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

EDESIO CESAR FARIAS DOS SANTOS

MODELO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES APLICADO NA ORGANIZAÇÃO ALFA

Brasília
2016

EDESIO CESAR FARIAS DOS SANTOS

MODELO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES APLICADO NA ORGANIZAÇÃO ALFA

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 Gerência de Projetos de Tecnologia da Informação.

Orientador: Prof. Dr. Mauricio Lyra

Brasília
2016

EDESIO CESAR FARIAS DOS SANTOS

MODELO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES APLICADO NA ORGANIZAÇÃO ALFA

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 Gerência de Projetos de Tecnologia da Informação.

Orientador: Prof. Dr. Mauricio Lyra

Brasília, ___ de _____ de 2016.

Banca Examinadora

_____

Prof. Dr. Nome completo

_____

Prof. Dr. Nome completo

Dedico este trabalho a minha esposa Isabel Cristina C. Araújo, as minhas filhas Danielle A. Santos e Karine A. Santos, pelo apoio incondicional e incentivo durante todo o curso.

AGRADECIMENTO

Agradeço aos professores do curso que com seu trabalho e orientação souberam criar o ambiente necessário ao conhecimento e a aprendizagem. Aos meus amigos e companheiros de trabalho Sr. André Gustavo Monteiro Lima, Sr. Abner Alves de Melo, Sr. Márcio de Souza Oliveira, Sr. Túlio Fernandes de Melo Lima e Sr. Adão dos Santos, excelentes profissionais, que com seus conhecimentos, orientações precisas e suas experiências contribuíram para a realização deste trabalho.

Ouça os conselhos e aceite as instruções e você
acabará sendo sábio. (Provérbios: 19.20)

RESUMO

A Segurança da Informação é atualmente um assunto de grande importância para as organizações, sejam públicos ou privados. Os esforços para alcançar o ambiente suficientemente seguro, envolve investimentos em recursos financeiros, pessoas e tecnologia de ponta. O presente trabalho trata da interação necessária entre os fatores de segurança que permitam o equilíbrio entre Política de Segurança da Informação e Comunicações, competências dos recursos humanos e solução tecnológica de segurança, para o sucesso da Segurança da Informação nas organizações. Com objetivo de comprovar a relação necessária entre esses fatores, utilizou-se o resultado obtido na organização Alfa, que constitui uma organização pública federal da área de tecnologia da informação, na qual implantou-se um modelo de segurança, baseado nos três fatores citados, com detalhamento para as iniciativas e os resultados verificados em cada uma das fases do processo de implantação, baseando-se nos em indicadores de vulnerabilidade da própria organização.

Palavras-chave: Segurança de Informação e Comunicações. Modelo de Segurança de TI. Organização Pública Federal.

ABSTRACT

The Information Security is a very important issue for such organizations, whether public or private. The effort to get sufficiently secure environment It involves investents in financial resources , people and technology modern technology. The present work treats the interaction between security factors that allow the balance between Security Policy Information and Communications, skills human resources and security technology solution, for the success of organizations Information Security. With the objective to prove the necessary relationship between processes factors, used the results obtained from the organization Alfa, which is a federal government organization in the area of Information Technology, where was implemented hum security model based on the three mentioned factors, with detail as initiatives and the actual outcomes in each of the deployment process phases, based on the own organization vulnerability indicators.

Key words: Information Security and Communications, IT security model. Federal Public Organization.

LISTA DE ABREVIATURAS E SIGRAS

APF	Administração Pública Federal
ADDS	Serviços de Domínio Diretório Ativo
CGSIC	Comitê Gestor da Segurança da Informação
CI-SIC	Comitê Interno de Segurança da Informação e Comunicações
DHCP	Protocolo de Configuração Dinâmica de Host
DSIC	Departamento de Segurança da Informação e Comunicações
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
GPL	Licença Pública Geral
IPS	Sistemas de Prevenção de Intrusões
ISACA	Information Systems Audit and Control Association
MD	Ministério da Defesa
PDCA	Plan-Do-Check-Act (Planejar, Executar, Verificar e Agir)
PDTI	Plano Diretor de Tecnologia da Informação
PEO	Planejamento Estratégico Organizacional
POSIC	Política de Segurança da Informação e Comunicações
RH	Recursos Humanos
SGSI	Sistema de Gestão de Segurança da Informação
SIEM	Security Information and Event Management
SO	Sistema Operacional
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicações

SUMÁRIO

INTRODUÇÃO

A importância estratégica do tema Segurança da Informação e Comunicações e Segurança Cibernética para as organizações exige um tratamento apropriado e prioritário por parte da alta administração, que deve implantar recursos computacionais e de software. Esses recursos quando associados à aplicação adequada de regulamentação de políticas de segurança, combinados com ações de envolvimento dos recursos humanos, visam a interação desses fatores para a redução da vulnerabilidade da estrutura de rede de dados interna e externa das organizações, produzindo assim resultados expressivos no campo da segurança da informação.

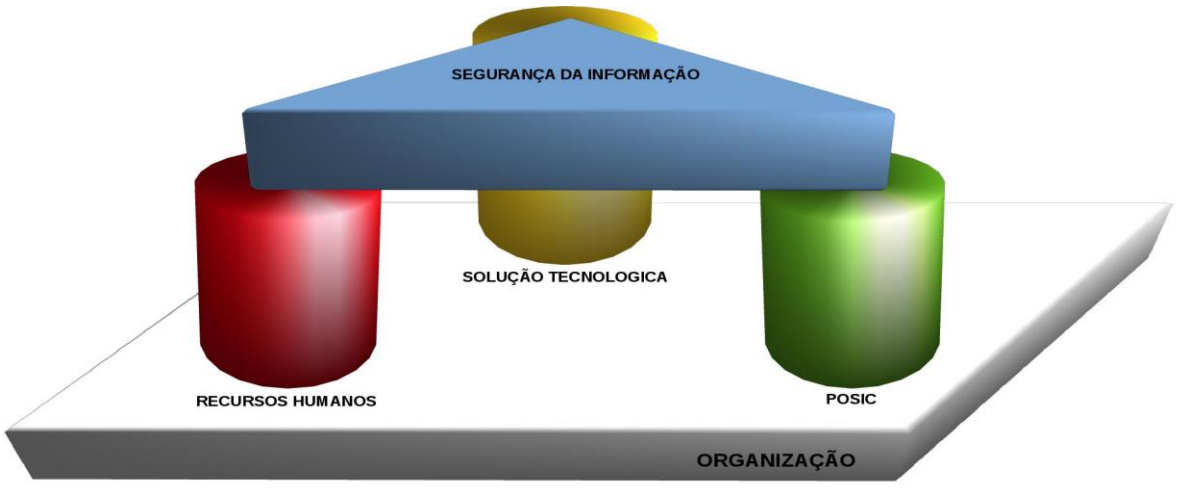
O presente estudo se propõe a compreender como se dá o processo de interação entre recursos humanos, solução tecnológica de segurança e a política de segurança da informação e comunicações, dentro do contexto de redução de incidentes de segurança nas organizações. Para tanto, este trabalho utilizará os resultados apurados a partir da aplicação de uma solução tecnológica, baseada na customização do sistema operacional Debian, ajustado à Política de Segurança da Informação e Comunicações (POSIC) e as competências relacionadas aos recursos humanos na organização Alfa.

Para alcançar esse objetivo, procedeu-se da seguinte maneira, a partir de pesquisa feita na Organização Alfa, foram identificadas as ações executadas para a produção de resultados positivos em segurança da informação, das quais foram analisados e comparados os relatórios gerados na coleta de dados pelos sensores de detecção de intrusão (*Intrusion Prevent System* – IPS) pertencente à Organização, nos períodos anterior e posterior à aplicação da solução. Foi analisada

a documentação referente à POSIC e as medidas de fiscalização e implantação na organização Alfa, além de identificar a rotina de programação adotada para a síntese da solução tecnológica baseada na customização do sistema operacional e dos ativos de rede existente na Organização.

Espera-se demonstrar com o presente estudo, a importância da segurança da informação em uma organização pública federal, na qual a existência do equilíbrio na interação entre os três fatores: solução tecnológica de segurança em tecnologia da informação (TI), Política de Segurança da Informação e Comunicações e competências relacionadas aos recursos humanos dos usuários de TI, baseado no caso prático pesquisado na organização Alfa (Figura1).

Figura 1: Esquema de equilíbrio



Forte: O autor, 2016.

A motivação para a execução deste trabalho, por parte do autor, vem da experiência pessoal, uma vez que trabalha na organização Alfa e teve a oportunidade de participar de todas as fases do processo que será apresentado no capítulo referente ao estudo de caso.

O presente trabalho foi então estruturado em 4 (quatro) capítulos. No primeiro capítulo apresenta-se o estudo, expondo uma breve contextualização e apresentando a problemática vislumbrada, assim como os objetivos geral e específico.

No segundo capítulo é realizada uma revisão literária sobre o assunto Política de Segurança da Informação e Comunicações, com detalhamento da sua estrutura e das normas relativas ao assunto. Em seguida, apresentada-se a revisão sobre solução tecnológica de segurança, com a apresentação de sistemas tecnológicos para esta finalidade. Finalmente, faz-se a revisão dos assuntos relacionados aos recursos humanos em TI, com detalhamento das competências relacionadas aos usuários da TI em uma organização.

O terceiro capítulo apresenta o estudo de caso referente à aplicação do recurso tecnológico de segurança em TI, da POSIC e dos recursos humanos na segurança da informação aplicados na organização Alfa. Esse capítulo divide-se em três partes, sendo: (a) um detalhamento do modelo lógico utilizado na customização do SO Debian versão 8.1, apresentando resumidamente a finalidade de cada um dos comandos necessários a adaptação às necessidades da organização, (b) a descrição da política de segurança adotada pela organização Alfa, e utilizada como base para customização do sistema operacional; e (c) as competências necessárias aos recursos humanos juntamente com as ações de fiscalização e manutenção da referida organização envolvida no estudo.

Por fim, o quarto capítulo o autor apresenta a conclusão sobre os resultados apurados na organização Alfa, apresentando detalhes sobre a combinação das ações envolvidas e os resultados registrados, no contexto causa efeito, sugerindo-se a continuidade em trabalho futuros.

1 REFERENCIAL TEÓRICO

1.1 Segurança da Informação e Comunicações (SIC)

Os avanços tecnológicos ocorridos nos últimos anos fizeram surgir na sociedade uma grande dependência pelos meios de comunicações e recursos computacionais, característica da chamada Sociedade da Informação (FERREIRA, 2003). A informação é atualmente um ativo intangível que pode estar entre os bens mais valiosos de uma organização (NOBRE; RAMOS; NASCIMENTO, 2010). “Em função da grande valorização dos ativos intangíveis, torna-se importante entender como gerenciá-los de forma a criar e manter o valor econômico das empresas” (KAYO et al. 2006, p. 87).

Segundo Nakamura e Geus (2009), o papel da informática como parte do processo de negócios de qualquer organização pode ser verificado mais claramente pelo aumento dos investimentos realizados na área de Tecnologia da Informação. Sendo a informação um ativo importante, tanto do ponto de vista econômico quanto para o suporte aos processos organizacionais, a gestão da segurança da informação assume papel fundamental na gestão de riscos nas organizações.

Com as evoluções recentes nas tecnologias de transmissões, melhorou-se a conectividade e o aumento da importância das comunicações no ambiente das organizações, contribuindo para sua disseminação e disponibilização entre organizações e dentro das organizações (SÊMOLA, 2003).

As ameaças relacionadas à tecnologia e às facilidades de comunicação em rede aumentam a importância da Segurança da Informação, seja ela privada ou

pública, podem ser comparadas às tentativas de invasão de um espaço físico de uma empresa, abrindo portas e cofres para a subtração de bens e recursos financeiros. Assim como no mundo real, as propriedades e as organizações virtuais necessitam de proteção e controle de acesso (NAKAMURA; GEUS, 2009, p.7).

Segundo Sêmola (2003, p. 43) podemos definir a Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Esse conceito pode ser completado com a definição dada por Beal (2005) em que a segurança da informação como o processo utilizado pelas organizações para proteger os ativos de informação das ameaças à sua integridade, disponibilidade e confidencialidade, principais características de Segurança da Informação.

Segundo Fontes (2006, p. 9), a Segurança da Informação existe para minimizar os riscos do negócio em relação à dependência do uso dos recursos de informação para o funcionamento da organização. Sem a informação ou com uma incorreta, o negócio pode ter perdas que comprometam o seu funcionamento e o retorno de investimento dos acionistas.

Mas como abordar essa proteção da informação? O que significa exatamente proteger a informação?

Segundo Fontes (2006, p. 11), proteger a informação significa garantir:

Disponibilidade: a informação deve estar acessível para o funcionamento da organização e para o alcance de seus objetivos e missão;

Integridade: a informação deve estar correta, ser verdadeira e não estar corrompida;

Confidencialidade: a informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na organização; para tanto, deve existir uma autorização prévia;

Legalidade: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos, bem como os princípios éticos seguidos pela organização e desejados pela sociedade;

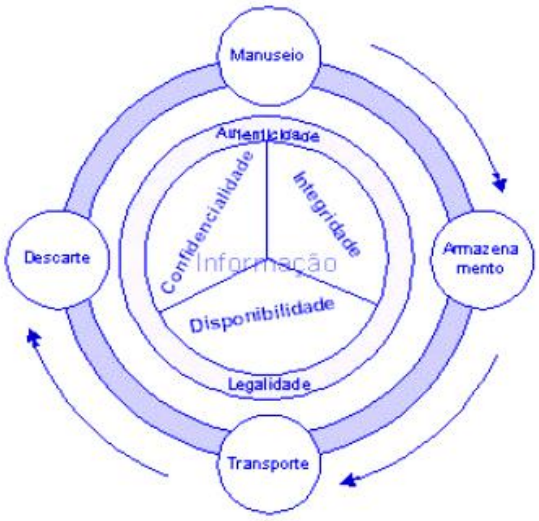
Auditabilidade: o acesso e uso da informação devem ser registrados possibilitando a identificação de quem fez o acesso e o que foi feito com a informação; e.

Não repúdio de autoria: o usuário que gerou ou alterou a informação (arquivos texto, mensagens de correio eletrônico ou *downloads*) não pode negar o fato, pois existem mecanismos que garantem sua autoria.

A Information Systems Audit and Control Association (ISACA, 2009), afirma que somente a tecnologia não pode corrigir as falhas de segurança que são resultado de governança ou gestão inadequada, ou provocadas por razões culturais ou por despreparo do pessoal. Em todos os processos organizacionais, não importando o tamanho ou a natureza da organização, a informação sempre está presente, fluindo entre os usuários e suportando a consecução das rotinas da empresa.

O ciclo de vida da informação é composto e identificado pelos momentos vividos pela informação dentro da organização Figura 2. Em todos esses momentos a informação é colocada em contato com riscos. Esses momentos acontecem quando os ativos físicos, tecnológicos e humanos fazem uso da informação, fazendo parte dos processos que compõem a operação das empresas (SÊMOLA, 2003).

Figura 2 –Ciclo de vida da informação



Fonte - Sêmola 2003

Segundo a NBR ISSO/IET 27002 da Associação Brasileira de Normas Técnicas (2013, p. 4), o valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, idéias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requer proteção contra vários riscos.

A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização são atendidos (NBR 27002, 2013).

Ainda, que é essencial que uma organização identifique os seus requisitos de segurança da informação, sendo que existem três fontes principais de requisitos de segurança da informação abaixo listados.

Uma fonte é obtida a partir da avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócio da organização. Por meio da avaliação de riscos, são identificadas as ameaças aos ativos, e as vulnerabilidades destes e realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio.

Uma outra fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural.

A terceira fonte é composta por conjuntos particulares de princípios, objetivos e os requisitos do negócio para o manuseio, processamento, armazenamento, comunicação e arquivo da informação, que uma organização tem que desenvolver para apoiar suas operações.

Conforme a Segundo a NBR ISSO/IET 27001 da Associação Brasileira de Normas Técnicas (2013 p.5), que especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) documentado dentro do contexto dos riscos de negócio globais da organização. Ela especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes.

O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar

confiança às partes interessadas. Com isso as organizações podem constituir ações para adequar sua estrutura visando à melhoria no campo da segurança da informação

Ao se falar em organizações, podemos dividi-las em públicas e privadas, nas quais a forma de abordar o assunto segurança da informação apresenta características diferentes em cada um dos segmentos. Apesar das normas que tratam da segurança da informação não fazerem referências a essa particularidade, cabe citar algumas normas do Governo Federal que tratam do assunto.

