Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

MARCO ERICK PEREIRA MARQUES

DEFINIÇÃO E IMPLANTAÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NUMA EMPRESA DE GESTÃO DA SAÚDE – UM ESTUDO DE CASO

BRASÍLIA
2016

MARCO ERICK PEREIRA MARQUES

DEFINIÇÃO E IMPLANTAÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NUMA EMPRESA DE GESTÃO DA SAÚDE – UM ESTUDO DE CASO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Redes de Computadores com ênfase em Segurança.

Orientador: Prof. M.Sc. Gilberto de Oliveira Netto

BRASÍLIA
2016

MARCO ERICK PEREIRA MARQUES

DEFINIÇÃO E IMPLANTAÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NUMA EMPRESA DE GESTÃO DA SAÚDE – UM ESTUDO DE CASO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu em* Redes de Computadores com ênfase em Segurança.

Orientador: Prof. M.Sc. Gilberto de Oliveira Netto

Brasília, 30 de março de 2017.

Banca Examinadora

_____

Prof. M.Sc. Gilberto de Oliveira Netto

_____

Prof. Gilson Ciarallo

_____

Prof. Robertson Schitcoski

DEDICATÓRIA

A Deus, toda honra e toda glória das minhas decisões, ações e conquistas, sem a fé no criador, nenhum sonha se torna real em minha vida.
A minha querida esposa e companheira Letícia Targine pela compreensão e apoio, por ter administrado nosso lar e cuidado das responsabilidades de mãe das nossas duas filhas lindas e ativas!
As minhas filhas, verdadeiras princesas, Yasmin e Victória, os dois motivos de meu esforço contínuo em se tornar um homem melhor e um pai honrado e amado por essas bênçãos de Deus.
Ao meu pai Sebastião que é o meu exemplo de fé e conquista das bênçãos de Deus. Um grande guerreiro!
A minha mãe Maria da Penha que sempre me apoiou a seguir o extinto de vencedor e acreditar que grandes coisas o Senhor Deus preparou para minha vida.
A minha querida avó Maria Marques *in memorian*, que foi muito mais que uma avó, foi um grande exemplo de simplicidade e humildade e que tive a honra de viver a aprender na prática o significado de disciplina, obediência e respeito ao próximo.

AGRADECIMENTOS

A Deus pela inteligência e sabedoria que me deu. Porque dEle, por Ele e para Ele são todas as coisas. Obrigado Senhor!
Ao meu Professor Orientador Gilberto de Oliveira Netto, pelo empenho e êxito na aplicação de sua disciplina, pela atenção, dedicação e apoio na elaboração desta obra.
A Professora Tânia Cristina pelas envolventes e motivadoras aulas, com criatividade nas abordagens dos assuntos que nos dão ideias e nos incentivam a concluir uma obra com méritos.

RESUMO

O presente trabalho foi baseado na aplicação de conceitos e metodologias extraídos de livros de autores consagrados e conhecedores das melhores práticas em Segurança da Informação que se baseiam nas normas ABNT ISO/IEC 27001 e 27002. O principal objetivo é demonstrar o cenário de uma Empresa do ramo da Saúde que identificou fraquezas na segurança das suas informações e implantou medidas para reduzir os riscos e evitar possíveis perdas, tanto financeiras como relacionadas com a sua imagem. Para isso, o envolvimento da alta direção foi primordial, onde envidaram os recursos necessários para alcançar seus objetivos. Com essas demonstrações de comprometimento iniciou-se uma cultura diferenciada na organização, aplicando técnicas, ferramentas e campanhas de conscientização, treinamento e divulgação das políticas elaboradas, tudo para contribuir com a excelência dos serviços prestados na seara da saúde ocupacional. Para preservação da imagem, foi usado de forma fictícia o nome da Empresa HL Saúde em relação à verdadeira Empresa que é referência nacional dentre as demais neste ramo de atuação e optou por não ter sua imagem exposta.

Palavras-chave: Segurança da Informação. Política de Segurança da Informação NBR ISO/IEC 27001. Análise de riscos.

ABSTRACT

The present work was based on the application of concepts and methodologies extracted from books by renowned authors who are familiar with the best practices in Information Security, which are based on ISO / IEC 27001 and 27002 standards. The main objective is to demonstrate the scenario of a Branch of Health that identified weaknesses in the security of its information and implemented measures to reduce risks and avoid possible losses, both financial and related to its image. For this, the involvement of the top management was paramount, where they invested the necessary resources to reach their objectives. With these demonstrations of commitment began a differentiated culture in the organization, applying techniques, tools and awareness campaigns, training and dissemination of the policies developed, all to contribute to the excellence of the services provided in the field of occupational health. For the preservation of the image, the name of the Company HL Saúde was used in a fictitious way in relation to the true Company that is a national reference among the others in this field and opted not to have its image exposed. The present work was based on the application of concepts And methodologies extracted from books by renowned authors who are familiar with the best practices in Information Security based on ABNT ISO / IEC 27001 and 27002 standards. The main objective is to demonstrate the scenario of a Health Company that identified weaknesses in the safety of Its information and implemented measures to reduce risks and avoid possible losses, both financial and related to its image. For this, the involvement of the top management was paramount, where they invested the necessary resources to reach their objectives. With these demonstrations of commitment began a differentiated culture in the organization, applying techniques, tools and awareness campaigns, training and dissemination of the policies developed, all to contribute to the excellence of the services provided in the field of occupational health. For the preservation of the image, the name of the Company HL Saúde was used in a fictitious way in relation to the true Company that is a national reference among the others in this field and opted not to have its image exposed.

Key words: Information security. Security Policy Information NBR ISO / IEC 27001. Risk Analysis.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

INTRODUÇÃO

O crescimento das ameaças cibernéticas tem aumentado a necessidade da adoção dos padrões de segurança da informação pelas organizações. O risco de vazamento dos dados e informações ameaçam as Empresas e preocupam Analistas de Segurança e os Gestores de Negócio. No cenário em que a informação é o principal ativo de uma Organização, a falta dos devidos cuidados e conhecimentos dos funcionários em relação às políticas da Empresa e procedimentos básicos adotados como medidas de segurança destacam-se entre as maiores vulnerabilidades geradoras de perdas financeiras e de imagem a uma Organização.

Em se tratando de segurança da informação, onde o risco de invasões, fraudes, roubos e até mesmo a desmoralização da imagem perante terceiros e concorrência é alto, quanto mais rápido os diretores, gestores e técnicos tomam ações para mitigar os riscos, menores serão as chances de um prejuízo. Na tecnologia, para que algo dê errado, basta que os responsáveis não se importem ou não tomem nenhuma ação a respeito.

A Empresa HL Saúde possui sede em Brasília e foi fundada em 26 de abril de 1990 por um grupo de funcionários bancários. Devido à demora na autorização de procedimentos clínicos, falhas em liberações de procedimentos diversos, e inúmeros outros problemas, gerados pela falta de um sistema integrado com informações dos atendimentos, controle de prontuários, acompanhamentos e evoluções clínicas, dados unificados ou cadastro de funcionários e dependentes para que as clínicas ou hospitais particulares pudessem consultar e realizar ações ou cuidados preventivos com a saúde de seus prestadores, um grupo de funcionários iniciaram as ações para criação da HL Saúde. Atualmente, a HL Saúde ampara aproximadamente 700 mil vidas e tem como missão assegurar ações para promoção da saúde e do bem-estar de seus participantes, cuidando desde a prevenção até as medidas de recuperação e superação cabíveis aos seus participantes.

Na década de 90, os sistemas de informação começaram a ser utilizados para suportar as adesões e o crescimento exponencial do número de participantes no Plano. Embora já se falasse em segurança da informação, os meios adotados

para proteção dos dados e informações na HL Saúde não refletiam o nível ideal apontado pelo corpo técnico, pois os recursos não eram suficientes para garantir o nível de confiabilidade da empresa em relação a salvaguarda das informações através da segurança da informação. Após a virada do milênio, ferramentas antivírus e *Firewall* foram implementadas como medidas de proteção dos dados. Em 2010, após identificação de invasões em sua infraestrutura tecnológica, a empresa iniciou estudos de viabilidade técnica para aumentar os níveis de segurança às suas informações, e direcionar melhor seu investimento em tecnologia da informação.

A partir de então, a informação passou a ser tratada pela organização como um bem que possui valor, e que deveria ser mais bem cuidada e gerenciada, para assim garantir sua disponibilidade, integridade, confidencialidade e legalidade.

