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

SELMA CÂNDIDA DA CRUZ VIEIRA

ANÁLISE DA MITIGAÇÃO DOS RISCOS DA ENGENHARIA SOCIAL NAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO DOS ÓRGÃOS PÚBLICOS FEDERAIS

Brasília
2016

SELMA CÂNDIDA DA CRUZ VIEIRA

ANÁLISE DA MITIGAÇÃO DOS RISCOS DA ENGENHARIA SOCIAL NAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO DOS ÓRGÃOS PÚBLICOS FEDERAIS

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 *Sensu* em Governança em Tecnologia da Informação.

Orientador: Prof. Dr. Maurício Rocha Lyra.

Brasília
2016

SELMA CÂNDIDA DA CRUZ VIEIRA

ANÁLISE DA MITIGAÇÃO DOS RISCOS DA ENGENHARIA SOCIAL NAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO DOS ÓRGÃOS PÚBLICOS FEDERAIS

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 Governança em Tecnologia da Informação.

Orientador: Prof. Dr. Maurício Rocha Lyra.

Brasília, 09 de Agosto de 2016.

Banca Examinadora

_____

Prof. Dr. Maurício Rocha Lyra

_____

Prof. Dr. Gilson Ciarallo

_____

Prof. Dr. Paulo Rogério Foina

Dedico este trabalho as minhas filhas que foram minha fonte de superação, a Evelyn que abdicou seus muitos momentos ausentes a minha pessoa e compreendeu o meu esforço e a Elise que mesmo ainda em meu ventre pôde ser meu alicerce na construção deste saber.

RESUMO

A tecnologia da informação tem facilitado em muito na otimização dos processos nas organizações, porém, quem adere ao recurso esquece de capacitar o recurso humano para atuar de forma eficiente e eficaz. Nos dias atuais, para invadir uma rede fragilizando a segurança da informação, utiliza-se técnicas mais simples do que se imagina, onde a mente do ser humano é posta à prova. Basta ser cativante para se obter informações que por mais simples que sejam, ajudam na ação do engenheiro social, para chegar no ponto focal dentro da instituição e causar prejuízos muitas vezes financeiros. Pensando nisso, este trabalho foi elaborado para analisar a mitigação dos riscos da engenharia social dentro da esfera federal. O estudo de caso apresentado foi estruturado com conceitos sobre a segurança da informação, a política de segurança da informação e os recursos humanos. Como resultado notou-se que é preciso divulgação do que é a engenharia social e quais os perigos que ela representa, além de manter treinamento constante a seus usuários.

Palavras-chave: Engenharia Social.Mitigação.Usuários

ABSTRACT

Information technology has facilitated much the optimization of processes in organizations, however, those who adhere to the resource forgets to empower the human resource to work efficiently and effectively. Nowadays, to invade a network handicapping information security, simpler techniques is used than you think, where the mind of man is put to the test. Just be captivating to obtain information as simple as they are, help the action of the social engineer to arrive at the focal point within the institution and cause damage often financial. Thinking about it, this study was designed to analyze the mitigation of risks of social engineering within the federal sphere. The case study was structured with concepts of information security, information security policy and human resources. As a result it was noted that it takes disclosure of which is social engineering and what dangers it represents, in addition to maintaining constant training to its members.

Keywords: Social.Mitigation.User Engineering

SUMÁRIO

INTRODUÇÃO

O mundo tornou-se refém dos meios tecnológicos, nenhuma instituição por menor que seja, sobrevive sem a implantação de um sistema de controle e uma infraestrutura de rede adequada. As pessoas que antes se comunicavam pessoalmente, hoje utilizam a tecnologia da informação para manterem contato. Reuniões do dia-a-dia são realizadas por meio de videoconferência, palestras acontecem por meio de transmissão via holograma e outros.

Com o passar dos anos houve a necessidade de manter as redes mais seguras, devido a presença de invasores dotados de conhecimento, que se aproveitavam de falhas na segurança da informação para atacar.

A segurança da informação preza pela integridade, confidencialidade e disponibilidade da informação, porém, por mais que se invista em aparatos que amenizem o risco de invasão, há de se pensar no fator humano (usuário), pois é a principal porta de entrada para ataques.

A Engenharia Social é habilidade que os engenheiros têm de enganar pessoas, adquirindo confiança e afinidade, através do seu comportamento (charme, educação e ser agradável) com o objetivo de obter informações sigilosas de empresas e afins (MITNICK;SIMON, 2003). Ele ainda diz que o engenheiro social utiliza a vulnerabilidade que o ser humano tem para realizar os planos maliciosos. Ressalte que a TI não é o único meio que estes utilizam para execução de seus atos, uma simples ligação se passando por um técnico ou uma visita domiciliar, podem ser usadas para obter informações que levam o engenheiro social a alcançar o seu alvo. Destaca-se que, o engenheiro tem por finalidade

atingir um negócio e não o indivíduo, ele apenas o usa como ponte para a coleta de informações.

Para mitigar os riscos da segurança da informação as entidades federais se empenham e geram diretrizes nas políticas de segurança da informação e comunicação para bloquear ataques. Mas, quais os recursos utilizados na estratégia da governança de tecnologia da informação para inibir a ação de engenheiros sociais nos órgãos públicos federais?

A Política de Segurança da Informação e Comunicação - POSIC tem, entre outras, a finalidade de orientar o usuário a comportar-se de maneira adequada dentro de sua entidade, resguardando sua própria identidade e evitando o comprometimento muitas vezes da rede de seu ambiente corporativo. Para isso as POSICs dos órgãos buscam ressaltar a importância da implantação dessas políticas de forma consciente a seus usuários e a inibir atos que acarretem ao setor público prejuízos como, a instabilidade dos serviços de TI. A NBR ISO/IEC 27002:2013 - Código de prática para gestão da segurança da informação atua como orientador sobre os controles de segurança da informação.

Este trabalho tem como objetivo geral verificar o uso das melhores práticas no combate à Engenharia social nas POSICs dos órgãos da administração pública federal que tornou-se popular na década de 90 (noventa). Para isso, foram analisadas 10(dez) POSICs dos órgãos de forma aleatória e comparadas com os critérios elaborados a partir da norma ISO/IEC 27002:2013

Os objetivos específicos deste trabalho foram: elencar as melhores práticas e analisar a aderência das POSICS às melhores práticas.

Vale ressaltar que, devido o tema ser de amplitude técnica, este trabalho não elenca práticas da governança de TI.

Para realizar o presente estudo e alcançar os objetivos geral e específico para a Análise da Mitigação dos Riscos da Engenharia Social Políticas de Segurança da Informação dos Órgãos Públicos Federais foram analisadas a realidade da segurança da informação nas entidades públicas e como estes se preocupam em disseminar e instruir seus usuários a prevenção de ataques externos como a engenharia social. Foram realizadas pesquisas bibliográficas em livros técnicos, que tem como foco a segurança da informação e de engenharia social assim como pesquisas via web e acesso ao repositório do Uniceub. Tem como destaque os autores Kevin Mitnick, Beal e Puricelli, que trazem uma abordagem bem relevante para o assunto.

Após a coleta das políticas de segurança da informação, foi traçado um panorama geral dos dados obtidos e comparados às instruções das normas estabelecidas na ISO/IEC 27002:2013.

O presente trabalho foi então estruturado em 4 capítulos.

O trabalho conta com uma breve introdução onde tem uma visão geral do assunto, além de relatar o problema, a solução e os meios para desenvolvimento da pesquisa.

No primeiro capítulo são apresentados alguns conceitos referentes a Segurança da Informação, neste escopo são citados os ativos de informação, o ciclo de vida da informação, onde são expostos alguns conhecimentos necessários para o desenrolar deste trabalho.

O segundo capítulo proporciona uma visão geral (conceito, quem elabora e quais critérios importantes para sua criação) da política de segurança da informação e comunicação.

No terceiro capítulo é abordado em breves citações os aspectos humanos da segurança da informação e dentro deste contexto a Engenharia social, trazendo o conceito, tipos, técnicas de invasão e formas de mitigar os riscos.

No quarto e último capítulo são apresentados os resultados da pesquisa realizada com a análise das POSICS dos órgãos públicos federais selecionados de acordo com os critérios estipulados com base na ISO/IEC 27002:2013.

1 SEGURANÇA DA INFORMAÇÃO

Há de se pensar na importância da informação, principalmente por ser o meio pelo qual as pessoas interagem em uma comunicação. Segundo Lyra (2014) informações “são dados que possuem significado em um determinado contexto”. Ou seja, um conjunto de dados gera uma informação.

De acordo com Izidoro (2016, p.3) “A comunicação é imprescindível para a gestão da informação. O controle terminológico/semântico serve para melhorar os mecanismos de busca e, originalmente, para que dados, informações e conhecimentos sejam catalogados.”

Dantas (2011, p. 9) conceitua a informação como dados que passam por algum tipo de processamento para serem utilizados de uma forma inteligível.

As informações são tramitadas em sua maioria por meio de tecnologias, ou seja, via rede, necessitam ser protegidas.

> As redes de computadores são essenciais para o trabalho nas organizações de todos os portes. No entanto, apesar de todos os benefícios que uma rede possa proporcionar, a partir do momento que os computadores são ligados em rede esses ficam mais vulneráveis a ataques por pessoas mal intencionadas que podem capturar ou destruir informações, e até mesmo sigilosas, das organizações. (SILVA, 2010, p. 261)

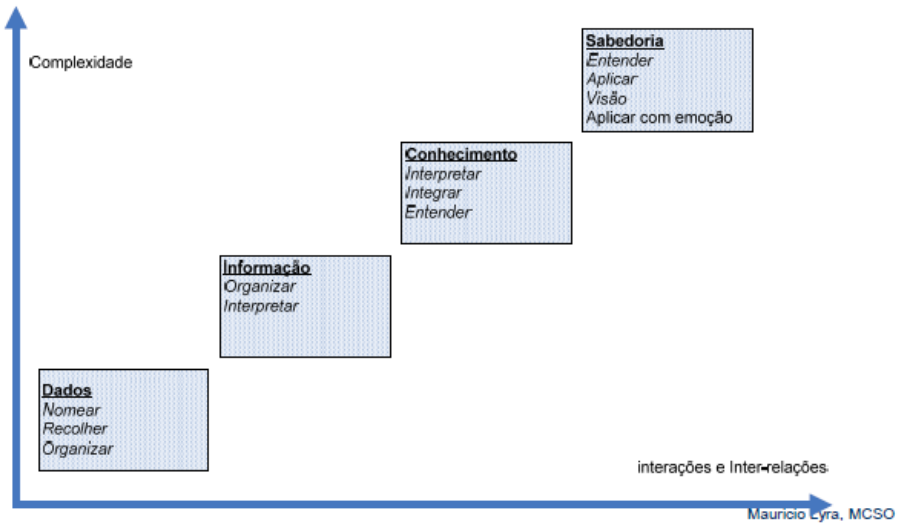
Seja por acesso a via intranet ou internet, a informação está sujeita a vulnerabilidades.

> O tema Segurança da Informação desperta muito interesse em várias audiências desde executivos e gerentes até técnicos. Isto ocorre, principalmente, porque a segurança cobre diversas áreas, tais como: segurança física, infraestrutura tecnológica, aplicações e conscientização organizacional, cada uma delas com seus próprios riscos, ameaças potenciais, controles aplicáveis e soluções de segurança que podem minimizar o nível de exposição ao qual a

> empresa está exposta, com o objetivo de garantir segurança para o seu principal patrimônio: a informação. (MAIA**,** 2013, p.1)

Segundo Lyra (2014, p.2) os níveis hierárquicos da informação se desintegram como abaixo:

Figura 1: Níveis hierárquicos da informação



Fonte: slide aula segurança da informação, parte 2, (Lyra, 2015)

A ISO/IEC 27002:2013 diz que informação é um ativo que, como qualquer outro ativo importante, tem valor para o negócio da organização e consequentemente requer proteção contra vários riscos.

A norma estabelece as estratégias fundamentais de proteção utilizadas pela Segurança da Informação, são elas:

a) Privilégio mínimo – evitar exposições desnecessárias que possam aumentar o nível de risco de segurança;

b) Defesa em profundidade – utilizar diversos controles de segurança complementares ao invés de um só;

c) Elo mais fraco – nas estratégias utilizadas no desenvolvimento de sistemas de proteção, deve-se considerar que a segurança total do sistema é igual à segurança oferecida pela sua proteção mais frágil;

d) Ponto de estrangulamento – qualquer tipo de acesso é realizado somente por um local;

e) Segurança através da obscuridade – é a estratégia de que quanto menos informações relevantes puder ser divulgada, menor a chance de uma quebra de segurança; deve ser utilizada com outros controles;

f) Simplicidade – quanto mais simples for um sistema, mais fácil é de torná-lo seguro.

1.1 Gerenciamento do Ciclo de Vida da Informação

O ciclo de vida da informação é abordado por alguns autores de forma diferenciada, alguns a descrevem com quatro fases, outros com mais, como é o caso deste referido estudo.