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR), órgão do Governo Federal, por meio do Departamento de Segurança da Informação e Comunicações (DSIC), visualizou a necessidade de regulamentar a gestão da Segurança da Informação e Comunicações (SIC), publicando a Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, essa Norma aprovar orientações para Gestão de Segurança da Informação e Comunicações a serem implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta, definindo as competências dos atores envolvidos no processo de Segurança da Informação. A Instrução Normativa em seu Art. 2º, inciso VII, revelou o entendimento de que a Gestão da Segurança da Informação e Comunicações, em sua plenitude, corresponde:

As ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais, estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação e Comunicações. (BRASIL, 2008).

Após a publicação da Instrução Normativa GSI/PR nº 1, o DSIC, aprovou a Instrução Normativa nº 2 - 02/IN01, definindo a metodologia de gestão de SIC a ser utilizada pelos órgãos e entidades da Administração Pública Federal (APF), conforme descrito:

A metodologia de gestão de segurança da informação e comunicações baseia-se no processo de melhoria contínuo denominado ciclo “PDCA” (Plan-Do-Check-Act), referenciado pela NBR ISO/IEC 27001:2013.

A escolha desta metodologia levou em consideração três critérios: a) Simplicidade do modelo; b) Compatibilidade com a cultura de gestão de segurança da informação em uso nas organizações públicas e privadas brasileiras; c) Coerência com as práticas de qualidade e gestão adotadas em órgãos públicos brasileiros.

Sobre regulamentos, políticas, normas e regras, Fontes (2006, p. 3), observa que esses instrumentos têm como objetivo fazer com que o uso da informação na organização aconteça de uma forma estruturada, possibilitando que o negócio não seja prejudicado por um mau uso da informação: seja por erro ou por acidente. Ainda sobre isso, Fontes (2006, p. 3) declara: [...] proteger a informação é responsabilidade de cada pessoa na organização, independentemente de seu nível hierárquico! Do mais alto executivo ao mais novo estagiário.

As organizações sejam públicas ou privadas mesmo sabendo da importância de proteger a informação, por vezes preocupam-se apenas em criar proteções aos acessos internet apenas, deixando de fora o seu parque computacional, os seus colaboradores e as políticas de segurança, criando dificuldades na gestão da segurança. Existe no Brasil um grupo destinado ao tratamento dos incidentes de segurança em computadores conectados à internet,

chamada CERT.br. O Grupo de Resposta a Incidentes de Segurança para a Internet Brasileira (CERT.br) funciona como ponto centralizador de notificações de incidentes de segurança, possibilitando a coordenação e o apoio necessário ao processo de resposta a incidentes, sendo mantido pelo Comitê Gestor da Internet no Brasil . O CERT.br atua através do trabalho de conscientização sobre os problemas de segurança, da análise de tendências e correlação entre eventos na Internet brasileira, que tem objetivo aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

São atividades principais conduzidas pelo CERT.br listadas em sua página na internet:

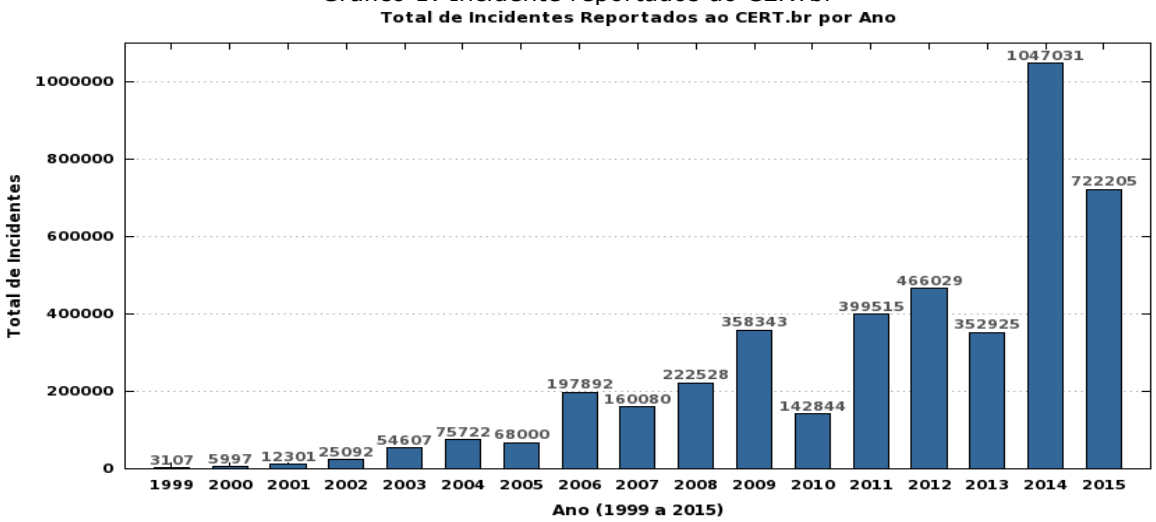
> Principais Atividades:
>
> 1 Tratamento de Incidentes
>
> • Dar suporte ao processo de recuperação e análise de ataques e de sistemas comprometidos;
>
> • Estabelecer um trabalho colaborativo com outras entidades, como outros Grupos de Resposta a Incidentes de Segurança em Computadores (CSIRTs), empresas, universidades, provedores de acesso e serviços Internet e *backbones*;
>
> • Manter estatísticas públicas dos incidentes tratados e das reclamações de spans recebidas.
>
> • Realizar reuniões com setores diversos da Internet no Brasil, de modo a articular a cooperação e implantação de boas práticas de segurança.
>
> • Aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço

Internet brasileiro, através da manutenção de uma rede de honeypots distribuídos em diversas redes do país;

- Obter, através de honeypots de baixa interatividade, dados sobre o abuso da infraestrutura de redes conectadas à Internet para envio de spans.

Avaliando as informações sobre a estatística dos incidentes reportados ao CERT.br, conforme gráficos 1, observa-se que houve um crescente número de incidentes ocorridos e relatados no Brasil nos últimos cinco anos.

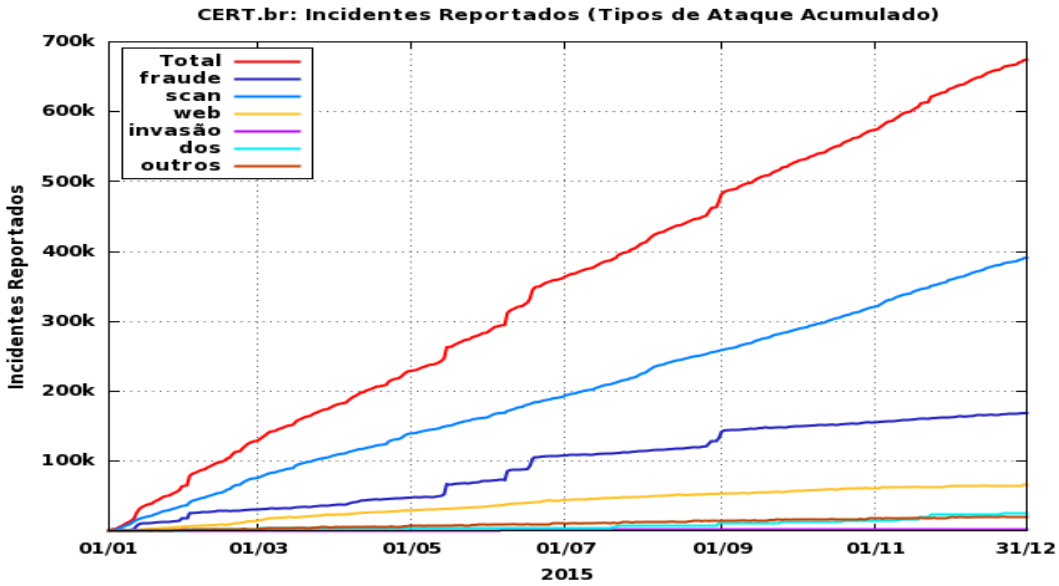
Gráfico 1: Incidente reportados ao CERTbr



Fonte - CERT.br (http://www.cert.br/stats/incidentes/)

Quanto aos tipos de ataques reportados no ano de 2015. O gráfico 2 detalha o quantitativo de cada tipo de incidente, com destaque para a ocorrência de *scan* que é amplamente utilizado para identificar possíveis alvos para ataques.

Gráfico 2: Tipos de ataque reportados ao CERTbr



Fonte – CERT.br (http://www.cert.br/stats/incidentes/)

worm: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.

Dos (DoS --*Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.

invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.

web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.

scan: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

fraude: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

1.2 Solução Tecnológica de Segurança

As soluções tecnológicas de segurança da informação são barreiras que impedem ou limitam o acesso à informação, que se encontra em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposto à alteração não autorizada por elemento mal intencionado, sendo denominado como controles lógicos. Segundo Nakamura e Geus (2009), as soluções tecnológicas devem ser

adaptativas e flexíveis a fim de suprir necessidades estratégicas da organização, e são antagônicas à produtividade – quanto maiores as funcionalidades, maiores as vulnerabilidades existentes. Em ambiente cooperativo, a segurança será resultado do conjunto de esforços para entender o ambiente e as tecnologias, e saber como utilizá-las e implementá-las de modo correto.

Nas soluções tecnológicas, os controles lógicos podem ser mecanismos de cifração ou encriptação, assinatura digital, mecanismos de garantia da integridade da informação, mecanismos de controle de acesso, mecanismos de certificação, integridade, honeypot e protocolos de segurança.

Encriptação ou cifração: a informação é transformada de forma a torná-la inelegível a terceiros, podendo o processo ser reversível. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.

Assinatura digital: é um algoritmo para garantir integridade e autenticidade de dados digitais. Os dados criptografados associados a um documento garantem a integridade e autenticidade do documento, mas não sua confidencialidade.

Mecanismos de garantia da integridade da informação: usam as funções de "Hashing" (particionamento de P em um número finito de classes P1, P2... Pn > 1, técnica de conversão de chaves) ou de checagem, é garantida a integridade através de comparação do resultado do teste local com o divulgado pelo autor.

Mecanismos de controle de acesso: Palavras-chave, sistemas biométricos, *firewalls*, cartões inteligentes. Segundo Ferraiolo, Kuhn e Chandramouli (2003), o controle de acesso é crítico na preservação da confidencialidade e integridade da informação, evidenciando assim que qualquer aplicação que demande certo nível de confidencialidade necessita de algum mecanismo de controle de acesso.

Mecanismos de certificação: Atesta a validade de um documento.

Integridade: Medida em que um serviço/informação é genuíno, isto é, está protegido contra a personificação por intrusos.

Honeypot: É uma ferramenta que tem a função de propositalmente simular falhas de segurança de um sistema e colher informações sobre o invasor enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema. É uma espécie de armadilha para invasores. O *HoneyPot* não oferece nenhum tipo de proteção.

Protocolos seguros: Uso de protocolos que garantem um grau de segurança e usam alguns dos mecanismos acima citados.

Na maioria das vezes deve-se usar a combinação de várias estratégias de segurança de acordo com o nível de segurança que a empresa deseja atingir. Dentre elas destacam-se: Políticas de segurança, cópias de segurança, controles de acesso, segurança física, f*irewall,* política de senha, detecção de intrusão e treinamento/conscientização dos usuários.

Atualmente no mercado estão disponíveis algumas soluções tecnológicas de segurança que abrangem o controle do parque computacional, controle de atualizações e proteção dos ativos de rede, podendo ser configurado conforme as

características de emprego para cada uma das soluções. Para completar a idéia seguem abaixo alguns exemplos de soluções tecnológicas de segurança disponíveis no mercado.

1 Activity Diretory Serve Domain Service (ADDS) – solução da Microsoft, o Serviços de Domínio Ativo de Diretório (ADDS) é uma função de servidor no diretório ativo que permite aos administradores gerenciar e armazenar em um banco de dados as informações sobre os recursos de rede, bem como os dados de aplicativos. O ADDS ajuda os administradores a gerenciar os elementos de uma rede (computadores e usuários finais) e reordená-los em uma hierarquia personalizada.

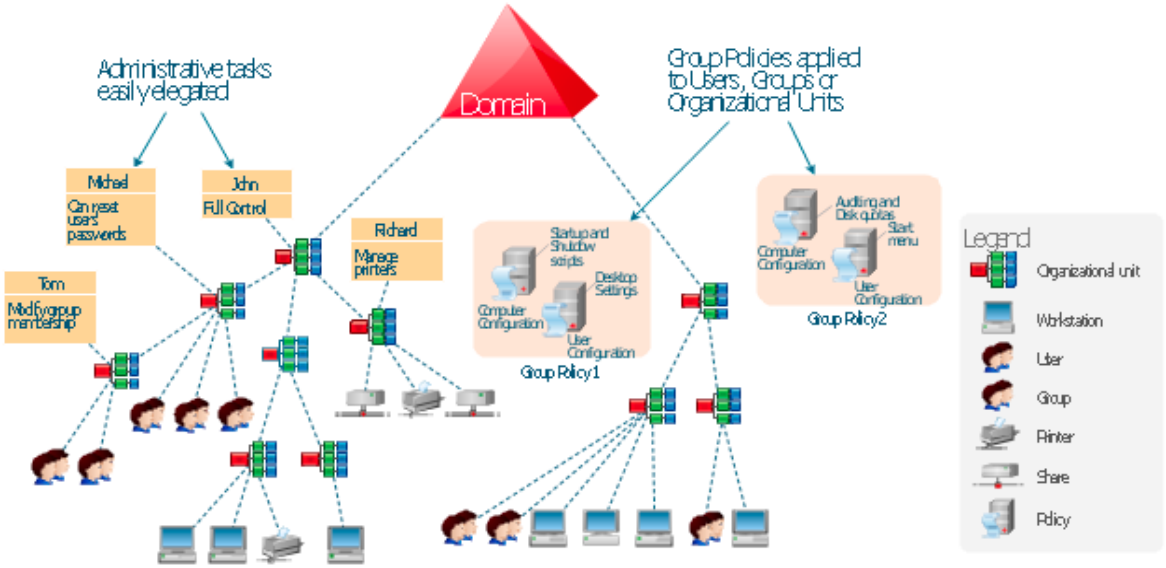


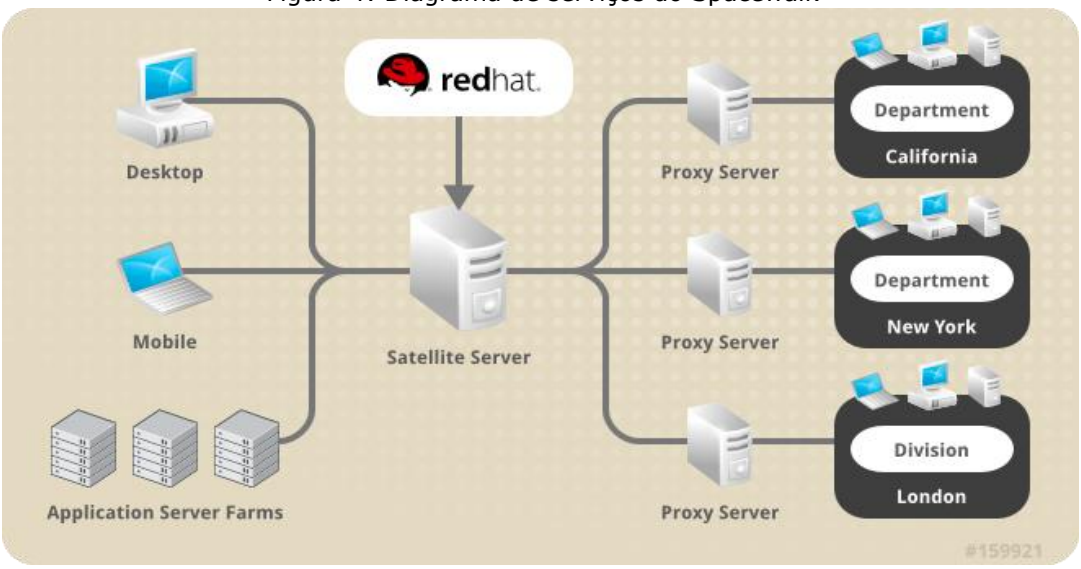
Figura 3 - Esquema de serviços do ADDA

Fonte - Microsoft (https://conceptdraw.com/a195c3/preview)

2 Spacewalk – solução da Red Hat baseada em código fonte aberto com aplicação em gerenciamento de sistemas Licença Pública Geral (GPL) v2 Linux.