No ano de 2013, enquanto os diretores discutiam a estratégia para o negócio, considerou-se a Segurança da Informação como um elemento que pode alavancar ou comprometer qualquer estratégia. Com isso, fora definido e aprovado um planejamento de cinco anos a ter início em 2014. Neste ano, trabalhos de pesquisa foram realizados levando em consideração o crescimento de sua rede de associados e a expansão do seu negócio, com a inclusão de novos procedimentos. Ainda em 2014, a Empresa HL Saúde prospectou, adquiriu e iniciou a implantação de um Sistema de Senhas e Acessos, com o investimento total de R$1.200.000,00 (um milhão e duzentos mil reais), que além da implantação, integração com sistemas legados, customização, treinamento da equipe técnica também contemplava a garantia de manutenção e suporte para 36 meses. Este projeto iniciado em 2014, foi concluído em março de 2015, antes do início da fase de implementação da segurança.

Em 2015, o projeto de implantação da segurança da informação na empresa HL Saúde pode contar com o sistema de controle de senhas e acesso. Com isso, a possibilidade de novos controles de segurança serem implementados agradou o corpo diretivo que apoiou completamente a ideia e solicitou ao Gestor Executivo de TI (Tecnologia da Informação) que prosseguisse com suas implementações, incorporando assim a abordagem *Top Down*, em que, o comprometimento da alta direção nas ações a serem implementadas é proporcional à busca pelo seu sucesso, e com isso os níveis abaixo (operacionais e técnicos) sentem-se motivados a colaborar e participar ativamente das etapas definidas.

Num projeto com tamanha proporção e num ambiente corporativo, certamente ocorrerão interferências na cultura e no poder que as pessoas possuem dentro da organização, por isso o modelo *Top Down* é fundamental para o sucesso. As mudanças são necessárias, porém elas nem sempre são bem-aceitas por todos, pois naturalmente tirarão as pessoas da “zona de conforto”, entretanto são necessárias para o crescimento de uma organização séria e comprometido com suas entregas de valor.

A segurança da informação passou a ser tratada como um processo na organização, que deve se relacionar com outros processos já definidos de forma a estabelecer critérios, definir responsabilidades, executar ações práticas que possam levantar e mitigar riscos associados ao negócio em sua amplitude e ainda avaliar as ações para melhoria continuada.

Motivação

Com o avanço tecnológico, é fundamental que a tecnologia da informação possa apoiar e potencializar a visão de negócio. Desta forma, a proposta deste trabalho é definir critérios para atender recomendações do órgão regulador da saúde (ANS - Agência Nacional de Saúde Suplementar) e a necessidade de implantação de políticas de segurança da informação e sua ampla divulgação aos funcionários da empresa HL Saúde.

Objetivo Geral

O objetivo geral do trabalho é aplicar um modelo de Gestão Corporativo de Segurança da Informação para reduzir os riscos na Segurança da Informação.

Objetivos Específicos

Este trabalho tem como objetivos específicos:

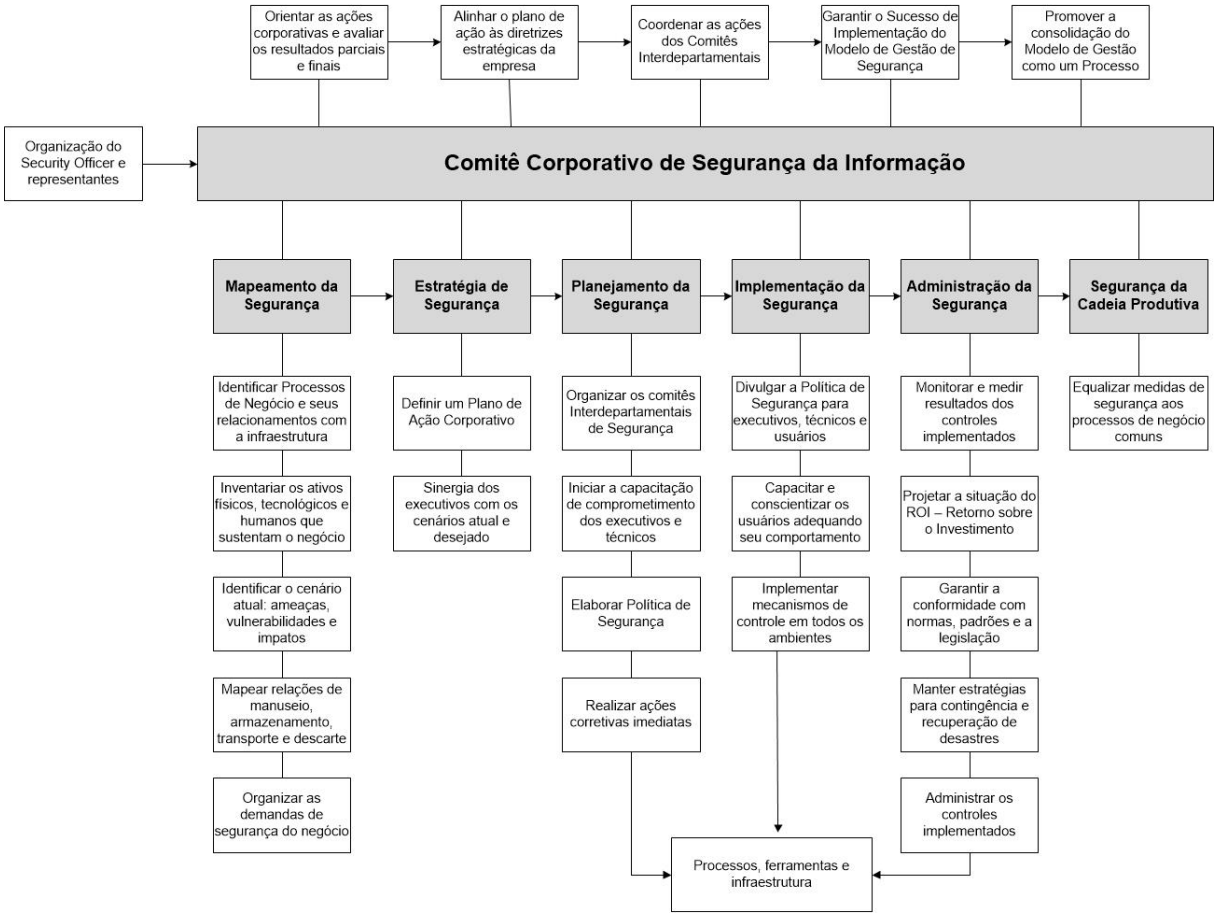
1. Definir a composição de um Comitê de Segurança da Informação;
2. Definir os critérios para o tratamento dos riscos encontrados nos ativos da empresa;
3. Identificar a necessidade de investimentos em Segurança da Informação;
4. Definir o tratamento das políticas de Segurança da Informação;
5. Aplicar item 7.2.2 da ABNT NBR ISO/IEC 27002:2013, “Conscientização, educação e treinamento em segurança da informação” aos funcionários da Organização.

Metodologia Aplicada

Este trabalho foi baseado em observações e participações in-loco numa Empresa da iniciativa privada do ramo de Saúde, que preferiu ter sua identidade preservada por motivos de políticas internas. O modelo de gestão corporativa de Segurança da Informação abordado por Sêmola (2003, p.32) e ilustrado abaixo, foi utilizado como um mapa para implantação de políticas que pudessem subsidiar um sistema de gestão de segurança da informação na Empresa HL Saúde. Suas diretrizes foram aplicadas para atender uma demanda de melhoria na eficiência da

Segurança da Informação, e mesmo não sendo aplicados à risca, serviu para guiar as ações no compasso em que se deslocam a cada etapa do projeto:

Figura 1 - Modelo de Gestão Corporativo de Segurança da Informação



Fonte - SÊMOLA (2003, p. 32)

Investimento

O orçamento destinado para o projeto de elaboração e implantação das políticas de segurança da informação foi de R$ 2.000.000,00 (dois milhões de reais). Abaixo, demonstramos como foi aplicado o investimento:

Quadro1 - Demonstrativo dos custos com o Projeto

Quadro demonstrativo do investimento para implementação das Políticas de Segurança da Informação na Empresa HL Saúde			
Atividades	**Medidas**	**Tempo / Quantidade**	**Custo total**
Treinamento da equipe técnica de Segurança	unidade	6	R$ 30.000,00
Capacitação para Gestores (processo de segurança da informação)	unidade	5	R$ 20.000,00
Aquisição de Software para Inventário	unidade	1	R$ 300.000,00
Treinamento Software Inventário	horas	6	R$ 30.000,00
Aquisição e implantação do Sistema de Senhas e Acessos	unidade	1	R$ 1.200.000,00
Treinamento Sistema de Senhas e Acessos	unidade	6	R$ 50.000,00
Aquisição de Norma ISO/IEC 27001:2013	unidade	1	R$ 128,00
Aquisição de Norma ISO/IEC 27002:2013	unidade	1	R$ 239,00
Aquisição de Bibliografias para consulta	unidade	7	R$ 1.000,00
Custo total do projeto (exclui-se a alocação dos profissionais do quadro da Empresa HL Saúde):			**R$ 1.631.367,00**

Fonte - Elaborado pelo autor

Do total disponibilizado para o projeto, houve uma sobra de R$368.633,00 reais, que ficará reservado para ser utilizado em projetos futuros relacionados à manutenção da Segurança das Informações na Empresa HL Saúde.

