊNDICE D – POLÍTICA PRINCIPAL DA EMPRESA BETA

Introdução

Este documento estabelece os regulamentos da empresa BETA, que visam à proteção dos ativos e deve ser cumprida e aplicada em todas as áreas da organização. Essa política está baseada na norma ABNT NBR ISO/IEC 27002 e está aprovada pela direção da organização.

A política aqui descrita tem o objetivo de aumentar a segurança da infraestrutura tecnológica da organização, além de visar à orientação dos colaboradores para a melhor utilização dos ativos disponibilizados pela empresa.

Escopo

Este documento é uma declaração formal do compromisso com a proteção das informações da empresa. Seu propósito é direcionar o *call center* no que diz respeito aos riscos e ameaças por meio de condutas, e visa à redução de ocorrência de riscos, a fim de garantir a continuidade dos negócios da organização.

Objetivo

Esta política objetiva instituir diretrizes, responsabilidades e competências, visando assegurar a disponibilidade, integridade e confidencialidade das informações durante todo o seu ciclo de vida, bem como garantir que os documentos e conhecimentos produzidos, armazenados ou transmitidos, estejam seguros contra ameaças e vulnerabilidades, de modo a preservar esses ativos. Estabelece também o comprometimento da direção da empresa com o devido apoio para implementação e continuidade da segurança da informação para a criação de um ambiente seguro, proporcionando melhor qualidade nos processos do negócio dentro das melhores práticas da segurança da informação.

Abrangência e vigência

A política é aplicada aos servidores, funcionários e colaboradores externos que prestam serviço à organização. O prazo de validade estabelecido pela organização foi de 2 anos e deve ser atualizado em cada nova edição da norma.

Princípios

As ações relacionadas à segurança da informação na organização são norteadas pelos seguintes princípios assim definidos:

- Confidencialidade: somente pessoas autorizadas devem ter acesso à informação.
- Integridade: garantia de que a informação disponibilizada pelo autor não sofreu nenhuma alteração e manteve-se íntegra.
- Disponibilidade: garantia de que a informação estará disponível em qualquer momento, sempre que forem solicitadas, e para o funcionamento da organização.

Órgão responsável

A TI é responsável por manter e atualizar esta política.

Documentos relacionados

Esta política é complementada pelas normas específicas de dimensões de segurança em conformidade e aprovadas pela direção da organização.

Penalidades

A não aderência à política de segurança da informação é considerada grave e pode gerar ações que podem ser aplicadas conforme a lei.

APÊNDICE E – DIMENSÕES DE SEGURANÇA DA EMPRESA BETA

Objetivo

Este apêndice serve de complemento à norma principal. Os responsáveis pelos sistemas da organização devem utilizar este complemento para determinar o nível de segurança adequado para as atividades que estão sob sua responsabilidade.

Abrangência

Esta política é aplicada a todos os colaboradores, prestadores de serviço e demais pessoas que exercem atividades e tenham acesso à informação da empresa BETA.

Diretrizes

Todas as informações geradas pelos sistemas ou usuários devem ser classificadas em relação ao seu nível de exposição e risco que pode causar, podendo ser:

- Pública: informação que pode ser divulgada para o público em geral;
- restrita ou interna: informação restrita a funcionários da empresa;
- confidencial: informação de grande valor ao negócio e que deve ser limitada ao mínimo necessário de usuários.

Papéis e responsabilidades

- Usuário: proteger a informação de exposições indevidas, de acordo com sua classificação. Ao identificar falhas de segurança, reportar ao gestor imediatamente.
- Gestor: classificar e rotular todas as informações sob sua responsabilidade. Reportar à TI os problemas de segurança de informação. Conscientizar os usuários quanto ao grau de exposição das informações.

Monitoramento

Esta norma será monitorada pelos gestores e pela TI.

Penalidades

Caso identificada a tentativa de violação das normas deste documento, uma ação disciplinar será aplicada, podendo ser advertências ou desligamento da empresa, combinada a ações civis e criminais, quando cabíveis.

POLÍTICA DE CONTROLE DE ACESSO LÓGICO – POLÍTICAS DE SENHAS

Objetivo

Esta política define regras e procedimentos para acesso lógico às informações, serviços e recursos de TI da organização.

Abrangência

As regras aplicam-se a todos os funcionários, estagiários e prestadores de serviço que utilizem os recursos de TI da organização.