Possibilita inventariar o sistema de informações (hardware e software), instalar e configurar os pacotes de atualizações para grupos personalizados, distribuir conteúdos remotamente de maneira eficiente e gerenciar e implantar arquivos de configuração para os seus sistemas.

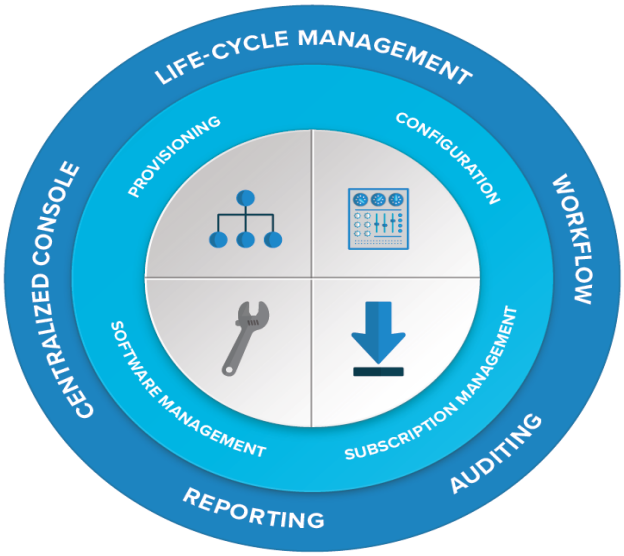
Figura 4: Diagrama de serviços do Spacewalk



Fonte - Redhat (http://www.aossama.com/tag/spacewalk/)

3 Satellite – solução da Redhat destinada a ambientes com a distribuição Redhat que possibilita o gerenciamento de configuração, gerenciamento de software, compatível com plataforma física ou virtual.

Figura 5: Diagrama de serviços do Satellite



Fonte - Redhat www.redhat.com/pt-br/technologies/management/satellite)

1.3 Recursos Humanos em TI

Nas organizações, os recursos humanos desempenham papel fundamental para a correta utilização dos dispositivos tecnológicos. De acordo com Igbaria, Parasuraman e Baroudi (1996), "o uso de microcomputadores por profissionais e gerentes não têm correspondido às expectativas das empresas". Isto resulta em que o benefício potencial destas tecnologias não vem sendo completamente realizado. Tal situação tem levado, frequentemente, a subutilização dos investimentos feitos em TI e à pressão sobre os recursos humanos das empresas para a utilização crescente de uma tecnologia em constante mutação que, muitas vezes, não é bem entendida e até os seus usuários lhe resistem (DAVIS; BAGOZZI; WARSHAW, 1992).

Fontes (2008, p. 33), afirma que uma organização que possui um bom clima organizacional terá mais facilidade na implantação do processo de segurança da informação, assim, o ambiente de não confiança entre os integrantes da organização, clima de inimizades, revoltas contra a organização, deficiência na comunicação entre outros problemas não impedem a implantação de um processo de segurança, mas pode dificultar em muito.

Esta afirmação é confirmada por Sêmola (2006, p. 81) quando cita que:

> O usuário é uma peça frágil e uma das mais críticas, capaz de pensar, e de forma não binária, adotar um comportamento diferente num piscar de olhos, bem diferente do que se pode esperar de uma máquina de proteção bem configurada e não suscetível a tomar decisões por conta própria diferentes daquelas pré-estabelecidas.

Um grande desafio aos profissionais da área de Segurança da Informação nas organizações é garantir que a POSIC contemple tanto os aspectos físicos e tecnológicos quanto os recursos humanos presentes nas organizações. Esses componentes são apontados como a base para o sucesso da Segurança da Informação, pois ajustam um conjunto de procedimentos e normas inerentes aos objetivos e às melhores práticas de gerenciamento das informações organizacionais. No entanto, a simbiose destes fatores esbarra, muitas vezes, na gestão e na forma com que os integrantes manipulam as informações.

Nenhuma área da informática é tão apreciada como a segurança da informação, todo processo de segurança inicia e tem seu termino em um ser humano. Segurança não é uma questão técnica, mas uma questão gerencial e humana. Não adianta adquirir uma série de dispositivos de hardware e software sem treinar e conscientizar o nível gerencial da empresa e todos os seus funcionários. (OLIVEIRA, 2001, p. 43).

O trato com o usuário de TI envolve a engenharia social que manipula as pessoas, para que possam entregar as chaves e explorar as franquezas humanas e sociais (NAKAMURA; GEUS, 2009).

A força do e*ndomarketing* vem da abrangência da conscientização através das técnicas utilizadas, tais como: treinamentos, publicações e divulgação da POSIC, comunicações internas, e-mails com orientações, *pop up* na intranet, reuniões de conscientização, *folders,* jornais internos, elaboração de material promocional, treinamento direcionados, palestras periódicas, apostilas, entre outros.

Segundo Ellwanger (2009, p. 16), existem maneiras e métodos distintos dirigidos ao público interno, que podem ser utilizados no processo de

Endomarketing, tais como: educativos/interativos, informacionais, promocionais e de reforços. O quadro 2 ilustra essas técnicas utilizadas em cada método.

Quadro 1 – Técnicas utilizadas para a conscientização dos usuários

MÉTODOS PROMOCIONAIS	**MÉTODOS EDUCATIVOS/INTERATIVOS**
▪ Eventos/Feiras ▪ Papéis de parede ▪ *Banners* na intranet ▪ Hiperlinks da intranet para o site de segurança ▪ Artigos com publicações internas ▪ Pôsteres ▪ Jogos e quebra-cabeças ▪ Bloco de notas ou adesivos ▪ Camisetas ▪ *Mouse pads*	▪ Apresentação de slides ▪ Treinamento ▪ Módulos de treinamento online ▪ Sessões breves ▪ Demonstrações ▪ Vídeos ▪ *Workshops*
MÉTODOS DE REFORÇO	**MÉTODOS INFORMACIONAIS**
▪ Assinatura dos princípios de segurança ▪ Contrato de confidencialidade ▪ Exames ou testes de conscientização ▪ Ações disciplinares para não conformidades ▪ Avaliações anuais ou critérios de promoção ▪ Mecanismos de recompensa	▪ Folhetos/Cartões ▪ Pequenos artigos ou novas histórias ▪ Postagens no site de segurança ▪ E-mails de advertência ▪ Guias de segurança da informação ▪ Notícias ▪ Dicas de segurança

Fonte- Adaptado de Ellwanger 2009

Portanto, o e*ndomarketing* quando aplicado nos processos de gestão de SIC fortalece a Segurança da Informação à medida que mantêm os usuários comprometidos e informados das ações necessárias para a conformidade, aumentando assim o nível de conscientização e comprometimento dos usuários, o que reflete na efetividade do processo de SIC na organização, que é o objetivo fim da POSIC.

Em relação à segurança da informação de um modo geral, Pemble (2004, tradução nossa) oferece um contraponto em relação à literatura técnica, que é pródiga em conceitos sobre o que a segurança da informação faz, mas não do que ela efetivamente é. O autor afirma que a segurança da informação deve ser definida, considerando-se as atribuições do profissional responsável por esta função. Em

função desta ótica diferenciada, o autor defende que o profissional de segurança da informação deve atuar em três esferas:

a) esfera operacional, que deve se ocupar dos impactos que os incidentes podem gerar a continuidade do negócio;

b) esfera da reputação, que se ocupa do impacto dos incidentes no valor da empresa ou da “marca”; e.

c) esfera financeira, que se ocupa dos custos incorridos na eventualidade de um incidente de segurança da informação.

Sêmola (2003) lembra que os recursos humanos são o elo mais frágil da corrente. Mesmo que se especifiquem normas, procedimentos e controles para garantir a segurança da informação, o descumprimento por parte de um recurso humano cria uma vulnerabilidade e compromete o sistema de gestão da segurança da informação.

A NBR ISO/IEC 27002 da Associação Brasileira de Normas Técnicas (2013, p. 97) disciplina que a organização deve ter como objetivo reduzir os riscos de erro humano, roubo, fraude assim como o uso indevido das instalações. Para isto, deve-se observar que as responsabilidades de segurança sejam atribuídas na fase de recrutamento, incluídas em contratos e monitoradas durante a vigência de todo o contrato de trabalho do funcionário.

Segundo a NBR ISO/IEC 27002 da Associação Brasileira de Normas Técnicas (2013, p. 5), a abordagem de processo para a gestão da segurança da informação encoraja que seus usuários enfatizem a importância do entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança de informação; da

implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização; monitoração e análise crítica do desempenho e eficácia do SGSI; e melhoria contínua baseada em medições objetivas.

Ainda segundo a NBR ISO/IEC 27002 da Associação Brasileira de Normas Técnicas (2013, p. 18), a organização deve assegurar que todo o pessoal que tem responsabilidades atribuídas definidas no SGSI seja competente para desempenhar as tarefas requeridas:

a) determinando as competências necessárias para o pessoal que executa trabalhos que afetam o SGSI;

b) fornecendo treinamento ou executando outras ações (por exemplo, contratar pessoal competente) para satisfazer essas necessidades;

c) avaliando a eficácia das ações executadas; e.

d) mantendo registros de educação, treinamento, habilidades, experiências e qualificações.

Quanto as habilidades comportamentais ou humanas são as adquiridas ao longo da vida, ou seja, na educação e nos relacionamentos humanos e corporativos. Destacam-se: iniciativa, criatividade, comunicação e expressão, relacionamento pessoal, espírito de equipe e/ou administração participativa, planejamento pessoal, organização, concentração, atenção, disponibilidade, responsabilidade, etc. O desenvolvimento dessas habilidades é um desafio individual, que deve ser enfrentado com dedicação pelo trabalhador que deseja ascender profissionalmente. Os profissionais não podem ficar inertes. Devem ter

iniciativa e buscar a qualificação para garantir seu diferencial competitivo, como solucionadores de problemas que requerem o uso dos recursos da TI.

O objetivo fundamental da gestão de recursos humanos numa organização é a identificação e desenvolvimento das competências que irão sustentar a intenção estratégica da organização. A área de recursos humanos precisa atuar como um parceiro estratégico. A incapacidade de estabelecer esta parceria e de evidenciar a importância da função de Recursos Humanos (RH) para a elaboração e implementação de estratégias competitivas é o que provoca, na maioria das vezes, o papel relativamente secundário alocado para o RH em muitas empresas (BRANDÃO; GUIMARÃES, 2001). Cada vez que equipes são treinadas e funcionários são escolhidos também pelo critério de relacionamento (pessoas que saibam trabalhar bem com as outras), ampliam-se as possibilidades de um aprendizado constante e uniforme de como operar complexos sistemas em rede. Equipes treinadas desenvolvem uma forte intuição perceptiva e passam a valorizar os investimentos

1.4 Política de Segurança da Informação e Comunicações (POSIC)

As organizações devem adotar políticas de segurança da informação, baseadas preferencialmente na ABNT NBR ISO/IEC 27001:2013, para 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. Sua concepção é necessariamente realizada em uma abordagem a partir do topo com assuntos tratados progressivamente (NAKAMURA; GEUS, 2009).

Segundo a NBR ISO/IEC 27002 da Associação Brasileira de Normas Técnicas (2013, p. 8), o objetivo primordial de uma POSIC é prover orientação da direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes conforme a Figura 6.

Figura 6 - Estrutura baseada na NBR ISSO 27002:2013

Fonte - COELHO, 2013, p. 73

A legislação que trouxe a regulamentação e a instituição da Política de Segurança da Informação no âmbito da Administração Pública Federal, a saber, o Decreto Federal nº 3.505, de 13 de junho de 2000, onde a Segurança da Informação está sistematizada de maneira muito abrangente e diretamente relacionada à idéia de proteção dos sistemas de informação.

Buscando a efetividade na implantação de uma POSIC, e no aumento da cultura de Segurança da Informação, muitas organizações procuram casos de sucessos em outras organizações, aproveitando o conhecimento acumulado nesses processos, esta busca de experiências possibilitou o surgimento das chamadas

Boas Práticas, que são as melhores técnicas e ações já testadas e implementadas com sucesso em diversas organizações.

Segundo Coelho (2013, p. 72), a POSIC deve ter como suas principais características ser claramente definida, mantida, formalmente publicada e principalmente estar alinhada a NBR ISO 27001:2013 e com as demais normas gerais para quais a organização se oriente. A POSIC de uma organização é composta por diretrizes gerais que servirão de base para as normas, procedimentos e instruções referentes a Segurança da Informação, seguindo uma sequência tal como: o estratégico, passando pelo tático, operacional e chegando aos registros de evidências, que é à base da pirâmide da política, conforme a Figura 6.

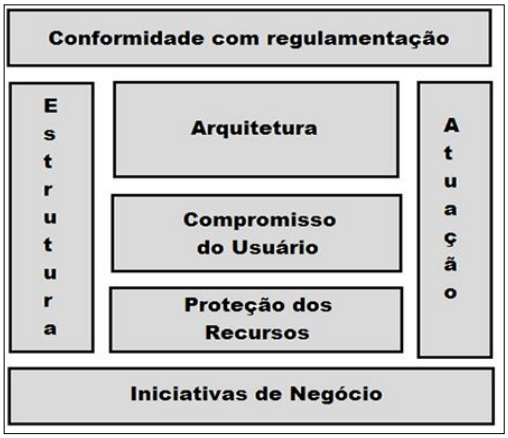
Figura 6 - Bases da Política de Segurança

Fonte - Adaptado pelo autor, COELHO, 2013, p 72.

Neste contexto, fica evidente que as políticas, normas e procedimentos de segurança fornecem um melhor direcionamento para as implementações técnicas. Não é aconselhável implementar procedimentos de segurança sem uma política formalmente definida. Porém, as políticas, normas e procedimentos de segurança devem ser um conjunto de ações que compõem a Gestão da Segurança na

organização, e que faz parte de um todo, envolvendo toda a organização, o usuário e em conformidade com a realidade da organização. Conforme sintetizou Fontes (2008, p. 18) na Figura 7.

Figura 7 - Segurança alinhada ao negócio



Fonte - FONTES, 2008

Conceitualmente, parece segura a idéia de que toda política deve ser formalizada. Porém, apesar de não parecer coerente, em tese, uma empresa pode ter políticas de conhecimento geral dos funcionários e que não estão formalizadas, sendo transmitidas oficialmente, por quem de direito, de forma oral, sem qualquer formalização. Apesar de pouco ortodoxo, é possível que isto aconteça em organizações de menor porte ou mais informais. Contudo, pressupõe-se que o correto é a formalização de todas as políticas que direcionam a organização.

De acordo com Campos (2006, p. 99), a Política de Segurança da Informação “é um conjunto de regras que determina qual deve ser o comportamento das pessoas que se relacionam com a organização no que se refere ao tratamento da informação”. Evidencia-se neste conceito que a política tem total relação com a gestão de pessoas e seu comportamento na organização, e que o risco de informação a ser gerenciado é, normalmente, resultado da interação das pessoas com os ativos da informação.

É importante observar que a política de segurança deve ser personalizada para cada organização, já que estabelecem os padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança aceitável pela empresa (SÊMOLA, 2003).

Segundo Beal (2005) a política de segurança da informação é a forma com que a direção da empresa demonstra seu comprometimento com a proteção da informação e cria a base para o comportamento de todos os usuários com relação aos processos de identificação e tratamento dos riscos.

A POSIC deve constar de um documento, publicado e de conhecimento geral dos usuários dos ativos de informação da empresa. Ferreira e Araujo (2006, p. 11) defendem que o documento da política de segurança da informação deve ser: simples, compreensível, homologado pela alta direção, estruturado de forma a permitir a implantação por fases, alinhado com as estratégias da empresa, com padrões e procedimentos preexistentes; orientado aos riscos identificados, flexível às mudanças de tecnologia e processos, com foco na proteção dos ativos de informação, priorizando os de maior valor e importância, com orientação positiva, ou seja, não concentrada em ações proibitivas ou punitivas.

A POSIC tem que apresentar consistência com as demais normas da organização, bem como com a legislação à que a empresa está sujeita. É importante ainda que a política defina as metas, informando os objetivos quantificáveis e em que tempo devem ser alcançados. Deve também definir as responsabilidades pelo uso da informação e de que forma se entende ser correto o seu uso. Por último, devem ser definidas as penalidades para os usuários que a desrespeitarem (CAMPOS, 2006).