1 REFERENCIAL TEÓRICO

1.1 Política de Segurança da Informação

> Segundo o livro “Writing Information Security Policies” de Scott Barman, publicado pela Editora New Riders nos Estados Unidos (sem tradução no Brasil) a Política de Segurança é composta por um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações e serviços importantes para a empresa recebam a proteção conveniente, de modo a garantir a sua confidencialidade, integridade e disponibilidade (FERREIRA, 2008, p.36).

1.2 Gestão da Segurança

Abrange a criação de processos voltados ao monitoramento contínuo da integridade das informações, à prevenção de ataques e furto dos dados, assegurando em casos emergenciais o pronto restabelecimento dos sistemas e o acesso seguro às informações da organização.

1.3 Importância de uma área de Segurança da Informação

A definição de uma área de Segurança da Informação visa centralizar as ações de análise e estabelecimento de critérios para prevenção e resposta a incidentes relacionados à Segurança da Informação de forma rápida e eficiente.

1.4 Capacitação e conscientização em segurança

A capacitação e conscientização dos usuários são realizadas adequando seu comportamento. O comportamento humano ainda é um dos maiores responsáveis pelo vazamento de informações e comprometimento da segurança da informação no ambiente corporativo. Em março de 2016, este assunto foi abordado pela colunista Flavia Alemi, do Jornal O Estado de São Paulo:

> SÃO PAULO - O alerta foi dado: o principal responsável pelo vazamento de dados confidenciais de uma companhia é o próprio trabalhador. De acordo com a Pesquisa Global de Segurança da Informação 2016, publicada pela PwC, 41% das 600 empresas ouvidas pela consultoria informaram que os funcionários atuais são os maiores causadores de incidentes de segurança da informação no Brasil. Tais incidentes vão desde o roubo de propriedade intelectual até o comprometimento de dados de clientes, o que levou 39% das empresas a relatar perdas financeiras após os ataques.
>
> Isso não significa, necessariamente, que os funcionários sejam maus elementos", explica o especialista em segurança da informação da PwC, Edgar D'Andrea. "Alguém pode abrir um e-mail com um software mal intencionado no computador e o funcionário acaba sendo inadvertidamente envolvido no ataque", detalha. No Brasil, o número de incidentes aumentou quatro vezes entre 2014 e 2015, para 8.695 casos (ALEMI , 2016).

1.5 Saúde ocupacional

É uma área da saúde que cuida da saúde do trabalhador, especialmente na prevenção de doenças ou problemas provenientes do trabalho. Seu objetivo é promover o bem-estar tanto físico como mental e social dos trabalhadores no exercício de suas ocupações.

1.6 ANS (Agência Nacional de Saúde Suplementar)

É a agência reguladora vinculada ao Ministério da Saúde responsável pelo setor de planos de saúde no Brasil. Através de suas regulamentações, determina requisitos de segurança da informação, como no artigo 3º da Resolução normativa – RN Nº 389, de 26 de Novembro de 2015 abaixo:

Art. 3° A operadora será responsável pela gestão do seu portal na Internet e dos aplicativos disponíveis em computadores, tablets e celulares, e realizará:

I – a manutenção e atualização periódica das bases de dados;

II – a preservação da estabilidade, segurança da informação e funcionalidade da rede e dos aplicativos, por meio de medidas compatíveis com os padrões técnicos estabelecidos para este fim; e

III - medidas e procedimentos para a segurança e sigilo dos registros de conexão e dos dados.

Também na Resolução normativa – RN Nº 395, de 14 de Janeiro de 2016, em seu artigo 3º, trata:

Art. 3º São diretrizes que devem orientar o atendimento das operadoras aos beneficiários:

I – transparência, clareza e segurança das informações;

II – rastreabilidade das demandas;

III – presteza e cortesia;

IV – racionalização e melhoria contínua.

1.7 Mecanismos de controle de acesso:

A HL Saúde adota em sua infraestrutura tecnológica controles de acesso utilizando recursos como a autenticação biométrica como no sistema de catracas e em portas corta-fogo (nestas também é necessário digitar uma senha numérica de 4 dígitos), este sistema é integrado ao sistema de Gestão de Senhas e Acessos, que possibilita implementar o modelo de controle de acesso baseado em papéis, o RBAC (*Role-Based Access Control*). O acesso a determinado ambiente somente é liberado após uma solicitação via link disponibilizado na intranet da Empresa HL Saúde, onde seguirá um fluxo definido para sua aprovação. Inicialmente deverá passar pela ciência do supervisor imediato ou Coordenador para somente depois possibilitar a autorização do gestor competente.

O Sistema de Senhas e Acessos pode permitir o cadastro e liberação do acesso de um colaborador desde que ele preencha os requisitos definidos para uma função, ou seja, cada ambiente ou sistema pode possuir um fluxo de permicionamento de acesso diferenciado.

1.8 Segurança da Informação no contexto global

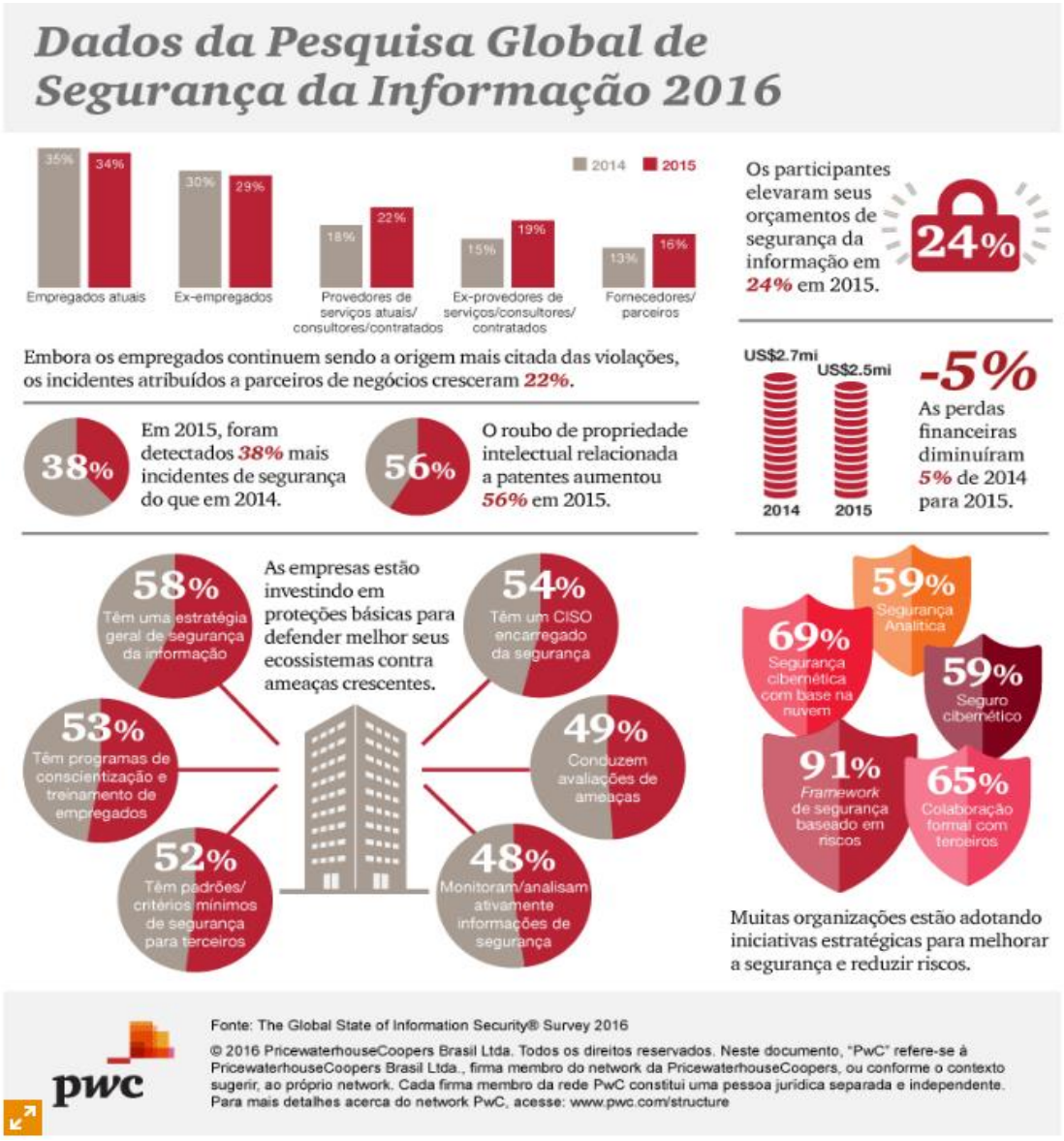
Abaixo citamos uma pesquisa realizada sobre o crescimento das ameaças à segurança das informações:

Pesquisa Global sobre Segurança da Informação 2015:

A Pesquisa Global sobre Segurança da Informação 2015 da PwC mostra que os casos de violação de segurança continuam crescendo e os prejuízos por eles causados também. Segundo os participantes do nosso estudo, o número de incidentes detectados subiu para 42,8 milhões em 2014 – uma alta de 48% em relação ao ano anterior. Esse aumento teve um alto custo para as empresas: a soma dos prejuízos financeiros atribuídos a violações de segurança cresceu 34% em um ano.