Diretrizes

- Todos os usuários da organização devem possuir um *login* único e uma senha única de acesso para cada sistema que for utilizar;
- não serão criados *logins* compartilhados;
- as senhas terão um tempo de vida útil pré-determinado (30 dias);
- é obrigatória a utilização de senhas fortes para autenticação nos computadores e sistemas da empresa, devendo atender aos requisitos:

a) Tamanho: no mínimo 8 caracteres. Estes devem incluir pelo menos 3 dos 4 tipos abaixo:

  - Letras maiúsculas;
  - letras minúsculas;
  - números;
  - caracteres especiais.

- Os *logins* e senhas serão bloqueados quando forem desnecessários.

Papéis e responsabilidades

- Usuário: as senhas de acesso são pessoais e intransferíveis e o usuário tem total responsabilidade por qualquer ação realizada por sua senha.
- TI: deve realizar o gerenciamento de senhas.

Monitoramento

As regras serão monitoradas pelo setor de TI da organização.

Penalidades

Caso identificada a tentativa de violação de senhas de acesso, uma ação disciplinar será aplicada.

POLÍTICA DE CONSCIENTIZAÇÃO DE SEGURANÇA NAS OPERAÇÕES

Objetivo

Esta política define regras e procedimentos voltados à segurança nas operações na organização, bem como a conscientização dos colaboradores quanto aos riscos à segurança da informação.

Abrangência

Todos os equipamentos e processos que criam, manipulam e descartam a informação na organização.

Diretrizes

- A instalação de qualquer *software* nas estações de trabalho só poderá ser feita pela TI;
- não é permitido guardar arquivos de cunho pessoal na estação, apenas arquivos que sejam homologados e instalados pela TI da empresa, e nem utilizar a estação para fins não profissionais;
- é proibido o uso de periféricos USB;
- todos os dados relativos ao trabalho devem ser mantidos na rede, na qual existe controle de *backup*. Arquivos armazenados localmente nas estações poderão ser excluídos sem aviso prévio;
- o uso da estação de trabalho e de seus aplicativos é monitorado remotamente;
- o acesso às informações da empresa só pode ocorrer em ambiente de trabalho;
- é proibida a cópia ou divulgação de qualquer informação da empresa por meio de dispositivos portáteis, mídias digitais, *e-mail* e outros.

Papéis e responsabilidades

O setor de TI deve controlar e verificar a procedência de *softwares* adquiridos de terceiros.

Monitoramento

O setor de TI realiza auditorias de *software* periodicamente, visando à conformidade de seus ativos de *software* e combate à pirataria.

Penalidades

Caso identificada a tentativa de violação de senhas de acesso, uma ação disciplinar será aplicada.

POLÍTICA DE USO DA *INTERNET*

Objetivo

Esta política determina regras e procedimentos para acesso à *Internet* na organização.

Abrangência

As regras aplicam-se a todos os colaboradores, estagiários e prestadores de serviço que utilizem a *Internet* da organização.

Diretrizes

- É proibido o acesso ao conteúdo considerado ofensivo, ilegal ou impróprio, ou seja, que não compete ao negócio da organização;
- o acesso à *Internet* é controlado pelo *firewall*, que gerencia acessos e permissões;
- a liberação da *Internet* é baseada no perfil do usuário.

Papéis e responsabilidades

- Usuário: cabe a todos os usuários da organização zelar pelo seu próprio usuário de acesso.
- TI: gerenciar acessos e auditar *logs* de acessos.

Monitoramento:

Os gestores podem solicitar acesso aos *logs* de acessos de cada usuário na rede.

Penalidades:

O uso indevido do acesso à *Internet* é de responsabilidade do usuário, podendo o mesmo ser responsabilizado legalmente pelos danos causados.

POLÍTICA DE UTILIZAÇÃO DE *E-MAIL*

Objetivos

Esta política estabelece regras e procedimentos para uso de *e-mails* e mensagens instantâneas na organização.

Abrangência

As regras aplicam-se a todos os colaboradores, estagiários e prestadores de serviço que utilizem *e-mail* na organização.

Diretrizes

- É proibido o uso do *e-mail* para assuntos pessoais;
- deve ser evitado o envio de anexos por *e-mail* sempre que possível;
- é proibido o uso de *e-mails* pessoais para assuntos profissionais relacionados à empresa;
- é proibido enviar informações da organização para *e-mails* que não competem ao negócio da empresa;
- todos os *e-mails* são monitorados.