Os principais elementos da POSIC segundo Ortalo (1996) são:

a) Elementos básicos, onde se descrevem os usuários, objetos, direitos de acesso e atributos presentes na organização ou no sistema. Estes elementos definem o vocabulário que norteará a construção da política;

b) Os objetivos da segurança, ou seja, as metas de segurança no que diz respeito a confidencialidade, integridade e disponibilidade; e

c) O conjunto de regras que descreve os mecanismos do sistema, relevantes à segurança, com as eventuais modificações necessárias.

É conveniente que o documento que registra a política de segurança contenha uma declaração introdutória, inserindo o problema e o conceito da segurança da informação no contexto mais amplo dos riscos do negócio e explicando a importância da segurança da informação e dos recursos computacionais para prevenir consequências advindas da destruição, alteração indevida ou da divulgação não autorizada das informações da organização (BEAL, 2005).

Campos (2006) apresenta a importância da participação das equipes de auditoria interna, que seriam responsáveis por elaborar, executar auditoria e propor planos de ação para adequar as áreas da organização.

A construção de uma cultura sobre a segurança da informação pode ser efetivada com a realização de seminários, campanhas de divulgação, cartas da diretoria, mostrando o comprometimento com a segurança, e, ainda, a assinatura de termos de responsabilidade e confidencialidade por todos os usuários de ativos de informação (SÊMOLA, 2003).

O documento da política da informação não pode ser estático. Para que continue efetivo, ele deve acompanhar as mudanças nas ameaças oriundas dos

ambientes externo, interno, nas vulnerabilidades associadas aos ativos da informação e nas necessidades do negócio. Faz-se necessário criar mecanismos que garantam a atualização constante do documento, com revisões periódicas do conteúdo (BEAL, 2005).

Ferreira e Araujo (2006, p. 125) sugerem que o intervalo médio utilizado para a revisão da política é de seis meses ou um ano, porém deve ser realizada uma revisão sempre que forem identificados fatos novos, não previstos na versão atual que possam ter impacto na segurança das informações da organização.

É inconteste a necessidade de realizar periodicamente a avaliação e a atualização da política de segurança da informação, principalmente em virtude das constantes mudanças no ambiente de negócios, das novas tecnologias e da usual remodelagem dos processos das organizações.

2 ESTUDO DE CASO

2.1 Contexto

A Organização ALFA, objeto da pesquisa desse trabalho, é um órgão integrante da Administração Pública Federal (APF), subordinada ao Ministério da Defesa (MD), tendo como principais atividades: os serviços de Tecnologia da Informação e Comunicações (TIC) no nível estratégico, projetos de TIC, logística de equipamentos de Tecnologia da Informação para organizações vinculadas, que no período de estudo desse trabalho totalizavam 70 organizações, as quais para o presente trabalho foram chamadas de Unidades Apoiadas.

Os dados que serão apresentados ao longo desse trabalho foram coletados junto aos arquivos da Organização e se referem ao período compreendido, entre os anos de 2014 e primeiro semestre do ano de 2016.

A organização ALFA tem como sua missão e responsabilidade as questões relacionadas à TIC das Unidades Apoiadas, que são unidades em sua maioria de caráter operacional, assim possuindo reduzidos quadros técnicos em TI, o que proporciona grande dependência dos serviços e suporte disponibilizados pela organização ALFA.

Dentre os principais serviços prestados pela organização ALFA às suas Unidades Apoiadas e constante em seu catálogo de serviços, podemos citar:

▪ Serviço de consultoria técnica, (Projetos de TI, Infraestrutura de Redes, redes *mobile* etc.);

- Hospedagem de sistemas corporativos;
- Hospedagem de sistemas regionais;
- Serviço de hospedagem de páginas de internet;
- Serviço de acesso à internet (provedor regional às Unidades Apoiadas);
- Correio corporativo oficial (@correio);
- Perícia forense computacional;
- Correio corporativo pessoal;
- Capacitação em diversas áreas da TI; e
- Auditorias.

Para prestar esses serviços e suporte às suas Unidades Apoiadas, a organização conta com *links* de internet de alta velocidade, um moderno parque tecnológico, tendo em suas instalações um recém-inaugurado data center. A organização conta ainda com equipamentos de segurança da informação, de segurança física e de hospedagens de sistemas com o estado da arte em tecnologia.

Diante das funções executadas e de sua missão institucional, a organização ALFA conta com um quadro de recursos humanos, composto por aproximadamente 120 (cento e vinte) integrantes, quantitativo esse que permaneceu praticamente imutável durante o período de estudo deste trabalho. Analisando seu quadro, a organização é composta, em sua maioria, por servidores de carreira, cerca de 64%. O quadro de pessoal é complementado por uma parcela significativa de pessoal técnico contratado, em torno de 36%, chamados de quadro de técnicos temporários. Estes servidores permanecem na organização por no máximo oito

anos, sempre com renovação contratual efetivada anualmente. Nesse contexto, o quadro de servidores da organização é em sua maioria composto por servidores que possuem suas formações nas áreas técnicas e de engenharia, sendo as de Engenharia Elétrica, Eletrônica, Comunicações, Computação e Analistas de Sistemas, entre outras. O quadro de servidores da organização ALFA é composto, em sua maioria, por profissionais de perfil técnico e que trabalham diretamente com tecnologia da informação no dia a dia da organização.

Diante de sua missão institucional, a organização ALFA ao apoiar as suas unidades, encontra-se diante de uma grande responsabilidade, pois integra um sistema maior, denominado de “Sistema de Telemática”, com abrangência nacional, tendo sobre sua responsabilidade uma ampla parcela do território nacional, com unidades geograficamente localizadas em quatro Estados da Federação, abrangendo municípios do Triangulo Mineiro e as cidades de Brasília, Palmas e Goiânia.

Após apresentar as qualificações referentes à organização Alfa, é possível afirmar que o maior “cliente” da organização ALFA é a sociedade, visto que a organização é integrante da APF, e que qualquer vazamento de informações tem o potencial de causar grande impacto na imagem da organização e de ser prejudicial à sociedade, uma vez que manipula informações sensíveis e estratégicas.

Ao ter como uma de suas atribuições o suporte a suas Unidades Apoiadas em assuntos relativos a Segurança da Informação, tais como prover serviços de Perícias Forense e auditorias nas áreas de SIC. A Organização vê-se obrigada a demonstrar um alto grau de conformidade com a SIC, pois constitui referência e exemplo a ser seguido por suas unidades apoiadas, ou seja, a referência em SIC deve ser a própria organização ALFA.

Por esse motivo, a partir do ano de 2014, a Organização iniciou esforços para executar as ações iniciais em segurança da informação, pois mesmo ainda sem ter uma POSIC estabelecida e divulgada, a organização já contava com um parque computacional expressivo baseado em software livre, com sistema operacional Linux instalado e alguns dispositivos de segurança de rede, com foco na proteção para saída de internet. Com isso, já havia alguma preocupação em se realizar algumas medições por observação e amostragens, as quais revelavam um nível de maturidade em Segurança da Informação muito aquém do esperado para sua missão.

Então foram adotadas ações de melhoria nos serviços disponibilizados e existentes na organização Alfa, com foco na segurança cibernética e nos serviços de TI. O ponto de partida foi à elaboração de um Planejamento Estratégico Organizacional (PEO), com a definição da identidade organizacional e as iniciativas estratégicas de TI, alinhadas com os objetivos estratégicos da instituição enquadrante. Após o PEO, foi elaborado o Plano Diretor de Tecnologia da Informação (PDTI), que contribuiu para nortear as ações de melhoria na gestão dos recursos computacionais e de logística de TI voltada para Alfa e as unidades apoiadas.

2.2 Implantação da POSIC na organização Alfa

Ao final do ano de 2014, a Organização deu um passo importante para transformar o cenário de baixa maturidade em TI na organização, executando as seguintes ações: estabeleceu formalmente um grupo de trabalho com a missão de

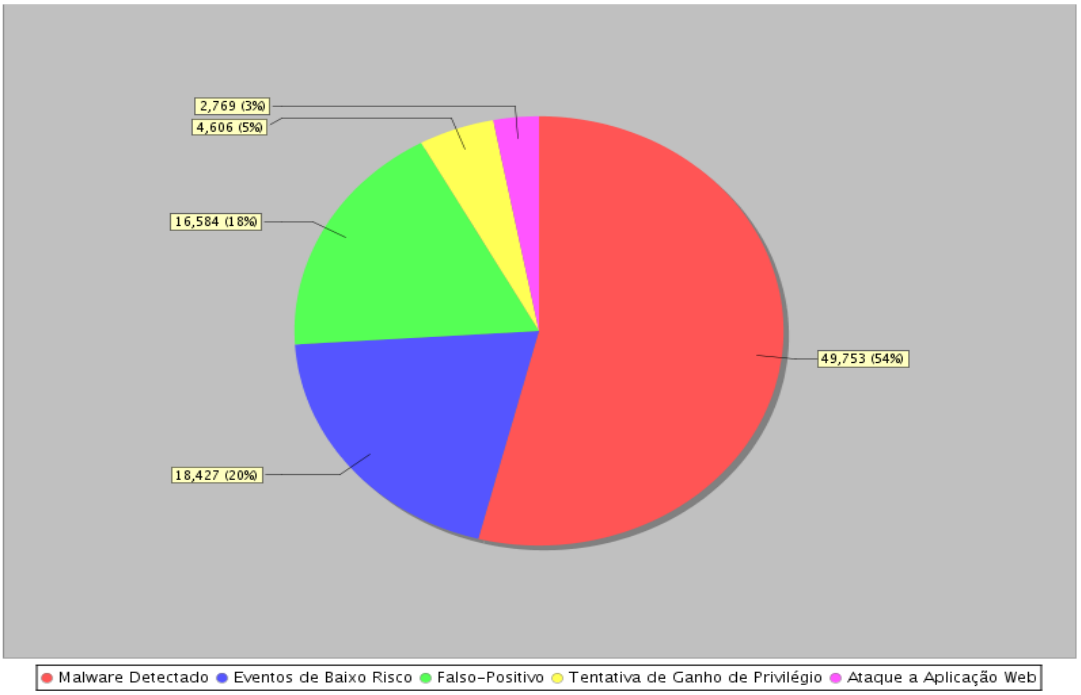
elaborar uma POSIC que refletisse melhor a realidade da organização e suas finalidades, tendo como base o que prescrevia na ABNT NBR 27001:2013 e os manuais de Boas Práticas existentes para a APF.

Este grupo de trabalho, formalmente designado, completou o trabalho no prazo de 60 (sessenta) dias, assim a partir da conclusão do trabalho e sua publicação oficial, a organização pôde contar com uma POSIC atual e formalizada.

Após o estabelecimento da POSIC deu-se também o segundo passo importante: o estabelecimento de uma Seção de Segurança, composta por servidores tecnicamente capacitados em Segurança da Informação, contando com modernos equipamentos e softwares específicos, tais como: *Firewalls* de Aplicação, Sistemas de Prevenção de Intrusões (IPS), *Security Information and Event Management* (SIEM), entre outros.

Com o estabelecimento desta Seção, a organização passa a contar com uma equipe responsável e voltada exclusivamente para ações da segurança da informação interna da organização e por extensão atuando como suporte ás Unidades Apoiadas. Um dos primeiros trabalhos apresentados por essa Seção foi em relação às vulnerabilidades a que Alfa estava exposta, conforme verificado no relatório de incidentes apresentados no final do ano de 2014, conforme Gráfico 3. A organização apresentava altos índices de incidentes de rede, provocados por pragas virtuais, como: vírus, spywares, worms e outros malwares. Os usuários também tinham sua parcela de responsabilidade nos problemas detectados, uma vez que continuavam negligenciando aspectos básicos de segurança da informação e aproveitando-se de deficiências na configuração dos dispositivos de segurança de rede, compartilhando arquivos entre máquinas via *pen drives* e execução de *downloads* para fins particulares (filmes e jogos).

Gráfico 3 – Relatório de incidentes de rede da organização Alfa



Fonte – Produzido pelo autor do trabalho com os dados coletados na organização Alfa, 2016.

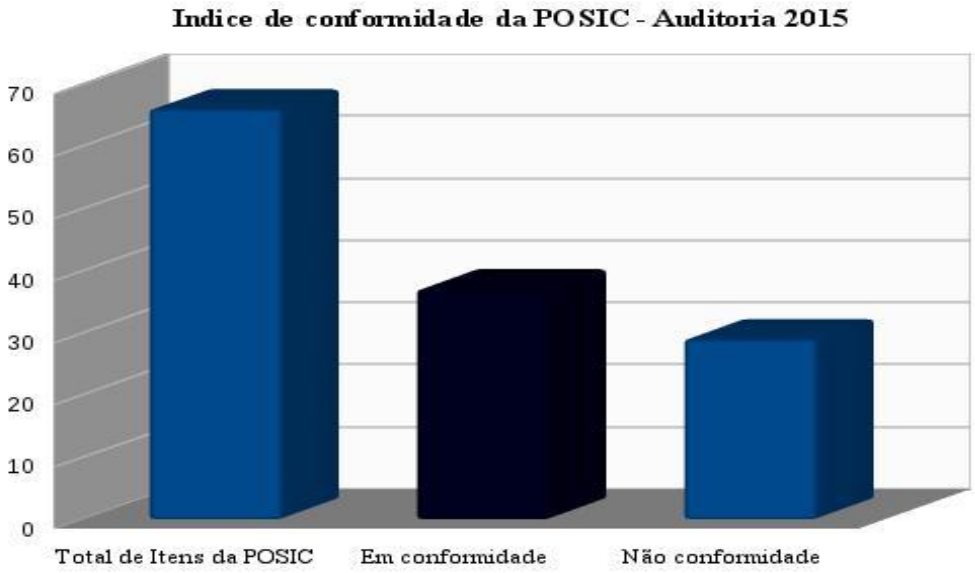
2.2.1 Auditoria de conformidade da POSIC

Assim, após o estabelecimento da POSIC foi necessária a execução da auditoria de verificação de conformidade da POSIC. Os resultados apurados nessa primeira auditoria apontaram um alto índice de não conformidade, o que não refletiam a qualidade esperada para o perfil da organização.

Diante desse diagnóstico, somado ao elevado índice de incidentes de segurança, decidiu-se realizar um estudo para a mudança de paradigma na organização, pois era urgente a necessidade de obter níveis aceitáveis de segurança da informação, fato imprescindível para tornar-se à referência para suas Unidades Apoiadas nos assuntos de SIC.

A auditoria foi realizada com uma lista de verificação com 66 itens, assim sendo, dentre os itens, a organização atingiu a conformidade em 37 itens, atingindo um percentual de 56,06% de conformidade e efetividade com a POSIC. Conforme demonstrado (Gráfico 3):

Gráfico 3 – Indicadores de conformidade da POSIC



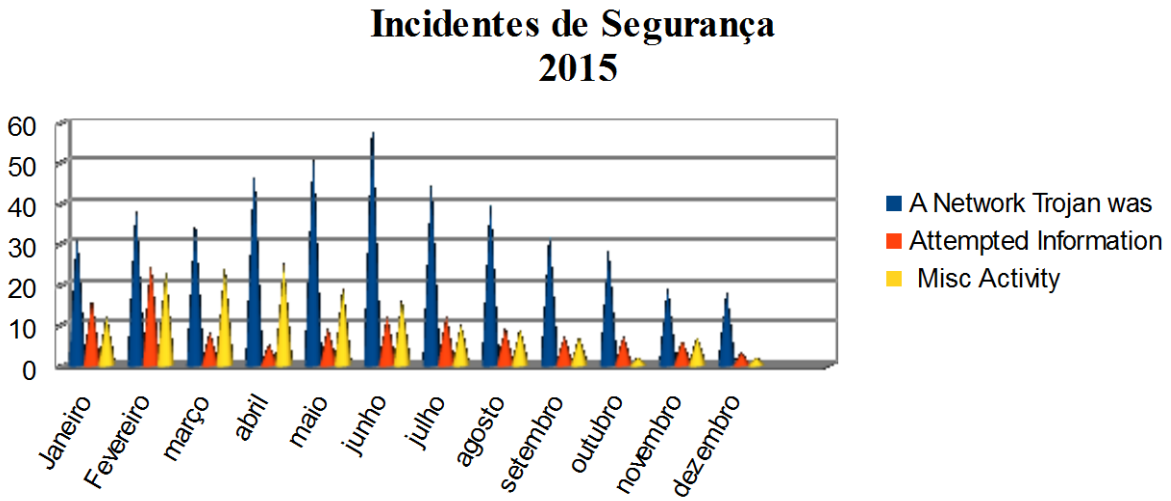
Fonte – O Autor, 2016

O resultado da primeira auditoria de verificação de conformidade da POSIC na organização não revelou dados animadores, porém, evidenciou as questões mais críticas e demonstrou áreas que necessitavam de atuação imediata. Uma das mais importantes evidências foi o desconhecimento da POSIC por grande parcela de usuários, apontado pelos auditores como um fator de destaque negativo, pois alguns itens descumpridos demonstravam a falta de comprometimento dos usuários.