Sousa (2006) afirma que o gerenciamento do Ciclo de vida da informação é um processo que pretende tratar necessidades de negócio. E que semelhante a outros modelos de ciclo de vidas, o ciclo de vida da informação é baseado na filosofia que a informação tem período útil. A Informação é criada, utilizada e eventualmente destruída, e o seu valor flutua de acordo com a necessidade do negócio. Dados críticos precisam estar bem protegidos e facilmente acessíveis em contrapartida dados de menor valor precisam de menor proteção, e podem tolerar um acesso mais lento. [...]

Figura 2: Ciclo de Vida da Informação

Fonte: Produzido pelo autor do trabalho

As etapas abaixo formam o ciclo de vida da informação de acordo com Lyra (2015, p.19):

a) Criação: Identificar as necessidades de informação dos grupos e indivíduos que integram a organização e de seus públicos externos é um passo fundamental para que possam ser desenvolvidos serviços e produtos informacionais orientados especificamente para cada grupo e necessidade interna e externa. O esforço de descoberta das necessidades e dos requisitos de informação é recompensado quando a informação se torna mais útil e os seus destinatários, mais receptivos a aplicá-la na melhoria de produtos e processos (usuários internos) ou no fortalecimento dos vínculos e relacionamentos com a organização (usuários externos).

b) Obtenção: “Nesta etapa são desenvolvidos procedimentos para captura e recepção da informação proveniente de uma fonte externa (Em qualquer mídia ou formato), ou da sua criação.”

c) Tratamento: O uso dessas técnicas deve levar em conta a preservação das características de quantidade e qualidade necessárias para que a informação efetivamente sirva ao fim a que se propõe. No caso das atividades de reprodução da informação para posterior distribuição, as questões relacionadas à preservação da confidencialidade podem adquirir grande relevância, uma vez que a existência de diversas cópias de uma mesma informação, qualquer que seja a mídia utilizada (computador, papel, disquete, fita de áudio ou vídeo, etc.), amplia os problemas de restrição de acesso aos usuários devidamente autorizados.

d) Distribuição: Esta etapa consiste em levar a informação até seus consumidores. Quanto mais capilar for a rede de distribuição, mais eficiente será esta etapa. Fazendo chegar a informação certa a quem necessita dela para tomada de decisão.

e) Uso: Não é a existência da informação que garante melhore resultados em uma organização, mas sim o uso, dentro de suas finalidades básicas: conhecimento dos ambientes interno e externo da organização e atuação nesses ambientes.

f) Armazenamento: Momento em que a informação é armazenada seja em um banco de dados compartilhado, em uma anotação de papel posteriormente postada em um arquivo de ferro, ou ainda, em uma mídia de disquete depositada na gavetada mesa de trabalho, por exemplo.

g) Descarte: Quando a informação perde a utilidade.

1.2 Ativos de Informação

“Ativos são objetos de ameaças, tanto acidentais como deliberadas, enquanto que os processos, sistemas, redes e pessoas tem vulnerabilidades inerentes ”. NBR ISO/IEC 27002:2013

> Ativo é qualquer elemento de valor para a organização, isto é, qualquer item tangível (como hardware) ou intangível (por exemplo, propriedade intelectual), recursos ou habilidade que tenha valor para a existência da organização, e que por consequência necessite de proteção. (BEZERRA, 2013, p.59)

As informações com o surgimento da tecnologia da informação, necessitaram ser protegidas:

> 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. (ISO/IEC 27002:2013)

A informação necessita de garantia de que onde quer seja armazenada não sofrerá risco de ser alterado o seu conteúdo ou até de perde-la. A segurança da informação tem por objetivo preserva-la. Os riscos de vazamento de informações sigilosas podem gerar prejuízos incalculáveis a uma instituição.

As informações são classificadas a nível de sigilo de acordo a lei 12527 art. 24 em:

1. Secretas;
2. Ultra-secretas;
3. Reservada;

Cabe as autoridades específicas na lei 12527 atribuir o grau de sigilo de cada informação.

Segundo a ABNT NBR ISO/IEC 27002:2013 uma organização necessita identificar os seus requisitos de segurança da informação. Cita ainda três fontes principais destes requisitos, são eles:

1. 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.

2. 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.

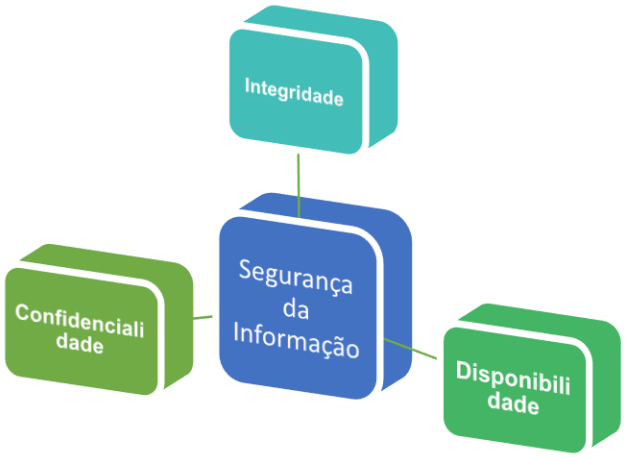
3. Os conjuntos particulares de princípios, objetivos e os requisitos do negócio para o manuseio, processamento, armazenamento, comunicação e arquivo da informação que uma organização tem que desenvolver para apoiar suas operações.

> A segurança da informação é caracterizada pela aplicação adequada de dispositivos de proteção sobre um ativo ou um conjunto de ativos visando preservar o valor que este possui para as organizações. A aplicação destas proteções busca preservar a confidencialidade, a integridade e a disponibilidade (LYRA, 2015, p.10)

1.3 Elementos da Segurança da Informação

Também conhecido como CID a confidencialidade, integridade e disponibilidade, juntos representam a segurança da informação.

Figura 3: Elementos da Segurança da Informação



Fonte: Adaptado <http://segurancadainformacao.modulo.com.br/seguranca-da-informacao>

Esses são os elementos da segurança da informação:

1.3.1 Confidencialidade

"Garantia de que o acesso à informação é restrito aos seus usuários legítimos." (LYRA, 2015, p. 10).

Diferente de ser um segredo ou algo inacessível, é um conceito no qual o acesso à informação deve ser concedido a quem de direito, ou seja, apenas para as entidades autorizadas pelo proprietário ou dono da informação (MAIA, 2013).

1.3.2 Integridade

Lyra (2015, p. 45) diz que toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protege-las com alterações indevidas, intencionais ou acidentais.

Segundo Maia (2013) O conceito de Integridade está ligado à propriedade de manter a informação armazenada com todas as suas

características originais estabelecidas pelo dono da informação, tendo atenção com o seu ciclo de vida (criação, manutenção e descarte).

1.3.3 Disponibilidade

"Garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna". (LYRA, 2015, p. 15)

De acordo com Maia (2013), deve-se garantir que a informação esteja sempre disponível para uso quando usuários autorizados necessitarem.

Além destes elementos também contribuem para a gerar a garantia da segurança da informação segundo Lyra (2015, p. 11), a autenticidade, o não repúdio, a legalidade, a privacidade e a auditoria.

1.4 Gestão de Riscos da Segurança da Informação

Segundo a ISO/IEC 27005:2011 a gestão de riscos são atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.

De acordo com a ISO/IEC 27005:2011 convém que a gestão de riscos de segurança da informação contribua para:

a) Identificação de riscos;

b) O processo de avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência;

c) A comunicação e entendimento da probabilidade e das consequências destes riscos;

d) O estabelecimento da ordem prioritária para tratamento do risco;

e) A priorização das ações para reduzir a ocorrência dos riscos;

f) O envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e para que elas sejam mantidas informadas sobre a situação da gestão de riscos.

g) A eficácia do monitoramento do tratamento dos riscos;

h) O monitoramento e análise crítica periódica dos riscos e do processo de gestão de riscos;

i) A coleta de informações de forma a melhorar a abordagem de gestão de riscos;

j) O treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los

1.4.1 Vulnerabilidade

Vulnerabilidade é uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. (BIZU, 2015, p.1)

De acordo com Beal (2005, p. 14) “é a fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque.”

Segundo a ISO/IEC 27005:2011 as vulnerabilidades podem ser identificadas nas seguintes áreas:

- ✓ Organização;
- ✓ Processos e procedimentos;
- ✓ Rotinas de gestão;
- ✓ Recursos humanos;
- ✓ Ambiente físico;
- ✓ Configuração do sistema de informação;

- ✓ Hardware, software ou equipamentos de comunicação;
- ✓ Dependência de entidades externas.

1.4.2 Ameaça

É todo e qualquer evento que possa explorar vulnerabilidades. (BEZERRA, 2013, p.3)

Ameaça é uma causa potencial de incidente um indesejado, que pode resultar em um dano para um sistema ou organização. (BIZU, 2015, p.1)

Uma ameaça tem o potencial de comprometer ativos (como informações, processos e sistemas) e por isso, também as organizações.

Ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais

1.4.3 Impacto

Segundo Beal (2005) é o efeito ou consequência de um ataque ou incidente para a organização.

1.4.4 Incidente

De acordo com Beal (2005, p.14) é o evento com consequências negativas resultantes de um ataque bem sucedido.

> Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade. (UFRJ)

Para Beal (2005, p.13) é a expectativa de acontecimento acidental ou proposital, causado por um agente, que pode afetar um ambiente, sistema ou ativo de informação.

É a possibilidade de um agente, interno ou externo, explorar acidentalmente ou propositalmente uma vulnerabilidade específica. (ALERTA SECURITY, 2016)

1.4.5 Ataque

Beal (2005, p.13) define como evento decorrente da exploração de uma vulnerabilidade por uma ameaça.

De acordo com o sítio Meu Bizu (2016) Ataque é qualquer ação que compromete a segurança da informação. Cita ainda que os ataques podem ser divididos em dois tipos: Ataque ativo que viola os princípios da autenticidade (disfarce) integridade (repetição e modificação de mensagens) e disponibilidade (negação de serviços DOS(Denial of service) ou interrupção) e Ataque passivo viola o princípio da confidencialidade.

Para Beal (2005, p.13) além dos citados acima existem: o agente, e o alvo como questão do risco no contexto da segurança da informação.

2 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Com o intuito de preservar a segurança da informação nos órgãos do poder público, foi solicitado, segundo a norma complementar 03 a criação de comitê capaz de gerar diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

A política de segurança da informação segundo a Norma Complementar 03 é um documento aprovado pela autoridade responsável do órgão ou entidade da Administração Pública Federal - APF, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.

De acordo com a ISO/ IEC 27001:2013 a alta direção deve estabelecer uma política de segurança da informação que:

a) Seja apropriada ao propósito da organização;
b) Inclua os objetivos de segurança da informação ou forneça a estrutura para estabelecer os objetivos de segurança da informação;
c) Inclua o comprometimento em satisfazer os requisitos aplicáveis, relacionados com a segurança da informação;
d) Inclua o comprometimento com a melhoria contínua do sistema de gestão da segurança da informação.

Ainda diz que a política de segurança deve:

a) Estar disponível como informação documentada;
b) Ser comunicada dentro da organização; e

c) Estar disponível para as partes interessadas, conforme apropriado.

Fontes (2006) conceitua a POSIC como um documento que deve conter um conjunto de normas, métodos e procedimentos, os quais devem ser comunicados a todos os funcionários, bem como analisado e revisado criticamente, em intervalos regulares ou quando mudanças se fizerem necessárias. É o SGSI que vai garantir a viabilidade e o uso dos ativos somente por pessoas autorizadas e que realmente necessitam delas para realizar suas funções dentro da empresa.

Beal (2005, p.43) afirma que a POSIC: Estabelece as linhas mestras a serem seguidas na implementação da segurança da informação, formalizando todos os aspectos relevantes para a proteção, o controle e o monitoramento de seus ativos de informação. Por meio dela a direção da organização demonstra seu comprometimento com a proteção da informação, e cria a base para a colaboração de todos os integrantes com os processos de identificação e tratamento dos riscos.

2.1. Comitê de segurança

Segundo a Norma Complementar 03 é o grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF.

A NC 03 recomenda que para a elaboração da POSIC seja instituído um Grupo de Trabalho constituído por representantes dos diferentes setores do órgão ou entidade da APF, como por exemplo: segurança patrimonial, tecnologia da informação, recursos humanos, jurídico, financeiro e planejamento;

De acordo com Lyra (2008, p.55) a norma 27002 recomenda a criação de dois comitês: um corporativo e outro departamental.

Lyra (2008) também destaca as principais atribuições que o comitê corporativo tem por responsável, são elas:

a) Organizar, centralizar e planejar as ações de segurança que vão interferir em todos os ambientes e processos, a priorização das ações e dos investimentos;
b) Aprovar as políticas, normas e procedimentos de segurança da informação;
c) Aprovar novos controles de segurança para a melhoria contínua de medidas de proteção;
d) Apoio à implantação de soluções para minimizar riscos;
e) Deliberar sobre incidentes de segurança corporativa.

De acordo com a NC 03, comitê de segurança tem por responsabilidades:

a) Assessorar na implementação das ações de segurança da informação e comunicações no órgão ou entidade da APF;

b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações; e

c) Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.

