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

RICARDO BRUNO BREUSTEDT

SEGURANÇA DA INFORMAÇÃO COM ÊNFASE NA CONSCIENTIZAÇÃO DE USUÁRIOS DE REDE

Brasília - DF
2017

RICARDO BRUNO BREUSTEDT

SEGURANÇA DA INFORMAÇÃO COM ÊNFASE NA CONSCIENTIZAÇÃO DE USUÁRIOS DE REDE

Trabalho acadêmico apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção do Certificado de Conclusão do curso de Pós-Graduação *Lato-Sensu* em Redes de Computadores com Ênfase em Segurança.

Orientador: Prof. Me. Gilberto Netto

Brasília - DF
2017

RICARDO BRUNO BREUSTEDT

SEGURANÇA DA INFORMAÇÃO COM ÊNFASE NA CONSCIENTIZAÇÃO DE USUÁRIOS DE REDE

Trabalho acadêmico apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção do Certificado de Conclusão do curso de Pós-Graduação *Lato-Sensu* em Redes de Computadores com Ênfase em Segurança.

Orientador: Prof. Me. Gilberto Netto

Brasília, ___ de _____ de 2017.

Banca Examinadora

_____

Prof. Dr. Nome completo

_____

Prof. Dr. Nome completo

Agradecimentos

A Deus, por me permitir alcançar novos objetivos, me dar força e persistência para vencer as batalhas de cada dia;

Aos meus pais, pela educação e ensinamentos necessários à construção do meu caráter;

À minha namorada Nathalia, mulher de fé, amorosa, companheira em todos os momentos e compreensiva;

Ao meu amigo Marcos Medeiros, por me motivar a continuar e ajudar nos dias de estudo na biblioteca;

Ao meu orientador, Prof. Gilberto de Oliveira Netto, por ter me direcionado, por acreditar em minha capacidade e pela competente orientação.

RESUMO

O presente trabalho destina-se a estudar uma proposta para tornar o sistema de segurança da informação de um órgão público mais seguro, com ênfase na conscientização de usuários de rede. Ao contextualizar o assunto em âmbito nacional, é notável a necessidade de aprimoramento dessa área nos órgãos da Administração Pública Federal (APF), os quais vem sendo direcionados por legislações e órgãos encarregados pela garantia da segurança da informação. A informação está inserida num contexto muito amplo e seu valor deve ser revisado periodicamente, uma vez que o uso de papéis vem reduzindo drasticamente e mais dados trafegam na rede, com a ausência da confidencialidade, disponibilidade ou integridade das informações, é possível haver grandes prejuízos para a execução de atividades necessárias à finalidade a que o órgão se destina. Há diversas ferramentas para se aprimorar o Sistema de Gestão de Segurança da Informação (SGSI) em ambientes corporativos, a NBR ISO/IEC 27.002:2013 permite um estudo mais a fundo para se planejar, implementar, fiscalizar e executar os procedimentos de segurança em todos os setores do órgão, bem como medidas de controle e técnicas para cada ativo. A pesquisa busca demonstrar no contexto da segurança da informação que a responsabilidade pelas informações do órgão não é exclusiva do setor de tecnologia da informação, mas de todos os funcionários, tendo em vista que as informações exigem tratamentos e armazenamentos adequados para que sejam preservadas, onde se faz necessária a criação de alguns hábitos e procedimentos proativos dos *stakeholders* para a garantia da segurança dos dados, o que pode ser feito mediante palestras e divulgações de cartilhas por diversos locais do ambiente de trabalho. Visa, ainda, analisar o contexto de Segurança da Informação de um setor de licitações num Órgão Público, avaliando o comportamento dos funcionários diante de situações hipotéticas, conscientizar os usuários de rede mediante palestra, orientando sobre boas práticas para preservar a segurança das informações e verificar os resultados obtidos pela conscientização através de questionário. Demonstrar, através do estudo de caso, se o método de conscientização afetou o tratamento com as informações manipuladas pelo setor.

Palavras-chave: Segurança da informação. Conscientização de usuários. Administração Pública Federal. Sistema de Gestão de Segurança da Informação. NBR ISO/IEC 27002:2013.

ABSTRACT

The present work aims to study a proposal to make the information security system of a public agency more secure, with an emphasis on the awareness of network users. When contextualizing the subject in national services, it is remarkable the need to improve our area in the Federal Public Administration (FPA), which are being directed by legislation and bodies in charge of guaranteeing information security. Information is embedded in a very broad context and its value should be reviewed periodically, as the use of paper has been drastically reducing and more data travels on the network, with the absence of confidentiality, availability or integrity of the information, and possible major losses for the execution of activities for the purpose and for the organ is intended. There are a number of tools for the development of Information Security Management System (ISMS) in corporate environments, an ISO / IEC 27.002: 2013 NBR allows further study to plan, implement, monitor, and enforce security procedures in all the sectors of the body, as well as control measures and techniques for each asset. The research seeks to demonstrate in the context of information security that the responsibility for the information of the organ is not exclusive to the information technology sector, but of all the employees, since the information requires appropriate treatments and storage to be preserved, where it is necessary to create some proactive habits and procedures of stakeholders to ensure data security, which can be done through lectures and booklet releases across various places in the work environment. It also aims to analyze the Information Security context of a public sector biddings sector, evaluating the behavior of employees against hypothetical situations, raising awareness of network users through a lecture, guiding good practices to preserve information security and verifying the results obtained through the questionnaire. Demonstrate, through the case study, whether the awareness method affected the treatment with the information manipulated by the sector.

Keywords: Information security. Awareness of users. Federal Public Administration. Information Security Management System. NBR ISO / IEC 27002: 2013.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE GRÁFICOS

SUMÁRIO

INTRODUÇÃO

O uso, cada vez mais comum, da tecnologia a favor do homem vem facilitando as formas de comunicação interpessoal, facilitando e reduzindo o tempo demandado para transmissão das informações. Nesse contexto, é importante observarmos que há pessoas que utilizam desses recursos de forma mal-intencionada, o que torna necessário estabelecer algumas medidas para assegurar que essas informações transmitidas cheguem ao destino com segurança. Dessa forma, profissionais da área de Segurança da Informação tem trazido novas soluções para garantir uma melhoria nos padrões utilizados pela Tecnologia da Informação.

Não é diferente no cenário público brasileiro, o qual necessita cada vez mais de ferramentas de Tecnologia da Informação, pois divulga dados que exigem publicidade, implementa melhorias nas infraestruturas de redes, novos softwares públicos e sistemas que aprimoram o desempenho dos trabalhos executados pelos funcionários. Grandes volumes de dados são produzidos pelos próprios órgãos e armazenados em computadores, e-mails, servidores e bancos de dados, os quais necessitam proteção lógica e física, pois parte das informações são sigilosas e os usuários necessitam da alta disponibilidade de acesso aos documentos armazenados. Essa modernização do ambiente de trabalho tem aumentado a utilização de serviços on-line através da rede mundial de computadores [Internet], facilitando assim a possibilidade de comprometimento dos dados, mesmo que a origem do risco esteja fisicamente distante do local onde estão armazenados.

Problema

Os órgãos públicos lidam com informações que envolvem documentações, processos administrativos e assuntos sigilosos que, se acessados por pessoas de má fé, podem comprometer a vida do cidadão na sociedade, ou até mesmo do próprio funcionário que atua diretamente nas atividades dirigidas pelo órgão. O atraso causado pela indisponibilidade do sistema pode comprometer a execução dos processos e a inserção indevida ou perda de dados pode trazer prejuízos ao andamento das atividades inerentes ao serviço prestado, o qual possui grande importância.

O órgão, onde o objeto da pesquisa encontra-se inserido, possui uma estrutura com entrada controlada de pessoal e material, guarnições de segurança, sistema de monitoramento de câmeras e funcionários responsáveis por manter a segurança física em boas condições. Possui também servidores de rede internos trancados em racks e guardados em salas isoladas de acesso restrito ao setor de Tecnologia da Informação. As soluções para segurança da informação são facilmente melhoradas com aquisição de equipamentos e aplicativos, porém a necessidade de conscientização dos *stakeholders* que utilizam as ferramentas de T.I. é evidente, pois precisam de capacitação para o uso correto da tecnologia, aplicação dos conhecimentos oriundos de outras áreas e preservação dos dados produzidos diariamente, os quais são fundamentais para a continuidade das atividades rotineiras.

A necessidade da conscientização supracitada se torna mais evidente quando avaliamos o cenário atual de guerras cibernéticas, inclusive em escala mundial, o qual demonstra a fragilidade à qual esses dados podem estar expostos a partir do uso e armazenamento incorreto pelos usuários inseridos na rede. O contexto

descrito implicou no estudo e aplicação de legislações, normas, portarias e regulamentos internos das instituições do governo brasileiro, os quais vem sendo aprimorados para evitar *leaks* de informações valiosas e perdas de dados.

Descrito brevemente o cenário, insere-se o questionamento chave do objeto da presente pesquisa: qual o nível de conhecimento dos usuários de rede sobre o risco de vazamento ou perda de informações e como conscientizá-los a reduzir a possibilidade de correr esses riscos.

Justificativa

A pesquisa foi motivada pela necessidade de conscientizar os usuários de rede de um órgão público sobre o valor das informações que manipulam, demonstrando que o trabalho desenvolvido diariamente necessita de medidas preventivas para preservação das informações transmitidas internamente, onde a vazão destas pode acarretar no acesso indevido por parte de pessoas não autorizadas. É de extrema importância que a seção de tecnologia da informação do órgão tenha controle e garanta a segurança dos dados transmitidos através da rede, porém o usuário é quem os produz e os manipula, podendo se tornar uma vulnerabilidade ou alvo de invasores mal-intencionados, o que evidencia seu papel e importância no contexto da Segurança da Informação.

A informação é um recurso que possibilita o conhecimento de dados à pessoa que a acessa, podendo ser utilizada tanto de forma benigna quanto de forma maligna, por isso a importância que esses dados tem para o órgão que a administra deve ser enfatizada, pois a perda ou vazão de informações geralmente incide em crimes cibernéticos, onde hackers estão no ambiente virtual estudando formas de capturar dados, de tornar os serviços indisponíveis ou de se passar por outras

pessoas para se aproveitar das informações, danificando o que já vem sendo feito pelos funcionários dos órgãos. Geralmente os grandes diretores e chefes não se preocupam com a segurança e infraestrutura das redes de computadores interna até que ocorram problemas com vazamento de dados e intrusões na mesma.

A implementação da segurança depende de um planejamento e padronizações de procedimentos, cabe ressaltar que a segurança é inversamente proporcional ao conforto e agilidade, portanto quanto maior o nível de segurança, maior é a burocracia dos processos e insatisfação dos usuários e, por consequência, é necessário encontrar um equilíbrio que deve ser acordado com a alta direção do órgão, padronizando as medidas que serão adotadas, concretizadas através da Política de Segurança da Informação. A perda ou vazão de dados pode prejudicar significativamente a imagem do órgão, fazendo os usuários se questionarem sobre a confiabilidade dos sistemas utilizados internamente, acarretando inclusive em prejuízos financeiros, podendo gerar também processos contra o órgão na justiça.

O estudo desse tipo de trabalho acrescenta questões importantes no âmbito da Segurança da Informação, trazendo à tona indagações sobre a real necessidade de conscientização de *stakeholders* e a responsabilidade dos detentores dessas informações que irão ou não comunicar esses dados a outras pessoas. Cabe ressaltar que a evolução da tecnologia tem extinguido o uso do papel para documentos, armazenando informações e documentos em computadores, servidores, bancos de dados e outros meios virtuais. O campo tecnológico é bem amplo e necessita de formas que possibilitem aumentar a confiabilidade dos sistemas e da rede, sejam elas físicas ou virtuais, o que também envolve motivação e compromisso por parte da chefia, planejamento da implementação da segurança, orientação aos usuários da rede e investimentos financeiros.

O compromisso do Governo Brasileiro com a Segurança da Informação já vem sendo trilhado nas últimas décadas, com algumas iniciativas, inclusive através de documentações oficiais, como a Instrução Normativa GSI/PR Nr 01/2008, que definiu algumas formas de executar a gestão da segurança da informação e comunicações na Administração Pública Federal. Medidas criadas por profissionais da área atuantes do Governo Brasileiro, bem como diversas outras que possuem a finalidade de normatizar e melhorar as medidas aplicadas em relação aos dados produzidos e armazenados nos órgãos possuidores de informação.