Colaborando com o esforço na melhoria da segurança da informação e permitindo uma melhor avaliação técnica do impacto da implantação da POSIC na Organização. A Seção de Segurança realizou medições mais detalhadas quanto à

ocorrência de incidentes no período da execução da auditoria, empregando relatórios gerados pelo IPS. No gráfico 4 observa-se os seguintes resultados. Foram observadas ocorrências de atividades de malwares nas estações de trabalho, marcados na cor azul (a netework was detected). Tentativas de ganho de privilégio, acesso a funcionalidades restritas, na cor vermelha (attempted information). Eventos de baixo risco, falso positivo e tráfego anômalo, na cor amarela (misc activity).

Gráfico 4 - Relatório de Incidentes de Segurança – Seção de Segurança/ ALFA



Fonte – Produzido pelo autor do trabalho com os dados coletados na organização Alfa, 2016.

Assim a organização Alfa estava diante de um problema no qual apesar de possuir uma POSIC conhecida e obedecida por parte de seus usuários, ainda apresentava problemas de segurança de TIC, conforme verificado nos relatórios de incidentes de rede apresentados. No Anexo A do presente trabalho encontra-se a POSIC da organização Alfa.

2.2.2 Pesquisa de perfil do usuário

Com base nos resultados apurados, a alta administração decidiu realizar uma pesquisa com os seus servidores, com a finalidade de levantar o perfil dos usuários e os itens de não aderência a POSIC. Tal ação possibilitou mapear os pontos críticos de segurança e as áreas de atuação para que a POSIC apresentasse a os resultados esperados e ocorresse uma melhoria nos resultados nos indicadores de incidentes de rede na Organização.

A pesquisa realizada com os servidores contou com um questionário simples que permiti resposta direta por parte dos usuários, segue abaixo, as perguntas que fizeram parte do questionário da pesquisa, as quais obtiveram os maiores indicadores de descumprimento da POSIC, são elas:

◦ Os controles sobre as impressoras de forma a evitar que documentos sejam deixados em impressoras, estão sendo cumpridos?

◦ Todos na Organização assinaram o Termo de Compromisso e Manutenção de Sigilo?

◦ Os controles sobre documentos inservíveis, obrigando sua destruição, previsto na POSIC, estão sendo cumpridos?

◦ Os controles sobre a organização de mesas, evitando que documentos fiquem expostos (política de mesa limpa), estão sendo cumpridos?

◦ A proibição de compartilhamento de *login*/senhas, prevista na POSIC, está sendo cumprida?

◦ As normas estabelecidas na POSIC para utilização de dispositivos de armazenamento removíveis estão sendo cumpridas?

◦ As normas para utilização de *notebooks* institucionais, estabelecidas na POISC, estão sendo cumpridas?

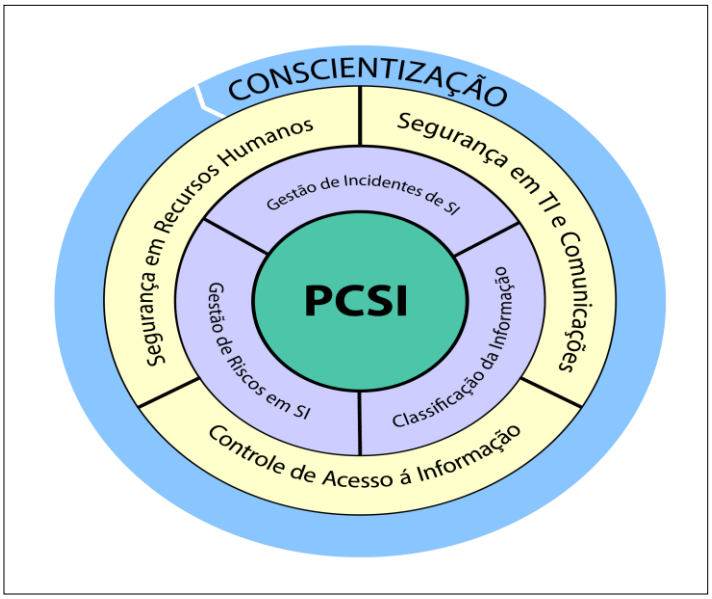
◦ A instalação de aplicativos nos computadores da rede local é controlada de forma a impedir que sejam instalados aplicativos desnecessários ou

contraproducentes?

◦ Prestadores de serviços terceirizados assinam Termo de Compromisso e Manutenção de Sigilo?

Depois de evidenciado os baixos índices de conformidade, a organização procurou ações para a melhoria do cenário. Uma das ações foi implementar técnicas de *Endomarketing* focando o usuário e ações que fortalecesse o comprometimento destes.

Figura 8 – Política Corporativa de Segurança da Informação (PCSI)



Fonte: TCU http://portal.tcu.gov.br (2016)

Foi designado formalmente o Comitê Interno de Segurança da Informação e Comunicações (CI-SIC), este grupo ficou responsável pela implantação da POSIC e sua fiscalização, formado por servidores de perfil multidisciplinar e abrangendo todas as divisões/seções da organização.

A direção da organização entendeu que a POSIC era um dos instrumentos mais importantes para que uma instituição pudesse atingir níveis

mínimos de maturidade no gerenciamento de seus próprios recursos de TI. Sem esta ferramenta, que passou obrigatoriamente pela nomeação de um Comitê Interno de Segurança da Informação e Comunicações e definição formal de responsabilidades no cumprimento de regras fundamentais, entendeu-se que qualquer trabalho de reestruturação do ambiente que porventura fosse executado ficaria desamparado pelas próprias diretrizes da organização. A POSIC deveria agir como uma garantia da continuidade de boas práticas a serem permanentemente adotadas.

Assim, foi nomeado como presidente do comitê o vice-chefe da organização, possibilitando que o comitê tivesse em posição de cobrar o cumprimento das regras previstas dentro da organização, sendo este a representação da chefia da organização na aplicação das normas da POSIC.

Um importante papel foi o compromisso dos integrantes do comitê nas observações e orientações diárias dentro de suas respectivas seções e divisões. Assim, ao presenciar qualquer irregularidade com a POSIC, esses passaram a atuar de forma educativa buscando sempre a conscientização e o comprometimento dos usuários.

A POSIC formalmente assinada foi amplamente divulgada na organização através da distribuição de uma cópia impressa entregue a cada chefe de seção ou divisão mediante recibo. Foi disponibilizado através da intranet um *link* para *downloads* e acesso a POSIC, facilitando aos usuários o acesso ao documento.

2.3 Solução tecnológica de segurança – Seção de TI Padrão

Uma outra ação que foi desenvolvida paralelamente as da implantação da POSIC, foi à execução de um projeto de solução tecnológica de segurança desenvolvido pela própria Seção de Segurança da Organização, que se baseava na customização do sistema operacional já utilizado no parque computacional da organização e dos servidores da rede de dados, ajustando-os as regras definidas na POSIC. O projeto chamado de Seção de TI Padrão foi apresentado com cronograma de execução de 180 (cento e oitenta) dias para implantação total da customização baseada na POSIC, sendo executado e finalizado ao final do ano de 2015.

Antes de ser adotado como solução, o projeto passou por um período de maturação, o sistema operacional customizado foi testado por usuários comuns que auxiliaram no processo de levantamento de requisitos. O sistema então passou por diversas rodadas de modificação, o que o aperfeiçoou cada vez mais até resolver diversos problemas de incompatibilidade com sistemas legados usados na Organização, como impressoras e acesso a *sites* específicos.

O Projeto Seção de TI Padrão foi conduzido por uma equipe multidisciplinar de técnicos, com especialização na área de Defesa Cibernética e Segurança da Informação, com o objetivo principal de oferecer um conjunto completo de soluções a problemas recorrentes de TI, corrigindo-os e ajustando-os aos serviços da POSIC. Tal ação visou a correção das falhas existentes que produziam incidentes de segurança registrados no período, a partir de varredura dos sensores na rede interna e já apresentados anteriormente no Gráfico 4.

A adequação do parque computacional e da rede interna necessitou de intervenção técnica para as configurações necessárias aos requisitos da customização baseada no Debian 8.1, no Samba 4, no OCS *Inventory* (recursos baseados em softwares livres) e no treinamento dos recursos humanos.

Sobre Debian, é um o sistema operacional de distribuição livre que reúne um conjunto de programas básicos e utilitários que funcionam por meio de um programa principal chamado Kernel, que executa todas as operações necessárias ao funcionamento do outros programas. O Linux/GNU é uma peça de software criada inicialmente por Linus Torvalds (programador finlandês criador do Linux em 1991) com a ajuda de milhares de programadores espalhados por todo o mundo. O FreeBSD é um sistema operacional de código aberto, incluído no Kernel e em outros softwares. O Debian vem com mais de 43000 pacotes (softwares pré-compilados e empacotados em um formato amigável, o que faz com que sejam de fácil instalação em sua máquina), um gerenciador de pacotes (APT) e outros utilitários que torna possível gerenciar milhares de pacotes em milhares de computadores de maneira tão fácil quanto instalar um único aplicativo.

A solução de segurança tecnológica implementada na organização Alfa teve como base a customização do Sistema Operacional Debian versão 8.1, do servidor de arquivos Samba 4 e do *One Computer and Software Inventory* (OCS *Inventory*).

Inicialmente, como parte do trabalho de implantação foi feita a migração dos sistemas operacionais instalados nas estações de trabalho dos usuários, que em alguns casos eram sistemas operacionais Windows, para o Sistema Operacional Debian 8. Essa primeira ação, por si só, já constitui um passo importante para a solução de um dos problemas mais graves e comuns, o uso disseminado de *software* proprietário não-licenciados, o popular “programa pirata”, que contrariam as normas legais de utilização de softwares, constituindo crime previsto na Lei Nº 9.609, de 19 de fevereiro de 1998 (Lei de Software). O uso desses softwares modificados oferecia riscos sérios aos seus usuários, pois eram vetores passíveis de

serem explorados por criminosos digitais para a propagação de outras aplicações maliciosas. No parque computacional, algumas das estações de trabalho já utilizavam o Sistema Operacional Linux/GNU, mas ainda havia um número expressivo de máquinas com SO Windows XP, Vista e 7, sobretudo esses sistemas operacionais encontravam-se instalados em estações de trabalho relacionadas a atividades de risco como: controle de acessos, sistema de pagamento e terminais com softwares de projetos de engenharia.

Quanto a customização do sistema operacional Debian 8, destaca-se que é um sistema operacional de distribuição livre, que reúne programas básicos e utilitários necessários ao funcionamento dos computadores, sendo o Kernel o principal programa relacionado às operações básicas.

No caso da organização Alfa foi utilizado o Sistema Operacional Debian versão 8.1, que recebeu papel de parede e tela de bloqueio institucional (Figura 9), com a finalidade de lembrar ao usuário a quem pertence o terminal no qual se está trabalhando. Bloqueio por senha ao acesso ao terminal e ao “apt-get”, com a finalidade de impedir a instalação por parte do usuário de qualquer tipo de software ou hardware, em seus terminais de trabalho.

Figura 9 - Logotipo da organização da proteção de tela

Fonte: Seção de Segurança – Alfa

Nos terminais de todos os usuários foram instalados pacotes de softwares básicos necessários ao trabalho diário normal. Para os casos especiais em que houve a necessidade de instalação de determinados softwares, como por exemplo, os de execução de projetos com aplicativos Lumini e Autocad, esses foram instalados pelos técnicos que também são responsáveis pela manutenção e atualização dos softwares.

Todos os programas instalados são baseados em software livre e possuem repositório padrão do próprio Debian, com qualidade garantida e sincronismo com os “espelhos” disponíveis na internet.

A instalação automática das atualizações para o sistema foi configurada para ser executada diariamente entre as 12:00 h e 13:00 h, no horário do almoço, fato que não atrapalha o trabalho do usuário e garante a atualização e proteção contra ataques cibernéticos. Os espelhos são capazes de atualizarem os sistemas operacionais instalados em máquinas de 32 e 64 bits, máquinas antigas e novas respectivamente.

Na implantação da Seção de TI Padrão utilizou-se das funcionalidades do aplicativo OCS *Inventory*, que é um software livre que permite ao usuário inventariar (listar) os ativos de TI na rede, monitorando os softwares e hardwares das máquinas em funcionamento na rede. A sua aplicação na Organização Alfa contribuiu para que os usuários cumprissem as restrições previstas na POSIC, quanto à instalação de periféricos, softwares e sistemas operacionais não autorizados. Além disso, pôde-se monitorar o endereço IP, as configurações da CPU, memória e espaço em disco.

O Samba 4 constituiu uma parte importante da solução tecnológica empregada na organização Alfa, pois executa as seguintes tarefas: utiliza a configuração do controlador de domínio, funciona como servidor de arquivos, possibilita o uso da base autenticação *Lightweight Directory Access Protocol* (LDAP) para executar a autenticação dos usuários, utiliza o kerberos como responsável por gerenciar os usuários da rede e fazendo com que sejam utilizadas senhas fortes. Além dessas, contribuiu para a solução de um grande problema para a segurança, eliminando completamente do uso de “pen drives”, que constituem a maior fonte de contaminação da rede por vírus trazidos pelos usuários de suas máquinas particulares, já que as entradas de dados por meio dos terminais são totalmente configuráveis. Outra função habilitada na rede de dados foi à criação de acesso seguro de comunicação entre usuários e o serviço, por meio da configuração de privilégios aos usuários, permitindo que esses possam acessar a rede em qualquer máquina da organização, bastando a utilização de seu login e senha, contribuindo assim para a prevenção de crimes cibernéticos, uma vez que os logs de acessos permanecem gravados no servidor da rede.

Ao fim do processo de implementação técnica, foi realizada uma auditoria por uma equipe da Organização para a validação do projeto executado. Essa auditoria avaliou não só apenas se os aspectos técnicos que foram implantados com sucesso, mas também se o público interno da organização havia aderido às práticas previstas na POSIC. Outra avaliação feita foi se a Seção de Informática, após os trabalhos realizados em parceria com a Seção de Segurança, reunia as condições necessárias para manter o gerenciamento efetivo dos ativos sob sua responsabilidade.

2.4 Capacitação e conscientização dos Recursos Humanos

O processo de capacitação e conscientização dos funcionários da Organização Alfa, para que fossem capazes de fazer com que as ações de segurança apresentassem a eficácia esperada e que os níveis de aderência a POSIC melhorassem, constituiu o mais importante e demorado processo, já que foram realizadas campanhas internas, que consistiam na leitura semanal de trechos da POSIC, aproveitando os ajuntamentos e outras reuniões que ocorreram no auditório da organização. Assim foram ministradas aulas de segurança, nas quais os funcionários foram capacitados e incentivados a criarem e memorizarem senhas fortes e complexas para seus acessos aos serviços da rede da organização, acabando com os “Admin 123”, login e senha que eram comumente utilizados na Organização.

Foi feita uma ampla divulgação por todos os meios de instruções com conteúdo da POSIC, utilizando-se da técnica de *Endomarketing* para a conscientização dos usuários. Essas ações foram introduzidas como Boas Práticas e conduzidas pela Seção de Segurança**.**

Outras ações de envolvimento e motivação dos recursos humanos da Organização para a aderência as normas de segurança, como as abaixo listadas, foram executadas:

a Capacitação

Algumas capacitações e treinamentos foram realizados por servidores para atuar como disseminadores de Boas Práticas na organização, tais como a certificação em Auditor Líder em Segurança da Informação baseados na NBR ISO

27001/2013, a participação de integrantes da organização em eventos, *Workshops,* palestras e encontros relativos a Segurança da Informação. A equipe da Seção de Segurança participou de diversos cursos de interesse da área, nesse período.

b Palestras aos usuários

A Seção de Segurança conduziu com certa periodicidade palestras sobre a POSIC em seu programa de instrução da organização, o qual divulgou procedimentos básicos de Segurança da Informação, possibilitando ampla divulgação das normas em vigor.