Papéis e responsabilidades

O usuário é responsável pelo conteúdo dos *e-mails* e, constatada irregularidade, será penalizado conforme gravidade e impacto ao negócio.

Monitoramento

Os gestores podem solicitar acesso aos *e-mails* dos seus subordinados sempre que houver necessidade.

TI pode auditar *e-mails* a cada espaço de tempo determinado pela direção.

Penalidades

A utilização do *e-mail* corporativo deve ter finalidade exclusivamente profissional, logo advertências, suspensões e até demissão por justa causa são penalidades que podem ser aplicadas caso haja irregularidade.

POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

Objetivos

Esta política determina regras e procedimentos para a classificação da informação na organização.

Abrangência

Esta norma aplica-se aos usuários que estejam relacionados à criação, manipulação, comunicação e armazenamento de informações na organização

Diretrizes

- Todas as informações geradas por sistemas ou usuários deverão ser classificadas em relação ao seu grau de exposição, podendo ser:

  a) Pública: pode ser distribuída sem restrição;

  b) interna: limitada ao público interno da organização;

  c) restrita: limitada ao grupo de usuários envolvidos com o assunto;

  d) confidencial: limitada ao mínimo necessário de usuários.
- Toda informação criada na organização é considerada de uso confidencial da organização por padrão;
- toda informação pode ser reclassificada conforme a necessidade do negócio;
- o processo de classificação da informação deve acontecer tanto no formato eletrônico como no físico;
- controles de acesso poderão aplicar medidas restritivas evitando a exposição das informações.

Papéis e responsabilidades

- Usuário: preservar o grau de exposição da informação, conforme sua classificação.
- Gestor: classificar ou reclassificar as informações que são de sua responsabilidade.

Monitoramento

Os gestores podem auditar as normas de classificação da informação.

Penalidades

O não cumprimento desta política pode acarretar advertências, suspensões e até demissão por justa causa.

POLÍTICA DE CONTROLE DE DIVULGAÇÃO DE INFORMAÇÃO NAS LIGAÇÕES

Objetivo

Esta política define as condutas ao efetuar ligações no âmbito da organização.

Abrangência

As regras aplicam-se a todos os operadores da organização.

Diretrizes

- É proibida a divulgação de qualquer informação da empresa por meio das ligações efetuadas;
- o operador deve seguir o *script* elaborado pela equipe da monitoria;
- a comunicação referente às informações da empresa só pode ocorrer em ambiente de trabalho;
- as ligações são monitoradas e armazenadas com a finalidade de auditoria;
- o uso do *software* de discador é restrito a atividades do negócio e não de uso pessoal.

Papéis e responsabilidades

- Usuário: tem total responsabilidade por qualquer divulgação indevida de informação realizada por sua senha.
- Setor de Monitoria: faz a monitoria das ligações.

Monitoramento

As ligações serão monitoradas pelo setor de monitoria da organização.

Penalidades

Caso identificada a divulgação indevida de informações, uma ação disciplinar será aplicada.

APÊNDICE F – MEDIÇÃO DE EFICIÊNCIA DOS CONTROLES

Quadro 15 – Medição de eficiência do controle de acesso lógico – política de senha

(continua)

Identificação do modelo de medição	
Nome do modelo de medição	**Qualidade da senha**
Identificador numérico	1
Propósito do modelo da medição	Avaliar a qualidade de senhas usadas pelos usuários para acessar os sistemas da organização BETA.
Objetivo de controle/processo	Prevenir os colaboradores de escolherem senhas inseguras, a fim de dificultar *hacks* e, por meio do apêndice F, compreender o que os colaboradores entendem por senha segura e confidencialidade da mesma.
Controle(1)/Processo(1)	Deve ser exigido que os usuários sigam as diretrizes de segurança ao escolher e usar senhas. Todos os usuários devem escolher senhas fortes para todos os sistemas da organização BETA, as quais devem: 1. Ser maiores que 8 caracteres. 2. Não ser baseadas em algo relacionado à pessoa, nomes, números de telefone, data nascimento, etc. 3. Não consistir em palavras do dicionário. 4. Não ter caracteres idênticos consecutivos.
Objeto de medição e atributos	
Objeto de medição	Banco de dados de senha de usuários.
Atributo	Senhas individuais
Especificação da Medida Básica (1)	
Medida Básica	1. Número de senhas existentes 2. Número de senhas que satisfazem à política de senhas
Método de medição	1. Contabilizar o número de senhas no banco de dados; 2. Contabilizar o número de senhas que que satisfazem à política de senha;
Tipo do método de medição	1. Objetivo 2. Objetivo