As atividades fins dos comitês departamentais segundo Lyra (2008, p.56) são:

- Implementar ações de segurança e medir os resultados planejados pelo comitê corporativo;
- Reportar novas necessidades e situações que exponham os ativos de informação.

2.2. Sistema de Gestão de Segurança da Informação

É a parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação. (ISO/IEC 27001:2006)

> A ISO/IEC 27001 é um padrão para sistema de gestão da segurança da informação (ISMS - *Information Security Management System*) publicado em outubro de 2005 pelo *International Organization for Standardization e pelo International Electrotechnical Commision*. Seu nome completo é ISO/IEC 27001:2005 - Tecnologia da informação - técnicas de segurança - sistemas de gerência da segurança da informação - requisitos mais conhecidos como ISO/IEC 27001. Esta norma foi elaborada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

2.3. Controle de acesso

Para Lyra (2008, p.43) o acesso à informação deve ser controlado, para que se possa garantir os três princípios básicos da segurança (confidencialidade, integridade e disponibilidade), mas não deve impedir os processos de negócio da organização.

2.3.1. Controle de acesso lógico

> O controle de acesso lógico, por sua vez, permite que os sistemas de tecnologia da informação verifiquem a autenticidade e a identidade dos usuários que tentam adentrar em seus sistemas ou utilizar seus serviços. (DIMEP, 2016)

Segundo Lyra (2008, p.43) dentre alguns recursos a serem protegido na modalidade de dados, existem: sistemas, banco de dados, software e outros. Reporta ainda que os ativos de controle lógico se dividem em: identificação do usuário, administração de privilégios de usuários e monitoração do uso e acesso ao sistema.

2.3.2. Controle de acesso físico

> O controle de acesso físico pode ser compreendido como o tipo de sistema que torna o acesso físico a uma determinada área, como, por exemplo, um prédio, uma sala, uma empresa, uma casa, um container etc., totalmente controlado, sendo que somente pessoas autorizadas são permitidas a adentrar. (DIMEP, 2016)

De acordo com Dantas (2011, p. 132) como a política deve ser divulgada por toda a organização, e ela é o ponto de partida para a segurança da informação, assunto até certo ponto áspero, a adoção dessa linha de ação (se detalhar todos esses controles) não parece ser uma decisão que venha facilitar o processo de cultura pela segurança da informação.

2.4. Recursos humanos

> Pessoas são ativos que tem sentimento, emoções, vontades. São ativos que são educados. Em Segurança da Informação, os valores individuais são considerados juntamente com os corporativos, uma vez que o indivíduo passa a ser responsável pelo que é valoroso para a sua organização, seus clientes, parceiros ou fornecedores. (Silva, 2011)

Segundo Purser (2011) não existem regras prontas sobre como monitorar o comportamento dos usuários, mas é essencial comunicar os procedimentos de segurança para a equipe e garantir que eles sejam seguidos no dia-a-dia.

Segundo a ISO/IEC 27005:2011 os tipos de recursos humanos compreendem todas as classes de pessoas envolvidas com os sistemas de informação e se dividem em:

a) Tomador de decisão: são aqueles responsáveis pelos ativos primários (informação e processos) e os gestores da organização ou, se for o caso, de um projeto específico.

b) Usuários: são recursos humanos que manipulam material sensível no curso de suas atividades e que, portanto, possuem uma responsabilidade especial nesse contexto. Eles podem ter direitos especiais de acesso aos sistemas de informação para desempenhar suas atividades rotineiras.

c) Pessoal de produção/manutenção: são recursos humanos responsáveis pela operação e manutenção dos sistemas de informação. Eles possuem direitos especiais de acesso aos sistemas de informação para desempenhar atividades rotineiras.

d) Desenvolvedores: são responsáveis pelo desenvolvimento dos sistemas aplicativos da organização. Eles possuem acesso com alto privilégio a uma parte dos sistemas de informação, mas não interferem com os dados de produção.

2.4.1 Conscientização

De acordo com a ISO/IEC 27001:2013 Pessoas que realizam trabalho sob o controle da organização devem estar cientes da:

a) Política de segurança da informação;

b) Suas contribuições para a eficácia do sistema de gestão da segurança da informação, incluindo os benefícios da melhoria do desempenho da segurança da informação; e

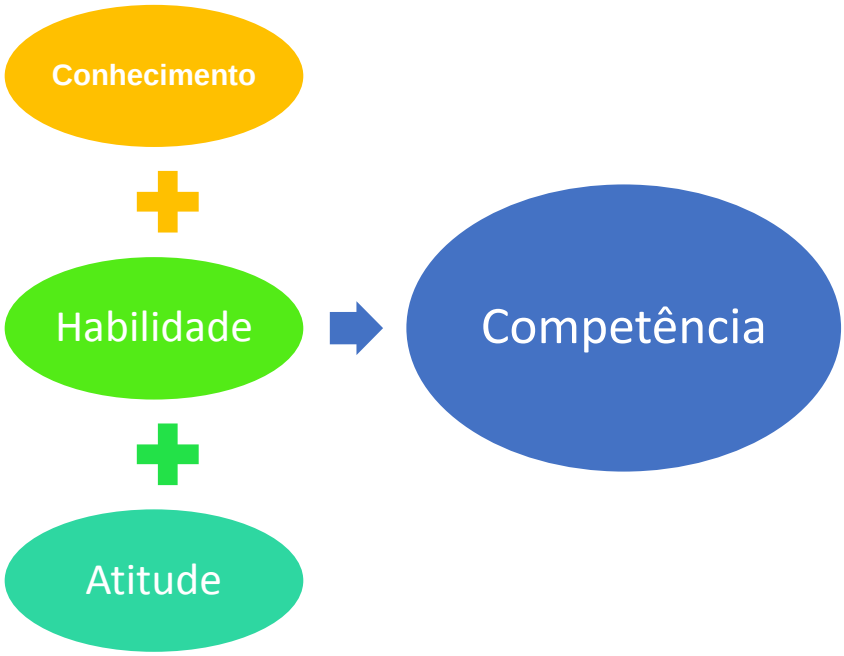
c) *Implicações da não conformidade com os requisitos do sistema de gestão da segurança da informação.*

2.4.2 Competência

> As competências podem ser classificadas como humanas (relacionadas ao indivíduo) ou organizacionais (relacionadas à organização). Vale ressaltar que é o conjunto de competências profissionais que sustenta a competência organizacional. Não haverá competência organizacional onde não houver competência profissional. (NOVAES, 2015)

Os três elementos que compõe a competência são conhecimento, habilidade e atitude.

Figura 4 – Elementos da Competência



Fonte: Produzido pelo autor do trabalho

Para Campos (2012) conhecimento é a junção de saber e treinamento teórico; habilidade é o saber fazer e o treinamento prático e atitude depende do profissional o querer fazer.

A ISO/IEC 27001:2013 diz que a organização deve determinar a competência necessária das pessoas que realizam trabalho sob o seu controle e

que afeta o desempenho da segurança da informação garantindo tais competências com base na educação, treinamento ou experiência apropriados.

2.5. Prevenção e tratamento de incidentes

O cert.br conceitua incidente de segurança como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, ou, o ato de violar uma política de segurança, explícita ou implícita.

> Medidas preventivas, detectivas e reativas compõem a multicamada de proteção contra incidentes da organização, podendo incluir firewalls de rede e de internet, scanners de rede e de sistema, detectores de abusos e anomalias, softwares de filtragem de conteúdo, antivírus e programas de auditoria, entre outros controles para prevenir e detectar ataques e responder a quebras de segurança. (BEAL, 2005, p.)

2.5.1 Administração de incidentes na APF

A existência de pessoas formalmente designadas para tratar incidentes é fundamental para garantir uma resposta rápida e eficaz após a ocorrência de eventos danosos.

No setor público foi criado o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal.

> A criação de um Centro de Tratamento de Incidentes de Segurança de Redes de Computadores deve se inserir em uma estratégia de fortalecimento da segurança da informação. É fundamental considerar o processo de implementação de segurança como uma tarefa permanente, que deve ser constantemente atualizada e planejada. (CTIR Gov, 2011)

A norma complementar 08, disciplina que para o correto gerenciamento de incidentes de segurança da informação sejam trocadas informações entre a ETIR e a CGTIR pois facilita:

a) promover o intercâmbio científico-tecnológico relacionado a incidentes de segurança em redes de computadores;

b) apoiar órgãos e entidades da APF nas atividades de gerenciamento e tratamento de incidentes de segurança em redes de computadores, quando necessário;

c) monitorar e analisar tecnicamente os incidentes de segurança em redes de computadores da APF, permitindo a criação de métricas e/ou alertas;

d) implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança em redes de computadores da APF;

e) apoiar, incentivar e contribuir, no âmbito da APF, para a capacitação no tratamento de incidentes de segurança em redes de computadores.

2.5.2 Notificação de incidentes

Para Beal (2005, p.120) todos os funcionários que prestam serviço devem estar informados dos procedimentos disponíveis para notificar incidentes, incluindo falhas nos sistemas de informação, inoperância de serviços, erros resultantes de dados incompletos ou inconsistentes e violação de confidencialidade, entre ou outros. Os usuários devem ser estimulados a relatar tais incidentes assim que tenham sido detectados.

2.5.3 Plano de contingência

Segundo Lyra (2015, p.127) o Plano de Contingência é um plano para a resposta de emergência, operações backup, e recuperação após um desastre em um sistema como a parte de um programa da segurança para assegurar a

disponibilidade de recursos de sistema críticos e para facilitar a continuidade das operações durante uma crise.

> O Plano de Contingência é um documento onde estão definidas as responsabilidades estabelecida em uma organização, para atender a uma emergência e também contêm informações detalhadas sobre as características da área ou sistemas envolvidos. É um documento desenvolvido com o intuito de treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate às ocorrências anormais. (CELEPAR, 2009)

Figura 5 :Etapas do Planejamento do Plano de Contingência

Fonte: Lyra, 2015

De acordo com o guia de elaboração do plano de contingência elaborado pela CELEPAR, para que um plano possa ser redigido é necessário realizar previamente as seguintes reflexões:

a) Identificar os processos de negócio importantes para a organização e os serviços do sistema que automatizam estes processos;

b) Avaliar os impactos em caso de falhas e identificar como e quem deve resolver as mesmas.

Além do plano de contingência é necessário que se tenha um plano de continuidade.

2.5.4 Plano de continuidade no negócio

De acordo com Lyra (2015, p. 118) o plano de continuidade do negócio é o processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado.

> Uma avaliação de impacto nos negócios deve ser realizada para identificar os impactos nas atividades críticas de negócios, cuja análise deve considerar o tempo de aceitabilidade da interrupção, a perda financeira, o tempo para a recuperação e a relação custo-benefício das medidas de continuidade a serem adotadas. (DANTAS, 2011, p. 138)

De acordo com as diretrizes de implementação da ISO/IEC 27002, convêm que uma organização avalie se a continuidade da segurança da informação está contida dentro do processo de gestão de continuidade do negócio ou processo de gestão de recuperação de desastre. Requisitos de segurança da informação podem ser determinados quando do planejamento da continuidade do negócio e da recuperação de desastre.

> As políticas de segurança são instruções claras que fornecem as orientações de comportamento do empregado para guardar as informações, e são um elemento fundamental no desenvolvimento de controles efetivos para contra-atacar as possíveis ameaças à segurança. Essas políticas estão entre as mais significativas no que diz respeito a evitar e detectar os ataques da engenharia social. (MITNICK; SIMON, 2003)

3 ASPECTOS HUMANOS DA SEGURANÇA DA INFORMAÇÃO

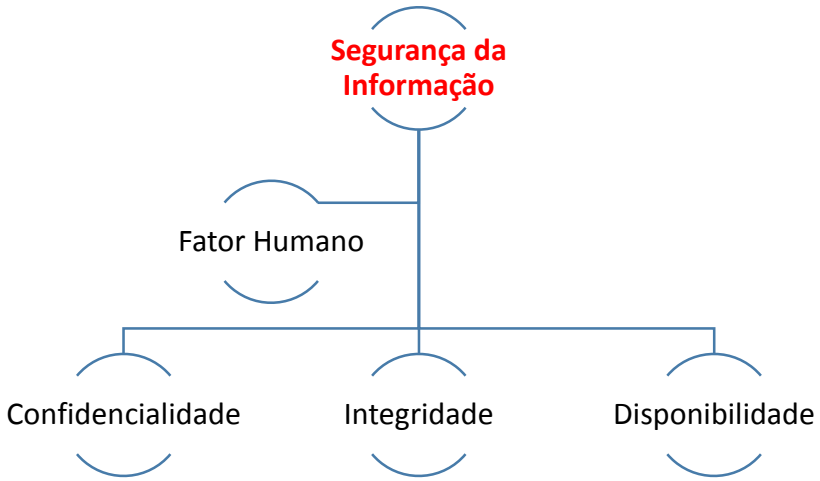
> As pessoas são, acertadamente, consideradas o elo frágil da segurança da informação. A associação pode ser entendida quando se imagina que qualquer esquema de segurança, por mais sofisticado que seja, pode ser derrubado pela atuação de uma única pessoa que decida abusar de seus privilégios de acesso a dados ou instalações de processamento da informação. (BEAL, 2005, p.71)

Pessoas são os elementos centrais de um sistema de segurança da informação. Os incidentes de segurança sempre envolvem pessoas, quer do lado das vulnerabilidades exploradas quer das ameaças que exploram essas vulnerabilidades. (LYRA, 2008)

O nível de importância da segurança da informação, foi alterado ao se perceber que o fator humano deve ser treinado para a concepção de uma rede segura. Avaliar, monitorar e exercer outras atividades somente de cunho técnico, permanecia em deixar portas abertas a invasão.