A organização também realizou um evento chamado “Encontro de Chefes de Seção de TI”, voltado aos multiplicadores internos e das Unidades Apoiadas. O evento obteve grande adesão e demonstrou ser uma Boa Prática na divulgação de ações em prol da Segurança da Informação.

c Ações na Intranet

Uma ferramenta utilizada foi à inserção de *Pop Up* com artigos da POSIC e informações sobre SIC na tela de acesso a Intranet da rede, para cada primeiro acesso na intranet era disponibilizado uma tela com mensagens, só avançando na navegação após o fechamento da mesma, ou seja, aumentando a chances de leitura pelo usuário, uma forma diferente e que mostrou ser eficiente, tanto que essa técnica se encontra em uso atualmente. A Figura 10 traz um exemplo desses *Pop Up*

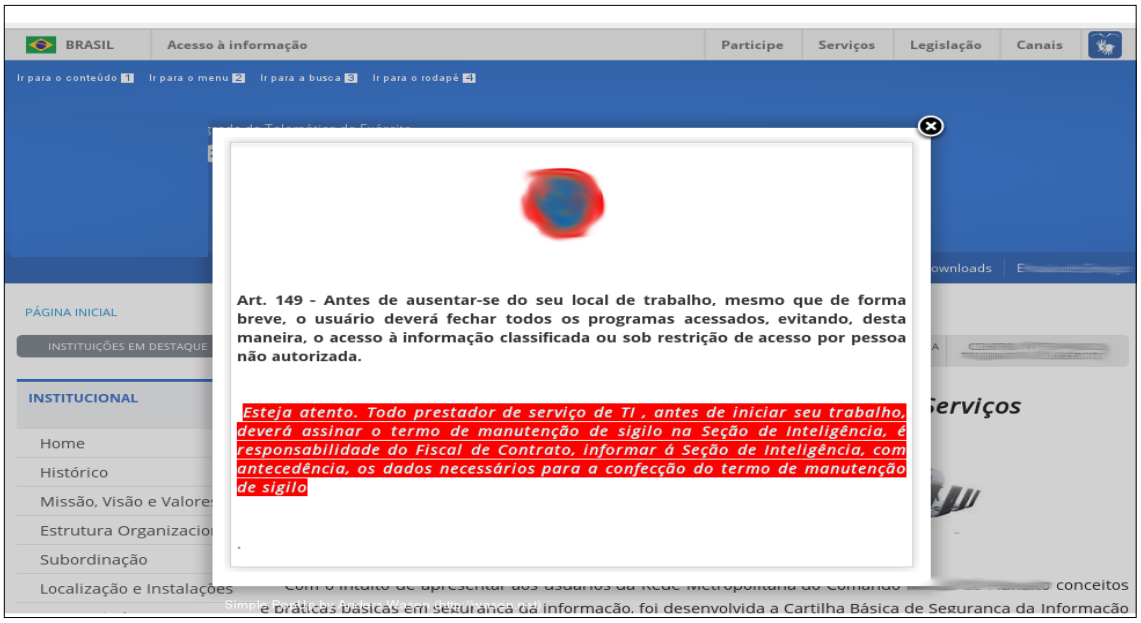


Figura 10 - *Pop Up* de 1º Acesso - disponível na Intranet da Organização

Fonte - adaptada pelo autor – Intranet da Organização Alfa

d Conscientização via e-mail

Há que se destacar o trabalho da Seção de Segurança, que através do e-mail corporativo divulgou assuntos relacionados à Segurança da Informação. Estes e-mails enviados a todos os usuários da rede interna, quase que diariamente, se mostraram uma boa técnica de e*ndomarketing*, despertando o interesse por leituras com alertas e dicas de SIC, sempre com abordagem cativantes e ressaltando a

importância da atitude dos usuários neste contexto. As matérias divulgadas foram retiradas de sites e periódicos especializados em TI e SIC, como o CERT.br.

e Assinatura de termo de compromisso de sigilo das informações

A assinatura do Termo de Compromisso de Sigilo das Informações foi uma importante ação para melhorar o comprometimento dos usuários com a POSIC. O ato formal de assinatura de um documento é uma prática empregada há séculos pela humanidade, assim, os usuários não podem alegar desconhecimento de suas responsabilidades.

Foram conduzidas ações para que todos os usuários e colaboradores terceirizados assinassem o termo de compromisso de sigilo das informações, assim, essa ação reduziu os casos de descumprimentos desse importante item da POSIC.

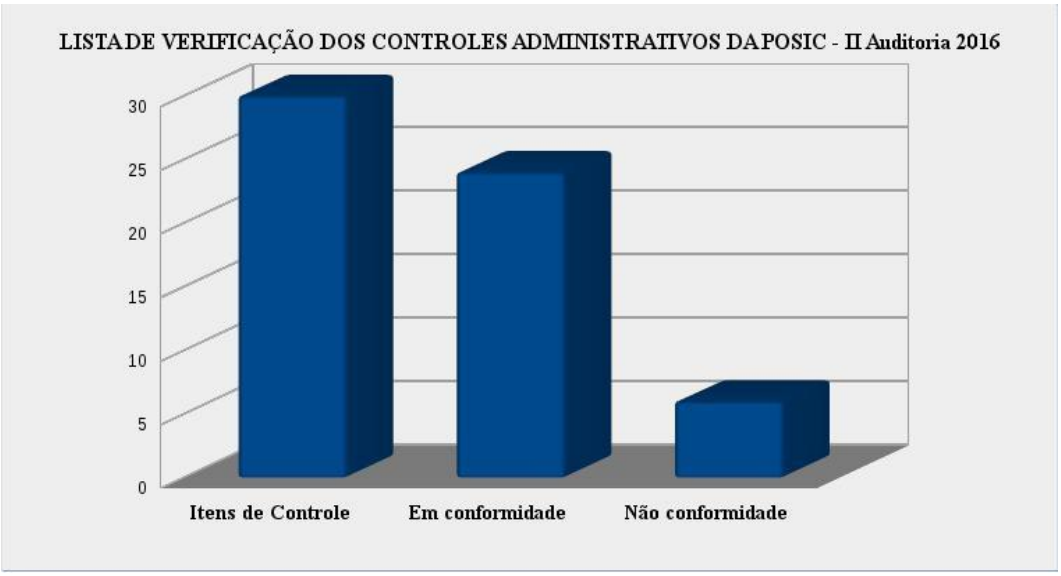
2.5 A evolução dos resultados na Organização

Após a implantação da Seção de TI Padrão, seguida pela capacitação e conscientização dos usuários quanto ao cumprimento das normas estabelecidas na POSIC, cuja divulgação do conteúdo foi amplamente difundida e fiscalizada pelo Comitê Interno de Segurança da Informação e Comunicações. Esse por sua vez, precisou aplicar punições em alguns casos, para que o equilíbrio desejado fosse atingido na organização, visando a melhoria dos indicadores de desempenho da segurança da informação.

Nesse período, foi realizada nova auditoria interna, que utilizou a mesma metodologia de listas de verificações de itens, de controles e verificações *in loco* do ambiente de TI, avaliando o nível de aderência a POSIC, o correto uso dos terminais

pelos usuários em relação à solução tecnológica de segurança, verificando o envolvimento dos usuários e a efetiva implementação dos controles propostos na POSIC. Observou-se uma importante melhora nos níveis de conformidade, como demonstrado no Gráfico 5.

Gráfico 5 – Indicadores de conformidade da POSIC



Fonte – O Autor, 2016.

2.6 Funcionamento como solução de segurança em TIC

Com a implementação das ações, a organização passou a funcionar com a preocupação de todos com a segurança em TIC. Dentre os vários benefícios gerados a partir da implantação da Seção de TI Padrão destacam-se as seguintes:

a Todo o parque computacional funcionando com software livre padronizado e atualizado automaticamente por meio de repositório mantido e definido pela Seção de Informática. O pacote de programas disponibilizado também

foi de software livre, como visualizador de arquivos PDF, editor de texto, editor de imagem etc. Com atualização constante e manutenção periódica, houve uma redução nas para manutenção dos terminais e uma redução no nível de indisponibilidade de computadores na organização.

Ainda sobre software livre, a eliminação do uso do SO Windows constituiu uma vantagem técnica, já que o Windows constitui alvo principal de pragas virtuais, proporcionando mais segurança para os usuários e administrador da rede. O Windows também necessita de atualizações periódicas que requerem cada vez mais espaço em disco e processamento. Tal característica exige que a organização faça a renovação periódica do parque computacional. Além de utilizar pacote de programas para tarefas como edição de texto e imagem proprietários, de custo elevado de manutenção e aquisição.

b Melhoria na segurança de acesso a rede interna com a utilização por parte do usuário de senha única de acesso aos computadores, internet, sistemas corporativos e servidor de arquivos. Tal configuração facilita a rotina de trabalho dos usuários, uma vez que não precisa possuir várias senhas.

Para esse mecanismo de autenticação, implementou-se a comunicação entre o cliente e servidores criptografada, proporcionando maior segurança na rede, uma vez que as senhas não trafegam em claro, evitando possível interceptação por terceiros.

As telas de bloqueio automático dos terminais foram configurados para o bloqueio no tempo de 5 (cinco) minutos de inatividade, exigindo senha pessoal de desbloqueio. Todas as configurações foram definidas via terminal pela Seção de Informática, sendo senhas de acesso ao root (superusuários) controladas e trocadas periodicamente pela referida Seção.

c A possibilidade de manutenção e instalação de software remotamente por meio do OCS Inventary, com processo transparente ao usuário. Tal facilidade reduziu o tempo de alocação de pessoal (homem-hora) na atividade de manutenção dos terminais. Além de executar o controle de inventário eletrônico da rede aumentou o nível de segurança orgânica, uma vez que se tornou possível detectar imediatamente, a retirada não autorizada de qualquer ativo de rede ou periférico orgânico da rede.

d Foram definidas ilhas de impressão para funcionamento em rede, facilitando o controle da documentação impressa e das copiadas escaneadas em cada equipamento, o trafego de dados e a manutenção e fornecimento de suprimentos.

e Quanto a espaço para arquivo, foram definidos servidores de arquivos dedicados, liberando espaço em disco nos terminais de trabalho e criando um serviço de arquivo institucional para informações de conteúdo corporativo e segurança dos arquivos. Com isso, os usuários não mais necessitam de serviços como Google drive, Dropbox ou mesmo de qualquer tipo de mídia removível. Pode-se também gerenciar os tipos de arquivos que podem ser guardados ou aqueles que transitam na rede local, possibilitando a execução com facilidade de back ups automáticos para cada terminal.

f Com o controle do *Dynamic Host Configuration Protocol* (Protocolo de configuração dinâmica de host) – DHCP o sistema controla automaticamente o acesso de computadores estranhos à rede de dados não distribuindo IP/visitante, e alarmando a ocorrência desse tipo de incidente aos responsáveis da Seção de Informática, negando acesso à rede conforme proibição da POSIC.

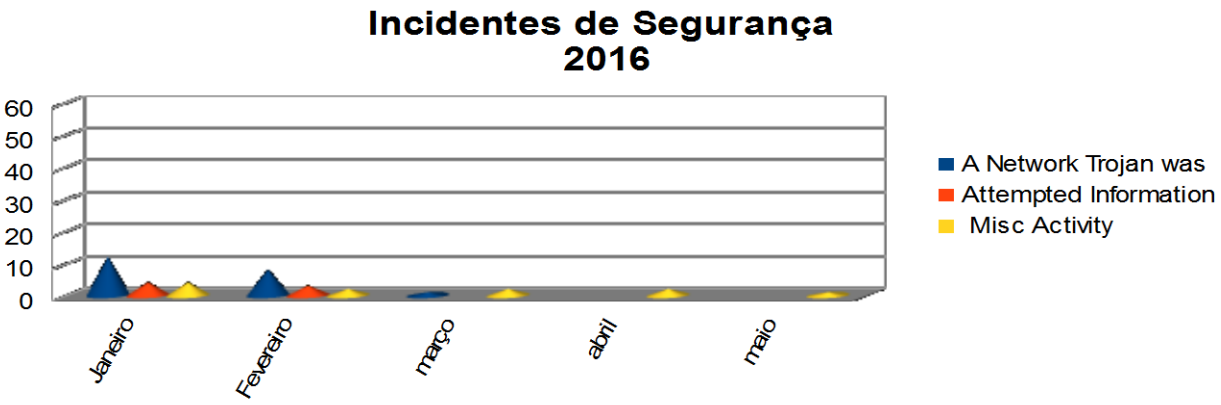
g A solução adotada apresentou elevado nível de eficiência, qualidade e segurança, quando comparado aos sistemas semelhantes disponíveis no mercado, conforme os apresentados no capítulo 1 (Serviços de Domínio de Diretório Ativo (ADDS), Redhat Satellite e Redhat Spacewalk). Essas soluções diferenciam-se do aplicado em Alfa, por constituem softwares proprietários de custo elevado para aquisição e manutenção e necessitam de renovações contratuais periódicas para suporte técnico.

h Outro aspecto importante a ser considerado sobre a solução empregada foi quanto à utilização de softwares antivírus. Como não há necessidade de utilização de antivírus para o SO Debian, houve uma grande economia de recursos financeiros, uma vez que não mais houve necessidade de aquisição de licenças anualmente e nem de renovações de suporte. Mas mesmo para aqueles terminais que por necessidade técnica continuaram utilizando o SO Windows, utilizou-se como antivírus um software livre, o Av Ware Defesa BR.

i Com a rede livre de problemas houve um aumento expressivo na velocidade de acesso disponibilizada aos usuários, melhorando assim o desempenho dos diversos programas que dependiam de boa velocidade de acesso à internet.

Assim os resultados apurados alcançados com a implantação da solução tecnológica foram muito favoráveis, atingindo e até mesmo superando os resultados esperados por parte do comando, conforme verificado no gráfico 6, da Seção de Segurança e obtido por meio de varreduras, feita por sensores de segurança corretamente ajustados e configurados, executadas para o Relatório de Incidentes de Segurança.

Gráfico 6 - Relatório de Incidentes de Segurança – Seção de Segurança/ ALFA



Fonte – Produzido pelo autor do trabalho com os dados coletados na organização Alfa, 2016.

Conforme apresentado no gráfico de incidentes de segurança anterior a seguir o significado da legenda do gráfico 6, com ocorrências de atividades de malwares nas estações de trabalho, marcados na cor azul (a netework was detected). Tentativas de ganho de privilégio, acesso a funcionalidades restritas, na cor vermelha (attempted information). Eventos de baixo risco, falso positivo e tráfego anômalo, na cor amarela (misc activity).

Com o sucesso alcança com o modelo implantado em Alfa, o comando decidiu compartilhar com suas unidades apoiadas a documentação referente à Seção de TI Padrão, com objetivo de melhorar as condições do serviço para os clientes dos serviços de TI da organização.

Como incentivo à adoção da solução de segurança em TI de Alfa, foi criado um programa de recompensa para aquelas unidades apoiadas que implementarem a referida solução. Todas a documentação e consultoria técnica necessária foram disponibilizadas visando à replicação do trabalho no nível cliente local.

CONCLUSÃO

No presente estudo, tratou-se dos processos envolvidos na segurança da informação nas organizações. Buscou-se compreender como se deu a interação entre recursos humanos, solução tecnológica de segurança e a Política de Segurança da Informação e Comunicações. Tal interação permite que se estabeleça um equilíbrio entre esses três fatores, necessário a segurança da informação. No estudo de caso da organização Alfa, em que foram apresentadas as fases de implantação de um modelo de segurança da informação, com as interações necessárias entre os fatores envolvidos e os respectivos resultados apurados a partir de indicadores gráficos, conforme abaixo será detalhado.

Na interação entre os recursos humanos e a POSIC, pode-se verificar que inicialmente houve alguma dificuldade de implantação. Tal fato foi verificado na primeira auditoria de conformidade em que ocorreu baixa aderência à POSIC. Com as ações de conscientização com aplicação do endomarketing, treinamentos e palestras, ocorrendo com isso, maior envolvimento dos funcionários no cumprimento da política de segurança. Assim, pode-se comprovar o sucesso da interação a partir dos resultados apurados no gráfico da segunda auditoria de conformidade da POSIC, no qual foi atingido elevado nível de aderência.