Sabemos que os riscos cibernéticos nunca serão eliminados. Por isso mesmo, as empresas precisam se manter vigilantes e ágeis para operar em um ambiente de ameaças crescentes. Conheça os resultados da pesquisa e descubra por que a sua organização deve avaliar a implementação de uma abordagem de segurança baseada em riscos, que priorize seus ativos mais valiosos e trate de maneira proativa as ameaças mais relevantes. (PWC,2015)

Figura 2 - Pesquisa de Segurança da Informação



Fonte - PWC (2016)

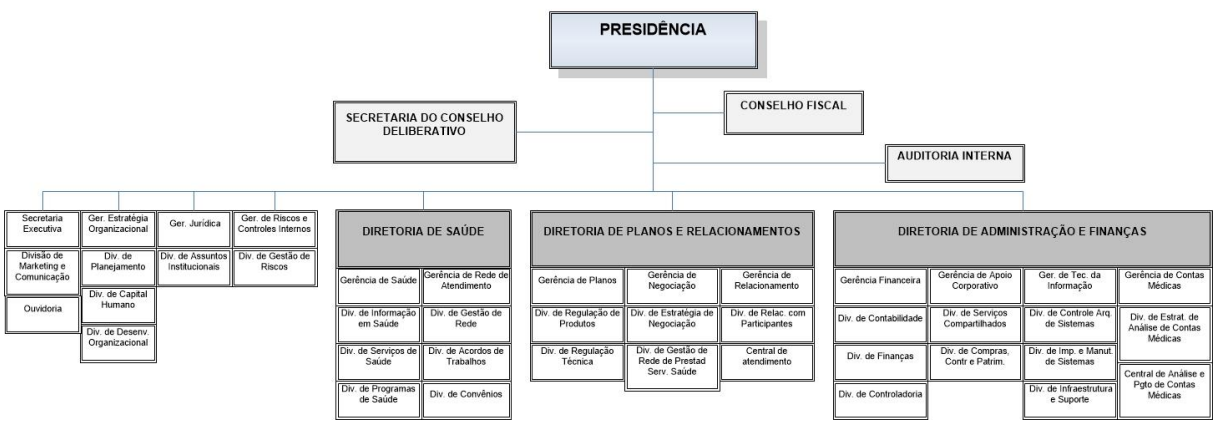
A pesquisa global realizada pela PWC expressa a preocupação das grandes Empresas em relação à segurança de suas informações. A Empresa HL Saúde acompanha as tendências de mercado e compartilha desta preocupação.

2 PREPARAÇÃO DO PROJETO E CENÁRIO ATUAL

A Gerência Executiva de TI da Empresa HL Saúde foi encarregada pela Diretoria com a autorização da Presidência da Empresa, de estabelecer as diretrizes para implantação de políticas que possam subsidiar um sistema de gestão de segurança da informação, definindo processos, alocando pessoas, utilizando a tecnologia necessária e garantindo sua eficiência. Para isso, a alta direção, comprometida com o sucesso desta implantação, direcionou um orçamento de R$2.000.000,00 (dois milhões de reais) para capacitação de seu corpo funcional, contratação de consultoria para condução das atividades dentro das melhores práticas aplicadas ao mercado de TI (Tecnologia da Informação) e aquisição de ferramentas ou tecnologia necessária. Foi recomendado pela Diretoria a formação de um comitê composto por colaboradores dotados em áreas estratégicas da organização, com dois objetivos específicos: primeiro, para se obter uma visão holística da organização e mitigar os riscos relacionados à Segurança da Informação, protegendo os dados e sistemas que os gerenciam; segundo, para garantir a disseminação e formação de multiplicadores, envolvendo outras áreas e assim obter o apoio do corpo funcional da organização. Uma equipe técnica também foi formada para dar apoio às atividades. O prazo inicial para conclusão das atividades foi de 9 meses.

A Empresa HL Saúde possui a seguinte estrutura organizacional:

Figura 3 – Organograma da Empresa HL Saúde



Fonte - HL Saúde (2016)

2.1 Comitê de Segurança da informação

A Empresa HL Saúde entende que a alocação de profissionais com as devidas competências é essencial para o sucesso do projeto. A formação do comitê de Segurança da Informação é uma determinação da alta direção, e é constituído por profissionais de diversos setores, como Tecnologia, Riscos e Controles Internos, Jurídico, Recursos Humanos, Marketing e representante da Presidência. O comitê é responsável por estabelecer os procedimentos de segurança e definir os critérios de divulgação, deve haver encontros mensais com o objetivo de disseminar, monitorar e manter a segurança em todas as áreas da organização. O Comitê é composto pelos seguintes perfis:

2.1.1 Gerente de Infraestrutura

Líder do comitê e responsável direto pelas ações que envolvem os gestores da organização. Deve fornecer as informações do status do projeto aos Gestores e demais superiores da Organização, bem como solicitar os recursos necessários para andamento e conclusão do projeto.

2.1.2 Analista Sênior de Segurança da Informação

Sua principal função é buscar soluções técnicas aos diversos riscos e ameaças apontados pelos membros do comitê, prospectando soluções e definindo metodologias para disseminar a cultura de segurança da informação na Empresa HL Saúde. Deve ainda manter as estações de trabalho e servidores com os agentes de antivírus e patches de segurança atualizados. Sistemas desatualizados estão entre as maiores vulnerabilidades de segurança da informação.

2.1.3 Analista Sênior de Desenvolvimento de Sistemas

Tem como função colher dados de vulnerabilidades e ameaças de código malicioso para as linguagens de programação e ferramentas de desenvolvimento,

deve analisar o código desenvolvido e aplicar as melhores práticas de desenvolvimento, com vistas à segurança e proteção das informações.

2.1.4 Analista Sênior de Banco de Dados

Deve manter os Sistemas Gerenciadores de Banco de Dados (SGBD's) atualizados, apontar as vulnerabilidades e riscos relacionados aos SGBD's em uso na organização. Deve analisar consultas realizadas (*querys*) e seus tempos de respostas, sugerir melhorias para integridade dos dados e evitar alto consumo na utilização dos recursos de *CPU (Central Processing Unit),* Memória e disco. Deve elaborar um plano de recuperação em caso de desastre para continuidade do serviço de TI.

2.1.5 Analista Sênior de Infraestrutura e Suporte

Deve manter os Sistemas Operacionais, *firmwares* e *softwares* atualizados e monitorados. Os Sistemas de armazenamento de dados (*Storages*) e virtualizadores devem estar atualizados e serem monitorados por ferramentas de monitoramento de infraestrutura. Manter uma matriz de compatibilidade de softwares é fundamental para controle da infraestrutura. Deve definir e manter *backup* dos dados adotando políticas de *backup* e *restore*.

2.1.6 Analista de Riscos e controles internos

Sua função é executar análise de riscos e realizar uma Análise de Impactos no Negócio, para identificar todos os prováveis impactos de forma Qualitativa e Quantitativamente dos principais processos de negócios mapeados e entendidos na organização, no caso de interrupção dos mesmos (D'ADDARIO, 2008).

2.1.7 Analista de Marketing

Deve compreender o tema e sugerir a divulgação de forma clara ao público-alvo na Organização. Dois tipos de divulgações devem ser realizados de

acordo com a classificação das informações, sendo um de âmbito interno e outro externo à organização. Na divulgação interna, a informação a ser direcionada ao corpo diretivo deve ser mais estratégica, com indicadores, tendências, ações corretivas e preventivas, diferenciando-se das demais áreas da organização que devem ser apenas informativas.

2.1.8 Representante do Jurídico (Analista ou Advogado)

É importante que este profissional traga pontos de vista relacionados às leis e suas aplicações no âmbito organizacional, relembre os processos disciplinares formais, implantados e comunicados para ações contra funcionários que tenham cometido uma violação de segurança da informação, conforme determina o item 7.2.3 da ISO/IEC 27002:2013.

2.1.9 Representante da Diretoria

Tem como principal função servir de interface entre a Direção e a operação, trazendo pontos de vista do corpo diretivo ao comitê, e levando informações sobre as ações a serem implementadas, bem como os status de suas implementações na organização.

2.1.10 Secretário (a)

Sua função é agendar reuniões, convidar os participantes, manter o controle dos presentes, redigir as atas, colher assinatura dos participantes e posteriormente divulgá-la apenas aos interessados.