(continuação)

Especificação da Medida Básica (1)	
Escala	1. Inteiros de 0 até infinito; 2. Inteiros de 0 até infinito;
Tipo da escala	1. Ordinal 2. Ordinal
Unidade de Medição	1. Senhas 2. Senhas
Especificação de medida derivada	
Medida derivada	Número total de senhas que atendam aos requisitos de segurança.
Função de medição	Razão entre o número total de senhas e as que atendam aos requisitos de segurança para cada usuário, vezes 100
Especificação de indicador	
Indicador	1. Razão de senhas que atendem ao requisito de segurança. 2. Tendência da situação de conformidade relacionada à política de senha.
Modelo Analítico	1. Dividir o número total de senhas em conformidade, pelo número de senhas registradas. 2. Comparar com a razão anterior.
1. **Especificação do critério de decisão**	
Critério de decisão	Quando o resultado da razão for maior que 90%, o objetivo é atingido e não é necessário tomar nenhuma ação. Se estiver entre 80% e 90%, o objetivo não é atingido, mas a tendência indica melhora. Se for menor que 80%, deve-se tomar ações imediatas.
Resultado da medição	
Interpretação do indicador	1. Satisfatório, se a razão é maior que 90%; atingido insatisfatoriamente, se a razão é maior que 80% e menor ou igual a 90%. não atingido, se a razão é menor que 80%. 2. Tendência ascendente indica melhoria e descendente indica não conformidade. O impacto de não ser atingido aumenta o risco de violações de confidencialidade.
Formatos de relatórios	Gráfico de linha que descreve o número de senhas em conformidade sobreposta com as tendências produzidas anteriormente.

(conclusão)

Partes interessadas	
Cliente da medição	Direção
Revisor da medição	Gestor de TI
Proprietário da informação	Alexandre Tagliari
Coletor da informação	Alexandre Tagliari
Comunicador da informação	Alexandre Tagliari
Frequência/período	
Frequência de coleta dos dados	1 mês
Frequência de análise dos dados	1 mês
Frequência de relato dos resultados da medição	Mensal
Revisão de medição	12 meses
Período de medição	12 meses

Quadro 16 – Medição de eficiência do controle de conscientização de segurança nas operações

(continua)

Identificação do modelo de medição	
Nome do modelo de medição	Conformidade da política de segurança nas operações
Identificador numérico	2
Propósito do modelo da medição	Treinar e conscientizar os colaboradores no que diz respeito à segurança da informação na organização.
Objetivo de controle/processo	Assegurar que os colaboradores estão conscientes e cumprem com suas responsabilidades pela segurança da informação, a fim de reduzir o risco de erro humano.
Controle(1)/Processo(1)	Todos os funcionários da organização BETA devem receber treinamento, atualizações e conscientizações apropriadas quanto às políticas e procedimentos relevantes para suas funções.
Controle(2)/Processo(2)	A direção deve solicitar aos funcionários que pratiquem a segurança da informação de acordo com o estabelecido nas políticas da organização.

(continuação)

Objeto de medição e atributos	
Objeto de medição	Colaboradores que assinaram os termos de responsabilidade.
Atributo	1. Colaboradores que assinaram os termos de responsabilidade. 2. Colaboradores presentes no treinamento
Especificação da Medida Básica (1)	
Medida Básica	2. Número de colaboradores presentes para o treinamento. 3. Número de colaboradores que assinaram o termo de responsabilidade.
Método de medição	1. Contar o número de colaboradores presentes para assinar o termo de responsabilidade. 2. Contabilizar o número de colaboradores que efetivamente assinaram o termo de responsabilidade.
Tipo do método de medição	1. Objetivo 2. Objetivo
Escala	1. Inteiros de 0 até o infinito; 2. Inteiros de 0 até o infinito;
Tipo da escala	1. Ordinal 2. Ordinal
Unidade de medição	1. Pessoal 2. Pessoal
Especificação de medida derivada	
Medida derivada	Número de pessoal que assinou o termo de ciência da PSI.
Função de medição	Dividir os colaboradores que assinaram pelos que estavam planejados assinar o termo, vezes 100
Especificação de indicador	
Indicador	1. Expresso pela razão de pessoas presentes e que assinaram. 2. Tendência da situação de conscientização.
Modelo analítico	1. Dividir a quantidade de pessoas presentes pela quantidade de pessoas que efetivamente assinaram o termo na data do treinamento. 2. Comparar a situação com as anteriores.