Quanto à interação entre os recursos humanos e a solução tecnológica de segurança, inicialmente não apresentou maiores dificuldades de ser executada, já os usuários já tinham conhecimento das restrições de segurança contidas na POSIC. Da mesma maneira com que foi tratada a interação com a POSIC, os funcionários foram capacitados para a correta utilização do produto chamado Seção de TI Padrão, a solução tecnológica de segurança. Destaca-se a necessidade de ações

de fiscalização mais efetivas. A comprovação da interação entre os fatores recursos humanos e solução tecnológica de segurança, pode ser verificada no relatório Gráfico 6, com a redução dos incidentes de segurança apurados.

Dentre as interações demonstradas no estudo de caso apresentado, a interação ocorrida entre a solução de segurança tecnológica e a POSIC apresentou menor complexidade quanto a sua execução. Tal fato ocorreu, pois no caso a Seção de TI Padrão foi dimensionada a partir da POSIC, possibilitando total interação entre os dois fatores. Porém ao contrário das interações anteriores, essa se pode verificar a partir da configuração e características de cada uma das partes componente da solução tecnológica de segurança, em que as suas funcionalidades visaram atender aos requisitos da POSIC.

Analisando as informações do gráfico 6 (Incidentes de Segurança 2016), é possível verificar que no modelo de segurança da informação da organização Alfa, apresentado no estudo de caso, o equilíbrio entre os recursos humanos, a solução tecnológica de segurança e a Política de Segurança da Informação e Comunicações, foi atingido com sucesso, produzindo um expressiva redução da vulnerabilidade de TI na Organização.

Por fim, conclui-se que o equilíbrio obtido a partir da interação entre os fatores envolvidos na Segurança da Informação e Comunicações, constitui fator de sucesso para o atendimento dos níveis de segurança de TI requeridos para as organizações.

Dando continuidade a este trabalho, fica a proposta para trabalhos futuros, o estudo da aplicação, como modelo de segurança de baixo custo, em organizações da administração pública ou privada.

REFERÊNCIAS

ALEXANDRIA, J. C. S. de. **Gestão de Segurança da Informação –** Uma Proposta para Potencializar a Efetividade da Segurança da Informação em Ambiente de Pesquisa Científica**.** Tese de Doutorado, Universidade de São Paulo, São Paulo. 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, NBR 27001: **Sistemas de gestão de segurança da informação**. Rio de Janeiro. 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, NBR 27002: **Código de Prática para a Gestão da Segurança da Informação**. 2013.

BEAL, A. **Segurança da Informação: Princípio e Melhores Práticas para a proteção dos Ativos de Informação nas Organizações**. 1o edição. São Paulo: Atlas, 2005.

BRANDÃO, H. P.; GUIMARÃES, Tomás de Aquino. **Gestão de competências e gestão de desempenho:** tecnologias distintas ou instrumentos de um mesmo construto? RAE – Revista de Administração de Empresas, São Paulo, v.41, n.1,p.8-15, jan./mar. 2001.

Brasil. Tribunal de Contas da União. Diretoria de Auditoria da Tecnologia da Informação do Tribunal de Contas da União. **Boas Práticas em Segurança da Informação**, Brasília, 2007.

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

Brasil. Tribunal de Contas da União. **Política Corporativa de Segurança da Informação (PCSI**). Fonte: http://portal.tcu.gov.br/comunidades/seguranca-da-informacao/home/home.htm. Acesso em 21 junho de 2016.

Brasil. PRESIDÊNCIA DA REPÚBLICA. **Guia de Orientações ao Gestor em Segurança da Informação e Comunicações.** Gabinete de Segurança Institucional. Versão 01 –Fev/2014, Brasília, 2014.

Brasil. **Norma Complementar 02/IN01/DSIC/GSIPR**, de 13 de outubro de 2008 - Disciplina a metodologia gestão de segurança da informação e comunicações na administração pública federal, direta e indireta, e dá outras providências. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_2_metodologia.pdf>. Acesso em: 10 julho 2016.

Brasil. Presidência da República. **Instrução Normativa GSI Nº 01**, de 13 de junho de 2008 - Disciplina a gestão de segurança da informação e comunicações na administração pública federal, direta e indireta, e dá outras providências. Disponível em: < http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf>. Acesso em: 3 julho 2016.

CAMPOS, A. L. N., **Sistema de Segurança da Informação:** Controlando os Riscos. ed. Florianópolis: Campus, 2006.

COELHO, F. E. S. **Gestão da Segurança da Informação**: NBR 27001 e NBR 27002. Rio de Janeiro, RNP/ESR, 2013.

DAVIS, F. D.; BAGOZZI, R. P.; WARSHAW, P. R. **User acceptance of computer technology:** a comparison of two theoretical models. Management Science, Ann Arbor (MI), v.35, n.8, p.982-1003, 1989.

ELLWANGER, C. **Impacto da Utilização de Técnicas de Endomarketing na Efetividade das usage. Journal of management information systems, v. 13, n. 1, p. 127-143, 1996.**

KAYO, E. K. et al. Ativos intangíveis, ciclo de vida e criação de valor. **Revista de administração contemporânea**, v. 10, n. 3, p. 73-90, 2006.

MARCIANO, J. L. P. **Segurança da Informação – uma abordagem social**. Tese de Doutorado, Universidade de Brasília, Brasília, 2006.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec, 2009.

NOBRE, A. C. S.; RAMOS, A. S. M.; NASCIMENTO, T. C. **Fatores que Influenciam a Aceitação de Práticas Avançadas de Gestão de Segurança da Informação**: um estudo com gestores públicos estaduais no Brasil. In: XXXIV Encontro da ANPAD – EnANPAD. Rio de Janeiro, 2010. Anais... Rio de Janeiro: ANPAD, set.2010.

OLIVEIRA, D. P. R. **Estratégia Empresarial e Vantagem Competitiva:** como estabelecer implementar e avaliar. 3 ed. São Paulo: Atlas, 2001.

Pemble, M. **Transferring business and support functions:** the information security risks of outsourcing and off-shoring. Computer Fraud & Security 12(1), 5-9. 2004. https://repository.asu.edu/attachments/56621/content/Li_asu_0010E_10626.pdf

LI, M. **The Impacts of Bridge Transfer on Service Outsourcing Social Network** Perspective. Tese de Doutorado. Arizona State University. 2011.

SÊMOLA, M. **Gestão da Segurança da Informação**: visão executiva da informação: aplicada ao Security Officer. ed. Rio de Janeiro: Elsevier,2003.

SILVA, D. R. P. and L. M. Stein . **Segurança da Informação:** uma reflexão sobre o componente humano, Ciências & Cognição, 10, pp. 43-56. 2007.

SCOTT, W. R. **Institutional Theory: Contributing to a Theoretical Research Program** in Smith, K., M. A. Hitt (eds.) Great Minds in Management: The Process of Theory Development, Oxford: Oxford University Press, pp. 460-484. 2005.

SANTOS, Vinicius Souza dos, Ed Porto Bezerra, and Bráulio Alturas. **Análise de mecanismos de controle de acesso nas redes sociais**. *Revista Portuguesa e Brasileira de Gestão* 9.3 (2010): 50-60.

Políticas de Segurança da Informação. Santa Maria, UFSM, 2009. Tese de Mestrado

FERNANDES, J. H. C. **Sistema, informação & comunicação.** Universidade de Brasília, Curso de Especialização em Gestão de Segurança da Informação e Comunicações. CEGSIC, Brasília, 2009, Apostila.

FERREIRA, F.N. F. **Segurança da Informação.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2003.

FERRAIOLO, D. F.; KUHN, D. R. e CHANDRAMOULI, R. , **Role-Based Access Control**, 1.ª ed., Artech House, Londres e Boston. 2003.

FONTES, E. L. G. **Segurança da Informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006.

IGBARIA, M.; PARASURAMAN, S.; BAROUDI, J. J. **A motivational model of microcomputer usage**. Journal of management information systems, v. 13, n. 1, p. 127-143, 1996.

KAYO, E. K. et al. Ativos intangíveis, ciclo de vida e criação de valor. **Revista de administração contemporânea**, v. 10, n. 3, p. 73-90, 2006.

MARCIANO, J. L. P. **Segurança da Informação – uma abordagem social**. Tese de Doutorado, Universidade de Brasília, Brasília, 2006.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec, 2009.

NOBRE, A. C. S.; RAMOS, A. S. M.; NASCIMENTO, T. C. **Fatores que Influenciam a Aceitação de Práticas Avançadas de Gestão de Segurança da Informação**: um estudo com gestores públicos estaduais no Brasil. In: XXXIV Encontro da ANPAD – EnANPAD. Rio de Janeiro, 2010. Anais... Rio de Janeiro: ANPAD, set.2010.

OLIVEIRA, D. P. R. **Estratégia Empresarial e Vantagem Competitiva:** como estabelecer implementar e avaliar. 3 ed. São Paulo: Atlas, 2001.

Pemble, M. **Transferring business and support functions:** the information security risks of outsourcing and off-shoring. Computer Fraud & Security 12(1), 5-9. 2004. https://repository.asu.edu/attachments/56621/content/Li_asu_0010E_10626.pdf

LI, M. **The Impacts of Bridge Transfer on Service Outsourcing Social Network** Perspective. Tese de Doutorado. Arizona State University. 2011.

SÊMOLA, M. **Gestão da Segurança da Informação**: visão executiva da informação: aplicada ao Security Officer. ed. Rio de Janeiro: Elsevier,2003.

SILVA, D. R. P. and L. M. Stein . **Segurança da Informação:** uma reflexão sobre o componente humano, Ciências & Cognição, 10, pp. 43-56. 2007.

SCOTT, W. R. **Institutional Theory: Contributing to a Theoretical Research Program** in Smith, K., M. A. Hitt (eds.) Great Minds in Management: The Process of Theory Development, Oxford: Oxford University Press, pp. 460-484. 2005.

SANTOS, Vinicius Souza dos, Ed Porto Bezerra, and Bráulio Alturas. **Análise de mecanismos de controle de acesso nas redes sociais**. *Revista Portuguesa e Brasileira de Gestão* 9.3 (2010): 50-60.

ANEXO A – EXTRATO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (POSIC) / ORGANIZAÇÃO ALFA

MINISTÉRIO DA DEFESA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES/ALFA

1 FINALIDADE

Art. 1º Este documento tem por finalidade implantar Diretrizes de Segurança da Informação e Comunicações a serem adotadas obrigatoriamente pelos integrantes da organização Alfa, de modo a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação armazenada ou em trânsito nos sistemas computacionais.

Art. 2º Constituem propósitos destas Diretrizes:

I – formalizar direitos e responsabilidades de usuários, profissionais de administração de redes e profissionais de segurança da informação;

II – garantir o bom uso dos recursos de Tecnologia da Informação e Comunicações (TIC) de Alfa;

III – atribuir papeis e responsabilidades na elevação dos níveis de segurança da informação no âmbito de Alfa;

IV – disseminar a cultura de segurança da informação.

2. OBJETIVOS

Art. 3º São objetivos desta Política:

I – definir e estabelecer procedimentos relacionados à Segurança da Informação e Comunicações a serem adotados obrigatoriamente por todos integrantes;

II – normatizar, o uso dos recurso de TIC;

III – estabelecer regras para o controle de acesso aos recursos de TIC e à Rede Mundial de Computadores a partir da rede local de Alfa;

IV – atribuir papeis e responsabilidades na utilização, operação e manuseio dos recursos computacionais.

3. CONCEITOS E PRESSUPOSTOS BÁSICOS

Art. 4º Compreende-se como recurso de TIC, para os efeitos desta Política, todo e qualquer dispositivo eletrônico que possibilite a transmissão, o armazenamento e a reprodução de voz e dados em equipamento isolado ou em rede, além do conhecimento técnico do pessoal especializado que viabiliza o fluxo da informação pelos canais de comunicações, mediante o emprego da tecnologia disponível.

Art. 5º Entende-se por dispositivo móvel: qualquer tipo de notebook, tablet, smartphone, telefone celular ou similares a estes.

Art. 6º Os dispositivos de TI incluídos no patrimônio são colocados à disposição dos seus usuários para uso exclusivo em atividades estritamente relacionadas às funções institucionais por eles desempenhadas.

Art. 7º Considera-se como matéria ilícita: a pornografia; o erotismo; qualquer forma de discriminação seja ela étnica, religiosa, ideológica, política ou de orientação sexual; os assuntos contrários à ética, à disciplina, à moral e aos bons costumes, bem como atentatória à ordem pública ou que viole qualquer direito de terceiros conforme definido na Constituição, em leis, em decretos e em regulamentos.

Art. 8º A fim de facilitar a compreensão deste documento e elucidar conceitos, as seguintes definições são necessárias:

I – ameaças: condições que podem causar incidentes por meio da descoberta de vulnerabilidades;

II – antivírus: programa que detecta e anula ou remove malwares de um computador;

III – ativo: a informação em si ou qualquer componente que compõe os processos e interfere direta ou indiretamente no fluxo de informação na instituição desde sua origem até seu destino, tais como equipamentos computacionais, sistemas, manuais, ferramentas e mídias;

IV – backup: cópia de segurança ou meio de armazenamento secundário que contém uma reprodução da informação de arquivos ou conjunto de dados;

V – correio eletrônico (e-mail): ferramenta que possibilita a transferência de mensagens e qualquer outro documento eletrônico para fins de comunicação;

VI – cookie: arquivo com informações que os sítios de Internet, ao serem visitados, podem armazenar nos navegadores (browsers) de forma que, na próxima visita ao mesmo endereço, este já possua informações úteis sobre o usuário;

VII – dispositivo de armazenamento: dispositivo físico no qual se registram informações para recuperação futura, podendo ser fixo ou removível (HD, CD, DVD, pen drive, fita, disquete, cartão de memória flash, entre outros);

VIII – estação de trabalho: computador com recursos voltados para a produtividade pessoal e que completa suas necessidades com recursos de outros computadores na rede;

IX – firewalls: dispositivos constituídos pela combinação de software e hardware, utilizados para dividir e controlar o acesso a computadores (firewall pessoal) ou redes (firewall de rede);

X – hardware: é o conjunto de elementos de um sistema computacional formado pelos componentes eletrônicos e partes físicas, como, por exemplo monitores, processadores, teclados, discos rígidos, placas e qualquer outro material que seja necessário ao funcionamento de um equipamento de TI;

XI – hardening: é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas. Em geral, o processo inclui remover ou desabilitar nomes ou logins de usuários que não estejam mais em uso ou não são mais necessários, desabilitar serviços desnecessários e atualizar softwares;

XII – informação: principal ativo das corporações e que requer grande proteção, de acordo com o seu valor para a organização;

XIII – log: registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;

XIV – NTP (Network Time Protocol): protocolo para sincronização dos relógios dos sistemas e computadores;

XV – risco: probabilidade de exploração das vulnerabilidades pelas ameaças, causando impacto na organização;

XVI – software: componente lógico e intangível de um computador, que engloba arquivos executáveis, bibliotecas, programas e sistemas operacionais;

XVII – usuários internos: integrantes da organização ou pessoas autorizados que se encontrem prestando serviço;

XVIII – usuários externos: todos os usuários de organizações externas que, direta ou indiretamente, acessam os recursos de TIC disponibilizados, incluindo-se os empregados de empresas prestadoras de serviços terceirizados e consultores autorizados a utilizar em caráter temporário os recursos tecnológicos;

XIX – vírus: malware que se propaga inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos de um computador, necessitando para isso, de ação por parte do usuário.