2.2 Equipe técnica

O Comitê de Segurança da Informação sugeriu a criação de uma equipe técnica especializada em tratamento de eventos relacionados à Segurança da

Informação. Esta equipe foi formada por 04 Analistas de Infraestrutura e devem, dentre outras atividades, estudar e apresentar ferramentas e metodologias necessárias, desenhar e propor soluções técnicas, elaborar procedimentos e instruções de trabalho, ministrar treinamentos operacionais para capacitação dos funcionários, tratamento dos incidentes relacionados à Segurança da Informação e geração dos indicadores de segurança em relação aos incidentes tratados.

3 PLANEJAMENTO E EXECUÇÃO

O projeto foi realizado conforme o cronograma abaixo:

Quadro 2 - Cronograma do Projeto.

Gráfico de Gantt

	Nome da tarefa	Duração
1	**Projeto de Implantação de Políticas de Segurança da Informação na Empresa HL Saúde**	**180 dias**
2	Reunião estratégica para definições	1 dia
3	**Mapeamento e Estratégia da Segurança**	**134 dias**
4	Inventário de ativos de TI	59 dias
5	Política de inventário de ativos de TI	5 dias
6	Análise de riscos de Segurança da Informação	15 dias
7	Gestor da Informação	2 dias
8	Classificação da informação	5 dias
9	Manuseio, armazenamento e descarte da Informação	5 dias
10	Perda ou roubo de informações	3 dias
11	Monitoramento da Infraestrutura de TI	30 dias
12	Demandas e incidentes de Segurança da Informação	10 dias
13	Planejamento e elaboração da Política de Segurança da Informaç	5 dias
14	Implementação da Segurança	15 dias
15	Publicação das Políticas de Segurança	7 dias
16	Administração da Segurança das Informações	15 dias
17	**Aplicação das Políticas de Segurança da Informação**	**45 dias**
18	Capacitação e treinamento	30 dias
19	Aceitação e prática pelos usuários	3 dias
20	Avaliações	3 dias
21	Manutenção e revisão	3 dias
22	Auditoria interna	3 dias
23	Metas	1 dia
24	Conclusão do Projeto	2 dias

Fonte - Elaborado pelo autor

3.1 Mapeamento e Estratégia da Segurança

As seguintes ações foram realizadas para mapear a segurança na Empresa HL Saúde:

3.1.1 Inventário de ativos de TI

O inventário dos ativos foi realizado com o auxílio da ferramenta de inventário SNOW, adquirida como forma de aumentar o controle de uso de softwares e suas versões, onde foi identificado risco pois softwares desatualizados são vulneráveis. Seu investimento foi de R$ 330.000,00 (trezentos e trinta mil reais) e que permite, dentre outras as seguintes ações:

a) Descoberta automática de equipamentos estações de trabalho e servidores com sistema operacional Windows e UNIX (AIX);

b) Cadastrar todos os produtos instalados nos equipamentos (estações de trabalho e servidores);

c) Inserir links e documentos em anexo para cada ativo, podendo inclusive criar manuais de operação dos ativos e suas características;

d) Integrar com Sistema de Gerenciamento Empresarial SAP para possibilitar o controle de licenças SAP (uma abreviação de *Systeme, Anwendurgen und Produkte in der Datenverarbeitung*, no idioma alemão, que quer dizer, em português: Sistemas, Aplicativos e Produtos para Processamento de Dados);

e) Adicionar objetos que serão tratados como ativos, integrar com outros sistemas para possibilitar o inventário de recursos humanos, físicos e sua dotação na organização;

f) Associar os contratos de manutenção e suporte aos ativos mapeados e fazer a gestão dos contratos;

3.1.2 Política para realização do inventário de ativos de TI

a) Identificamos as estações de trabalho, notebooks, servidores, impressoras, Switches (ethernet e fibre Chanel), roteadores, Links, virtualizadores, sistemas de armazenamento, Firewall, IDS, IPS, banco de dados, aplicativos instalados, e outros hardwares ou softwares que geram custos, relacioná-los aos contratos e identificar se os contratos estão vigentes ou para vencer, se os produtos estão atualizados e se estão sendo utilizados de forma eficiente, ou seja, não geram despesas inúteis. Os contratos também são considerados ativos.

b) O inventário é atualizado, no mínimo, uma vez ao ano e apresentado ao Gerente de Infraestrutura que o aprovará.

c) Após aprovado, o inventário é publicado no sistema de documentação da HL Saúde.

d) O responsável pelo inventário dos ativos é o Coordenador de Infraestrutura, que demandará seu corpo técnico.

3.1.3 Análise de riscos de Segurança da Informação

Sêmola (2003) define riscos como a probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios, sendo extremamente importante sua análise visando mitiga-los através de ações práticas e possíveis, como:

a) Definir, gerar e analisar os indicadores de riscos e aplicar ações para tratar ou mitigar os riscos relacionados aos ativos de TI.

b) A análise deve ocorrer no mínimo uma vez ao ano.

c) O responsável pela análise de riscos é o Coordenador de Infraestrutura que demandará seu corpo técnico.

Na HL Saúde, a identificação dos riscos associados aos serviços e demais ativos deve ser realizada. Para cada risco associado a um ativo, deve ser definido um plano de ação eficiente para trata-lo ou mitiga-lo. Foi realizado um levantamento dos riscos e considerados, inicialmente, apenas os riscos cuja probabilidade seja alta (por haver um baixo controle ou nenhum) e o impacto crítico, ou seja, eventos que possam gerar indisponibilidade total de um sistema ou serviço e com isso, causar perdas financeiras, de imagem ou quebra de acordos com usuários e prestadores. Abaixo segue o quadro com o levantamento:

Quadro 3 - Análise de riscos críticos em TI

ANÁLISE DE RISCOS CRÍTICOS DE TI -- EMPRESA HL SAÚDE			
Risco	***Impacto***	***Medida***	***Ação***
Ataques externos e internos aos servidores e serviços produtivos da Empresa HL Saúde	Serviços indisponíveis / procedimentos de atendimento não autorizados / pacientes em estado crítico podem não ser atendidos pela rede credenciada. / Exposição da empresa HL Saúde pela fragilidade com a Segurança das Informações, vazamento de informações sigilosas, como prontuário de pacientes / Perdas financeiras / interceptação e manipulação de dados.	Monitoração	Implantar monitoramento proativo
		Firewall	Definir e revisar mensalmente as regras de segurança e perfis de acesso
		IDS / IPS	Verificar logs e gerar indicadores com estatísticas de tentativas de ataques e ataques com sucesso. Criar procedimentos e gerar informações para as campanhas de conscientização na empresa HL Saúde.
		Tratamento de Incidentes de Segurança da Informação	Alerta interno de atividade suspeita;
			Medidas de contenção imediata do incidente;
			Coleta de informações e evidências;
			Análise das informações e evidências;
			Notificação dos envolvidos;
			Análise crítica e medidas corretivas;
		VPN	Controlar acesso à rede virtual privada com perfis de acesso e fluxos para aprovação, liberação e expiração de acesso.
		Teste	Manter ambiente de homologação para realizar testes e simulação de ataques
		Revisão do processo	Gerar indicadores para justificar investimentos e ações de melhoria

Uso inadequado da internet, acesso à sites e download de arquivos e executáveis.	Indisponibilidade por Infecção da rede, perda de sigilo das informações, instalação de vírus. Ação de malwares.	Monitoração	Implantar ou melhorar o monitoramento proativo
		Firewall e Filtros de conteúdo	Definir e revisar mensalmente as regras
		Controle de Acessos	Definição de perfis de acesso através de ferramenta de gestão de identidades.
		IDS / IPS	Manter IDS e IPS atualizados e revisar suas regras mensalmente. Toda alteração em item de configuração deve ser realizada seguindo as diretrizes do processo de mudanças tecnológicas.
		Antivírus	Adotar política de atualização das ferramentas de antivírus e antispayweres nas estações de trabalho e servidores.
		Controle de versão e processos	Documentar e manter o controle de versão das ferramentas de segurança, infraestrutura, roteadores, sistemas de gerenciamento de atualizações e instalação de aplicativos. Manter ambiente de homologação e testes em redes isoladas da produção.
Falha na configuração da rede Física	Acessos indevidos, monitoramento não funciona, sistemas ou equipamentos não atualizados.	Configuração de Segurança	Rever a configuração da rede física e propor melhorias (caso haja necessidade de consultoria externa, submeter para aprovação administrativa e financeira)
		Teste	Testar nova configuração
		Documentação	Documentar os testes e evidências da nova configuração
		Monitoração	Implantar monitoramento proativo
		Firewall	Definir e revisar mensalmente as regras
		IDS / IPS	Verificar logs e gerar indicadores com estatísticas de tentativas de ataques e ataques com sucesso. Criar procedimentos e gerar informações para as campanhas de conscientização na empresa HL Saúde.
Sistemas Operacionais, Softwares e aplicativos desatualizados	Atualizações de segurança não aplicados, acesso e uso não registrado, uso de senhas padrão, modificações de dados e indisponibilidades não planejadas	Controle de versões dos aplicativos	Deve haver um inventário de softwares e ações para atualizações de softwares. Diariamente deve ser avaliado e aplicado atualizações de segurança dos sistemas operacionais. As demais atualizações deve ser realizada sem impacto para a organização.
		Controle de uso de softwares e sistemas	Deve haver ações de controle de uso dos softwares e sistemas, que permite identificar softwares não utilizado, e assim proceder com seu bloqueio ou desinstalação. Softwares não homologados pela tecnologia da informação não podem ser utilizados pelos usuários.
		Política de uso de softwares com implementação de controles de acessos por contas administrativas	Controlar ativação, senha e validade de senha para usuários administrativos. Senhas para usuários administrativos são controladas por um sistema de senhas e acessos. Apenas o Gerente Executivo pode permitir/aprovar seu uso.