> Infelizmente, essa não é a realidade atual. A questão não se resume aos profissionais de segurança de TI de empresas visadas terem implantado os melhores processos, tecnologias e soluções (estar em conformidade total com práticas e padrões do setor). Em vez disso, o fato relevante é que essas medidas de segurança não são mais suficientes. Os ataques de segurança dependem cada vez mais de vulnerabilidades humanas, portanto, é fundamental ampliar a governança de segurança de TI para incluir o fator humano em análises e avaliações de riscos corporativos. Para fazer isso de maneira eficiente, é crucial compreender e mensurar o risco real, bem como propor contramedidas eficazes e personalizadas para mitigá-lo. (PURICELLI, 2015)

Figura 6 - Fator humano na segurança da informação



Fonte: Adaptado < http://blog.segr.com.br/o-fator-humano/>

> Um dos principais problemas que a segurança da informação deve tratar é a segurança em pessoas. A cooperação dos usuários é essencial para a eficácia da segurança. Eles exercem um forte impacto sobre a confidencialidade, a integridade e a disponibilidade da informação, pois, por exemplo, o usuário que não mantiver a confidencialidade da senha, não evitar o registro da mesma em papéis que não estão guardados em locais seguros, não utilizar senhas de qualidade ou ainda que compartilhe senhas individuais, compromete a segurança da informação. (LYRA, 2015)

Para Puricelli (2015) o erro humano ou comportamento inadequado estão frequentemente relacionados à falta de percepção de riscos associada a fatores não racionais, como experiência pessoal e atitude psicológica, especialmente em casos de pouca ou falta de conscientização.

A frequência de erros que geram transtornos a equipe de segurança da informação se dá muitas vezes pela falta de habilidade que os usuários pouco têm. Ao se atualizar um *browser* por exemplo, é comum que o mesmo informe que computador foi danificado ao realizar tal processo, quando na verdade não sabe manuseá-lo.

3.1 Engenharia Social

“Um aspecto de grande importância e muitas vezes negligenciado na segurança da informação é a proteção contra ataques de engenharia social.” (BEAL, 2005)

Silva Filho (2004) considera a engenharia social como um termo utilizado para qualificar os tipos de intrusão não técnica, que coloca ênfase na interação humana e, frequentemente, envolve a habilidade de enganar pessoas objetivando violar procedimentos de segurança.

De acordo com o entendimento de Ribeiro (2014) Engenharia Social é definida como uma técnica capaz de manipular pessoas, enganando-as, para que forneçam informações ou executem uma ação desejada pelo executor (engenheiro social), podendo ocorrer interna ou externamente ao ambiente da empresa é uma ameaça às organizações.

> É o nome atribuído a técnica utilizada para obter informações importantes e sigilosas das empresas ou usuários domésticos sem a utilização de uma ameaça virtual. Essa técnica consiste em explorar as falhas de segurança dos humanos para recolher informações. (SILVA, 2010, p.1)

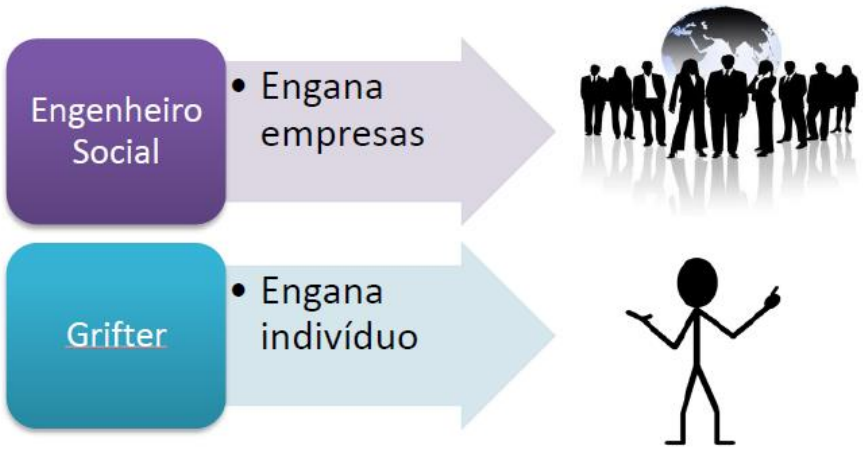
Figura 7: Perfil do Engenheiro Social

Fonte: Produzido pelo autor do trabalho

> Um engenheiro social vive da sua capacidade de manipular as pessoas para que elas façam coisas que o ajudem a atingir o seu objetivo, mas o sucesso quase sempre requer uma grande dose de conhecimento e habilidade com os sistemas de computador e telefonia. (MITNICK; SIMON 2003, p.139)

Para Mitnick e Simon (2003) a diferença entre o engenheiro social e o *grifter* é que este tem a intenção de enganar indivíduos e o engenheiro as empresas.

Figura 8: Diferença entre engenheiro social e grifter



Fonte: Produzido pelo autor do trabalho

> Os espiões industriais e invasores de computador eventualmente fazem uma entrada física na empresa-alvo. Em vez de usar um pé de cabra para quebrar a porta, o engenheiro social usa a arte da fraude para influenciar a pessoa que está do outro lado da porta para abri-la para ele. (MITNICK; SIMON 2003, p.145)

> O engenheiro social emprega as mesmas técnicas persuasivas que usamos no dia-a-dia. Assumimos papéis, tentamos obter credibilidade. Cobramos obrigações recíprocas. Mas o engenheiro social aplica essas técnicas de uma maneira manipuladora, enganosa, altamente antiética, frequentemente com efeito devastador. (MITNICK; SIMON, 2003, p. 188))

De acordo com Silva (2011) em uma organização, cada setor tem um processo que ele é prioritário, Assim entre o importante e o urgente, haverá uma

tomada de decisão que pode desprezar alguns procedimentos de segurança da informação em prol da volta à normalização naquele ambiente. Vulnerabilidade humana, que variam de pessoa para pessoa e conforme as circunstâncias. Exemplos a vaidade, a ambição, o medo, o entusiasmo, a paixão. Coisas que podem nos cegar ou turvar consciência. Essas e outras vulnerabilidades são exploradas por crackers que usam a engenharia social. O valor da informação nem sempre é pago em dinheiro. Muitas vezes é com carinho e atenção.

3.1.1 Tipos de Engenharia Social

Para Ribeiro a Engenharia Social se divide em:

a) Engenheiro social interno: o interno existe e pode ser muito, mas muito mais perigoso. São exemplos: Um colaborador formal, um terceiro atuando em período integral nas instalações da empresa, um parceiro/terceiro que não atue de maneira integral, mas é rotineira sua presença na empresa.
b) Engenheiro Social externo: é comumente falado que atua de fora da instituição procurando meios de acesso interno.

Ribeiro ainda informa que os dois tipos têm os mesmos objetivos: enganar, manipular pessoas para que façam o que desejam: informações que eles não poderiam obter de forma lícita e ações que somente essas pessoas podem executar para favorecê-lo de alguma forma. Com as informações coletadas ou ações tomadas pelo seu alvo, podem iniciar uma lista de ilícitos.

3.1.2 Tipos de Hackers

Koch (2016) relata que o termo hacker surgiu em meados dos anos 60 e originou-se da palavra ***phreak*** (acrônimo de phone hacker), que eram os hackers que estudavam o sistema de telefonia e com isso conseguiam fazer ligações de graça. Naquela época os sistemas de informática (assim como os de telefonia)

eram restritos a poucos: apenas tinham acesso a eles os envolvidos com computação nos grandes CPDs (Centros de Processamento de Dados) de universidades e empresas.

Koch (2016) ainda descreve que movidos pela curiosidade de saber como tudo aquilo funcionava, alguns grupos de estudantes quebravam os cadeados dos CPDs usando um machado. Hack significa cortar, golpear em inglês, daí o termo ter sido adotado para designar aqueles que quebram a segurança para aprender sobre algo que pessoas comuns não têm acesso.

De acordo com Mitnick e Simon (2003) existem três tipos de hackers:

3.1.2.1 *Scriptkiddies*

São hackers novatos que não possuem interesse em aprender a tecnologia, seu desejo é invadir os computadores.

Koch (2016) define scriptkiddies como o nome atribuído de maneira depreciativa aos crackers inexperientes que procuram alvos fáceis para aplicar seus poucos conhecimentos técnicos. Eles não possuem conhecimento de programação e têm como objetivo ganhar fama e lucros pessoais com seus ataques. Ainda segundo o portal um scriptkiddie desenvolve ações relacionadas à segurança da informação com base nos trabalhos de hackers profissionais que realmente entendem sobre o assunto e possuem considerável conhecimento técnico.

3.1.2.2 *Hackers programadores*

Desenvolvem programas para hackers e expõe na web;

Para Koch (2016) há os seguintes tipos de hackers:

a) **White Hats (hackers éticos):**

Seguem a mesma linha de pensamento original do hacking. Gostam apenas de saber e conhecer mais das coisas, principalmente as fechadas ao público. Para essas pessoas, aprender é a diversão mais importante do mundo. Elas gastam boa parte de seu tempo estudando o funcionamento do que as cerca, como telefonia, internet e protocolos de rede e programação de computadores.

No mundo da segurança de software, os hackers éticos são os responsáveis por “informar” as grandes empresas de vulnerabilidades existentes em seus produtos. Fora do mundo da segurança, essas pessoas são responsáveis por desenvolver software livre, como o sistema operacional GNU/Linux.

b) **Black Hats (hackers mal-intencionados):**

Assim como os White Hats, os Black Hats também são movidos pela curiosidade. O que os distingue é o que cada um faz com a informação e o conhecimento.

O Black Hat vê poder na informação e no que ele sabe fazer. São aqueles hackers que descobrem uma vulnerabilidade em um produto comercial ou livre e não contam para ninguém até que eles próprios criem meios de obter dados sigilosos de outras pessoas e empresas explorando a vulnerabilidade recém-descoberta.

3.1.2.3 *Estelionatários*

Usam o computador como meio fraudulento para roubar dinheiro, bens ou serviços.

Vale lembrar que o engenheiro social, visa conseguir informações valiosas com técnicas de enganar pessoas, sem se dar o trabalho de invadir um sistema. Através de um diálogo convincente e envolvente o indivíduo de um help

desk por exemplo chega a gerar nova senha no sistema e informa ao transgressor, este consegue de forma fácil e rápida se passar pelo usuário final e tendo em mãos todas as informações precisas sem muito esforço.

3.1.3 Técnicas de invasão de engenharia social mais comuns

os caminhos mais utilizados para uma invasão segundo Mitnick (2003) são:

a) Contatos telefônicos, simulando atendimento de suporte ou uma ação de emergência;

b) Contato através de e-mail, atuando como estudante com interesse em pesquisa sobre determinado assunto ou como pessoa com interesse específico em assunto de conhecimento da vítima;

c) Contato através de ferramentas de mensagens simulando pessoa com afinidades com a vítima;

d) Obtenção de informações vazadas por parte da administração de rede e funcionários em geral em listas de discussão ou comunidades virtuais na Internet, o que motivaria também um contato posterior mais estruturado;

e) Uso de telefone público, para dificultar detecção;

f) Varredura do lixo informático, para obtenção de informações adicionais para tentativas posteriores de contato;

g) Disfarce de equipe de manutenção;

h) Visita em pessoa, como estudante, estagiário ou pessoa com disfarce de ingenuidade.

Dessas técnicas é comumente utilizada o "*spear-phishing*" onde o usuário é atraído clicar em um link dentro de um e-mail ou a preencher formulário contendo informações que fragilize a segurança da empresa.

3.1.4 Formas de mitigar os riscos de ataques por engenheiros sociais

Orientar o usuário a agir da forma correta, facilita em muito no tocante a segurança da informação. Fazê-lo entender que com um simples clique, pode gerar um prejuízo incalculável a corporação. É importante que haja uma maturidade visível com relação ao que lhe atrai e para isso é necessária uma estratégia que envolva a todos que de alguma maneira desempenha alguma função dentro da corporação. Orientar e treinar ainda são as melhores escolhas.

> Do ponto de vista da governança de segurança de informações, o objetivo final de incluir o fator humano em avaliações de vulnerabilidades é identificar formas adequadas de mitigação. As contramedidas mais eficazes contra os riscos destacados são conscientização e treinamento, que ajudam a melhorar a cultura de segurança dos funcionários. (PURICELLI, 2015)

Para Ribeiro (2014) a forma de mitigar o risco da engenharia social nas organizações é entender o tamanho do risco e implantar conscientização e treinamento.