Objetivo geral

Analisar o contexto de Segurança da Informação de um setor de licitações num Órgão Público, avaliando o comportamento dos funcionários diante de situações hipotéticas, conscientizar os usuários de rede mediante palestra, orientando sobre boas práticas para preservar a segurança das informações e verificar os resultados obtidos pela conscientização através de questionário. Demonstrar, através do estudo de caso, se o método de conscientização afetou o tratamento com as informações manipuladas pelo setor.

Objetivos específicos

- Expor o valor da informação contida no setor de licitação do Órgão Público a ser estudado, demonstrando a motivação da pesquisa e possíveis impactos caso haja incidentes que prejudiquem a Segurança da Informação;
- Analisar e avaliar o nível de Segurança da Informação no setor supramencionado, através de práticas rotineiras dos usuários de rede.

Efetuando uma pesquisa através de questionário com os funcionários daquele setor;

- Orientação dos usuários de rede com registro das ações executadas: palestra e medidas necessárias para aprimorar a Segurança da Informação em Recursos Humanos no setor de licitações do Órgão;
- Avaliação dos resultados após aplicação das medidas de segurança, identificando se os resultados foram positivos ou negativos.

1 REVISÃO BIBLIOGRÁFICA

1.1 SEGURANÇA DA INFORMAÇÃO

Como já foi mencionado anteriormente, o presente estudo tem por finalidade fazer uma análise do contexto de Segurança da Informação de um setor de licitações num Órgão Público, avaliando o comportamento dos funcionários diante de situações hipotéticas, conscientizar os usuários de rede mediante palestra, orientando sobre boas práticas para preservar a segurança das informações e verificar os resultados obtidos pela conscientização através de questionário. Demonstrar, através do estudo de caso, se o método de conscientização afetou o tratamento com as informações manipuladas pelo setor.

Para embasar o referido estudo, foi necessário buscar apoio nos artigos e pesquisas de especialistas pertencentes ao campo da Ciência da Informação e Segurança da Informação. É importante lembrar que, através da transformação causada pela tecnologia na sociedade, várias informações são transmitidas pela Internet e a possibilidade delas serem interceptadas ou perdidas, nos levam a refletir sobre o valor dessas informações para quem as possui, seja uma pessoa ou uma organização. Primeiramente, cabe priorizar a definição de segurança da informação que, segundo Marciano, é um

> fenômeno social no qual os usuários dos sistemas de informação têm razoável conhecimento acerca do uso destes sistemas, incluindo os ônus decorrentes expressos por meio de regras, bem como sobre os papéis que devem desempenhar no exercício deste uso. (MARCIANO, 2006, p.114)

Sobre o assunto, destacamos os estudos de Leandro Ramalho Fróio (2008) que nos fala sobre o tratamento diferenciado para informações sensíveis, a necessidade investimentos compatíveis para garantir a proteção da informação e adequação das organizações às leis e códigos em vigor. Para o autor,

> Os benefícios de implantar, gerenciar e controlar a segurança da informação nas organizações transpõe as características de privacidade inicialmente pretendidas e agregam propriedades que auxiliam as organizações a alcançarem seus objetivos. Isto possibilita que os serviços e negócios sejam executados em qualquer situação operacional, que as comunicações com fornecedores e clientes sejam eficientes, que as informações sensíveis tenham tratamentos diferenciados, que os investimentos para proteger a informação sejam compatíveis com as necessidades da organização e com o valor da informação. Além disso, permite que a organização se adeque às legislações e códigos de ética vigentes, mantendo sua imagem íntegra e transparente para investidores, auditores e sociedade. (FRÓIO, 2008, p. 4).

Para os benefícios supracitados, cabe destacar que a responsabilidade pela segurança da informação não é exclusiva do setor de tecnologia, mas da organização como um todo. Segundo Kelson Corte (2014):

> a segurança da informação não foi vista como de responsabilidade única da tecnologia; pelo contrário, a tecnologia sozinha é incapaz de solucionar a questão. A segurança da informação foi vista como de responsabilidade do negócio, o que requer que todas as áreas da organização se envolvam com o problema. Nesse sentido, é preciso que se considere o ser humano como fator relevante para o resultado das ações de segurança da informação. (CORTE, 2014, p. 9).

Ao observar o contexto em que estamos vivendo, onde a tecnologia está presente em quase tudo que fazemos e envolvida até no armazenamento das nossas informações pessoais, é importante destacar que diversos ataques cibernéticos vêm sendo realizados nos últimos anos, inclusive em escala mundial, prejudicando pessoas e organizações das mais variadas formas, incidindo em perdas financeiras, roubos, “sequestros” de dados e paralizações de serviços, como podemos observar em diversos noticiários por todo o mundo. Essa gama de crimes cibernéticos atinge os mais variados tipos de vítimas, desde pessoas físicas até grandes organizações como bancos, hospitais, empresas ou aeroportos, sejam elas públicas ou privadas. Suas consequências podem ser gravíssimas e atrasar o desenvolvimento de algumas áreas do país, trazer prejuízos financeiros ou comprometer vidas que dependem de certos serviços prestados pelas organizações que se tornam alvos de ataques cibernéticos. Segurança da Informação é uma preocupação que tem aumentado nas altas diretorias de empresas, onde indaga-se o real valor da informação que pode ser roubada, alterada, interceptada ou retida por algum malfeitor e quais as consequências desse possível “descuido”.

A segurança da informação busca minimizar esses riscos, implementando algumas medidas para que isso ocorra. Sêmola (2003, p.39) definiu a informação como uma representação da inteligência competitiva dos negócios e como sendo reconhecida como ativo crítico para a continuidade operacional e saúde da empresa. Dessa forma, é importante observarmos alguns conceitos de segurança da informação, descrevendo seus objetivos e características.

Sobre o assunto, Zapater e Suzuki (2005 apud CORTE, 2014) afirmam que a segurança da informação pressupõe a identificação das diversas vulnerabilidades e a gestão dos riscos associadas aos diversos ativos informacionais de uma corporação, independentemente da forma ou do meio em que são compartilhados ou armazenados.

Claudia Dias nos traz à luz um conceito de segurança da informação pertinente, que envolve o que o esperado pelos *stakeholders*, onde o usuário tem a expectativa de manter seus dados onde estão, pois quando se pensa em segurança de informações,

> a primeira ideia que nos vem à mente é proteção das informações, não importando onde estejam (no papel, na memória do computador, em um disquete ou trafegando pela linha telefônica). Conceitualmente, um computador ou sistema computacional é considerado seguro se houver uma garantia de que é capaz de atuar exatamente como o esperado. Porém, segurança não é só isso. A expectativa de todo usuário, no que diz respeito à segurança de dados, é que as informações armazenadas hoje em seu computador, lá permaneçam, mesmo depois de algumas semanas, sem que pessoas não autorizadas tenham tido qualquer acesso a seu conteúdo. Em outras palavras, o usuário espera que suas informações estejam disponíveis no momento e local que ele determinar, que sejam confiáveis, corretas e mantidas fora do alcance e das vistas de pessoas não autorizadas. (DIAS, 2000, p.42).

É importante mencionar que a concepção de Segurança da Informação também possui um enfoque no valor da informação e na proteção dos ativos, com base em algumas características fundamentais da segurança da informação, sendo eles: confidencialidade, integridade e disponibilidade. Afinal, ela 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 (CID), não estando restritos somente a sistemas ou aplicativos, mas também informações armazenadas ou veiculadas em diversos meios além do eletrônico ou em papel. Outras propriedades podem ser relacionadas à CID, como autenticidade, responsabilidade não-repúdio e confiabilidade. (BASTOS; CAUBIT, 2009, p.17).

Para dar mais credibilidade no armazenamento das informações, é necessário utilizar-se de diversos recursos para avaliar, organizar, monitorar e padronizar as atividades internas. Sobre o assunto, podemos dizer que a segurança da informação é alcançada

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

Cabe salientar que ativos podem ser definidos como

> todo elemento que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada. (SÊMOLA, 2003, p. 45).

Na visão de Kelson Côrte, ao considerar que as informações possuem valor e tramitam por diversos meios, a preocupação

> não pode ser exclusiva do setor de tecnologia da informação, mas de todos, desde a alta direção até o usuário de rede, pois existe a necessidade de um compromisso entre as áreas, com a preservação das informações e adoção de procedimentos adequados, o que requer uma postura diferente nos momentos de criar informações, tomar decisões, armazenar dados ou formalizar processos, por exemplo. Afinal, a segurança da informação não visa estabelecer segurança total, mas busca identificar as vulnerabilidades de um processo, gerenciar riscos e mitigar o impacto, caso algum risco se concretize. (CÔRTE, 2014, p.74).

Dessa forma, podemos dizer que Segurança da Informação é definida como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade (SÊMOLA, 2003).

Os conceitos supracitados demonstram claramente que a proteção dos ativos é o objeto principal da Segurança da Informação, onde pretende-se preservar o valor que possuem para as organizações. Ao mesmo tempo o usuário tem uma expectativa de que a informação esteja armazenada no local desejado, permanecendo inalterada. Há um grande esforço para manter a confiabilidade, integridade e disponibilidade das informações dentro das organizações, entretanto é importante considerar que elas são produzidas, armazenadas e transmitidas por funcionários, que as manipulam diariamente e possuem autonomia sobre elas

enquanto as tem sob sua posse. Um sistema de alto investimento, complexo e altamente seguro pode ser comprometido se os funcionários que possuem as informações não forem conscientizados sobre riscos, procedimentos e valor das mesmas. Dessa forma, reforça Marciano (2006, p.73-74) que “há que se implementar soluções por meio da regulamentação ou de aspectos culturais, e não meramente por meios tecnológicos”. O que nos traz um enfoque na conscientização de usuários para aprimorar aspectos de segurança.

A Instrução Normativa GSI/PR nº 1 (BRASIL, 2008), vai além da CID ao mencionar os objetivos de segurança da informação, incluindo a autenticidade, considerando que suas “ações objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações”.

A NBR ISO/IEC 27002 (2013), considera a confidencialidade, a integridade e a disponibilidade da informação como objetivos da segurança da informação. Para esta pesquisa iremos considerar outros princípios que também serão relevantes, afim de trazer melhor entendimento para esta monografia, sendo eles: autenticidade, não repúdio e confiabilidade.

1.1.1 Confidencialidade

Um dos objetivos que mais se comenta em Segurança da Informação é o da Confidencialidade, a ISO/IEC 27000 (2014, tradução nossa) define que se trata da “propriedade que a informação não está disponível ou divulgada para pessoas, entidades ou processos não autorizados”.

Segundo Sêmola (2003, p.45), a confidencialidade na SI abrange que “toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas”.

Para Dias (2000, p.42), confidencialidade é “proteger as informações contra acesso de qualquer pessoa não explicitamente autorizada pelo dono da informação, isto é, as informações e processos são liberados apenas a pessoas autorizadas”.

Dessa forma, podemos dizer que a confidencialidade atinge seu objetivo quando somente pessoas autorizadas conseguem ter acesso a certas informações e o controle dos acessos está sob manipulação do dono dela.

1.1.2 Integridade

A integridade é mantida quando toda informação permanece na mesma condição em que foi disponibilizada pelo seu proprietário, buscando a proteção contra alterações indevidas, intencionais ou acidentais (SÊMOLA, 2003, p.45).

De acordo com Dias (2000, p.42), a integridade tem como objetivo

> evitar que dados sejam apagados ou de alguma forma alterados, sem a permissão do proprietário da informação. [...] O conceito de integridade está relacionado com o fato de assegurar que os dados não foram modificados por pessoas não autorizadas.

A NBR ISO/IEC 27002 atribui a completeza e exatidão à integridade como forma de assegurá-la durante o processamento da informação (NBR ISO/IEC 27002, 2013). Basicamente, trata-se de assegurar que os dados que chegaram ao destinatário são os mesmos que foram remetidos pelo autor.