Funcionários (descontentes, insatisfeitos, curioso, negligente, malicioso...)	Assalto a um empregado, chantagem, fraude e roubo, suborno, manipulação de dados para gerar perdas financeiras ou de imagens, erros nos sistemas, sabotagens, acessos não autorizados a outros sistemas e informações sigilosas, disseminação de vírus, deleção de arquivos importantes.	Conscientização / Treinamentos e Palestras	Elaborar e ministrar treinamentos e palestras (para gestores e áreas estratégicas). Elaborar, divulgar e constantemente revisar políticas, propagandas e documentos internos para conscientização dos funcionários quanto a importância em se preocupar com ações voltadas a segurança das informações
		Controles	Definir fluxo para que o setor de recursos humanos controle a participação dos funcionários nos treinamentos, palestras e eventos que visem a conscientização da Segurança da Informação
		Documentação	Evidenciar e manter registros dos treinamentos e repasse de conhecimento aos funcionários

Fonte - Elaborado pelo autor

3.1.4 Gestor da Informação

É o responsável pela autorização do acesso à informação. Deve ter o domínio das informações geradas em sua área. Deve classificar e revisar as informações classificadas bem como seus acessos liberados. Também é responsável por identificar quais os dados são críticos para a organização.

3.1.5 Classificação da informação

Classificar a informação é uma forma de identificar o que é mais crítico e para a organização. Isso possibilita, por exemplo, determinar ações como estabelecer acordos de níveis de serviços diferenciados para informações armazenadas em áreas onde sua restauração é garantida em tempos aceitáveis e ainda definir os níveis de acesso a essas informações.

A NBR 27002:2013 recomenda que, na classificação da informação, a organização leve em consideração o seu valor, requisitos legais, sensibilidade e criticidade, bem como os controles de proteção necessários (compartilhamento ou restrição de acesso) à informação. A norma também recomenda que o proprietário

do ativo defina a classificação deste e assegure que o mesmo esteja atualizado e no nível apropriado. A empresa HL Saúde classifica sua informação como:

a) Pública: não necessita de sigilo, em caso de divulgação externa, não gera impactos à organização. (FERREIRA, 2008).

b) Interna: de uso apenas da organização que devem ser evitados sua divulgação externa, porém se ocorrer, não trarão consequências críticas. (FERREIRA, 2008).

c) Confidencial: é sensível ao risco de impacto negativo e por isso deve ser mantida em sigilo, sua divulgação pode comprometer operações na organização, gerar prejuízos financeiros, de competitividade, de credibilidade e/ou desgaste de imagem. Somente pessoas autorizadas podem acessar. (FERREIRA, 2008).

A Política para classificação da informação foi definida com as seguintes especificações:

a) A informação deve ser classificada quanto ao seu uso, como Pública, Interna e Confidencial.

b) A organização deve promover a revisão da Classificação da Informação.

c) A revisão deve ocorrer anualmente.

d) Numa organização, cada área deve definir quem será o responsável pela informação, quem definirá os critérios e autorizará ou delegará a liberação dos acessos às informações de sua área.

3.1.6 Manuseio, armazenamento e descarte da Informação

Esta ação tem por objetivo atender às necessidades de confidencialidade da informação, conforme sua classificação.

a) Informações públicas

Armazenamento: é feito disponibilizando sistemas de armazenamento com menor custo de manutenção, não é necessário monitorado.

Descarte: é realizado o descarte das informações não modificadas há mais de trinta dias automaticamente via script em ferramenta de execução de rotinas batch.

b) Informações internas

Armazenamento: são armazenadas em áreas de acesso reservado e monitorado com a geração de logs de utilização do tamanho da área. É realizado backup diário, semanal e mensal com retenção de 5 anos destas informações.

Descarte: Podem ser descartadas pelo gestor ou responsável pela área de criação.

c) Informações confidenciais

Armazenamento: em local com acesso controlado cuja concessão é feita por meio de fluxo de autorização que deve passar por, ao menos, um nível hierárquico acima do solicitante antes de chegar no gestor da informação. O acesso é monitorado com a geração de logs para auditoria. É realizado backup diário, semanal e mensal com retenção mínima de 20 anos.

Descarte: é realizado por meio de ferramentas. Sua destruição deve seguir após autorização formal do gestor da informação.

3.1.7 Perda ou roubo de informações

Em caso de perda ou roubo, deve ser verificado se houve quebra da confidencialidade da informação e em seguida a área responsável deve ser comunicada formalmente. Um registro na ferramenta de service desk deve ser aberto.

3.1.8 Monitoramento da Infraestrutura de TI

O monitoramento da infraestrutura de TI é essencial para identificar as falhas ou eventos que possam gerá-las. Através do monitoramento é possível construir estatísticas e prever as necessidades para provisionamento futuro, analisando indicadores para possibilitar uma melhor tomada de decisão para direcionamento dos investimentos em tecnologia da informação de forma justificada.

A Política para monitoramento da infraestrutura de TI foi definida com as seguintes especificações:

a) Os seguintes indicadores são gerados:

Quantidade de tentativas de acesso a sistema crítico negado (deverá apresentar informar qual usuário, horário, origem e o que tentou acessar);

Usuário com maior quantidade de acessos negados;

Ameaças e ações corretivas;

Infecções e ações corretivas;

Quantidade de bloqueios de mensagens (spams e fishing);

Revisão das métricas de monitoramento.

b) A cada trimestre os indicadores deverão ser disponibilizados na intranet e via e-mail para os gestores de TI (para esta divulgação, deve ser ocultado o usuário e a origem do acesso).

c) A disponibilidade dos ativos e serviços, quando possível, deve ser monitorada.

d) Os responsáveis pela elaboração e atualização dos relatórios com os indicadores de segurança são os Analistas de Segurança da Informação.

O controle de acessos às informações é realizado por meio de um sistema de senhas e acessos que implementa fluxos e regras para liberação e revogação dos mesmos, bem como a definição das políticas de senha, o que garante ações proativas como bloqueio de estações, logout de sistemas, automaticamente, dentre outros. Integra a outros sistemas e ambientes, coleta logs e possibilita a geração de alertas em caso de tentativa de acesso não autorizado, com ações como informar determinada área (gestora, técnica ou ambas).

3.1.9 Demandas e incidentes de Segurança da Informação

A Empresa HL Saúde disponibilizou a seus funcionários, um canal para atendimento e tratamento de demandas e incidentes relacionadas à Segurança da Informação.

a) As demandas e incidentes de Segurança da Informação são registrados em ferramenta de service desk para atendimentos dos chamados internos. Em seguida, o primeiro nível de atendimento avalia e resolve caso tenha procedimentos descritos ou encaminha para atendimento no segundo nível.

b) Os registros cuja solução tenha procedimento devem ser tratados no primeiro nível de atendimento, os demais são redirecionados para o segundo nível que atenderá e se for incidente, estes deverão elaborar procedimento e encaminhar para o primeiro nível, e caso seja demanda devem avaliar e propor solução técnica.

c) A equipe técnica responsável pela segurança da informação é a responsável por definir as diretrizes para o atendimento deste item.

d) Caso o atendimento dependa de fornecedores externos, deverá ser respeitado o SLA com o fornecedor, caso contrário o tempo de resolução deverá atender o SLA interno.

3.2 Planejamento e elaboração da Política de Segurança da Informação

Todas as ações devem estar claras e direcionadas dentro da Empresa HL Saúde, para isso um treinamento para os Executivos e técnicos foi ministrado com a finalidade de norteá-los quanto aos próximos desafios, envolvendo-os nos resultados e compartilhando com eles a responsabilidade pelo sucesso.