(conclusão)

Especificação do critério de decisão	
Critério de decisão	1. A razão deve ter como resultado 100%. 2. Tendência deve ser ascendente ou estável.
Resultado da Medição	
Interpretação do indicador	Satisfatoriamente atendido, se em todos treinamentos obtiver 100% de assinaturas.
Formatos de relatórios	Gráfico com os intervalos satisfatórios e resultados das análises.
Partes interessadas	
Cliente da medição	Direção
Revisor da medição	Gestor de TI
Proprietário da informação	Alexandre Tagliari
Coletor da Informação	Alexandre Tagliari
Comunicador da informação	Alexandre Tagliari
Frequência/período	
Frequência de coleta dos dados	Mensal
Frequência de Análise dos dados	Mensal
Frequência de relato dos resultados da medição	Mensal
Revisão de medição	12 meses
Período de medição	12 meses

Quadro 17 – Medição de eficiência do controle de processamento ilegal de dados via *Internet*

(continua)

Identificação do modelo de medição	
Nome do modelo de medição	Controle de processamento ilegal de dados via *Internet*
Identificador numérico	3
Propósito do modelo de medição	Avaliar a conformidade de processamentos de dados via *Internet*
Objetivo de controle/processo	Avaliar a situação de conformidade do processamento de dados via *Internet*.

(continuação)

Identificação do modelo de medição	
Controle(1)/Processo(1)	Detectar atividades de processamento ilegal de dados não autorizado por meio dos *logs* fornecidos por *software.*
Objeto de medição e atributos	
Objeto de medição	Histórico de acessos.
Atributo	Arquivos de registros (*logs*) individuais
Especificação da Medida Básica (1)	
Medida Básica	1. Número de *logs* totais. 2. Número de *logs* sem irregularidades
Método de medição	1. Contabilizar o número de *logs* totais. 2. Contabilizar o número de *logs* sem irregularidades.
Tipo do método de medição	1. Objetivo 2. Objetivo
Escala	1. Inteiros de zero até o infinito 2. Inteiros de zero até o infinito
Tipo da escala	1. Ordinal 2. Ordinal
Unidade de medição	*1. Logs* *2. Logs*
Especificação de medida derivada	
Medida derivada	Número total de l*ogs* que atendam aos requisitos de regularidade.
Função de medição	Razão entre os arquivos de *logs* analisados e os sem irregularidades, vezes 100.
Especificação de indicador	
Indicador	Gráfico de linha da tendência dos períodos de tempo em que foi efetuada auditoria dos *logs.*
Modelo analítico	Tendência ascendente em direção a 100% é desejável.
Especificação do critério de decisão	
Critério de decisão	Examinar as causas de irregularidades, se o resultado for maior que 5%.
Resultado da medição	
Interpretação do indicador	Direção definiu como aceitável até 5% de irregularidades. Caso haja mais que 5%, deve ser tomada alguma ação.
Formatos de relatórios	Gráfico de linhas informando o percentual de *logs* regulares nas datas de análise.
Partes interessadas	
Cliente da medição	Direção
Revisor da medição	Gestor de TI
Proprietário da informação	Alexandre Tagliari
Coletor da Informação	Alexandre Tagliari

Comunicador da informação	Alexandre Tagliari

(conclusão)

Frequência/período	
Frequência de coleta dos dados	15 dias
Frequência de análise dos dados	15 dias
Frequência de relato dos resultados da medição	Mensal
Revisão de medição	12 meses
Período de medição	12 meses

Quadro 18 – Medição de eficiência do controle de processamento ilegal de dados via *e-mail*

(continua)

Identificação do modelo de medição	
Nome do modelo de medição	Controle de processamento ilegal de dados via *e-mail*.
Identificador numérico	4
Propósito do modelo de medição	Avaliar a divulgação de informações e dados via *e-mail*.
Objetivo de controle/processo	Avaliar a situação de conformidade dos dados enviados via *e-mail*.
Controle/Processo	Detectar com o uso de *software* as atividades de divulgação ilegal de dados não autorizado através dos *e-mails*.
Objeto de medição e atributos	
Objeto de medição	E-mails
Atributo	Análise das extensões dos anexos dos e-mails individuais
Especificação da Medida Básica (1)	
Medida Básica	1. Número de e-mails analisados 2. Número de e-mails analisados com irregularidade.
Método de medição	1. Contabilizar o número de e-mails analisados 2. Contabilizar o número de e-mails analisados que satisfazem à política de senha;
Tipo do método de medição	1. Objetivo 2. Objetivo
Escala	1. Numérico 2. Numérico