1.1.3 Disponibilidade

A disponibilidade está fortemente relacionada à redundância na NBR ISO/IEC 27002, pois ela é necessária para atender aos requisitos deste objetivo. A importância de manter os sistemas de informação disponíveis é crucial, pois os *stakeholders* precisam dos dados e, geralmente, utilizam com frequência, a indisponibilidade pode gerar pequenas crises no ambiente operacional e estratégico, tendo em vista o atraso que pode ser gerado no andamento dos processos e transmissão de informações.

Conforme Sêmola (2003, p.45), disponibilidade ocorre quando toda informação gerada ou adquirida por um indivíduo está disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade.

Nessa abordagem, Dias vai mais a fundo e nos traz um conceito mais complexo, considerando que a disponibilidade é atingida quando consegue

> proteger os serviços de informática de tal forma que não sejam degradados ou tornados indisponíveis sem a devida autorização. Para um usuário autorizado, um sistema não disponível, quando se necessita dele, pode ser tão ruim quanto um sistema inexistente ou destruído. [...] Disponibilidade pode ser definida como a garantia de que os serviços prestados por um sistema são acessíveis, sob demanda aos usuários ou processos autorizados. [...] Em relação à segurança de informações, sua principal preocupação é prevenir que ataques deliberados ou maliciosos evitem ou dificultem o acesso de usuários autorizados a seus sistemas. (DIAS, 2000, p.43)

1.1.4 Autenticidade

A autenticidade é a “propriedade de que uma entidade é o que ela diz ser”. (ISO/IEC 27000, 2014, tradução nossa).

A Instrução Normativa GSI/PR nº 1, nos traz o seguinte conceito: “propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade[...]” (BRASIL, 2008)

Isso demonstra a importância de ser relatado no sistema quem faz o que, pois os *stakeholders* precisam ter a garantia de que aquela pessoa que está trocando informações com eles é realmente quem ela diz ser, o que incide em diversos outros fatores que compõem a Segurança da Informação.

1.1.5 Não-repúdio

Côrte (2014) define que não repúdio é a propriedade que garante a impossibilidade de negar a autoria em relação a uma transação feita anteriormente.

A ISO/IEC 27000 define que não repúdio é a capacidade de comprovar a ocorrência de uma reivindicação de um evento ou ação e suas entidades originárias (ISO/IEC, 2014, tradução nossa).

Dessa forma, ele faz com que o responsável pela ação que foi executada não consiga negar que a fez, garantindo assim que o sistema irá apontar para a pessoa certa quando assim for exigido.

1.1.6 Confiabilidade

O conceito de confiabilidade na ISO/IEC 27000 (2014) é a propriedade de que o conceito e o resultado acham-se consistentes com a intenção. Para Dias (2000, p. 44), ela está relacionada à capacidade de

> garantir que, mesmo em condições adversas, o sistema atuará conforme o esperado. Exemplos de sistemas em que a confiabilidade é o objetivo de segurança mais importante são os sistemas de energia nuclear, de controle de tráfego aéreo e de controle de vôo. Uma falha desse tipo pode comprometer a vida de centenas de pessoas.

Essas definições estão inseridas principalmente na essência da consistência, onde o sistema deve permanecer funcionando, mesmo que surjam problemas ou fatores externos que possivelmente atrapalhariam seu desempenho,

ele deve cumprir suas funções afim de evitar prejuízos no andamento do trabalho feito pelos *stakeholders*.

1.2- SEGURANÇA DA INFORMAÇÃO E O GOVERNO BRASILEIRO

1.2.1 Contexto do Governo Brasileiro em relação à Segurança da Informação

O nosso convívio com a Tecnologia da Informação é cada vez mais notável e rotineiro, onde podemos vivenciar o dia a dia com várias informações armazenadas e de fácil acesso de forma atemporal e independente de local, através de diversos dispositivos eletrônicos de armazenamento, mídias ou outros, entretanto é notável que a facilidade em acessá-las tem sido aprimorada mais rápido do que sua segurança, a qual muitas das vezes é deixada de lado até que ocorram incidentes. No contexto nacional já havia uma preocupação com a preservação da privacidade das informações, inclusive através de leis, que criaram métodos com o intuito de mantê-las seguras sob a posse de seus portadores, através da legislação de direitos sobre a inviolabilidade de serviços postais e telegramas, ou violação de sigilo bancário, por exemplo. Em relação ao avanço da tecnologia, boa parte dessas informações saíram dos papéis e começaram a ser armazenadas em servidores, o que favoreceu a sustentabilidade ambiental e facilitou o acesso à informação, tanto para pessoas bem intencionadas quanto para as mal intencionadas, já que boa parte se encontra armazenada na Rede Mundial de Computadores (*World Wide Web*).

A título de conhecimento, podemos mencionar a Lei nº 12.527 (BRASIL, 2011), conhecida como Lei de Acesso à Informação (LAI), que determinou que os órgãos e entidades do poder público devem assegurar a gestão transparente de informação, protegendo-a com a garantia de disponibilidade, autenticidade e integridade, o que trouxe grande impacto no contexto de segurança da informação no âmbito nacional, tendo em vista a grande quantidade de informações fornecidas. Também preza pelo uso de meios tecnológicos para comunicar os dados que serão disponibilizados para o cidadão.

Apesar da vantagem concedida ao cidadão, a facilidade em acessar tal recurso tem sido alvo de ataques *hacker,* onde ações mal intencionadas geralmente resultam em sites desfigurados e indisponibilidade de informações. O mesmo ocorre com diversos outros sites do governo que buscam disponibilizar e facilitar o acesso às informações pelos cidadãos.

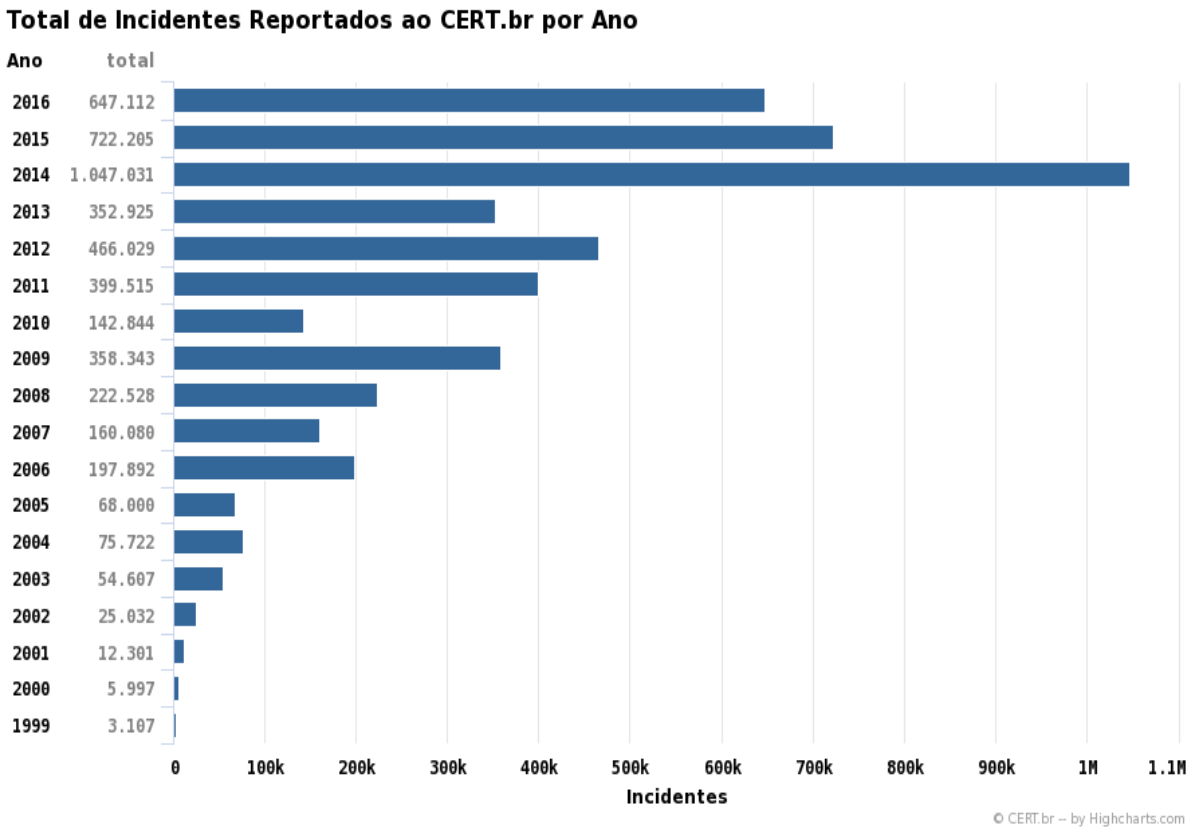
Um exemplo de invasão a sites do governo foi o ocorrido em 12 de junho de 2017, onde foram publicadas frases ofensivas ao presidente do Brasil no domínio www.df.gov.br [*site* do Governo de Brasília] no lugar de textos antes publicados, o

episódio é conhecido como pichação de sites (HANNA, 2017). Os sistemas de informática do Distrito Federal sofreram 52.032 tentativas de invasão em 2016 (LUIZ, 2017).

No início do corrente ano alguns dos ataques a instituições do governo ocorreram, trazendo prejuízos ao andamento de atividades, onde, por exemplo, o Hospital de Câncer de Barretos suspendeu em torno de três mil consultas no dia 27 de junho de 2017 em algumas unidades da instituição (EPTV, 2017). Na mesma notícia, consta que a invasão bloqueou os sistemas e pediram pagamento em Bitcoins [tipicamente um ataque de *ransomware*], e que aproximadamente mil máquinas foram afetadas. Podemos estimar que o prejuízo financeiro e institucional ao hospital foi de grande impacto para o atendimento ao cidadão e para a imagem da instituição.

No gráfico 1, podemos observar a quantidade de incidentes de rede por ano no Brasil [reportados ao CERT.br], o qual atingiu seu ápice em 2014 com mais de um milhão de incidentes.

Gráfico 1 - Quantidade de incidentes de rede no Brasil por ano



Fonte: https://www.cartilha.cert.br/stats/incidentes

O Gabinete de Segurança Institucional da Presidência da República é o órgão que possui como uma de suas responsabilidades coordenar as atividades de Segurança da Informação, através do Departamento de Segurança da Informação e Comunicações – DSIC (CONSELHO DE DEFESA NACIONAL, 2008).

Dessa maneira, uma das formas que demonstrou a preocupação tecnológica sobre Segurança da Informação em âmbito nacional foi concretizada através do Decreto Presidencial nº 3.505 (BRASIL, 2000), que instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. O qual deu ênfase à proteção de informações, capacitação de recursos humanos, proatividade e conscientização da APF. Bem como também delegou, através de seu Art. 4º, à Secretaria-Executiva do Conselho Nacional de Defesa, assessorada pelo Comitê Gestor de Segurança da Informação – instituído no Art. 6º do mesmo -, a responsabilidade de elaborar e implementar programas voltados para recursos humanos, normas, auditorias nos órgãos e entidades da APF, entre outras medidas, todas voltadas para a área de Segurança da Informação.

Outras medidas adotadas foram concretizadas pela Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008, onde foram determinadas as competências dos comitês de segurança da informação e equipes de trabalho, com a finalidade de implementar ações, soluções e tratamento de incidentes de segurança da informação e comunicações.