A Empresa HL Saúde considera a segurança das informações parte integrante do seu negócio e definiu sua Política de Segurança da Informação com as seguintes diretrizes:

a) Asseguramos a confidencialidade, integridade e a disponibilidade das informações, promovendo o gerenciamento, monitoramento e proteção das informações contra roubo, fraude, espionagem, perdas não intencionais, acidentes e outras ameaças;

b) Classificamos, atribuímos responsabilidades e segregamos o acesso às informações, patrimônio e ambientes de acordo com os níveis de acesso estabelecidos, grau de confidencialidade e criticidade para o negócio;

c) Disponibilizamos estrutura e recursos necessários para promoção, manutenção e melhoria contínua da segurança das pessoas, do patrimônio e das informações;

d) Mantemos canais de comunicação para registro, reporte e tratamento de incidentes de segurança;

e) Promovemos a capacitação e conscientização dos colaboradores e parceiros a fim de assegurar o comprometimento com a segurança;

3.3 Implementação da Segurança

Toda a documentação oficial da empresa HL Saúde é elaborada ou atualizada e em seguida aprovada através de um sistema específico de documentação. Este sistema permite as seguintes funcionalidades:

a) Identificar a área de elaboração do documento;

b) Definir o título, tipo, versão, descrição e autor do documento;

c) Definir os responsáveis pelas funções de visualizar, comentar, verificar e aprovar o documento;

d) Visualizar o log com informações de data, horário, responsável, descrição e motivo das alterações;

e) Incluir colaboradores específicos para realização de treinamento online do documento aprovado, avaliar seu entendimento com perguntas e permitir sugestões para melhoria.

3.4 Publicação das Políticas de Segurança

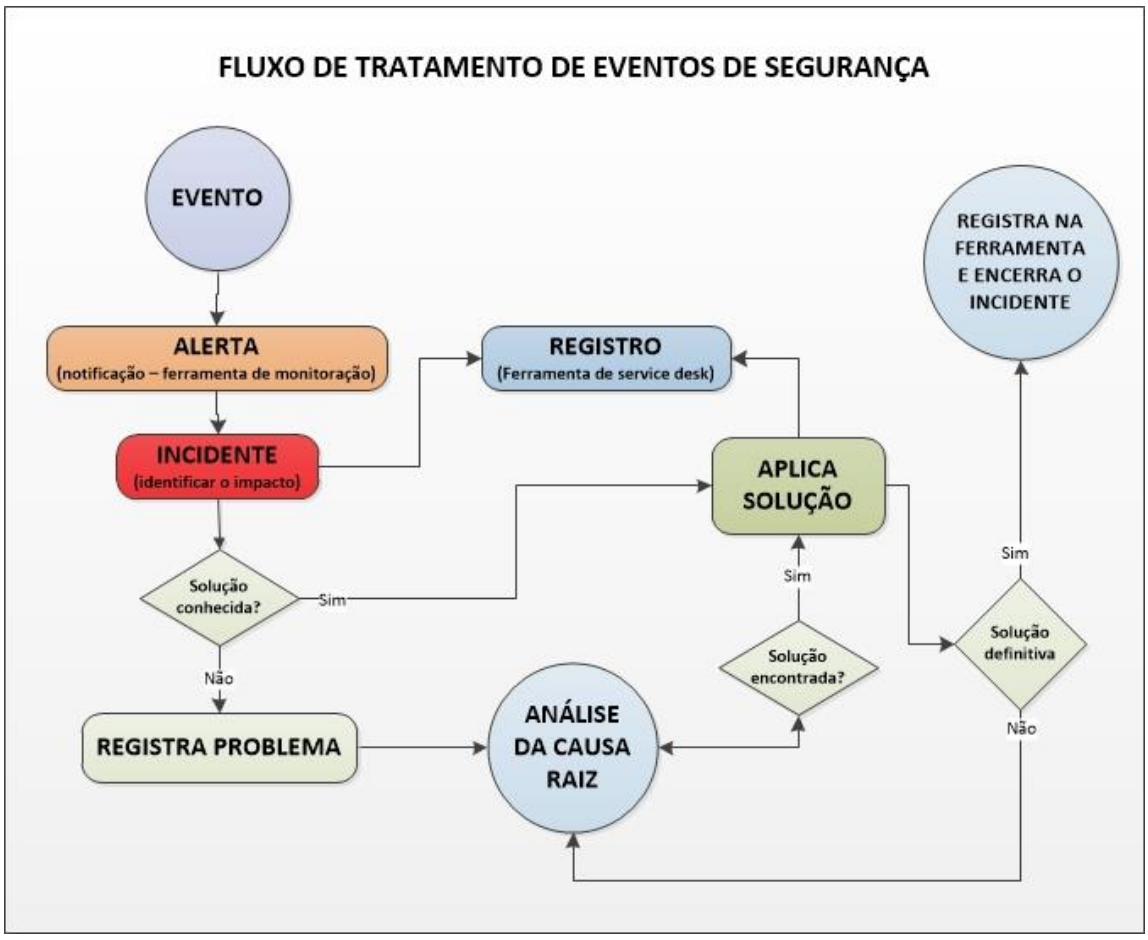
Após serem submetidas a análises e validação de seu conteúdo, serem aprovadas no Sistema de documentação, as políticas elaboradas conforme os itens 3.1.2, 3.1.5, 3.1.8 e 3.2 foram publicadas e divulgadas na organização.

3.5 Administração da Segurança das Informações

Monitorar e medir os resultados dos controles implementados: todo acesso à área restrita gera um evento que por sua vez pode emitir um alerta na ferramenta de monitoramento de infraestrutura (desde que tenha sido mapeado e configurado). Este alerta, por sua vez gera um registro ou uma notificação que pode

criar um incidente para proceder com ações investigativas, que serão registradas e poderão iniciar uma ação corretiva como solução, conforme fluxo de tratamento de eventos de segurança abaixo:

Figura 4 - Fluxo de tratamento de Eventos de Segurança



Fonte - Elaborado pelo autor

Mensalmente, um relatório de incidentes por tipo é gerado e uma análise crítica é realizada pelo responsável pela Segurança da Informação com o objetivo de promover ações para reduzir as ocorrências. Caso seja identificado que ações podem ser tomadas, um plano de ação é definido com prazos e responsáveis por cada atividade.

4 APLICAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

4.1 Capacitação e treinamento

Para que uma política possa ser aplicada, após sua elaboração, os colaboradores precisam ser comunicados e entendê-la. Segundo a ABNT. NBR ISO/IEC 27002:2013 (2013, p.3):

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

A equipe técnica responsável pelas ações em Segurança da Informação foi preparada para conscientizar, ministrar treinamentos e palestras sobre boas práticas em segurança da informação aos funcionários e inclusive a partes externas, conforme determina o item 7.2.2 da norma ISO/IEC 27002:2013. A Tecnologia da Informação participa ativamente no processo de integração de novos colaboradores e com a reciclagem de colaboradores antigos. A integração com a área de recursos humanos é fundamental para a promoção e controle da participação dos colaboradores e ainda para abordar assuntos como as penalidades e processos disciplinares a serem aplicadas no caso de descumprimento das políticas e regras da Empresa. A área de recursos humanos auxilia na obtenção da assinatura dos termos de responsabilidade de segurança da informação e também armazena em ficha funcional impressa e digitalizada. É de responsabilidade dos Recursos Humanos a solicitação à área de Tecnologia da Informação para retirada, suspensão ou cancelamento de acessos de colaboradores em caso de ausência ou desligamento. Ao final de cada treinamento, reciclagem ou evento de segurança da informação, um questionário é aplicado com o objetivo de mensurar o nível de conhecimento atingido pelos participantes. O envio de e-mails pela área de Marketing, citando dicas de segurança também é realizado mensalmente como estratégia para conscientização dos usuários. Outra funcionalidade para expansão dos métodos, técnicas e compartilhamento de informações está disponível na intranet da HL Saúde, o fórum de discursões online que tem como moderador um Analista de Segurança da Informação. Este fórum permite que os usuários

localizados em outros Estados possam sanar suas dúvidas com perguntas ou pesquisas no histórico de respostas.

As políticas de segurança são divulgadas para todos os colaboradores. Cada política relacionada à segurança da informação é disponibilizada no sistema de documentação da empresa HL Saúde e divulgada através de e-mail corporativo, banners na intranet e impressos nos murais de aviso da Empresa, seguindo as regras definidas pela Divisão de Marketing. Essas regras contêm diretrizes para cada público-alvo: gestor e os demais colaboradores da empresa HL Saúde.

O quadro de funcionários da Empresa HL Saúde é composto por 2.380 funcionários. A meta é manter o índice de 100% dos colaboradores treinados nas políticas de Segurança. Os novos colaboradores farão os treinamentos no período de sua adaptação na Empresa.