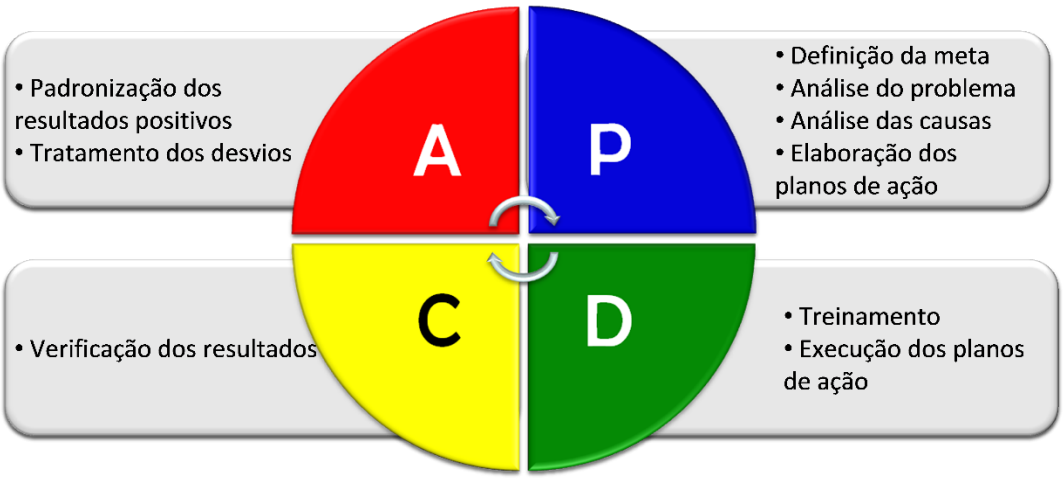
Ribeiro (2014) ainda relata que é necessário implantar um programa de treinamento e conscientização com objetivos claros:

a) Promover a conscientização sobre a ameaça do ataque de engenharia social (interno e/ou externo)
b) Treinar os usuários para cumprir e apoiar as medidas defensivas de segurança sistêmica que protegem as informações e sistemas de ataque.
c) Entender o perfil e como pensa e age um Engenheiro Social.

Não existe tecnologia que evite um ataque de um Engenheiro Social, portanto é necessário um treinamento contínuo para que as pessoas sempre saibam quais são as novas técnicas utilizadas e como lidar com cada uma delas. (MITNICK; SIMON, 2003)

Uma das ferramentas importantes para o melhoramento contínuo da segurança da informação é o PDCA, pois através dele pode se identificar as falhas e trata-las.

Figura 9 – Ciclo PDCA



Fonte: Disponível em : <http://www1.tce.pr.gov.br/multimidia/2012/11/png/00237966.png>

Conforme o TCE/PR, o ciclo PDCA é um ciclo de desenvolvimento que tem foco na melhoria contínua. Seu princípio é tornar mais claros e ágeis os processos envolvidos na execução da gestão, como, por exemplo, na gestão da qualidade, dividindo-a em quatro principais passos, com termos designados em inglês: P- Plan (planejar); D - Do (executar); C - Check (verificar) e A - Act (agir)

4 ANÁLISE DAS POSICS DA ADMINISTRAÇÃO PÚBLICA FEDERAL QUANTO A ENGENHARIA SOCIAL

4.1 Tabela de Requisitos de Análise dos Riscos da Engenharia Social nas POSICS dos Órgãos Públicos Federais

As modificações tecnológicas permitiram o avanço de ferramentas que contribuem para inibir eventuais ataques às redes corporativas, um exemplo disso é o fortigate adotados por alguns órgãos federais. Como citado nos capítulos anteriores, a ação humana é a porta de entrada para que engenheiros sociais possam agir e este é um aliado na prevenção de invasões.

Conforme orientações de Mitnick existem alguns atributos que inibem a ação de engenheiros sociais nas organizações.

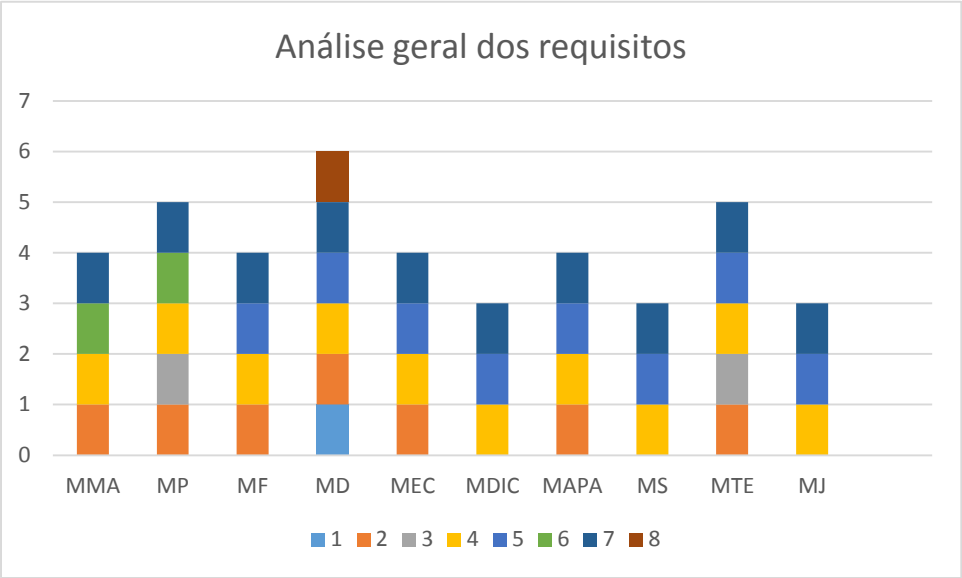
A tabela 1 dispõe dos principais requisitos necessários que devem ser inseridos numa Política de Segurança da Informação de acordo com Mitnick ex-engenheiro social.

Tabela 1 – Verificar se as POSICS dos ministérios atendem aos critérios de mitigação dos riscos de engenharia social

Requisitos essenciais na prevenção da engenharia social	**MMA**	**MP**	**MF**	**MD**	**MEC**	**MDIC**	**MAPA**	**MS**	**MTE**	**MJ**
1 – A política define que no processo de contratação de serviços terceirizados, a empresa valide se os funcionários contratados são pessoas de confiança e reputação ilibada, para desempenhar os papéis, principalmente se for papel crítico?	**Não**	**Não**	**Não**	**Sim**	**Não**	**Não**	**Não**	**Não**	**Não**	**Não**
2 - A política de segurança sinaliza que todos os funcionários sejam eles contratados ou concursados, que tenham acesso a informações sensíveis, assinem um termo de confidencialidade ou de não divulgação, antes de ser dado acesso aos serviços de TI?	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Não**	**Sim**	**Não**	**Sim**	**Não**
3 - A política propõe meios de divulgação, que instrui o usuário a utilizar métodos mais rigorosos de autenticação com senhas fortes e alteração de senhas periodicamente?	**Não**	**Sim**	**Não**	**Não**	**Não**	**Não**	**Não**	**Não**	**Sim**	**Não**
4 - A política de segurança propõe um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de segurança da informação?	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
5 – A política instrui à direção que seus stakeholders tenham habilidades e qualificações apropriadas e sejam treinados regularmente?	**Não**	**Não**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
6 - A política exige que sejam planejadas e executadas com frequência, divulgação e treinamento de conscientização dos perigos iminentes da engenharia social aos seus usuários?	**Sim**	**Sim**	**Não**	**Não**	**Não**	**Não**	**Não**	**Não**	**Não**	**Não**
7 – A política prevê em suas diretrizes, que seja aplicado processo disciplinar formal, implantado e comunicado, para tomar ações contra os stakeholders que tenham cometido uma violação de segurança da informação?	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
8 – Após o encerramento do contrato ou da exoneração do servidor com o órgão, a política explicita que as responsabilidades e obrigações contidas, permaneçam válidas evitando impacto para a segurança da informação?	**Não**	**Não**	**Não**	**Sim**	**Não**	**Não**	**Não**	**Não**	**Não**	**Não**

Fonte: Adaptado da ISO 27002:2013

Gráfico 1 – Análise dos critérios gerais dos Ministérios



Fonte: Elaborado pelo autor do trabalho

Para a análise do referido estudo foram necessárias as POSICS de 10 (dez) órgãos da administração pública federal direta, onde os ministérios foram escolhidos de modo aleatório dentre os 22 órgãos atualmente existentes na administração pública federal direta após recente mudança.

1. Ministério do Meio Ambiente – MMA

Conforme previsto na portaria 154, de 2 de Maio DE 2014 do Ministério do Meio Ambiente que institui a Política de Segurança da Informação e Comunicação deste órgão foi possível a análise segundo os critérios adotados em consonância com a ISO/IEC 27002:2013.

Tabela 2 – Análise dos critérios MMA

Requisitos essenciais na prevenção da engenharia social	**MMA**
1 – A política define que no processo de contratação de serviços terceirizados, a empresa valide se os funcionários contratados são pessoas de confiança e reputação ilibada, para desempenhar os papéis, principalmente se for papel crítico?	**Não**
2 - A política de segurança sinaliza que todos os funcionários sejam eles contratados ou concursados, que tenham acesso a informações sensíveis, assinem um termo de confidencialidade ou de não divulgação, antes de ser dado acesso aos serviços de TI?	**Item 2 , XII**
3 - A política propõe meios de divulgação, que instrui o usuário a utilizar métodos mais rigorosos de autenticação com senhas fortes e alteração de senhas periodicamente?	**Não**
4 - A política de segurança propõe um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de segurança da informação?	**Art. 13**
5 – A política instrui à direção que seus stakeholders tenham habilidades e qualificações apropriadas e sejam treinados regularmente?	**Não**
6 - A política exige que sejam planejadas e executadas com frequência, divulgação e treinamento de conscientização dos perigos iminentes da engenharia social aos seus usuários?	**Art.11, IX**
7 – A política prevê em suas diretrizes, que seja aplicado processo disciplinar formal, implantado e comunicado, para tomar ações contra os stakeholders que tenham cometido uma violação de segurança da informação?	**Art. 8**
8 – Após o encerramento do contrato ou da exoneração do servidor com o órgão, a política explicita que as responsabilidades e obrigações contidas, permaneçam válidas evitando impacto para a segurança da informação?	**Não**

Segue abaixo a análise por item deste órgão:

1. O primeiro critério não é citado em nenhum momento na POSIC do órgão.
2. Os agentes, além do termo de confidencialidade, só obterão acesso a informações sigilosas que são indispensáveis ao seu trabalho e necessitam de autorização de sua chefia imediata e do gestor das informações para tal recurso.
3. A norma cita sobre a credenciais de acesso que envolve a senha do usuário, mas não deixa explícito sobre a necessidade de divulgação dos cuidados com estes. Proíbe o seu mal uso para fins ilícitos como acessar indevidamente dados, sistemas ou redes.
4. Apesar de o texto não deixar claro que o usuário deverá possuir um meio de notificar eventuais incidentes de segurança, foi considerado para esta análise,

por constar em seu artigo 13 que a ETIR – Equipe de Tratamento e Resposta a Incidentes a segurança em Rede Computacionais deve continuar operando no âmbito do MMA.

5. Foi considerado apto o critério de número 5, pois a POSIC propõe promover a cultura da segurança da informação e comunicações elaborando e implementando programas capazes de conscientizar e capacitar o recurso humano de acordo a com os objetivos da política.
6. A política cita alguns meios dos quais são preventivos para a segurança da informação, mas não propõe diretrizes que oriente os usuários quanto aos riscos iminentes da engenharia social.
7. É proposto medidas de punição para os agentes que descumprir ou violar a integridade, confidencialidade, autenticidade e disponibilidade da informação.
8. O texto cita a intervenção da permissão dos acessos de imediato que este possuir porém não deixa claro a importância de manter sigilo das informações após o encerramento do vínculo do agente com o MMA.

2. Ministério do Planejamento Desenvolvimento e Gestão/Secretaria de Orçamento Federal – MP/SOF

Conforme previsto na portaria Nº 27, de 3 de fevereiro de 2012 do Ministério do Planejamento Desenvolvimento e Gestão (antigo Ministério do Planejamento Orçamento e Gestão) que institui a Política de Segurança da Informação e Comunicação em conjunto com a cartilha SIC deste órgão foi possível a análise segundo os critérios adotados em consonância com a ISO/IEC 27002:2013.