4. SEGURANÇA

Art. 10 São regras gerais:

I – todos os integrantes são responsáveis pela elevação dos níveis de segurança da informação no âmbito da organização;

II – todo usuário dos recursos de TIC deverá assinar o Termo de Compromisso e Manutenção de Sigilo;

III – todo integrante que for usuário dos recursos de TIC deverá ter o exato conhecimento destas regras;

IV – será adotado no âmbito da organização, para o direito de acesso aos recursos de TIC, o princípio do privilégio mínimo, ou seja, o usuário só terá privilégio para acesso ao que for estritamente necessário ao desempenho de suas funções;

V – a impressão de documento, nas impressoras disponibilizadas, é de inteira responsabilidade do dono do documento, devendo este zelar para que cópias ou rascunhos sem o devido controle não estejam disponíveis nas impressoras da organização;

VI – cópias de documentos inservíveis deverão ser destruídas, devendo o responsável pela produção do documento providenciar o seu descarte em local adequado;

VII – será adotado a política de mesa e tela limpa, ou seja, os usuários dos recursos de TIC não deverão deixar desnecessariamente documentos, classificados ou não, sobre a mesa. Os usuários deverão ainda providenciar para que ao se ausentar de sua estação de trabalho a mesma tenha sua tela bloqueada, impedindo assim o acesso à sua área de trabalho;

VIII – logs de sistemas corporativos e de acesso à Rede Mundial de Computadores serão armazenados pelo período de 24 meses;

IX – toda informação produzida, manuseada ou arquivada deverá passar por uma avaliação crítica quanto à classificação sigilosa;

X – a produção de documento com classificação sigilosa igual ou superior a RESERVADO deverá ocorrer, desde o início, observando-se os critérios previstos na legislação em vigor para a produção de documentos sigilosos;

XI –...;

XII –...;

XIII – todos os documentos sigilosos deverão ser protocolados, mesmo os de natureza interna;

XIV – poderá ser utilizado o serviço de correio eletrônico (e-mail) corporativo para troca de informações profissionais diversas, desde que essas não requeiram classificação sigilosa. Contudo, quando for necessária a formalização de determinada informação, essa deverá ser feita via produção de documento no SPED;

XV – é terminantemente proibido o armazenamento de arquivos e dados atinentes ao serviço em sistemas virtuais externos ao ambiente da rede corporativa tais como Google Drive, Dropbox, iCloud, Ubuntu One;

XVI – caso seja necessário à utilização de serviço em nuvem, poderá ser utilizado o serviço de armazenamento em nuvem disponibilizado pela organização, contudo apenas documentos de natureza ostensiva poderão ser armazenados em tal serviço;

XVII – a Seção de Segurança deverá trabalhar preventivamente na otimização da segurança da informação no âmbito da organização. Esse trabalho, além do operacional, deverá ocorrer através do processo de conscientização do público interno, seja este por meio de campanhas de divulgação de novas ameaças, instruções, workshops ou qualquer outro meio que leve ao aumento da eficiência dos processos de segurança da informação e comunicações;

XVIII – todo servidor ou estação de trabalho da rede interna deverá ter sua data e hora sincronizada como o serviço NTP;

XIX – todo documento inservível deverá ser picotado e descartado em lixeira adequada, devendo a Seção de Inteligência recolhê-lo semanalmente e executar a sua incineração, de maneira a evitar que lixo com informações sensíveis sejam recolhidos pelo serviço de coleta pública.

Art. 11 Da formação e uso de senhas:

I – o credenciamento para acesso aos sistemas utilizados organização será feito mediante cadastro de usuário (login) e senha, conhecimento desta Política e assinatura do Termo de Compromisso e Manutenção de Sigilo;

II – ao escolher sua senha o usuário requerente deverá observar os requisitos de formação de uma senha robusta, ou seja, este deverá formar sua senha mesclando letras maiúsculas e minúsculas, números e símbolos especiais, além de ter um tamanho mínimo de oito caracteres;

III – é proibido o compartilhamento de usuário e senha para acesso a qualquer sistema existente ou utilizado.

Art. 12 Da utilização de dispositivos móveis:

I – é expressamente proibida a utilização de dispositivos móveis pessoais na rede de dados;

II – o compartilhamento de arquivos deverá ocorrer utilizando-se os serviços fornecidos (servidor de arquivos, servidor de e-mail ou quando for o caso servidor FTP), sendo proibida a utilização de pen drives e HDs externos pessoais ou quaisquer dispositivos similares a estes;

III – poderá ser utilizado, para trâmite de arquivos entre organização e órgãos externos, apenas dispositivos móveis institucionais. Esse uso, contudo, deve ser evitado e caso seja necessário o dispositivo deverá ser criptografado, preferencialmente utilizando o software Truecrypt;

IV – notebooks institucionais deverão ter seus discos rígidos criptografados;

V – notebooks institucionais deverão ser configurados para não armazenarem cookies e históricos em seus browsers.

Art. 13 Da segurança do hardware:

I – todo material de TI de uso permanente deverá constar no Sistema de Controle Físico, devendo existir em cada seção um inventário atualizado do material a ela distribuído, bem como o nome do detentor indireto deste;

II – deverá haver trimestralmente a conferência do material existente nas seções do Centro, devendo as alterações serem informadas de forma documentada;

III – o material de TI destinado a consumo deverá ser controlado, ficando a cargo da Seção de Manutenção a execução desse controle;

IV –...;

V – microcomputadores pertencentes ao parque computacional deverão estar lacrados e com seus componentes e acessórios controlados por meio do Open Computer and Software Inventory (OCS Inventory);

VI – ativos de rede deverão ser acondicionados em armários chaveados, de forma a impedir o livre acesso a ele, exceção feita aos ativos localizados no data center;

VII – é proibida a mudança da disposição dos ativos de TI sem a devida autorização do Chefe da Divisão de Operação e sem haver previamente uma análise de risco;

VIII – a Seção de Manutenção deverá controlar o processo de lacre e cadastramento no OCS Inventory dos microcomputadores do parque computacional do Centro. Apenas a Seção de Manutenção, mediante abertura de chamado no sistema de Gestão Livre de Parque de Informática (GLPI), está autorizada a romper lacre e substituir acessório ou componentes dos microcomputadores.

Art. 14 Da segurança do software:

I – fica padronizado para utilização no âmbito da rede interna o sistema operacional GNU/Linux, preferencialmente nas distribuições Debian, Ubuntu e derivados, ficando as exceções restritas aos casos absolutamente necessários e sob a avaliação da Divisão de Operação;

II – sistemas operacionais que necessitam de antivírus devem utilizar a solução institucional configurada para ser atualizada automaticamente;

III – os antivírus institucionais instalados no parque computacional devem ser configurados para executarem automaticamente a varredura no sistema operacional e em mídias removíveis conectadas ou inseridas nos computadores ligados à rede interna;

IV – apenas a Seção de Manutenção, por meio de solicitação via sistema GLPI, tem autorização para instalar, remover ou modificar sistemas operacionais instalados na rede interna;

V – apenas a Seção de Manutenção deverá possuir senha de administrador (root) nos sistemas operacionais da rede interna e providenciar para que os usuários tenham acesso apenas como usuários comuns;

VI – a fim de padronizar o parque computacional, a Seção de Manutenção deverá instalar e configurar os sistemas operacionais da rede interna com todas as funcionalidades básicas (reprodução de áudio e vídeo, compactação e descompactação de arquivos, corretor ortográfico, acesso ao SIAFI, etc);

VII – não deverá haver compartilhamento de diretórios home. Contudo, caso haja necessidade de dois ou mais usuários compartilharem a mesma máquina, o login dos usuários deve ser individualizado (criação de quantos usuários forem necessários), sendo possível assim o rastreamento das ações de cada usuário;

VIII – a Seção de Manutenção deverá realizar o hardening básico dos sistemas para usuários internos, atentando para que estes não percam funcionalidades básicas.

Art. 15 Da utilização dos serviços da rede interna:

I – a exclusão das contas de acesso aos diversos sistemas para usuários a serem desligados se dará no momento em que for solicitada a assinatura do "Nada Consta" à Divisão de Operações. Só após a exclusão das contas o "Nada Consta" deverá ser assinado pelo Chefe da Divisão de Operações. Poderá haver ainda alteração de privilégios de acesso por ocasião de mudança de função, condicionada à publicação em boletim interno da mudança;

II – o serviço de e-mail corporativo destina-se a assuntos profissionais, não devendo seus usuários utilizá-lo para cadastro em sítios que não tenham relação com suas atividades profissionais;

III– é proibido aos usuários do serviço de e-mail disponível na rede interna a utilização deste para a disseminação de propagandas, de conteúdo que atente contra a ética, bem como de qualquer matéria que não esteja relacionada a atividades profissionais;

VI – é proibida a tramitação via e-mail corporativo de qualquer documento que tenha classificação sigilosa com grau igual ou mais restrito a RESERVADO;

VII – é proibido o acesso através da rede interna a qualquer sítio que disponibilize matéria considerada ilícita, contrária à disciplina, à moral e aos bons costumes, bem como atentatória à ordem pública ou que viole qualquer direito de terceiros;

VIII – os acessos a redes sociais via rede interna poderão ser realizados de forma controlada e desde que não interfira no desempenho da rede interna ou no bom andamento do serviço;

IX – é proibido o armazenamento no servidor de arquivos matéria considerada ilícita, contrária à disciplina, à moral e aos bons costumes, bem como atentatória à ordem pública, ou que viole qualquer direito de terceiros;

X – é proibido aos usuários da rede interna armazenar documentos relativos à sua atividade profissional em sua estação de trabalho. Para este armazenamento deverá ser utilizado o servidor de arquivos da rede interna;

XI – a Seção de Segurança deverá padronizar a imagem do plano de fundo da área de trabalho a ser utilizado. É proibido aos usuários manter no plano de fundo de sua área de trabalho qualquer outra imagem.

Art. 16 Da política de cópia de segurança (backup):

I – a cópia de segurança dos sistemas utilizados na rede interna (servidor de aquivos, SPED, servidor de e-mail, etc), deverá ser executada pela Divisão de Operação;

II – a Divisão de Operações deverá elaborar e executar um plano de backup dos sistemas utilizados na rede interna do Centro (servidor de aquivos, SPED, servidor de e-mail, etc);

III – a Divisão de Operações será responsável apenas pela cópia de segurança dos arquivos que estiverem nos sistemas utilizados na rede interna deste Centro. Arquivos em estações de trabalho serão de responsabilidade de seus usuários.

Art. 17 Da utilização de rede sem fio:

I – a utilização de redes sem fio deverá ser restrita aos laboratórios, ficando a utilização em outros ambiente condicionadas à necessidade e mediante análise de risco realizada pela Seção de Segurança;

II – quando autorizado o uso de redes sem fio, os dispositivos utilizados nesta devem ser configurados de modo a utilizar criptografia, no mínimo padrão Wi-Fi Protected Access II (WPA2) e seus acessos controlados por filtros de endereço Media Access Control (MAC);

III – quando houver necessidade e for autorizado o uso de redes sem fio, deverá ser nomeado um responsável pelo gerenciamento do ponto de acesso (access point), devendo este zelar para que o dispositivo seja ligado por ocasião do início do expediente e desligado ao término.

Art. 18 Da segurança do material de uso geral:

I – toda retirada de material deverá ser autorizada e documentada;

II – todas as repartições deverão ser fechadas ao final do expediente, sendo a posse da chave exclusiva do chefe de divisão ou seção;

III – é proibida a posse de chaves de qualquer repartição a qualquer militar que não seja o chefe ou o responsável pela repartição;

IV – as chaves das repartições guardadas no claviculário deverão ser lacradas e utilizadas apenas mediante autorização;

V – o controle do material deverá ser gerenciado e fiscalizado pelos chefes de seção, sendo esses os responsáveis pela efetividade dessas medidas de segurança.

Art. 19 Do controle de acesso físico:

I –...

II –...

Art. 20 Da utilização dos meios telefônicos:

I – os meios telefônicos deverão ser utilizados apenas para assuntos de natureza ostensiva, ficando vedada a utilização dos meios telefônicos para assuntos de natureza sensível;

II – é proibido o fornecimento de informações pessoais ou de natureza pessoal por telefone.

Art. 21 Das videoconferências:

I –....;

II – videoconferências deverão ser realizadas utilizando apenas equipamentos homologados ou autorizados pelo escalão superior;

III – videoconferências realizadas a partir da rede interna deverão tratar apenas de assuntos de natureza ostensiva.

Art. 22 Do pessoal terceirizado e estagiários:

I – todo prestador de serviço terceirizado, cujo período de prestação do serviço for superior a 15 (quinze) dias, deverá assinar o Termo de Compromisso e Manutenção de Sigilo;

II – a divisão que intermediar a contratação do serviço terceirizado, deverá informar em até três dias úteis antes do início da prestação do serviço os dados necessários à Seção de Segurança para a confecção do Termo de Compromisso e Manutenção de Sigilo (nome completo, identidade, CPF, período da prestação do serviço e serviço a ser prestado);

III - ...;

IV – a Seção de Segurança, por intermédio da Divisão Administrativa, deverá providenciar a assinatura do Termo de Compromisso e Manutenção de Sigilo por pessoal terceirizado que já presta serviço;

V - ...

VI –...;

VII –...

VIII – caso de estagiários, estes deverão conhecer e cumprir estas normas, bem como assinar o Termo de Compromisso e Manutenção de Sigilo, estando sujeitos, em caso de infração, à penalidades previstas nesta POSIC;

IX – a Seção de Segurança deverá providenciar a assinatura do Termo de Compromisso e Manutenção de Sigilo para os estagiários

Art. 23 Das penalidades:

I – a violação a estas normas será tratada como descumprimento de ordem, quando não constituir transgressão mais grave, devendo essa ser apurada conforme o Regulamento Disciplinar;

II – violações a esta política que configurarem crime serão tratadas à luz da legislação em vigor, seja o Código Penal Militar (CPM), Código Penal ou legislação própria da Administração Pública Federal (APF).

III – a violação destas normas por prestadores de serviço terceirizados ou por estagiários estará sujeita a penalidades de advertência e até rescisão contratual em caso de reincidência;

IV – caso configure crime tipificado no Código Penal Militar (CPM), Código Penal ou legislação própria da Administração Pública Federal (APF), as violações serão apuradas e tratadas na forma da lei

5. RESPONSABILIDADES

Art. 24 Do Comitê Interno de Segurança da Informação e Comunicações (CISC):

I – o Comitê Interno de Segurança Informação e Comunicações (CISC) será composto pelo ...;

II – ao CISC compete:

a. cumprir e fazer cumprir estas normas;

b. divulgar, de forma efetiva, a Política de Segurança da Informação e Comunicações;

c. promover no âmbito da organização, através de campanhas, instruções ou por qualquer outro meio conveniente, a cultura de segurança da informação, para isso o CISC poderá utilizar recursos materiais e humanos disponíveis em qualquer repartição da organização;

d. fiscalizar o exato cumprimento desta Política;

e. apurar e levar à autoridade competente, para aplicação de penalidades, os casos de infração a estas normas;

f. preparar a organização para as auditorias em segurança da informação previstas.

Art. 25 Ao presidente do CISC compete:

I – cumprir e fazer cumprir estas normas;

II – designar os membros do CISC fazendo constar anualmente no boletim interno da OM a composição do CISC;

III – dividir entre os membros do CISC as tarefas e responsabilidades para o fiel cumprimento desta Política;

IV – o presidente do CISC deverá, quando for o caso, distribuir o Formulário de Apuração de Transgressão Disciplinar (FATD) para apurar infração a estas normas.

6. PRESCRIÇÕES DIVERSAS

Art. 26 Das prescrições diversas:

I – esta política entra em vigor na data de sua publicação;

II – este documento deverá ser disponibilizado na intranet;

III – a Seção de Segurança deverá, como parte dos trabalhos de conscientização, preparar e apresentar instrução para todos os integrantes, a fim de que todos os membros tenham inteira compreensão da finalidade e objetivos desta política, bem como o conhecimento de seus direitos e deveres no tocante à execução desta;

IV – implementações que por ventura forem necessárias deverão ser providenciadas pela Divisão de Operação;

V – implementações que por sua complexidade necessitarem de recursos financeiros, deverão ser planejadas e executadas em consonância com as Normas vigentes na Administração Pública Federal;

VI – a Seção de Segurança será responsável pela posse e arquivamento dos Termos de Compromisso e Manutenção de Sigilo assinados em acordo com esta política;

VII – ações que violarem qualquer um dos pilares da segurança da informação (confidencialidade, integridade, disponibilidade e autenticidade) e que por ventura não constem neste documento não eximem seu executor de responsabilidade e serão apuradas à luz do Regulamento Disciplinar, se não constituir crime capitulado no Código Penal Militar (CPM), Código Penal ou em legislação própria da Administração Pública Federal.

VIII – a política de utilização dos servidores da Rede Metropolitana, bem como dos ativos necessários a operação desta, deverão ser elaboradas pela Seção de Segurança em conjunto com a Divisão de Operação e divulgada para as demais unidades apoiadas.