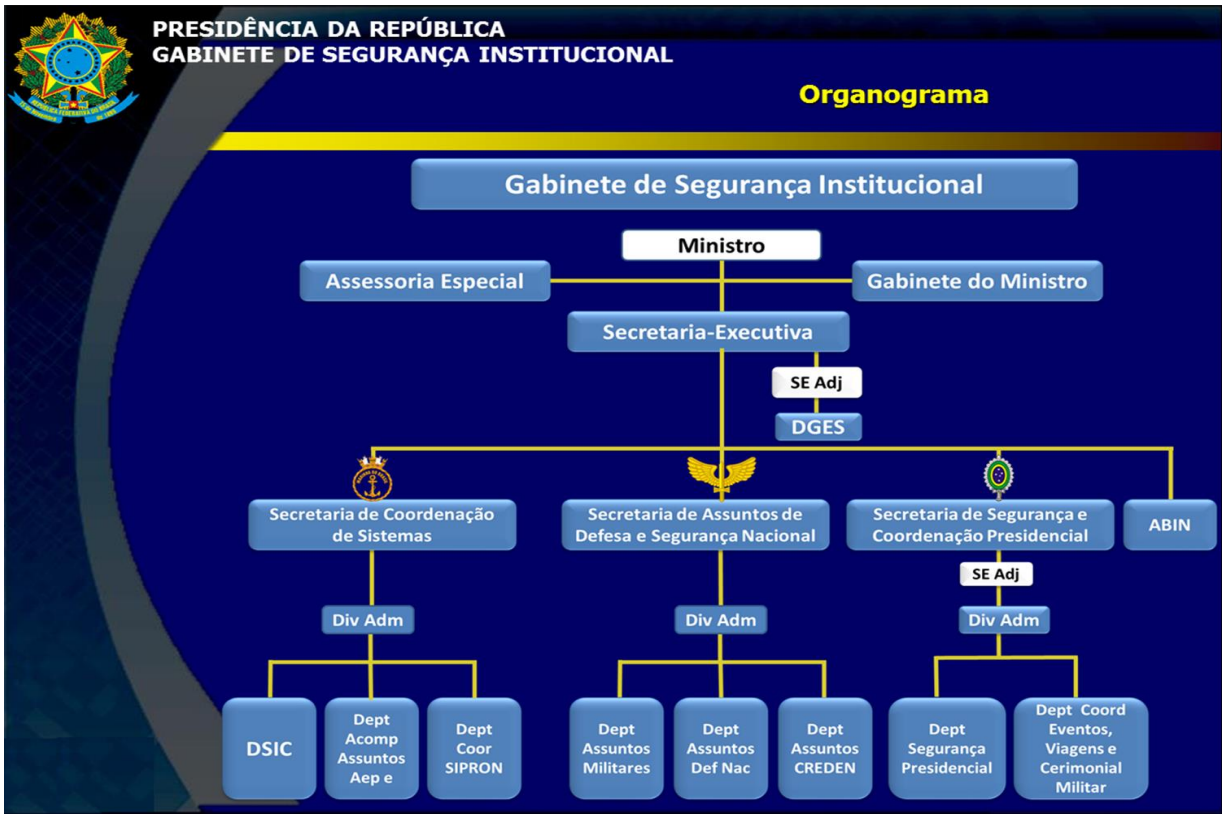
Uma ênfase ao tratamento das informações foi dada através do Decreto nº 7.845, (BRASIL, 2012), que regulamentou procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo. O qual determinou procedimentos relativos à expedição, tramitação, armazenamento, preservação e comunicação das informações, que dependem do grau de sigilo em que foram classificadas por agentes credenciados pelo Núcleo de Segurança e Credenciamento, regulamentando inclusive o uso de medidas como a criptografia adequada à sua classificação. Os graus de sigilo de informação, determinados no Art. 52 do Decreto supramencionado, são os seguintes:

- Ultrassecreto (U)
- Secreto (S)
- Reservado (R)

Os exemplos supracitados são apenas algumas das medidas adotadas pelo Governo Brasileiro, as quais ainda permanecem recentes e têm sido alteradas

e melhoradas de acordo com as necessidades do país, afim de melhor entender o atual contexto nacional, a figura a seguir demonstra o atual organograma do Gabinete de Segurança Institucional do país (órgão que possui como uma de suas responsabilidades coordenar as atividades de segurança da informação e comunicações no âmbito nacional):

Figura 1 - Organograma do Gabinete de Segurança Institucional



Fonte: http://www.gsi.gov.br/sobre/estrutura

Outra medida consolidada pela Norma Complementar nº 05 da Instrução Normativa GSI/PR nº 01, estabeleceu, inclusive, a criação da Equipe de Tratamento de Incidentes em Redes Computacionais nos órgãos da APF, que devem ser compostas por pessoas com conhecimentos técnicos na área de tecnologia, para que possam agir de forma reativa e proativa sobre os possíveis incidentes iminentes.

1.2.2 Valor da informação contida em setores de licitações de Órgãos Públicos

Quando falamos de informação, estamos tratando do bem mais importante para a humanidade, pois, por meio dela o conhecimento vem sendo

passado de geração a geração e a humanidade tem se desenvolvido (FONTES, 2000).

As informações armazenadas nos servidores devem ser avaliadas pela alta diretoria e constituem importante fator em questões decisivas no que tange ao investimento de sua proteção e diretrizes para preservação das mesmas. As avaliações dessas decisões devem ser feitas com base no valor que elas possuem para a empresa ou órgão, o que também serve como argumento para motivar a alta direção em investir numa infraestrutura aprimorada de segurança. Ao visualizar a questão da imagem da organização com os clientes, é importante observarmos que o impacto de uma invasão,

> seja interna ou externa, causando o roubo de informações, não é fácil de ser calculado. Muitas vezes não se sabe que fim levou aquela informação e, muito menos, como ela será explorada. Será que estará na mão de um concorrente? Ou ainda na mão da imprensa, pronta para um furo de reportagem?
> Trata-se de um problema sem dimensão definida. O impacto à imagem é coisa séria e custosa para ser revertida. Gasta-se muito mais recurso tentando reconstruir uma imagem sólida, segura, eficiente e compromissada com o cliente, do que o que foi gasto para construí-la. (SÊMOLA, 2003)

É nítido que a informação possui um valor que vai além do que se considera tangível e envolve diversas áreas nesse contexto, a NBR ISO/IEC 27002 (2013) reforça a necessidade da proteção de informações contra os riscos, já que o valor da informação

> vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requer proteção contra vários riscos. (ASSOCIAÇÃO, 2013)

Com um olhar generalizado de licitações, é importante observamos alguns princípios que as regem, o Art. 3º, da Lei nº 8.666/93 nos traz os principais:

> A licitação destina-se a garantir a observância do princípio constitucional da isonomia, a seleção da proposta mais vantajosa para a administração e a promoção do desenvolvimento nacional sustentável e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos. (BRASIL, 1993)

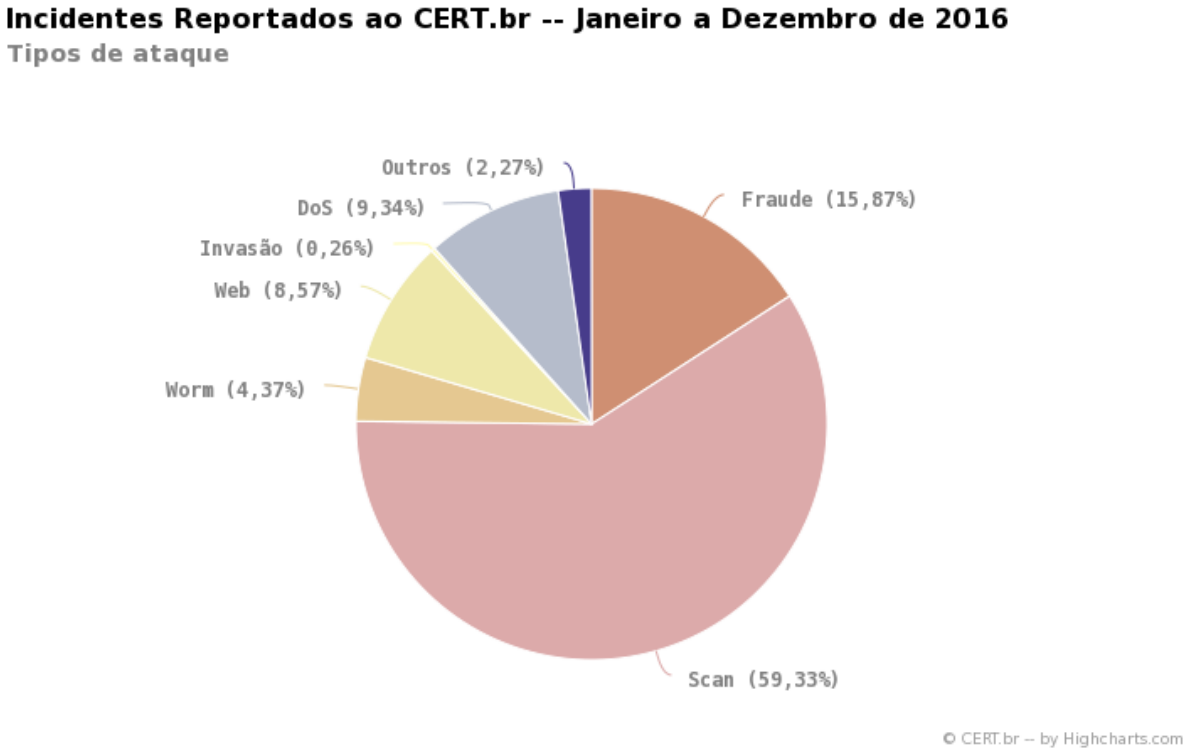
Em resumo e focando nos conceitos supracitados, que estão inseridos no contexto da segurança da informação, licitações envolvem propostas e nenhum dos fornecedores deve ser favorecido em qualquer fase do processo, é importante que certas informações sejam mantidas apenas sob posse de responsáveis autorizados pelo Órgão Licitante do certame, a vazão de informações ou quebra de sigilo podem prejudicar a imagem do órgão perante a sociedade e a preservação dos princípios da licitação previstos no artigo supracitado, dando nulidade ao processo desenvolvido, prejuízos financeiros à APF e, até mesmo, imputando penalidades ao condutor do processo (que geralmente se trata do pregoeiro). Dessa forma, é necessária uma preocupação especial com a forma que essas informações serão armazenadas e com os portadores delas, os quais devem ser conscientizados mediante a legislação em vigor e política de segurança da informação. Cabe ressaltar que a licitação permanece interna e em sigilo até a fase de lançamento do edital [tratando-se de pregão eletrônico], pois exige publicidade de seus atos a partir dessa fase, onde seus dados devem ser publicados para acesso de todos, inclusive de cidadãos comuns, garantindo uma melhoria na competição igual e leal entre os fornecedores [isonomia].

1.2.3 Importância da conscientização dos funcionários

A indagação principal desta monografia está associada à importância de se conscientizar o usuário de rede, afinal, qual seria a real necessidade de executar esse tipo de trabalho se tivermos uma infraestrutura de rede implementada através de altos investimentos e considerada extremamente segura? A preocupação com o usuário está inserida na forma como ele usa suas ferramentas de trabalho, pois muitas vezes acreditam que não serão alvo de ataques hacker, nem de *leaks* de informações, por considerar inexistente a possibilidade de se tornar uma vítima em potencial.

Ao observar o gráfico 2, podemos verificar que os tipos de incidentes de rede reportados ao CERT.br nos relatam que boa parte dos problemas tem relação ao fator humano inserido na Segurança da Informação, onde o *scan* pode fornecer informações pessoais de usuários e a fraude [nesse caso também estão inclusos os *scams*] busca obter vantagem sobre pessoas, ambos podem contribuir para uma possível engenharia social.

Gráfico 2 - Tipos de incidentes reportados ao CERT.br



Legenda:

- **worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

Fonte: https://www.cartilha.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html

As pessoas são o pilar mais frágil e também o mais visado pelos fraudadores, portanto carece de maior atenção e mais estudo (CÔRTE, 2014). A preocupação vai além do erro humano, pois é extremamente importante que o trâmite das informações seja registrado na rede, para imputar responsabilidades em casos de usuários mal intencionados, e que os *stakeholders* sejam conscientizados mediante palestras e políticas, afim de evitar desleixos ou descuidos com as informações sob sua posse.

Dias (2000, p. 140) já visualizava o ser humano como responsável pela maior parte de incidentes relativos às informações, pois de acordo com algumas pesquisas

> feitas em ambientes computacionais, as causas mais frequentes de acesso não autorizado, perda de dados ou pane nos sistemas informatizados são erros, omissões, sabotagem, extorsão ou invasões criminosas provocados por pessoas contratadas pela própria organização.