Tabela 3 – Análise dos critérios MP

Requisitos essenciais na prevenção da engenharia social	MP
1 – A política define que no processo de contratação de serviços terceirizados, a empresa valide se os funcionários contratados são pessoas de confiança e reputação ilibada, para desempenhar os papéis, principalmente se for papel crítico?	**Não**
2 - A política de segurança sinaliza que todos os funcionários sejam eles contratados ou concursados, que tenham acesso a informações sensíveis, assinem um termo de confidencialidade ou de não divulgação, antes de ser dado acesso aos serviços de TI?	**Art. 32**
3 - A política propõe meios de divulgação, que instrui o usuário a utilizar métodos mais rigorosos de autenticação com senhas fortes e alteração de senhas periodicamente?	**Cartilha ***
4 - A política de segurança propõe um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de segurança da informação?	**Art. 85, IV**
5 – A política instrui à direção que seus stakeholders tenham habilidades e qualificações apropriadas e sejam treinados regularmente?	**Não**
6 - A política exige que sejam planejadas e executadas com frequência, divulgação e treinamento de conscientização dos perigos iminentes da engenharia social aos seus usuários?	**Art. 39 e cartilha sic baseada na posic**
7 – A política prevê em suas diretrizes, que seja aplicado processo disciplinar formal, implantado e comunicado, para tomar ações contra os stakeholders que tenham cometido uma violação de segurança da informação?	**Art. 82**
8 – Após o encerramento do contrato ou da exoneração do servidor com o órgão, a política explicita que as responsabilidades e obrigações contidas, permaneçam válidas evitando impacto para a segurança da informação?	**Não**

Segue abaixo a análise por item deste órgão:

1. O MP de acordo com a análise, não exige a verificação de boa reputação e conduta de seus colaboradores terceirizados.
2. O termo de sigilo é obrigatório aos que possuem acesso aos ativos de informação além de solicitado o aceite do termo de responsabilidade.
3. Baseada na POSIC o MP elaborou cartilha que instrui seus usuários a utilizarem senhas fortes, além de informar para que sejam diferenciadas credenciais de senhas para os seus acessos, também alerta para que as senhas sejam alteradas com frequência.

4. A ETIR é o canal de notificação de incidentes e orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;
5. Não é declarado no escopo desta POSIC a exigência de qualificações profissionais e treinamentos de seus stakeholders.
6. Este item foi considerado em virtude da cartilha SIC – Segurança da Informação e Comunicação elaborada para seus usuários em que conceitua a engenharia social e alerta para seus perigos iminentes além de ser exigido o dever de estabelecer processos de conscientização, capacitação e sensibilização em segurança da informação conforme orienta a POSIC.
7. A política prevê em suas diretrizes punição em caso de violação dos ativos da informação.
8. É solicitado por meio da POSIC o cancelamento dos acessos que o stakeholder possuía no ato desligamento do agente público, porém, não orienta, sobre a manutenabilidade do sigilo das informações das quais obteve, devido o seu papel, mesmo após a extinção do vínculo empregatício.

3. Ministério da Fazenda – MF

Conforme previsto na portaria Nº 170, de 17 de abril de 2014 do Ministério da Fazenda que institui a Política de Segurança da Informação e Comunicação deste órgão, foi possível a análise segundo os critérios adotados em consonância com a ISO/IEC 27002:2013.

Tabela 4 – Análise dos critérios MF

Requisitos essenciais na prevenção da engenharia social	**MF**
1 – A política define que no processo de contratação de serviços terceirizados, a empresa valide se os funcionários contratados são pessoas de confiança e reputação ilibada, para desempenhar os papéis, principalmente se for papel crítico?	**Não**
2 - A política de segurança sinaliza que todos os funcionários sejam eles contratados ou concursados, que tenham acesso a informações sensíveis, assinem um termo de confidencialidade ou de não divulgação, antes de ser dado acesso aos serviços de TI?	**Art. 12**
3 - A política propõe meios de divulgação, que instrui o usuário a utilizar métodos mais rigorosos de autenticação com senhas fortes e alteração de senhas periodicamente?	**Não**
4 - A política de segurança propõe um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de segurança da informação?	**Art. 22**
5 – A política instrui à direção que seus stakeholders tenham habilidades e qualificações apropriadas e sejam treinados regularmente?	**Art. 17**
6 - A política exige que sejam planejadas e executadas com frequência, divulgação e treinamento de conscientização dos perigos iminentes da engenharia social aos seus usuários?	**Não**
7 – A política prevê em suas diretrizes, que seja aplicado processo disciplinar formal, implantado e comunicado, para tomar ações contra os stakeholders que tenham cometido uma violação de segurança da informação?	**Art. 30**
8 – Após o encerramento do contrato ou da exoneração do servidor com o órgão, a política explicita que as responsabilidades e obrigações contidas, permaneçam válidas evitando impacto para a segurança da informação?	**Não**

Segue abaixo a análise por item deste órgão:

1. A POSIC do ministério da fazenda não explicita a necessidade de verificação de vida pregressa de seus agentes públicos.
2. É exigido o termo de confidencialidade ressaltando ainda a obrigatoriedade de constar nos editais de licitação, nos contratos ou acordos de cooperação técnica com entidades prestadoras de serviços para a SPOA/MF, cláusula específica de atendimento às diretrizes da POSIC.
3. Entre as diretrizes da POSIC, não é citada a orientação de senhas fortes ou coisa que o valha.

4. A ETIR tem a responsabilidade de receber, analisar e responder a notificações e atividades que deve ser mantida pela coordenação geral de tecnologia da informação.
5. Foi considerado apto o item 5 por constar entre as diretrizes a adoção de processo permanente de divulgação, sensibilização, conscientização e capacitação dos agentes públicos sobre os cuidados e deveres com a segurança da informação e comunicações.
6. A engenharia social não é abordada entre as diretrizes desta POSIC, ficando a orientação quanto aos riscos de forma generalizada da SIC.
7. O MF em suas diretrizes propõe processo disciplinar para atos que violem a POSIC assegurando o contraditório e ampla defesa.
8. Falta o comprometimento por parte do agente de manter o sigilo dos ativos da informação após o encerramento do vínculo empregatício.

4. Ministério da Defesa - MD

Conforme previsto na portaria Nº 1.530 /MD, de 14 de maio de 2013 do Ministério da Defesa que institui a Política de Segurança da Informação e Comunicação deste órgão, foi possível a análise segundo os critérios adotados em consonância com a ISO/IEC 27002:2013.

Tabela 5 – Análise dos critérios MD

Requisitos essenciais na prevenção da engenharia social	MD
1 – A política define que no processo de contratação de serviços terceirizados, a empresa valide se os funcionários contratados são pessoas de confiança e reputação ilibada, para desempenhar os papéis, principalmente se for papel crítico?	**Item 5.16.3**
2 - A política de segurança sinaliza que todos os funcionários sejam eles contratados ou concursados, que tenham acesso a informações sensíveis, assinem um termo de confidencialidade ou de não divulgação, antes de ser dado acesso aos serviços de TI?	**Item 5.16.1**
3 - A política propõe meios de divulgação, que instrui o usuário a utilizar métodos mais rigorosos de autenticação com senhas fortes e alteração de senhas periodicamente?	**Não**
4 - A política de segurança propõe um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de segurança da informação?	**Item 5.4.1**
5 – A política instrui à direção que seus stakeholders tenham habilidades e qualificações apropriadas e sejam treinados regularmente?	**Item 5.1.1**
6 - A política exige que sejam planejadas e executadas com frequência, divulgação e treinamento de conscientização dos perigos iminentes da engenharia social aos seus usuários?	**Não**
7 – A política prevê em suas diretrizes, que seja aplicado processo disciplinar formal, implantado e comunicado, para tomar ações contra os stakeholders que tenham cometido uma violação de segurança da informação?	**Item 6.1 e 6.2**
8 – Após o encerramento do contrato ou da exoneração do servidor com o órgão, a política explicita que as responsabilidades e obrigações contidas, permaneçam válidas evitando impacto para a segurança da informação?	**Item 7.6.7**

Segue abaixo a análise por item deste órgão:

1. Foi considerado para esta análise o item 1 positivo, porque vai além do solicitado pelo critério, em suas diretrizes proibi que terceiros atuem em papéis da SIC e da infraestrutura de rede de seu órgão.
2. Além do termo de confidencialidade é exigido de acordo com a POSIC que o agente assine o termo de compromisso individual.
3. O texto não deixa explícito a orientação de cuidados com a senha pessoal dos agentes.
4. A ETIR é canal declarado em seu escopo para notificações que envolva a SIC e sua infraestrutura de rede.

5. A POSIC ressalta a importância da capacitação, conscientização e a proteção dos ativos da informação para seus stakeholders.
6. Apesar da análise acima não foi considerado positivo o item 6 por se tratar de forma generalizada e não da engenharia social em específico.
7. O processo disciplinar é requisito importante conforme uma das diretrizes desta POSIC.
8. Cita no item 7.6.7. que em caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, o sigilo das informações e documentos sigilosos em que o agente teve acesso deve ser mantido.

5. Ministério da Justiça – MJ

Conforme previsto na portaria Nº 3.530, de 3 de dezembro de 2013 do Ministério da Justiça que institui a Política de Segurança da Informação e Comunicação deste órgão, foi possível a análise segundo os critérios adotados em consonância com a ISO/IEC 27002:2013.

Tabela 6 – Análise dos critérios MJ

Requisitos essenciais na prevenção da engenharia social	**MJ**
1 – A política define que no processo de contratação de serviços terceirizados, a empresa valide se os funcionários contratados são pessoas de confiança e reputação ilibada, para desempenhar os papéis, principalmente se for papel crítico?	**Não**
2 - A política de segurança sinaliza que todos os funcionários sejam eles contratados ou concursados, que tenham acesso a informações sensíveis, assinem um termo de confidencialidade ou de não divulgação, antes de ser dado acesso aos serviços de TI?	**Não**
3 - A política propõe meios de divulgação, que instrui o usuário a utilizar métodos mais rigorosos de autenticação com senhas fortes e alteração de senhas periodicamente?	**Não**
4 - A política de segurança propõe um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de segurança da informação?	**Art. 4, II**
5 – A política instrui à direção que seus stakeholders tenham habilidades e qualificações apropriadas e sejam treinados regularmente?	**Art. 9 par. único**
6 - A política exige que sejam planejadas e executadas com frequência, divulgação e treinamento de conscientização dos perigos iminentes da engenharia social aos seus usuários?	**Não**
7 – A política prevê em suas diretrizes, que seja aplicado processo disciplinar formal, implantado e comunicado, para tomar ações contra os stakeholders que tenham cometido uma violação de segurança da informação?	**Art. 5**
8 – Após o encerramento do contrato ou da exoneração do servidor com o órgão, a política explicita que as responsabilidades e obrigações contidas, permaneçam válidas evitando impacto para a segurança da informação?	**Não**

Segue abaixo a análise por item deste órgão:

1. Não é declarada a exigência de verificação da conduta e antecedentes para seus agentes;
2. O termo de confidencialidade não é exigível para os papéis críticos da SIC;
3. A POSIC não propõe meios de divulgação preventiva dos cuidados com os acessos (senhas);
4. O MJ cita em suas diretrizes manter equipe de tratamento e resposta a incidentes em redes computacionais como canal de notificação de incidentes;
5. A POSIC atribui em suas diretrizes que os membros da ETIR tenha perfil técnico adequado para atuar em seus papéis;

6. Não é proposto na POSIC meios de conscientização dos perigos iminentes da engenharia social;
7. A política prevê sanções administrativas no caso de violação de sigilo das informações;
8. Não de cunho obrigatório manter sigilo das informações obtidas enquanto que agente público no caso de extinção do vínculo com o órgão.

6. Ministério da Educação – MEC

Conforme previsto na portaria Nº 1054 , de 02 de agosto de 2011 do Ministério da Educação que institui a Política de Segurança da Informação e Comunicação deste órgão, foi possível a análise segundo os critérios adotados em consonância com a ISO/IEC 27002:2013.

Tabela 7 – Análise dos critérios MEC

Requisitos essenciais na prevenção da engenharia social	**MEC**
1 – A política define que no processo de contratação de serviços terceirizados, a empresa valide se os funcionários contratados são pessoas de confiança e reputação ilibada, para desempenhar os papéis, principalmente se for papel crítico?	**Não**
2 - A política de segurança sinaliza que todos os funcionários sejam eles contratados ou concursados, que tenham acesso a informações sensíveis, assinem um termo de confidencialidade ou de não divulgação, antes de ser dado acesso aos serviços de TI?	**Art. 13**
3 - A política propõe meios de divulgação, que instrui o usuário a utilizar métodos mais rigorosos de autenticação com senhas fortes e alteração de senhas periodicamente?	**Não**
4 - A política de segurança propõe um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de segurança da informação?	**Art. 23**
5 – A política instrui à direção que seus stakeholders tenham habilidades e qualificações apropriadas e sejam treinados regularmente?	**Art.18**
6 - A política exige que sejam planejadas e executadas com frequência, divulgação e treinamento de conscientização dos perigos iminentes da engenharia social aos seus usuários?	**Não**
7 – A política prevê em suas diretrizes, que seja aplicado processo disciplinar formal, implantado e comunicado, para tomar ações contra os stakeholders que tenham cometido uma violação de segurança da informação?	**Art. 31**
8 – Após o encerramento do contrato ou da exoneração do servidor com o órgão, a política explicita que as responsabilidades e obrigações contidas, permaneçam válidas evitando impacto para a segurança da informação?	**Não**

Segue abaixo a análise por item deste órgão:

1. Não é exigida a verificação de conduta e antecedentes;
2. Entre suas diretrizes há a exigibilidade de assinatura do termo de confidencialidade;
3. A política não propõe meios de divulgação de prevenção quanto a autenticação dos acessos que o agente possui;
4. É de responsabilidade da Diretoria de Tecnologia da Informação a manter o canal de notificação;
5. Não há exigência de qualificação técnica para os agentes críticos;
6. Não é proposto orientação de treinamento e conscientização dos perigos iminentes da engenharia social;
7. A POSIC prevê penalidades em caso de descumprimento as diretrizes propostas;
8. Não há obrigatoriedade do comprometimento de manter o sigilo das informações após a no ato da exoneração;

7. Ministério do Desenvolvimento, Indústria e Comércio Exterior – MDIC

Conforme previsto na portaria Nº 4, de 23 de janeiro de 2013 do Ministério do Desenvolvimento, Indústria e Comércio Exterior que institui a Política de Segurança da Informação e Comunicação deste órgão, foi possível a análise segundo os critérios adotados em consonância com a ISO/IEC 27002:2013.