4.2 Aceitação e prática pelos usuários

O envolvimento da alta direção na idealização deste projeto é fundamental para a aceitação e prática pelos usuários. Com o objetivo de mensurar a eficiência das políticas na Empresa HL Saúde, semanalmente são realizadas avaliações com colaboradores distintos, com o objetivo de avaliar o nível de conhecimento e aplicabilidade das políticas de segurança. É disponibilizado aos usuários um canal aberto para dúvidas e sugestões via e-mail corporativo e através da ferramenta de abertura de chamados. Campanhas e mensagens por e-mail são lançadas com informações sobre a importância da segurança da informação com exemplos práticos de assuntos que sejam importantes não somente no âmbito Empresarial, como no dia a dia de cada indivíduo. A meta é atingir 100% dos usuários avaliados ao menos uma vez por ano. A demonstração de cuidado com os seus colaboradores aumenta a satisfação dos mesmos e reduz as vulnerabilidades.

4.3 Manutenção e revisão

As políticas devem ser revisadas, no mínimo uma vez por ano, ou sempre que for identificado um fato novo que possa impactar a segurança das informações na organização. Toda manutenção é realizada através do sistema de documentação da Empresa HL Saúde, o qual permitirá manter os registros das alterações.

4.4 Auditoria interna

Anualmente a segurança da informação será auditada com base no código de práticas ABNT NBR ISO/IEC 27002:2013 com o objetivo de aplicar a cada ano, novos controles. A auditoria é realizada apenas internamente (a própria empresa audita suas áreas) com a finalidade de identificar pontos de melhoria segundo diretrizes como o código de práticas da ISO/IEC 27002:2013.

4.5 Metas

Através destas ações, foi estabelecida uma meta de 95% para a satisfação dos usuários relacionados às campanhas de conscientização e disseminação do conhecimento sobre segurança da informação, e a redução das ocorrências de incidentes em segurança da informação de 80% ao final de 1 ano a partir da conclusão deste projeto.

CONCLUSÃO

Com base em todo o trabalho executado, podemos verificar os seguintes benefícios:

Elaboração e adoção da Política de inventário de ativos de TI conforme apresentado no item 3.1.2 ;

Elaboração e adoção da Política de classificação da informação conforme apresentado no item 3.1.5;

Elaboração e adoção da Política de Monitoramento da Infraestrutura de TI conforme apresentado no item 3.1.8;

Elaboração e adoção da Política de Segurança da Informação conforme descrito no item 3.2 ;

Além da implementação das políticas acima, observou-se uma melhoria no controle do uso dos ativos: a Empresa HL Saúde não conseguia identificar a quantidade de ativos antes deste projeto e se os mesmos estavam em uso ou atendiam as necessidades das áreas. O controle de licenciamento era precário, pois muitas estações de trabalho possuíam software que não era utilizado ou atualizado com a devida frequência, porém era contabilizado para cobranças e a Empresa mantinha gastos com produtos inutilizados.

Controle dos eventos relacionados à segurança da informação: não havia um fluxo de tratamento dos incidentes e suas recorrências não eram vistas como um problema que deve ser tratado e documentado. A análise de riscos permitiu elaborar procedimentos para tratamento dos eventos críticos, ajustar a ferramenta de monitoramento, descartar os alertas conhecidos como “falsos positivos”, e ajustar o monitoramento reduzindo o tempo dos atendimentos.

Geração de indicadores: através dos indicadores descritos no item 3.1.8, é possível identificar os pontos críticos e concentrar os esforços para combater as falhas e/ou vulnerabilidades específicas.

Cultura de Segurança da Informação: A criação de uma cultura de segurança da informação na Organização é importante, porém só funciona se houver continuidade na conscientização, treinamentos, palestras e avaliações periódicas para medir e estimular os funcionários alertando e lembrando-os de

sua importância com os cuidados abordados. O sucesso em se obter um nível de segurança satisfatório se deve à participação e envolvimento de todos os funcionários, principalmente a alta direção.

Necessidades de investimentos: com todos os controles aplicados, é possível identificar os pontos com maior necessidade de investimentos em Segurança da Informação, como as ferramentas de gestão de senhas e acessos, soluções de Firewall, IDS, IPS, capacitação da equipe técnica da Segurança da Informação, dentre outros.

Comprometimento da alta direção: o comprometimento e apoio do corpo diretivo direcionando orçamento e pessoas para o projeto, acompanhando as ações, cobrando os resultados e dividindo o êxito das conquistas com toda a Empresa, é o fator principal do sucesso desta implantação. Em seguida, o emprego de metodologias e tecnologia para operacionalizar cada processo, a conscientização e envolvimento das pessoas para criação de uma cultura de Segurança da Informação são elementos chaves para possibilitar a geração dos indicadores de Segurança da Informação que permitirá avaliar “onde estamos”, “como chegamos” e “para onde iremos” nos quesitos de segurança da informação. A certeza é que ações são constantemente tomadas com o objetivo de resguardar o recurso mais valioso que mantém uma organização, a Informação.

Formação de uma equipe técnica de Segurança da Informação: o projeto possibilitou a formação de uma equipe técnica responsável pela Segurança da Informação.

A imagem da Empresa HL Saúde perante seus clientes, parceiros e fornecedores manteve-se preservada.

A Empresa HL Saúde demonstrou sua preocupação e atenção com os riscos cibernéticos e determinou ações para implantação de políticas como parte de um Sistema de Gestão de Segurança da Informação baseado em requisitos definidos na ISO/IEC 27001/2013. A conclusão deste projeto se dá com a satisfação do corpo de Diretores da Empresa HL Saúde pela criação de uma cultura organizacional baseada nos princípios da Segurança dos seus dados que geram informações críticas para o negócio, pela elaboração, divulgação, conscientização e treinamento de 100% de seus funcionários.

A Empresa HL Saúde, através da alta direção, reconhece a necessidade de estabelecer novos desafios e metas para melhoria contínua de suas Políticas e ações em Segurança da Informação e avaliou como plenamente satisfatório o projeto de definição e implantação de Políticas de Segurança da Informação por ter alcançado os objetivos gerais e específicos, o que trouxe maior segurança ao patrimônio da Empresa.

GLOSSÁRIO

AIX	Um sistema operacional UNIX desenvolvido pela IBM projetado e otimizado para ser executado em hardware baseado em microprocessador *POWER*, como servidores, estações de trabalho e *blades*.
BACKUP	Significa cópia de segurança. Fazer uma cópia de segurança dos dados armazenados em seu computador ou seu site é muito importante, não só para se recuperar de eventuais falhas, mas também para evitar uma possível infecção por vírus ou até uma invasão do sistema de dados. As cópias podem ser simples como o armazenamento de arquivos em CD Rom ou em *Pendrives*, ou até mesmo em um outro disco rígido.
RESTORE	O processo de restaurar arquivos e diretórios selecionados de um backup anterior e devolvê-los a seus locais de diretório originais (ou a outro diretório).
STORAGE	dispositivos projetados especificamente para armazenamento de dados, onde através de uma conexão via rede, você pode conectar seu(s) servidor(es) à um *storage*, facilitando assim a expansão da capacidade de armazenamento sem impacto
UNIX	O sistema Unix é um sistema operacional multiusuário, multitarefas, ou seja, ele permite que um computador mono ou multiprocessadores execute, simultaneamente, vários programas, por um ou vários usuários.
VPN	VPN é uma sigla, em inglês, para “Rede Virtual Privada” e que, como o mome diz, funciona criando uma rede de comunicações entre computadores e outros dispositivos que têm acesso restrito a quem tem as credenciais necessárias.

REFERÊNCIAS

ABNT ISO27001, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos, 2013.

ABNT ISO27002, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação, 2013.

ALEMI; F. Funcionários são os maiores responsáveis por vazamento de dados, 2016. Disponível em: <http://economia.estadao.com.br/noticias/governanca,funcionarios-sao-os-maiores-responsaveis-por-vazamento-de-dados,10000022503>. Acesso em: 01 out. 2016.

D'ADDARIO; J., O que é BIA – Business Impact Analysis, 2008. Disponível em: < http://www.daddario.com.br/o-que-e-a-bia-business-impact-analysis/>. Acesso em: 04 out. 2016.

FERREIRA, N. F. **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** – Guia Prático para Elaboração e Implementação, 2008.

FONTES, E. L. G. **Praticando a Segurança da Informação** – Orientações práticas alinhadas com a Norma NBR ISO/IEC 27002 – Norma NBR ISO/IEC 27001 – Norma NBR 15999-1 – COBIT - ITIL

PWC. Pesquisa Global sobre Segurança da Informação, 2015. Disponível em: <http://www.pwc.com.br/pt/publicacoes/servicos/consultoria-negocios/2015/pesquisa-global-sobre-seguranca-informacao-2015.html>. Acesso em: 20 out. 2016.

PWC. Pesquisa Global de Segurança da Informação, 2016. Disponível em <http://www.pwc.com.br/pt/publicacoes/servicos/consultoria-negocios/giss-pesquisa-global-seguranca-informacao-2016.html>. Acesso em: 21 out. 2016.

SÊMOLA, M. **Gestão da Segurança da Informação** – Uma visão executiva. 3. Ed. Rio de Janeiro: Elsevier, 2003.