O conceito supracitado pode ser reforçado, ao verificar uma visão holística da Segurança da Informação no ambiente corporativo, pois as pessoas são

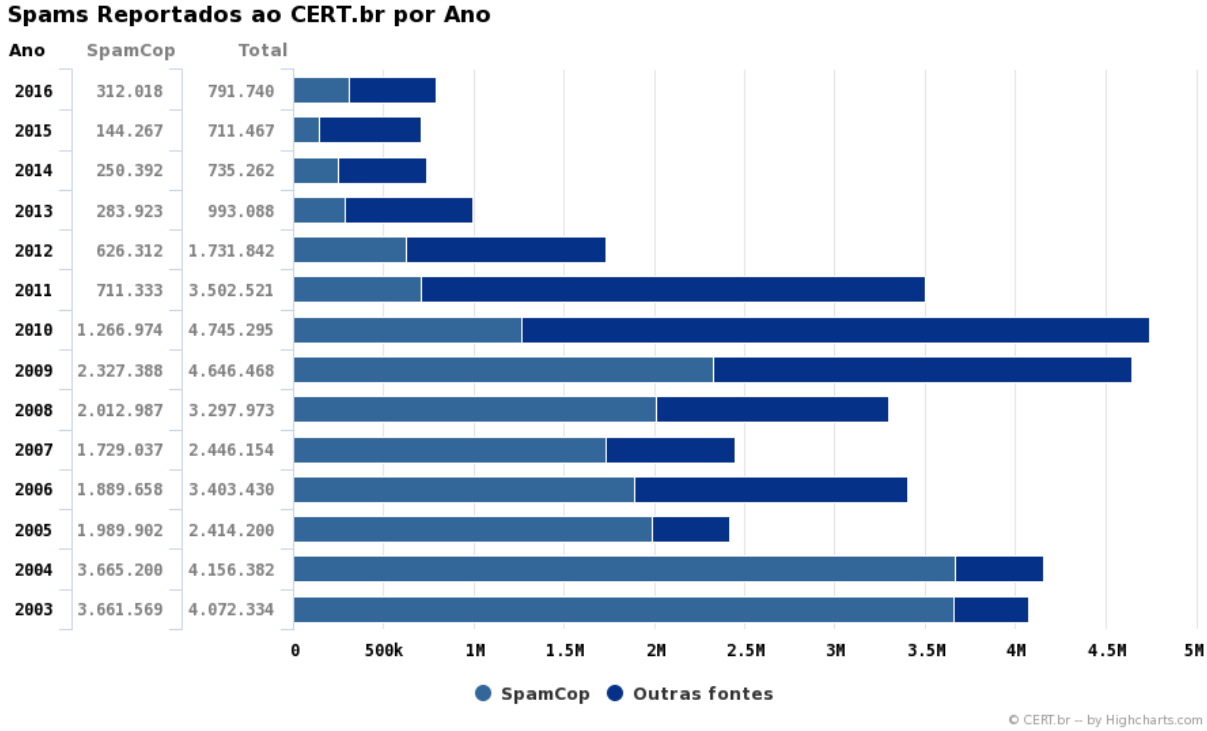
> consideradas o “elo frágil” da segurança da informação. A associação pode ser entendida quando se imagina que qualquer esquema de segurança, por mais sofisticado que seja, pode ser derrubado pela atuação de uma única pessoa que decida abusar de seus privilégios de acesso a dados ou instalações de processamento da informação. (BEAL, 2008, p. 71)

No contexto do Governo Brasileiro também já foi constatado que essa fragilidade foi notada por hackers e se tornou um dos alvos mais vulneráveis, o CERT.br afirma que, normalmente

> não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial e, por este motivo, golpistas vêm concentrando esforços na exploração de fragilidades dos usuários. Utilizando técnicas de engenharia social e por diferentes meios e discursos, os golpistas procuram enganar e persuadir as potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas.” (CERT.br, 2016)

Os *Spams* [envio abusivo de e-mails] também podem ser utilizados na engenharia social ou congestionamento da caixa de entrada do alvo, o CERT.br verificou que esse tipo de incidentes possui um número elevado de reportes por ano, conforme demonstrado no gráfico 3, índice que vem reduzindo drasticamente de 2010 até 2016.

Gráfico 3 - Spams reportados no Brasil por ano



Fonte: https://www.cartilha.cert.br/stats/spam

Esses riscos e conceitos de fragilidades precisam ser repassados à alta diretoria, que muito provavelmente irá se preocupar com o assunto, tendo em vista o valor das informações sob sua posse. Para que seja feita a conscientização e implementação dos aspectos de Segurança da Informação no ambiente corporativo, é necessário o envolvimento e motivação dos executivos da empresa, sobre o assunto, Sêmola (2003, p. 20) comunica que por se tratar de um problema generalizado e corporativo,

> envolvendo os aspectos físicos, tecnológicos e humanos que sustentam a operação do negócio, torna-se condição *sine qua non,* que se inicie os trabalhos no formato *top down,* ou seja, mobilizando os executivos da diretoria da empresa, para depois atingir os demais na hierarquia. Esta condição é fundamental, pois não haverá possibilidade de atingir simultaneamente, e com igualdade, as vulnerabilidades de todos os ambientes e processos distribuídos da empresa, senão houver uma ação coordenada e principalmente apoiada pela cúpula. Entende-se por apoio não só a sensibilização e percepção adequada dos riscos e problemas associados, mas também da consequente priorização das ações e definição orçamentária à altura.

Consolidando esse conceito, enfatizando a importância do envolvimento organizacional e mencionando o ser humano como um fator relevante, a segurança da informação

> foi vista como de responsabilidade do negócio, o que requer que todas as áreas da organização se envolvam com o problema. Nesse sentido, é preciso que se considere o ser humano como fator relevante para o resultado das ações de segurança da informação. (CÔRTE, 2014, p. 73)

É uma atribuição da gerência manter o quadro de profissionais tecnicamente atualizado e apto a desempenhar funções atuais e futuras, através do plano estratégico de informática (DIAS, 2000). Tal adequação do desempenho técnico-profissional é útil para que sejam mitigados os riscos de incidentes de rede, junto ao trabalho que é feito pelo setor de Tecnologia da Informação ao implementar melhorias na infraestrutura de rede corporativa. É importante enfatizarmos alguns assuntos em palestras de conscientização de usuários, pois

> aparentemente, há uma demasiada confiança na tecnologia, como se esta fosse capaz de resolver todos os problemas da segurança. Por essa razão, há, consequentemente, um relaxamento em se identificar as fragilidades a que as pessoas estão sujeitas e, por isso mesmo, elas são os alvos preferidos daqueles que querem roubar informações. (CÔRTE, 2014, p. 83)

O usuário de rede precisa ter consciência de sua responsabilidade acerca dos dados manipulados por ele, fazendo parte do Sistema de Gestão de Segurança da Informação. Para garantir essa consciência, é importante que o usuário tenha conhecimento das principais técnicas utilizadas por criminosos cibernéticos que buscam coletar informações corporativas para obter vantagens sobre os funcionários.

A proteção contra ataques de engenharia social é, muitas vezes, negligenciada na segurança da informação, onde *hackers* e outros tipos de pessoas mal-intencionadas se aproveitam da ingenuidade ou ignorância de usuários para obter informações confidenciais como senhas, equipamentos utilizados pela organização ou outros dados que podem comprometer a segurança da organização (Beal, 2008, p.78).

Uma das soluções para mitigar os riscos a que os usuários estão expostos, está relacionada ao preparo anterior a qualquer incidente, já que para evitar esse tipo de ataque [engenharia social]

> todas as pessoas da empresa precisam receber treinamento e reciclagem periódica. Todos precisam estar atentos o tempo todo. Precisam conhecer os procedimentos que a empresa definiu para se defender desses ataques. Este é um típico caso em que a prevenção é o melhor remédio. (DAWEL, 2005, p.78)

A NBR ISO/IEC 27001 (2013) reforça essa necessidade da conscientização na seção 12.2, ao falar sobre proteção contra *malware.* Propõe como medida a implementação de controles para detectar, prevenir e de recuperação para proteger contra *malware,* combinado com conscientização do usuário. (ASSOCIAÇÃO, 2013).

1.2.4 Ataques cibernéticos voltados a usuários de rede

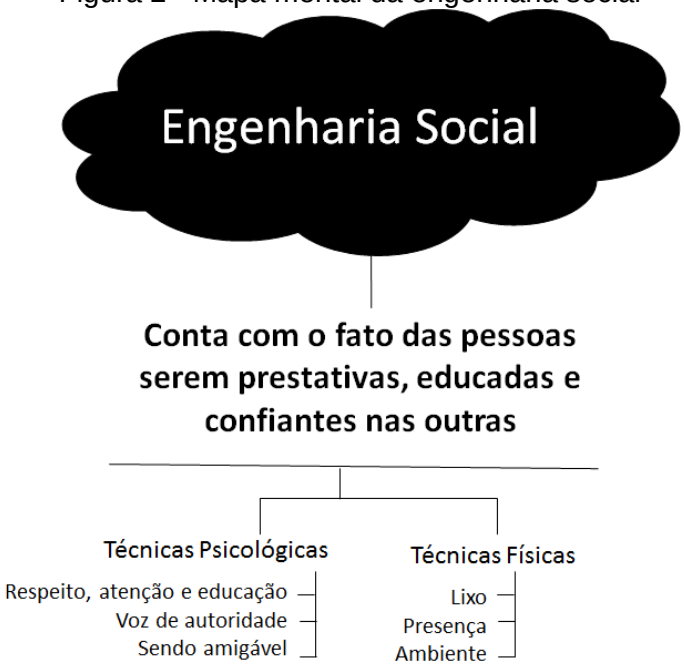
A ferramenta mais utilizada atualmente para adquirir informações de pessoas é a engenharia social, pois trata-se do uso de influência e persuasão para enganar pessoas e convencê-las, através do convencimento ou manipulação, de que o engenheiro social é alguém que na verdade ele não é, o qual se aproveita das pessoas para obter informações com ou sem o uso de tecnologia (MITNICK, 2002).

O que ocorre no meio tecnológico não é muito diferente do que ocorre nos meios antigos, onde estelionatários, por exemplo, utilizam de informações privilegiadas e persuasão para obter vantagem para si. No ambiente onde a tecnologia armazena dados, o criminoso faz uso de informações e ferramentas tecnológicas para conseguir ter acessos privilegiados, manipular dados ou indisponibilizar sistemas.

É comum o engenheiro social utilizar técnicas como vasculhar lixos para coletar dados em documentos descartados pela organização, analisar perfis em redes sociais para absorver informações de suas potenciais vítimas, efetuar ligações telefônicas simulando ser outra pessoa afim de obter dados relevantes, envio de e-mails falsos *[phishing]*, conversas pessoais com funcionários da organização, envio de anexos maliciosos e falsos antivírus *[rogueware].* Estas técnicas estão inseridas no conceito de engenharia social, onde as valiosas informações, de posse dos funcionários, são coletadas pelo ator mal-intencionado. Ao conseguir acessos privilegiados [senhas e autorizações], o atacante pode ter mais liberdade de agir sobre seu objetivo e executar o que foi planejado.

Dawel (2005, p.78) nos traz um mapa mental que explica, de forma sucinta, as técnicas utilizadas na engenharia social, classificando-as em psicológicas e físicas, conforme demonstrado na figura a seguir:

Figura 2 - Mapa mental da engenharia social



Fonte: A Segurança da Informação nas Empresas: Ampliando Horizontes além da Tecnologia. George Dawel, 2005.

1.2.4.1 Phishing

Phishing é “o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.” (CERT.br, 2017). O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil também menciona na Cartilha de Golpes na Internet que o *phishing* ocorre por envio de mensagens eletrônicas que buscam:

- Se passar pela comunicação oficial de uma instituição conhecida;

- Atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;

- Informar que a não execução dos procedimentos descritos pode acarretar sérias consequências;

- Induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso de páginas falsas, da instalação de códigos maliciosos e do preenchimento de formulários contidos na mensagem ou em páginas web.

Pelo conteúdo da cartilha, é possível notar que os cibercriminosos criam páginas falsas de internet, contendo mensagens e formulários falsos, onde conseguem armazenar as informações que são fornecidas pelo próprio usuário de rede, podendo assim utilizar desses dados para se passar pela vítima. Dependendo do tipo de informação recebida, o golpista executa operações para se passar pelo afetado, o que implica na possível perda financeira ou alteração de dados nas atividades permitidas por aquele *login* de usuário.