Tabela 8 – Análise dos critérios MDIC

Requisitos essenciais na prevenção da engenharia social	**MDIC**
1 – A política define que no processo de contratação de serviços terceirizados, a empresa valide se os funcionários contratados são pessoas de confiança e reputação ilibada, para desempenhar os papéis, principalmente se for papel crítico?	**Não**
2 - A política de segurança sinaliza que todos os funcionários sejam eles contratados ou concursados, que tenham acesso a informações sensíveis, assinem um termo de confidencialidade ou de não divulgação, antes de ser dado acesso aos serviços de TI?	**Não**
3 - A política propõe meios de divulgação, que instrui o usuário a utilizar métodos mais rigorosos de autenticação com senhas fortes e alteração de senhas periodicamente?	**Não**
4 - A política de segurança propõe um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de segurança da informação?	**Art. 13**
5 – A política instrui à direção que seus stakeholders tenham habilidades e qualificações apropriadas e sejam treinados regularmente?	**Art. 10**
6 - A política exige que sejam planejadas e executadas com frequência, divulgação e treinamento de conscientização dos perigos iminentes da engenharia social aos seus usuários?	**Não**
7 – A política prevê em suas diretrizes, que seja aplicado processo disciplinar formal, implantado e comunicado, para tomar ações contra os stakeholders que tenham cometido uma violação de segurança da informação?	**Art. 14**
8 – Após o encerramento do contrato ou da exoneração do servidor com o órgão, a política explicita que as responsabilidades e obrigações contidas, permaneçam válidas evitando impacto para a segurança da informação?	**Não**

Segue abaixo a análise por item deste órgão:

1. Não é citado em suas diretrizes a necessidade de verificação de conduta e antecedentes do agente;
2. A política cita a responsabilidade que o agente deve ter com suas credenciais, porém não deixa explícito a necessidade de aditamento do termo de confidencialidade.
3. Há uma preocupação com as credenciais, mas não há uma divulgação da adoção de senhas fortes e os cuidados com esta;
4. A política determina que o canal exclusivo de notificação do órgão seja a ETIR;

5. Entre as diretrizes está proposto a educação contínua em que os colaboradores devem ser capacitados nos procedimentos de segurança e no uso correto dos ativos de informação;
6. Não é previsto nesta POSIC divulgação de prevenção dos perigos iminentes da SIC em específico da Engenharia Social.
7. A política alerta que a não observância do disposto na POSIC acarretará penalidades administrativa, civil e penal, após apuração;
8. A POSIC não obriga assinar termo de garantia da segurança da informação após extinção do contrato.

8. Ministério da Agricultura Pecuária e Abastecimento – MAPA

Conforme previsto na portaria Nº 795, de 5 de setembro de 2012 do Ministério da Agricultura Pecuária e Abastecimento que institui a Política de Segurança da Informação e Comunicação deste órgão, foi possível a análise segundo os critérios adotados em consonância com a ISO/IEC 27002:2013.

Tabela 9 – Análise dos critérios MAPA

Requisitos essenciais na prevenção da engenharia social	MAPA
1 – A política define que no processo de contratação de serviços terceirizados, a empresa valide se os funcionários contratados são pessoas de confiança e reputação ilibada, para desempenhar os papéis, principalmente se for papel crítico?	**Não**
2 - A política de segurança sinaliza que todos os funcionários sejam eles contratados ou concursados, que tenham acesso a informações sensíveis, assinem um termo de confidencialidade ou de não divulgação, antes de ser dado acesso aos serviços de TI?	**Art. 5.4.5**
3 - A política propõe meios de divulgação, que instrui o usuário a utilizar métodos mais rigorosos de autenticação com senhas fortes e alteração de senhas periodicamente?	**Não**
4 - A política de segurança propõe um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de segurança da informação?	**Art. 5.4.5**
5 – A política instrui à direção que seus stakeholders tenham habilidades e qualificações apropriadas e sejam treinados regularmente?	**Item 5.7 e 5.22.1**
6 - A política exige que sejam planejadas e executadas com frequência, divulgação e treinamento de conscientização dos perigos iminentes da engenharia social aos seus usuários?	**Não**
7 – A política prevê em suas diretrizes, que seja aplicado processo disciplinar formal, implantado e comunicado, para tomar ações contra os stakeholders que tenham cometido uma violação de segurança da informação?	**Item 7**
8 – Após o encerramento do contrato ou da exoneração do servidor com o órgão, a política explicita que as responsabilidades e obrigações contidas, permaneçam válidas evitando impacto para a segurança da informação?	**Não**

Segue abaixo a análise por item deste órgão:

1. Não está definido que os agentes públicos tenham bons antecedentes nesta política;
2. É concedido o acesso a informação a seus agentes, após assinatura de termo de confidencialidade e responsabilidade de acordo com suas atribuições;
3. O texto não explicita a orientação de divulgação de prevenção de riscos com as credenciais de acesso;
4. A gestão de segurança da informação e a chefia imediata do agente são os meios de notificação segundo a política;
5. É estabelecido pela POSIC que os agentes envolvidos com segurança possuam qualificações técnicas e sejam capacitados regularmente;

6. Apesar de constar na POSIC a divulgação e treinamento sobre as diretrizes da SIC para seus agentes, o texto não abrange a engenharia social;

7. Há diretriz ressaltando que no caso de infringidas as normas declaradas nesta POSIC será acarretada penalidades de acordo com a Constituição, Código Civil e Penal, Lei 8112 e normas correlatas.

8. O texto orienta que o agente ao afastar-se ou desligar-se de suas atribuições deverá ser cancelado seus acessos e preenchido termo de desligamento, porém, não há termo definido para manter sigilo das informações de SIC.

9. Ministério da Saúde

Conforme previsto na portaria Nº 3.207, de 20 de outubro de 2010 do Ministério da Saúde que institui a Política de Segurança da Informação e Comunicação deste órgão, foi possível a análise segundo os critérios adotados em consonância com a ISO/IEC 27002:2013.

Tabela 10 – Análise dos critérios MS

Requisitos essenciais na prevenção da engenharia social	**MS**
1 – A política define que no processo de contratação de serviços terceirizados, a empresa valide se os funcionários contratados são pessoas de confiança e reputação ilibada, para desempenhar os papéis, principalmente se for papel crítico?	**Não**
2 - A política de segurança sinaliza que todos os funcionários sejam eles contratados ou concursados, que tenham acesso a informações sensíveis, assinem um termo de confidencialidade ou de não divulgação, antes de ser dado acesso aos serviços de TI?	**Não**
3 - A política propõe meios de divulgação, que instrui o usuário a utilizar métodos mais rigorosos de autenticação com senhas fortes e alteração de senhas periodicamente?	**Não**
4 - A política de segurança propõe um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de segurança da informação?	**Art. 15**
5 – A política instrui à direção que seus stakeholders tenham habilidades e qualificações apropriadas e sejam treinados regularmente?	**Art. 8 e 12**
6 - A política exige que sejam planejadas e executadas com frequência, divulgação e treinamento de conscientização dos perigos iminentes da engenharia social aos seus usuários?	**Não**
7 – A política prevê em suas diretrizes, que seja aplicado processo disciplinar formal, implantado e comunicado, para tomar ações contra os stakeholders que tenham cometido uma violação de segurança da informação?	**Art. 18**

8 – Após o encerramento do contrato ou da exoneração do servidor com o órgão, a política explicita que as responsabilidades e obrigações contidas, permaneçam válidas evitando impacto para a segurança da informação?	**Não**

Segue análise dos itens desta POSIC:

1. O texto não deixa explícito a orientação de bons antecedentes aos seus contratados;
2. Não há a exigibilidade na POSIC de aderir ao termo de confidencialidade, citando apenas sobre o termo de responsabilidade;
3. Não há diretriz que informe sobre a adoção de medidas preventivas quanto as credenciais de acesso do agente público;
4. Cabe ao Departamento de Informática do SUS (DATASUS) tratar a notificações sobre os incidentes que afetam a segurança dos ativos ou o descumprimento da POSIC/MS;
5. Este item foi considerado positivo por considerar que os gestores de SIC devem receber capacitação especializada além de ser difundido aos agentes públicos processo permanente de conscientização em segurança da informação;
6. Apesar do item anterior ser positivo, não há aprofundamento da conscientização do tema engenharia social, por isso para esta análise foi considerado como negativo;
7. A política prevê penalidades para o descumprimento das diretrizes impostas para o MS, além de suspensão temporária ou permanente dos privilégios de acesso;
8. Não há clausula que oriente a continuidade do sigilo dos ativos de informação após cancelamento do vínculo com o MS.

10. Ministério do Trabalho e Emprego – MTE

Conforme previsto na portaria Nº 1.047, DE 16 DE JULHO DE 2013 do Ministério do Trabalho e Emprego que institui a Política de Segurança da Informação e Comunicação deste órgão, foi possível a análise segundo os critérios adotados em consonância com a ISO/IEC 27002:2013.

Tabela 11 – Análise dos critérios MTE

Requisitos essenciais na prevenção da engenharia social	MTE
1 – A política define que no processo de contratação de serviços terceirizados, a empresa valide se os funcionários contratados são pessoas de confiança e reputação ilibada, para desempenhar os papéis, principalmente se for papel crítico?	**Não**
2 - A política de segurança sinaliza que todos os funcionários sejam eles contratados ou concursados, que tenham acesso a informações sensíveis, assinem um termo de confidencialidade ou de não divulgação, antes de ser dado acesso aos serviços de TI?	**Art. 33, IV**
3 - A política propõe meios de divulgação, que instrui o usuário a utilizar métodos mais rigorosos de autenticação com senhas fortes e alteração de senhas periodicamente?	**Cartilha***
4 - A política de segurança propõe um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de segurança da informação?	**Art. 20**
5 – A política instrui à direção que seus stakeholders tenham habilidades e qualificações apropriadas e sejam treinados regularmente?	**Art. 13**
6 - A política exige que sejam planejadas e executadas com frequência, divulgação e treinamento de conscientização dos perigos iminentes da engenharia social aos seus usuários?	**Não**
7 – A política prevê em suas diretrizes, que seja aplicado processo disciplinar formal, implantado e comunicado, para tomar ações contra os stakeholders que tenham cometido uma violação de segurança da informação?	**Art. 31 e 32**
8 – Após o encerramento do contrato ou da exoneração do servidor com o órgão, a política explicita que as responsabilidades e obrigações contidas, permaneçam válidas evitando impacto para a segurança da informação?	**Não**

Segue análise dos itens desta POSIC:

1. Entre as diretrizes do MTE não está imposta dever de verificação de vida pregressa dos agentes públicos desempenhados para os papéis de SIC. Ressalta apenas que os colaboradores dos contratos tenham conhecimento da POSIC;

2. A política impõe que é dever dos usuários do MTE assinar o termo de confidencialidade e outros que venham a ser instituídos por normas ou procedimentos decorrentes da POSIC;
3. Este item foi considerado levando-se em conta a divulgação exposta na cartilha SIC elaborada a partir desta POSIC.
4. É de responsabilidade da ETIR receber e tratar as notificações do órgão;
5. A política instrui sobre processo permanente de divulgação, sensibilização, conscientização e capacitação dos usuários para os cuidados e deveres relacionados à segurança da informação e comunicações.
6. Apesar do item anterior ser positivo, o tema engenharia social não é destacado entre as diretrizes da POSIC e nem na cartilha;
7. A política prevê processo disciplinar formal para violação da POSIC;
8. Não há documento específico que obrigue o ex-agente a manter o sigilo dos ativos de informação no MTE.

4.2 Análise consolidada das informações

Foi realizada análise individual dos ministérios e em seguida dos dois grupos formados de acordo com a hierarquia governamental.

De acordo com a análise, apenas o MD obteve mais critérios positivos contemplando 80% dos 8 critérios na POSIC, em contrapartida, 3 (três) só obtiveram a média de 50% dos critérios correspondidos, 2 ficaram na média de 70% e 4 quase a metade dos órgãos analisados obtiveram média de 60%.