Tipo da escala	1. Inteiros de 0 até infinito; 2. Inteiros de 0 até infinito;

(conclusão)

Unidade de Medição	1. E-mails 2. E-mails
Especificação de medida derivada	
Medida derivada	Número total de *e-mails* que atendam aos requisitos de regularidade.
Função de medição	Razão entre os e-mails analisados e os sem irregularidades vezes 100
Especificação de Indicador	
Indicador	Gráfico de linha da tendência dos períodos de tempo em que foi efetuada auditoria dos e-mails.
Modelo Analítico	Tendência ascendente em direção a 100% é desejável
Especificação do Critério de Decisão	
Critério de decisão	Examinar as causas de irregularidades se o resultado for maior que 5% de irregularidades
Resultado da Medição	
Interpretação do indicador	Direção definiu até 5% de irregularidades como aceitável. Mais que 5% de irregularidades deve ser tomada alguma ação.
Formatos de relatórios	Gráfico de linhas informando o percentual de e-mails regulares nas datas de análise.
Partes interessadas	
Cliente da medição	Direção
Revisor da medição	Gestor de TI
Proprietário da informação	Alexandre Tagliari
Coletor da informação	Alexandre Tagliari
Comunicador da informação	Alexandre Tagliari
Frequência / Período	
Frequência de coleta dos dados	15 dias
Frequência de análise dos dados	15 dias
Frequência de relato dos resultados da medição	Mensal
Revisão de medição	12 meses

Período de medição	12 meses

Fonte: Elaborado pelo autor (2017).

Quadro 19 – Medição de eficiência do controle de classificação da informação

(continua)

Identificação do modelo de medição	
Nome do modelo de medição	Controle de classificação da informação
Identificador numérico	5
Propósito do modelo da medição	Mostrar a qualidade da classificação da informação.
Objetivo de controle/processo	Prevenir que a informação seja disponibilizada de forma equivocada.
Controle(1)/Processo(1)	A informação deve ser classificada e disponibilizada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.
Objeto de medição e atributos	
Objeto de medição	Informações criadas, manipulas e armazenadas
Atributo	Informações contidas nos servidores aos quais a operação de *call center* acessa.
Especificação da Medida Básica	
Medida Básica	1. Número usuários com acesso indevido a informações com acessos restritos. 2. Número de usuários com devido acesso a informações restritas.
Método de medição	1. Contar o número de usuários com acesso indevido a informações com acessos restritos. 2. Contar o número de usuários com o devido acesso a informações restritas.
Tipo do método de medição	1. Objetiva 2. Objetiva
Escala	1. Inteiros de zero até 500; 2. Inteiros de zero até 500.
Tipo da escala	1. Ordinal
Unidade de Medição	1. Permissões de usuários 2. Permissões de usuários
Especificação de medida derivada	
Medida derivada	Número total de usuários que estão em conformidade com sua classificação.
Função de medição	Razão do número total de usuários analisados e o total de usuários que estão em conformidade com sua classificação vezes 100
Especificação de Indicador	

Medida derivada	Número total de usuários que estão em conformidade com sua classificação.

(continuação)

Função de medição	Razão do número total de usuários analisados e o total de usuários que estão em conformidade com sua classificação vezes 100
Especificação de Indicador	
Indicador	a) Razão entre os usuários analisados e os analisados em conformidade à classificação da informação.
Modelo Analítico	a) Dividir o total de usuários analisados pelos usuários em conformidade com sua classificação.
Especificação do Critério de Decisão	
Critério de decisão	Se o resultado da razão for maior que 85%, o objetivo do controle é atingido e não há necessidade de ações. Abaixo de 85% deve-se tomar uma ação imediata.
Resultado da Medição	
Interpretação do indicador	Satisfatório se o valor da razão for maior ou igual a 90%. Inferior a 90% o critério de conformidade não está atingido. O impacto do critério não ser atendido é um maior risco de violações à confidencialidade, divulgação indevida das informações causadas pela engenharia social.
Formatos de relatórios	Gráfico de linha informando o percentual de informações em conformidade com sua classificação e histórico das avaliações anteriores.
Partes interessadas	
Cliente da medição	Direção
Revisor da medição	Gestor de TI
Proprietário da informação	Alexandre Tagliari
Coletor da Informação	Alexandre Tagliari
Comunicador da informação	Alexandre Tagliari
Frequência / Período	