Pishing é um tipo de roubo de identidade,

> cuja popularidade está aumentando entre a comunidade de *hackers*. Através do uso de sites fraudulentos e e-mails falsos, os criminosos tentam roubar seus dados pessoais, normalmente senhas e informações de cartões de crédito. (NORTON, 2017)

Para a empresa Avast (2016), "*phishing* é uma maneira desonesta que cibercriminosos usam para enganar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias."

Uma das modalidades desse tipo de ataque é conhecido como *pharming*, trata-se de *"*um tipo de *phishing* que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS *(Domain Name System)*". (CERT.br, 2017).

Verifica-se que esse tipo de ataque surge como uma armadilha do meio tecnológico [elaborada por cibercriminosos], onde o usuário despreparado fornece seus dados a um site que aparenta ser oficial, porém está concedendo-os para uma página de internet falsa, onde as informações fornecidas serão enviadas ao criminoso que as está buscando.

1.2.4.2 Malware

São softwares maliciosos "que destinam-se a se infiltrar ilicitamente no sistema de um computador e danificar ou roubar informações confidenciais ou não" (VIEIRA, 2011). Eles podem estar inseridos em programas de computadores falsos, mídias removíveis, anexos de e-mails, páginas de *web*, entre outros.

Nesse caso a importância da conscientização de usuários de rede cresce, por se tratar do agente crítico para que o ataque possa ser iniciado, desta forma o manual do CISSP nos informa que

> existem vários tipos de códigos mal-intencionados ou malwares, como vírus, worms, cavalos de Tróia, e bombas lógicas. Eles geralmente estão dormentes até serem ativados por um evento, o usuário ou sistema inicia. Eles podem ser espalhados por e-mail, compartilhamento de mídia, compartilhamento de documentos e programas, ou baixar coisas da Internet, ou podem ser inseridos propositadamente por um atacante.
> Aderindo à regra usual de não abrir um anexo de e-mail que vem de uma fonte desconhecida é uma das melhores maneiras de combater o código malicioso. (HARRIS, 2013, p. 1197, TRADUÇÃO NOSSA).

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil classificou e conceituou os *malwares* conforme demonstrado no quadro a seguir:

Quadro 1 - Tipos de *Malwares*

Tipo de *Malware*	Descrição
Vírus	Programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. [e-mail, script, macro, telefone celular]
Worm	Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.
Bot e *Botnet*	Programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do *worm,* ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.
Spyware	Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.
Backdoor	Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.
Cavalo de Tróia *(Trojan)*	Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.
Rootkit	Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

Fonte: https://cartilha.cert.br/malware/

O *malware* se torna uma ferramenta poderosa nas mãos de cibercriminosos, uma vez que suas variáveis permitem a propagação rápida por computadores e redes, se misturando com outros *softwares* ou fornecendo o acesso a dados através do envio de informações para terceiros. Geralmente, é um tipo de

ataque sorrateiro e com alto poder de disseminação e, por estas características, pode trazer prejuízos elevados à uma organização.

1.2.4.3 Ransomware

Este tipo de ataque é bem recente e diferenciado, que busca vulnerabilidades focadas em usuários e softwares desatualizados, ao adentrar no computador infectado bloqueia o acesso do usuário aos seus arquivos [geralmente com uso de criptografia], ao concluir a infecção com êxito, é comum a exigência de um pagamento para que o usuário possa resgatar seus dados. É muito similar a um sequestro, porém o sequestrado, nesse caso, são arquivos digitais em vez de pessoas.

Ao utilizar esses recursos e se propagar pela rede, o *Ransomware* funciona de muitas maneiras diferentes,

> simplesmente bloqueando a Área de Trabalho do computador infectado criptografando todos os seus arquivos. Comparado ao *malware* tradicional, o *ransomware* exibe diferenças comportamentais. Por exemplo, o *malware* tradicional normalmente pretende alcançar o sigilo para que ele possa coletar credenciais bancárias ou pressionamentos de teclas sem suscitar suspeitas. Em contrapartida, o comportamento do *ransomware* está em oposição direta ao sigilo, já que todo o ponto do ataque é avisar abertamente ao usuário que ele está infectado.” (KHARAZ; et al., 2016, p. 757).

Este código malicioso ficou muito conhecido no Brasil após ataques cibernéticos em escala mundial, os quais ocorreram em maio do corrente ano. Onde centenas de países foram infectados pelo vírus, explorando uma falha nos sistemas Windows, exposta em documentos vazados da Agência Nacional de Segurança dos Estados Unidos, o qual trouxe prejuízos ou interrupção no andamento de atividades de grandes empresas (PRESSE, 2017). O ataque se alastrou por possuir facilidade em se propagar pela rede, principalmente através de *e-mails.*

Cabe, neste caso, a conscientização dos usuários de rede também, para que mantenham seus sistemas operacionais atualizados, evitem de clicar em e-mails de desconhecidos e façam backup de seus arquivos regularmente.

1.3 INSTRUMENTOS ÚTEIS PARA CONSCIENTIZAÇÃO DOS FUNCIONÁRIOS

1.3.1 Sistema de Gestão de Segurança da Informação

A NBR ISO/IEC 27001 (2013) nos traz a importância e influência do Sistema de Gestão de Segurança da Informação (SGSI), bem como sua adaptabilidade ao decorrer do tempo, tendo em vista que a adoção de um SGSI

> é uma decisão estratégica para uma organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais, funcionários, tamanho e estrutura da organização. São esperados que todos estes fatores de influência mudem ao longo do tempo.

A adoção do SGSI envolve uma decisão estratégica para uma organização, sendo que sua especificação e implementação são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais, funcionários, tamanho e estrutura da organização (ASSOCIAÇÃO, 2013).

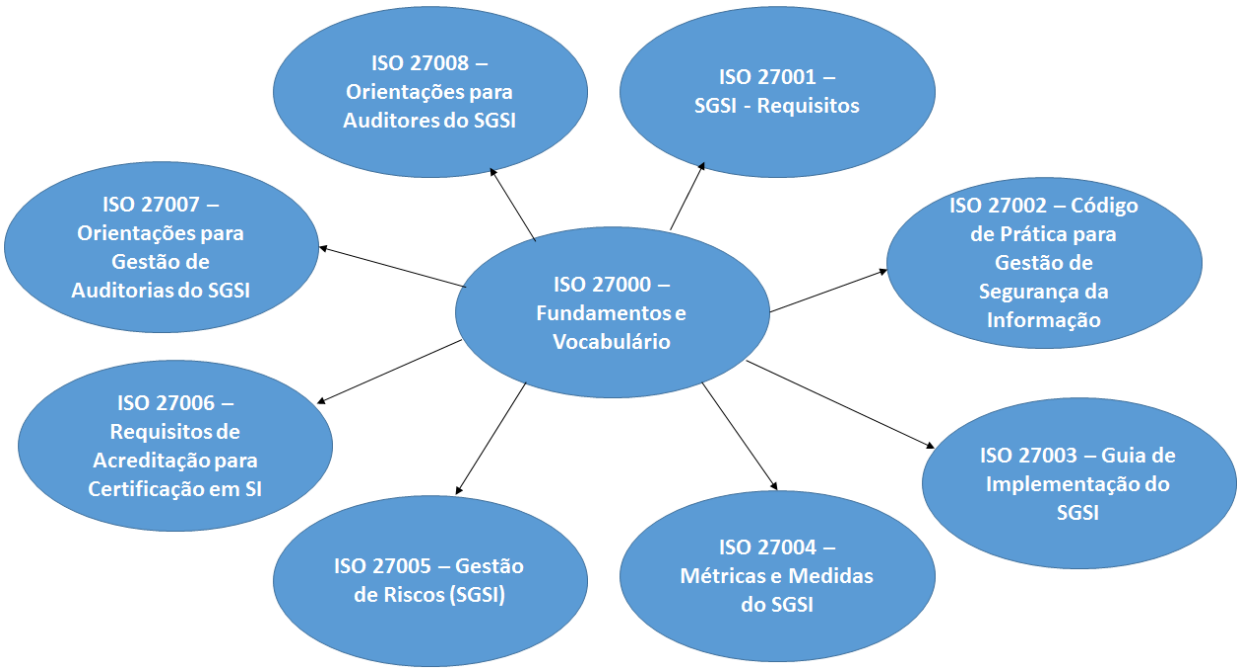
Trata-se de uma estrutura que garante a permanente atualização, adequação e avaliação de efetividade de dispositivos de segurança da informação (BASTOS; CAUBIT, 2009, p.17).

Tal estrutura permite à organização equacionar os desafios de proteção da informação, levando em conta os ambientes físico e lógico, pessoas, processos (BEAL, 2008).

Com base nisso, podemos dizer que o Sistema de Gestão de Segurança da Informação permite que toda a corporação fale a mesma linguagem e siga os mesmos procedimentos com relação ao tratamento com a informação, onde cada usuário deve ter conhecimento da existência da Política de Segurança da Informação e o discernimento para lidar com os dados, estando ciente de sua responsabilidade como portador deles. Também é importante definir as consequências para os funcionários que não cumprirem essas determinações, de forma bem clara, na política de segurança da informação.

As normas ISO 27000 e suas derivadas tratam basicamente de questões do SGSI, onde são tratadas questões sobre técnicas de segurança envolvendo implementações, procedimentos, medidas, gerenciamento de riscos, auditorias, entre outros. Vejamos a figura a seguir que nos traz as mais relevantes para estruturação do SGSI:

Figura 3 - Família ISO 27000



Fonte: adaptado de https://www.iso.org/ics/03.100.70/x/ e ISO 27001 e 27002: Uma Visão Prática. Bastos e Caubit (2009).

Para aplicação do que é definido pela NBR ISO/IEC 27001 (2013), existem algumas ferramentas úteis para se obter os resultados esperados. Assim, é adequado o uso do modelo proposto no PDCA (*Plan, Do, Check, Act*) para obtenção de uma visão holística do que será feito. Em seguida, deve ser feita uma estruturação do projeto de SGSI, através dos seguintes recursos: Planejamento do projeto, Criação e Manutenção SGSI e Auditoria Externa (BASTOS; CAUBIT, 2009).

Na visão de Bastos e Caubit (2009, p. 36), há alguns fatores críticos para que se obtenha sucesso na implementação de um SGSI:

- Comprometimento e apoio visíveis pela alta administração;
- Escolha do Gerente do Projeto de Preparação para Certificação;
- Unificação conceitual nos vários níveis dos participantes (usuários e gestores) sob o perímetro de abrangência do escopo e os princípios do SGSI;
- Definição clara do escopo do sistema de gestão de segurança da informação;
- Definir a abordagem para a implementação da segurança da informação consistente com a cultura organizacional;
- Divulgação das diretrizes da política de segurança e padrões para todos os funcionários, cliente e terceiros;
- Ativos identificados e controle de ativos (inventário) mantido atualizado;
- Análise/avaliação de riscos executada e resultados documentados;

- Decisões de gerenciamento de riscos (nível no risco aceitável aprovado pela direção).

Através do conteúdo demonstrado, é notável que o SGSI consegue envolver todo o ambiente corporativo, através de seus métodos e procedimentos direcionados, principalmente pela ISO 27001, motivando os executivos, investindo na infraestrutura de rede e nos dispositivos de Tecnologia da Informação, implementando controles de acesso e de material, conscientizando os *stakeholders* e expandindo para toda a organização através de políticas e documentações.

1.3.1.1 Ciclo PDCA

Esta ferramenta é muito útil na implementação e utilização do SGSI, pois delimita sua abrangência, estima metas, verifica o que vem sendo feito e age sobre um planejamento que é feito de forma premeditada, além de garantir um bom controle e visão generalizada do sistema como um todo, trazendo melhorias e agilidade relacionadas às atividades executadas, as quais são muito bem segregadas no momento em que é elaborado o planejamento.

De acordo com Beal (2008, p. 37) o PDCA é um “método utilizado em processos de gestão da qualidade que se aplica aos mais divesos tipos de níveis de gestão, é útil para fornecer uma visualização global das etapas que devem compor a gestão da segurança da informação.”