Apenas um órgão inseriu no contexto da cartilha (adaptada da POSIC) o tema engenharia social, sendo os outros atuantes de forma preventiva mais generalizadas quanto a SIC.

Outro critério de suma relevância é o item 1 em que apenas o MD formulou diretriz taxativa de proibição de terceiros atuando nos papéis críticos da instituição agindo assim como forma preventiva, neste caso este não houve ressalva de aceitação.

Os dados informados na tabela abaixo foram baseados na quantidade de itens do questionário da análise pela quantidade de itens positivos geral de cada ministério.

Tabela 12 – Análise consolidada

Classificação	Ministério	Porcentagem	Subtotal
Estratégicos	MP	60%	55%
	MF	50%	
Sociais	MAPA	50%	51,25
	MTE	60%	
	MS	40%	
	MDIC	40%	
	MMA	50%	
	MD	80%	
	MJ	40%	
	MEC	50%	
Total			**53,13**

Fonte: Dados fictícios, apenas para fins ilustrativos

Sobre o aspecto geral a análise dos critérios foram divididos em preventivos (itens 1,2,3, 5 e 8) e punitivos (itens 4 e 7). Notou-se que por unanimidade os critérios punitivos atingiram a margem de 100% positivos nos

itens, já os critérios preventivos obtiveram nos itens 1,2 e 5 de 70% acima estruturados nas respectivas POSICs e os itens 3 e 8 ficaram igual ou abaixo da média de 20%.

De fato verifica-se que pouco se adotou as melhores práticas no combate a Engenharia Social e ao mesmo tempo percebe-se que é um termo desconhecido dentro das instituições, não sabendo o quão importante e relevante é este tema para a segurança da informação. Agir preventivamente requer não só cuidados com os controles físicos e lógicos, mas também com o recurso humano, que por imperícia pode ocasionar situações desastrosas e desagradáveis.

CONCLUSÃO

A proposta deste trabalho conforme informado no início não agrega valor para a governança de TI, é um tema centrado na ação seja ela protetiva ou corretiva no combate a Engenharia Social.

De acordo com o problema que era: quais os recursos utilizados na estratégia da governança de tecnologia da informação para inibir a ação de engenheiros sociais nos órgãos públicos federais, as diretrizes agregadas as POSICS abrangem o cuidado da segurança da informação de forma generalizada e utilizam os recursos de proteção das credenciais de acesso na minoria dos órgãos, tem em sua maioria, a preocupação com os termos de confidencialidade dos ativos de informação que os agentes públicos adquirem, há a preocupação em se obter um canal de notificação.

O objetivo geral foi verificar o uso das melhores práticas no combate à Engenharia social nas POSICs dos órgãos da administração pública federal. De acordo com a análise, foi observado que a engenharia social ainda é desconhecida dos órgãos públicos, percebe-se que após a publicação das portarias das POSICs, alguns poucos órgãos criaram cartilhas explicativas, como é o caso do MP que alerta os usuários a respeito da engenharia social e de como criar senhas fortes, (um dos meios de infiltração utilizada pelos engenheiros para obter informações).

Como objetivo específico foram analisadas a aderência das POSICs às melhores práticas tendo identificado que não há divulgação dos perigos iminentes que a engenharia social pode provocar, mais grave ainda, verificou-se que quem atua no ramo da SIC desconhece tal informação ou não dá ênfase ao assunto por falta de capacitação.

Para mitigar os riscos da engenharia social na esfera pública federal é necessário a implementação e implantação de diretrizes com ênfase maior nos fatores críticos que atentam para impedir a atuação de engenheiros sociais na APF, além de treinamentos periódicos fundamentados, para impedir o comprometimento da segurança da informação e da infraestrutura de rede. Esse esforço deve ser em conjunto com o usuário comum que é o elo mais frágil da organização.

REFERÊNCIAS

ALERTA SECURITY. **Risco Vulnerabilidade e Ameaça**. 2015. Disponível em: <http://www.alertasecurity.com.br/blog/153-risco-vulnerabilidade-e-ameaca> Acesso em: 28 mar. 2016.

BEAL A. **Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos ativos de Informação nas organizações**. São Paulo: Atlas, 2005.

BEZERRA, E. K. **Gestão de Riscos de TI NBR 27005**. 2011. Escola Superior de Redes RNP(2013). Disponível em: <http://pt.scribd.com/doc/55387254/Gestao-de-Riscos-de-TI-NBR-27005#fullscreen>. Acesso em: 24 mar. 2016

BRASIL. ABNT NBR ISO/IEC 27002:2013. **Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão de segurança da informação — Requisitos.**

BRASIL. ABNT NBR ISO/IEC 27005:2011 **Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**.

BRASIL. ABNT NBR ISO/IEC 27001:2013. **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos**.

BRASIL. Ministério do Planejamento Orçamento e Gestão. **Segurança da Informação e Comunicação**. Disponível em: <http://www.sisp.gov.br/faq_segurancainformacao/one-faq?faq_id=13941646#13970935 estratégias fundamentais>. Acesso em: 01 abr. 2016

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal**. *Norma Complementar 03*. Disponível em: < http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf>
Acesso em: 02 fev 2016

BRASIL. Presidência da República. Casa Civil. **Lei 12527. Regula o acesso a informação**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm Acesso em: 31 mar. 2016

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Gestão de Etir: Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos Órgãos e Entidades da Administração Pública Federal**. *Norma Complementar 08*. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_8_gestao_etir.pdf>
Acesso em: 06 abr. 2016

CANALTECH. **O que scriptikiddie?** Disponível em: <http://canaltech.com.br/o-que-e/o-que-e/O-que-e-Script-Kiddie/ > Acesso em: 13 abr. 2016

CAMPOS, Gisele. **Competência habilidades em liderança**. Disponível em: <http://pt.slideshare.net/giselecristinacampos/habilidades-em-liderana>. Visto em: 31 mai. 2016

CELEPAR. **Guia para Elaboração de Plano de Contingência**. Metodologia CELEPAR. Disponível em: <www.documentador.pr.gov.br/documentador/pub.do?action=d...> Acesso em: 11 abr. 2016

CERT-BR. **Incidente de Segurança**. Disponível em: <http://www.cert.br/certcc/csirts/csirt_faq-br.html> Acesso em: 05 abr. 2016

CTIR gov. **Sobre o CTIR**. Disponível em <http://www.ctir.gov.br/sobre-CTIR-gov.html> . Visto em: 16 de abr. 2016

DANTAS M. L. **Segurança da Informação: Uma abordagem focada em gestão de riscos**. Disponível em: <http://www.marcusdantas.com.br/files/seguranca_informacao.pdf> 2011. Acesso em: 29 mar. 2016

DIMEP. **Controle de Acesso Físico ou Lógico: Qual é a indicação de cada um**. Disponível em:< http://www.dimep.com.br/blog/sistemas-de-acessos/controle-acesso-fisico-logico-indicacao> Acesso em: 05 abr. 2016

FONTES**,** Edson. **Segurança da Informação**: **o usuário faz a diferença**. São Paulo: Saraiva, 2006. TCEPR. Ciclo PDCA. Disponível em: <http://www1.tce.pr.gov.br/multimidia/2012/11/png/00237966.png> Acesso em 27 Abr 2016.

IZIDORO C. (Org.). **Gestão de Tecnologia e Informação em Logística**. São Paulo**:** Person, 2016

KOCH D. **Tipos de hackers e suas características**. Disponível em: <http://tecnologia.hsw.uol.com.br/cabeca-de-hacker1.htm>. Visto em: 12 de Abr. 2016

LYRA M. R. **Segurança e Auditoria em Sistemas de Informação**. Brasília: Ciência Moderna, 2008.

LYRA, M. R. (Org.). **Governança da Segurança da Informação**. ICPD. Brasília, 2015

MAIA, M. **O que é Segurança da Informação**. Disponível em: <http://segurancadainformacao.modulo.com.br/seguranca-da-informacao> Acesso em: 11 mar. 2016

MEU BIZU. **Tipos de Ataque**. Disponível em: <http://www.meubizu.com.br/tipos-de-ataque-blog> Acesso em: 28 mar. 2016

MITNICK, K. D.; SIMON, W. L. M. **A arte de enganar. Ataques de hackers: Controlando o fator humano na Segurança da Informação**.
PearsonEducation do Brasil Ltda, 2003.

MITNICK, K. D.; SIMON, W. L. M. **A arte de invadir: As verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos**. Pearson Education do Brasil Ltda, 2006.

NOVAES, D. **Gestão por competências**. Disponível em: <http://www.rhportal.com.br/artigos-rh/gesto-por-competncias/>. Visto em: 14 abr 2016.

Portaria nº 1530, de 14/05/13/Ministério da Defesa. **Institui a Política de Segurança da Informação e Comunicações da Administração Central do Ministério da Defesa**. Disponível em: http://www.jusbrasil.com.br/diarios/54405781/dou-secao-1-16-05-2013-pg-33. Acesso em: 01 abr. 2016.

Portaria nº 3.530, de 3/12/2013/Ministério da Justiça. **Institui a Política de Segurança da Informação e Comunicações do Ministério da Justiça**. Disponível em: http://www.jusbrasil.com.br/diarios/62532816/dou-secao-1-04-12-2013-pg-22. Acesso em: 2 mai. 2016

Portaria nº 154, de 02/05/2014/Ministério do Meio Ambiente. **Institui a Política de Segurança da Informação e Comunicação - POSIC, no âmbito do Ministério do Meio Ambiente.** Disponível em: <http://www.mma.gov.br/institucional/tecnologia-da-informacao>. Acesso em: 04 mar. 2016.

Portaria nº 27, DE 03/02/2012 **Ministério do Planejamento Orçamento e Gestão. Institui a Política de Segurança da Informação e Comunicação – PoSIC**

Portaria nº 1047 de 16/07/2013 / MTE - **Ministério do Trabalho e Emprego. Institui a Política de Segurança da Informação e Comunicações – POSIC do Ministério do Trabalho e Emprego**. Disponível em: http://www.diariodasleis.com.br/busca/exibelink.php?numlink=224048. Acesso em: 04 abr. 2016.

Portaria nº 4, de 23/01/2013/**Ministério do Desenvolvimento, Indústria e Comércio Exterior**. **Institui a Política de Segurança da Informação e Comunicações do Ministério do Desenvolvimento, Indústria e Comércio Exterior**. Disponível em: http://www.mdic.gov.br/arquivos/dwnl_1365523897.pdf >Acesso em: 02 mar. 2016.

Portaria nº 3.207, de 20/10/2010/MS- Ministério da Saúde. **Institui a Política de Segurança da Informação e Comunicações do Ministério da Saúde**.

Portaria n° 1054, de 02/08/2011/Ministério da Educação e suas alterações. **Política de Segurança da Informação e Comunicações – POSIC do Ministério d a Educação.**

Portaria nº 996 de 06/08/2012. **Política de Segurança da Informação e Comunicações - POSIC do Ministério da Educação – MEC**.

Portaria nº 795, de 5/09/12/Ministério da Agricultura. **Política de Segurança da Informação e Comunicações do Ministério da Agricultura, Pecuária e Abastecimento.**

Portaria nº 170, DE 17/04/ 2014/Ministério da Fazenda. **Política de Segurança da Informação e Comunicações do Ministério da Fazenda.**

PURICELLI R. **Engenharia Social: Uma Ameaça Subestimada na Governança e Gestão de Segurança de TI**, Isaca25 journal p.3

PURSER, S. **Pessoas são o maior desafio a segurança da informação**. Disponível em : <http://olhardigital.uol.com.br/fique_seguro/noticia/pessoas_sao_maior_desafio_a_seguranca_da_informacao_nas_empresas/18752> Visto em: 31 mai. 2016

RIBEIRO M. S. **Engenharia Social: uma ameaça silenciosa nas** empresas. Disponível em: <http://enigmaconsultoria.com.br/engenharia-social-uma-ameaca-silenciosa-nas-empresas-27fev14/> Acesso em: 17 abr. 2016

SILVA, C. C. **Trabalhando com redes de computadores** Conceito e Prática. São Paulo: Viena, 2010

SILVA FILHO, A. M. **Entendendo e Evitando a Engenharia Social: Protegendo Sistemas e Informações**. Disponível em: <http://www.espacoacademico.com.br/043/43amsf.htm> Acesso em: 01 out. 2015.

SOUSA F. C. C. **Gerenciamento do ciclo de vida da informação**. CONTECSI. 3º Congresso Internacional de Gestão da Tecnologia e Sistemas de Informação. Disponível em: <http://www.contecsi.fea.usp.br/envio/index.php/contecsi/3contecsi/paper/viewFile/2019/1133> Acesso em: 06 abr. 2016

SOUZA R. M. **O Fator Humano.** Disponível em: <http://blog.segr.com.br/o-fator-humano/> Figura 5. Acesso em: 11 abr. 2016

UFRJ TIC. **Incidentes de Segurança da Informação**. Disponível em: <http://www.tic.ufrj.br/index.php/o-que-sao-incidentes> Acesso em: 30 mar. 2016