Frequência de coleta dos dados	15 dias
Frequência de Análise dos dados	15 dias

(conclusão)

Frequência de relato dos resultados da Medição	Mensal
Revisão de medição	12 meses
Período de medição	12 meses

Fonte: Elaborado pelo autor (2017).

Quadro 20 – Medição de eficiência do controle de informações no contato telefônico

(continua)

Identificação do modelo de medição	
Nome do modelo de medição	Controle de divulgação indevida de informação através do contato telefônico.
Identificador numérico	6
Propósito do modelo de medição	Avaliar a conformidade de divulgação de informação através do contato telefônico.
Objetivo de controle/processo	Avaliar a situação de divulgação indevida de informação através do contato telefônico.
Controle(1)/Processo(1)	Detectar atividades de divulgação ilegal de dados não autorizados através de escutas de ligações.
Objeto de medição e atributos	
Objeto de medição	Gravação das ligações
Atributo	Gravação de ligações individuais
Especificação da Medida Básica	
Medida Básica	1. Número de ligações analisadas 2. Número de ligações analisadas com irregularidade.
Método de medição	1. Adicionar o total de ligações à lista de ligações para análise crítica.
Tipo do método de medição	1. Objetivo 2. Objetivo
Escala	1. Numérico 2. Numérico
Tipo da escala	1. Ordinal 2. Ordinal
Unidade de Medição	1. Ligações 2. Ligações
Especificação de medida derivada	
Medida derivada	Porcentagem de auditorias nas ligações analisadas quando requerido por um

	determinado tempo.
Função de medição	Razão entre os arquivos de ligações analisadas e as sem irregularidades vezes 100.
Especificação de Indicador	

(conclusão)

Indicador	Gráfico de linha da tendência dos períodos de tempo em que foi efetuada auditoria das ligações.
Modelo Analítico	Tendência ascendente em direção a 100% é desejável.
Especificação do Critério de Decisão	
Critério de decisão	Examinar as causas de irregularidades se o resultado for maior que 10% de irregularidades.
Resultado da Medição	
Interpretação do indicador	Direção definiu até 10% de irregularidades como aceitável. Mais que 10% de irregularidades, deve ser tomada alguma ação.
Formatos de relatórios	Gráfico de linhas informando o percentual de irregularidade nas datas de análise.
Partes interessadas	
Cliente da medição	Direção
Revisor da medição	Gestor de TI
Proprietário da informação	Alexandre Tagliari
Coletor da Informação	Setor de Monitoria
Comunicador da informação	Alexandre Tagliari
Frequência / Período	
Frequência de coleta dos dados	15 dias
Frequência de Análise dos dados	15 dias
Frequência de relato dos resultados da medição	Mensal
Revisão de medição	12 meses
Período de medição	12 meses

Fonte: Elaborado pelo autor (2017).

APÊNDICE G – TERMO DE CONFIDENCIALIDADE, COMPROMISSO E SIGILO

Eu, _____, assumo ter lido, estar ciente e de acordo com a política de segurança da informação, da mesma maneira que seus documentos complementares como as obrigações, os deveres, as penalidades, diretrizes e recomendações.

Declaro a ciência de que a PSI está a disposição impressa no RH da organização e na página inicial da *intranet* da empresa BETA, podendo ser requisitada ao RH a qualquer momento.

Declaro estar ciente de que os acessos a *Internet*, o conteúdo das mensagens enviadas por *e-mail* são da minha responsabilidade, bem como todos os recursos de TI disponíveis, visto que seu uso é restrito ao uso profissional.

Comprometo-me a manter total sigilo em relação a toda informação a que tiver acesso da empresa BETA, e não manipular estas informações para benefício próprio ou de terceiros.

Responsabilizo-me por todos colaboradores e terceiros que obtiverem acesso as informações confidenciais da organização, onde eu seja responsável.

Caxias do Sul, _____ de _____ de _____.

Nome Legível: _____

CPF: _____

TESTEMUNHAS:

1) _____

2) _____