Bastos e Caubit (2009) conceituam que Ciclo PDCA é uma “sigla que significa Planejar (P), Executar ou fazer (D), Verificar ou Checar (C), e Agir corretivamente (A), é uma ferramenta utilizada para garantir a evolução dos sistemas de gestão nas normas ISO 9001 e ISO 14000, por exemplo”. Na visão dos autores e, embasado em estudo das Normas ISO, a sigla PDCA envolve as etapas definidas no Quadro 2, a qual também foi estruturada pelos autores [com base no PMBOK de 2004], conforme a Figura 4.

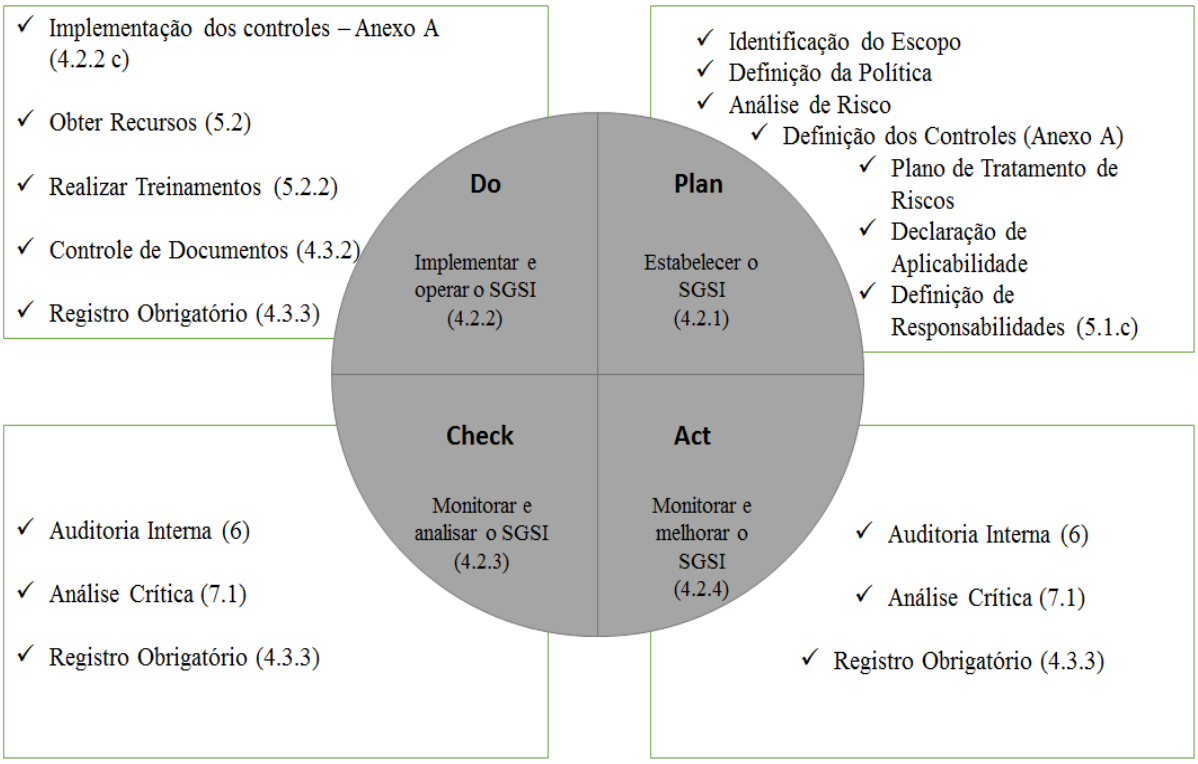
Quadro 2 - Fases do Ciclo PDCA

Fase	**Descrição**
Plan (planejar) (estabelecer o SGSI)	Estabelecer política do SGSI, objetivos, processos e procedimentos relevantes para o gerenciamento de riscos e a melhoria da segurança da informação para produzir resultados de acordo as políticas globais e objetivos globais de uma organização
Do (fazer) (implementar e operar o	Implementar e operar a política,

SGSI)	controles, processos e procedimentos do SGSI
Check (Checar) (monitorar e analisar criticamente o SGSI)	Avaliar e, onde aplicável, medir o desempenho de um processo frente a política, objetivos e experiência prática do SGSI e apresentar os resultados para análise crítica pela direção
Act (agir) (manter e melhorar o SGSI)	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI (ISO 27001:2005)

Fonte: Adaptado de ISO 27001 e 27002: Uma Visão Prática. Bastos e Caubit (2009)

Figura 4 - Estruturação do Ciclo PDCA no SGSI



Fonte: ISO 27001 e 27002: Uma Visão Prática. Bastos e Caubit (2009) [com base no PMBOK 2004]

Analisando a figura é possível observar uma visão geral da implementação do SGSI no âmbito corporativo, há uma série de medidas que definem o escopo, as regras e soluções a serem aplicadas [Plan]. Há medidas para fiscalizar, analisar e registrar melhorias nos processos [Check e Act]. Os quais são concretizados através de ações de controlar processos internos, obter recursos, **realizar treinamentos** [conscientização de usuários] e controlar documentos. Cabe

ressaltar a importância de efetuar registros, pois estão presentes em todas as fases do Ciclo, os quais podem servir de subsídio para facilitar ações futuras.

Não obstante, Bastos e Caubit (2009, p. 36) esclarecem que: “a maturidade de um sistema de gestão de segurança da informação é adquirida com as sucessivas rodadas do ciclo do PDCA, cujo tempo de execução pode variar de organização para organização.”

A partir do trabalho orientado pelo Ciclo PDCA, Bastos e Caubit (2009, p. 38) nos trazem algumas vantagens que podem vir do uso desta ferramenta, pois o SGSI estruturado de acordo com o PDCA

> será um sistema de gestão de segurança da informação que tende a amadurecer mais rapidamente e se estender pela organização além dos limites do seu escopo, ou simplesmente da abrangência prevista inicialmente para sua implementação.

Tendo em vista o conteúdo supramencionado, é possível dizer que quando esse ciclo é executado repetitivamente, há uma melhoria devido à sequência das atividades que é feita novamente, renovando a visão (de forma periódica) e enfatizando a melhoria dos pontos fracos do que já vinha sendo feito.

1.3.2 Segurança em Recursos Humanos

Outra ferramenta muito importante para o SGSI, com foco em pessoas, é o fator de segurança em Recursos Humanos (RH), que deve verificar um planejamento para o ser humano relacionado ao ambiente corporativo, desde o momento de sua seleção e contratação, permanecendo durante o exercício de sua atividade e executando procedimentos após o término de seu contrato. Sobre o assunto Bastos e Caubit (2009, p.70) nos dizem que a Segurança em RH tem como objetivo:

> reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações e recursos de processamento, bem como evitar o acesso ou a divulgação de informações indevidamente. As responsabilidades sobre a segurança devem ser atribuídas e identificadas para cada cargo ou função sob o escopo da certificação desde a fase de recrutamento, ou seja, antes da contratação (A.8.1), incluídas em contratos de trabalho e monitoradas durante a vigência de cada contrato de trabalho, no período de contratação (A.8.2), bem como após o desligamento deste profissional da organização (A.8.3).

Na visão dos mesmos autores, também é importante para

> assegurar que os usuários e demais envolvidos no SGSI estão cientes das ameaças e das preocupações de segurança da informação e equipados para apoiar a aplicação da política de segurança da organização durante a execução normal do seu trabalho. Os usuários devem ser treinados nos procedimentos de segurança e no uso correto das instalações de processamento da informação, de forma a minimizar possíveis riscos de segurança. As campanhas periódicas de conscientização buscam assegurar que a segurança da informação seja inserida na cultura corporativa, sendo primordial o apoio ostensivo da direção como auxílio no sucesso do processo de capacitação (liberando recursos, dando importância política à campanha, resolvendo conflitos etc.). Outras áreas internas, como Recursos Humanos e Marketing, devem se envolver com as campanhas e treinamento, não somente para dar apoio, mas também para desenvolver uma linguagem uniforme de tratamento da segurança da informação por toda a organização. (BASTOS; CAUBIT, 2009, p.71)

Da mesma forma, a NBR ISO/IEC 27001 (2013) distingue, na seção 7 do Anexo “A”, a Segurança em RH em 3 fases, conforme demonstrado no quadro 3:

Quadro 3 - A.7 Segurança em Recursos Humanos

Seção	Fase	Objetivo
A.7.1	Antes da contratação	Assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.
A.7.2	Durante a contratação	Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação.
A.7.3	Encerramento e mudança da contratação	Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.

Fonte: adaptado da NBR ISO/IEC 27001:2013

Beal (2008, p. 45) reforça medidas de controle em relação aos aspectos humanos de segurança, partindo de definições sobre

> a política de segurança de pessoal (processos de admissão e demissão, requisitos de segurança aplicáveis a funcionários e prestadores de serviço, treinamento em segurança). Diretrizes do comportamento esperado em relação ao uso dos diversos tipos de recursos computacionais disponíveis (tais como *e-mail,* Internet, Intranet, sistemas de informação etc.) e em caso de ocorrência de uma quebra de segurança.

Com base no estudo da Norma supramencionada e no conteúdo referenciado, podemos partir do princípio que, antes mesmo de ser contratado, o funcionário já deverá adquirir a consciência de que possuirá responsabilidades no

exercício de suas atribuições, a qual será reforçada durante a contratação (mediante conscientização e fiscalização) e garantida após o encerramento da contratação, comunicando as responsabilidades dos ex-funcionários e fazendo-as serem cumpridas.

1.3.3 Política de Segurança da Informação

A Política de Segurança da Informação tem por objetivo: “prover uma orientação e apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes”. (NBR ISO/IEC 27002, 2013)

Trata-se do documento que contém de forma clara e resumida as premissas e diretrizes para o SGSI (BASTOS; CAUBIT, 2009). Onde são descritos procedimentos importantes e relevantes associados ao uso da informação, bem como as responsabilidades atribuídas a cada funcionário.

Para Dias (2000, p. 48), a política de segurança é um

> mecanismo preventivo de proteção dos dados e processos importantes de uma organização que define um padrão de segurança a ser seguido pelo corpo técnico e gerencial e pelos usuários, internos ou externos. Pode ser usada para definir as interfaces entre usuários, fornecedores e parceiros e para medir a qualidade e a segurança dos sistemas atuais.

É importante mencionar que ela “estabelece padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida pela e para a empresa; portanto, a política deve ser personalizada.” (SÊMOLA, 2003, p. 105)

O inciso VII do Art. 1º do Decreto Presidencial nº 3.505 (BRASIL, 2000), onde foi instituída a PSI na APF, determina que um dos pressupostos básicos da Política é a conscientização de órgãos e entidades da APF acerca da importância das informações processadas e risco de sua vulnerabilidade. Ainda no Decreto supracitado, são delimitados os objetivos da PSI no Art. 3º, os quais se encontram demonstrados no quadro 4.

Quadro 4 - Objetivos das PSI em órgãos públicos

Inciso do Art. 3º	Descrição
I	Dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a

	confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis
II	Eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação
III	Promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação
IV	Estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação
V	Promover as ações necessárias à implementação e manutenção da segurança da informação
VI	Promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação
VII	Promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação
VII	Assegurar a interoperabilidade entre os sistemas de segurança da informação

Fonte: adaptado do Decreto Presidencial nº 3.505 (BRASIL, 2000).

A NBR ISO/IEC 27002 (2013) afirma que é conveniente a implementação da PSI no mais alto nível da organização, aprovado pela direção e estabelecendo a abordagem da organização para gerenciar os objetivos de segurança da informação. A Política de Segurança da Informação (PSI) é a ferramenta que pode trazer uma comunicação mais próxima da alta direção com seus funcionários.

Por fim, conforme citações e aplicações demonstradas, é possível afirmar que a PSI necessita de apoio e aprovação da alta direção, pois insere diretrizes de implementação que devem orientar quanto ao uso da informação, o que faz necessário que cada política seja adaptada e adequada ao seu ambiente corporativo. Todo esse esforço vale pouco se não houver ampla divulgação e conscientização dos *stakeholders* quanto às determinações e diretrizes relativos à informação.

2 PROCEDIMENTOS METODOLÓGICOS

Além da revisão bibliográfica que foi pesquisada, onde foi demonstrada uma visão geral sobre o valor das informações contidas no setor de licitações do Órgão Público estudado, foi feita uma análise e avaliação do nível de Segurança da Informação no setor, com foco nos usuários de rede. Através de um estudo de caso, foi feita a coleta de informações sobre comportamentos dos usuários de rede, necessárias à fundamentação do estudo ora pretendido através dos seguintes instrumentos metodológicos:

a) Verificação de decisões tomadas por usuários de rede sobre os riscos a que podem se expor mediante a má utilização de *internet, e-mails*, mídias e outros meios de comunicação utilizados diariamente;

b) Palestra de conscientização de funcionários, direcionada pela NBR ISO/IEC 27002:2013 e legislação em vigor, buscando oportunidades de melhoria na conscientização de usuários de rede, com enfoque na segurança da informação, apresentando boas práticas para o uso dos diversos recursos de TI;

c) Verificação dos conhecimentos adquiridos pelos funcionários na palestra, através de questionário.

O método utilizado foi direcionado pela obra de Gil (2008), onde o questionário é tratado como uma técnica de investigação através de questões com o propósito de obter informações sobre práticas e conhecimentos [garantindo o anonimato das respostas], através de questões fechadas sobre padrões de ação relacionadas ao problema pesquisado. Conforme orientado pelo autor, o questionário contém instruções acerca do correto preenchimento das questões, informações sobre a entidade patrocinadora, bem como importância e razões da realização desta pesquisa.

Para analisar o nível de conscientização dos usuários de rede do setor estudado, foi preciso considerar o comportamento individual sobre segurança da informação ao manipular informações, considerando o contexto situacional.

Foram objeto de estudo as decisões dos funcionários diante de situações hipotéticas ao utilizar os meios de comunicação, avaliando a forma como os seus recursos de TI são utilizados e o nível de conhecimento individual em Segurança da Informação, o qual foi feito através de questões de múltipla escolha.

A intenção do questionário foi demonstrar o comportamento de cada funcionário e se fazem uso de boas práticas com os dados que tem sob sua posse, uma vez que não houve qualquer tipo de conscientização prévia acerca do assunto abordado, ou seja, ainda não havia sido agregado conhecimento aos pesquisados. O questionário foi respondido por todos os funcionários do setor pesquisado, considerando-se o efetivo de sete pessoas.

Após o questionário preliminar, foi dado início ao próximo passo da pesquisa: a palestra de conscientização de usuários. Para este trabalho, foi elaborada e apresentada uma palestra sobre boas práticas para garantir um nível mais elevado de segurança da informação. Foram abordados assuntos relacionados aos principais ataques cibernéticos focados em usuários de rede e sobre engenharia social. A palestra foi criada com o auxílio do *software* Microsoft PowerPoint® e apresentada mediante o uso de notebook e projetor, numa sala adequada para a atividade. O conteúdo foi baseado em conceitos apresentados em sites de empresas de segurança como Avast, Norton e Kaspersky, e também do CERT.br.

Também foram divulgadas algumas medidas de ação preventiva sobre o assunto [cartilhas de conscientização], bem como a descrição de alguns tipos de métodos utilizados pelos cibercriminosos para afetar potenciais vítimas, o que permitiu consolidar ainda mais as informações que foram difundidas.

A palestra teve duração aproximada de uma hora e foi repetida uma vez, pois foi necessário dividir o efetivo de ouvintes para que o setor continuasse a execução de suas demandas de serviço.

Após o questionário inicial e a palestra de conscientização, foi efetuado o 2º questionário, com apenas 10 questões, focadas nas principais falhas encontradas no 1º questionário [preliminar]. A finalidade deste questionário era verificar se os *stakeholders* entenderam o que foi ministrado na palestra e se estavam aptos a tomar decisões mais seguras diante de situações que podem implicar em risco iminente de um ataque cibernético, conforme explanado na revisão bibliográfica. Os moldes utilizados foram similares aos do questionário preliminar, com questões de múltipla escolha, porém as questões eram voltadas às boas práticas apresentadas na palestra.

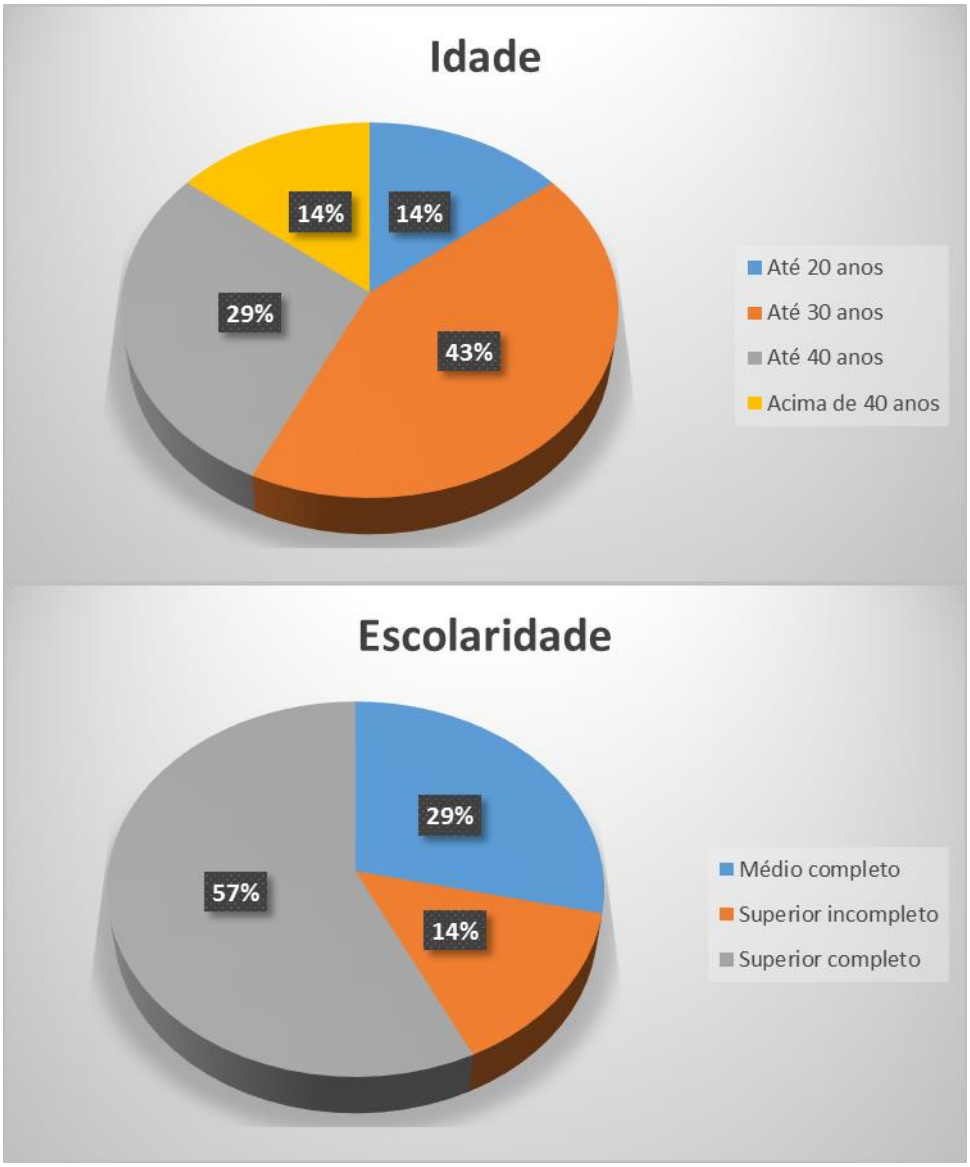
3 O ESTUDO DE CASO

O referido estudo está inserido no ambiente de um setor de licitações de um órgão público, cujo nome não é mencionado para preservação do nome da instituição, onde foi constatada a necessidade de conscientização dos usuários de rede [funcionários] sobre segurança da informação. O setor de licitações foi escolhido para estudo porque, no contexto de um órgão público, possui informações extremamente sensíveis, pois lida diretamente com as compras de produtos e serviços de empresas terceirizadas, qualquer dano aos seus dados pode significar prejuízos financeiros e à Administração Pública. Desta forma, ao analisar o seu contexto, foi verificado o comportamento dos funcionários diante de situações hipotéticas, para então conscientizar os usuários de rede mediante palestra, orientando sobre boas práticas para preservar a segurança das informações e verificados os resultados. O estudo foi voltado para prevenção das principais técnicas de ataque cibernético utilizadas por criminosos direcionadas a usuários: *phishing, malware* e engenharia social. Com foco nisto, foram enfatizados os seguintes assuntos: boas práticas no uso da internet, boas práticas no uso de computadores, elaboração de senhas, utilização de *backup* e evitando engenharia social.

3.1 Questionário preliminar à palestra

O questionário preliminar teve por finalidade analisar o comportamento dos usuários de rede, inseridos em aspectos de segurança da informação, verificando se sabiam atuar em situações hipotéticas de risco, leva-se em conta que não haviam sido informados sobre qualquer conteúdo da palestra ou das cartilhas. No questionário foram consideradas situações de ataques de *phishing, malware,* engenharia social, *spams*, *ransomware* e outros tipos de fraudes, os mais utilizados com foco em pessoas. Foram levados em conta alguns dados relevantes sobre os envolvidos nos questionários, considerando aspectos sobre idade, cursos na área de tecnologia e grau de escolaridade. Os quais encontram-se demonstrados abaixo [o gráfico de curso na área de TI não foi incluído, tendo em vista que todos afirmaram não possuir qualquer tipo de formação na área de TI]:

Gráficos 4 e 5 - Idade e escolaridade dos funcionários

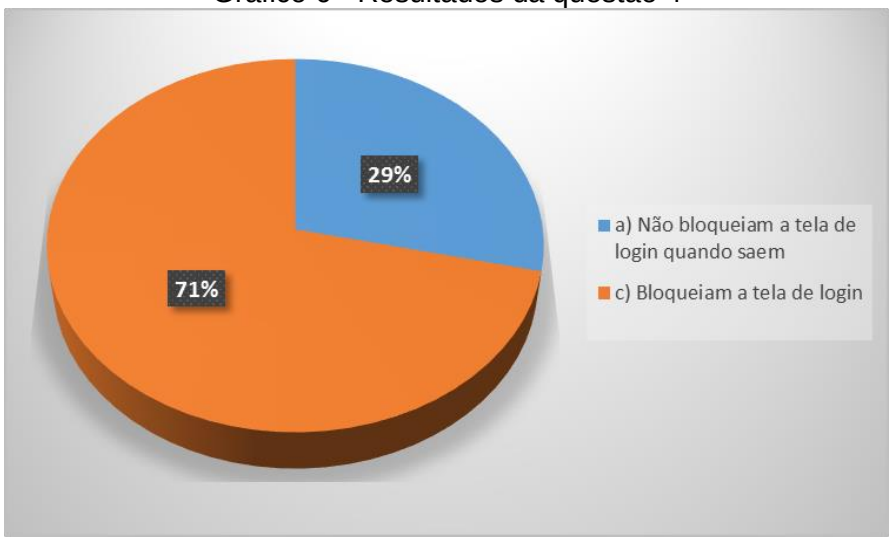


Fonte: elaboração própria

É perceptível o alto nível de escolaridade dos pesquisados, que somado com a idade e experiência de trabalho facilitaram a comunicação entre o palestrante e os funcionários. Seguem os dados das questões 4 a 18, que permitiram contextualizar os funcionários em situações cotidianas e avaliar quais posturas tomariam diante de possíveis acontecimentos:

Questão 4 - Os funcionários foram situados em uma ocasião na qual deveriam sair urgentemente de seus computadores para resolver um problema, apresentando as seguintes respostas:

Gráfico 6 - Resultados da questão 4



Fonte: elaboração própria

Foi constatado que 29% dos funcionários não se preocupam em bloquear a tela de login ao deixar o desktop, o que abre brechas para que outras pessoas tenham acesso aos seus arquivos enquanto estão ausentes dos seus ambientes de trabalho.

Questão 5 – Indagados sobre a elaboração de suas senhas, informaram que as criam da seguinte maneira:

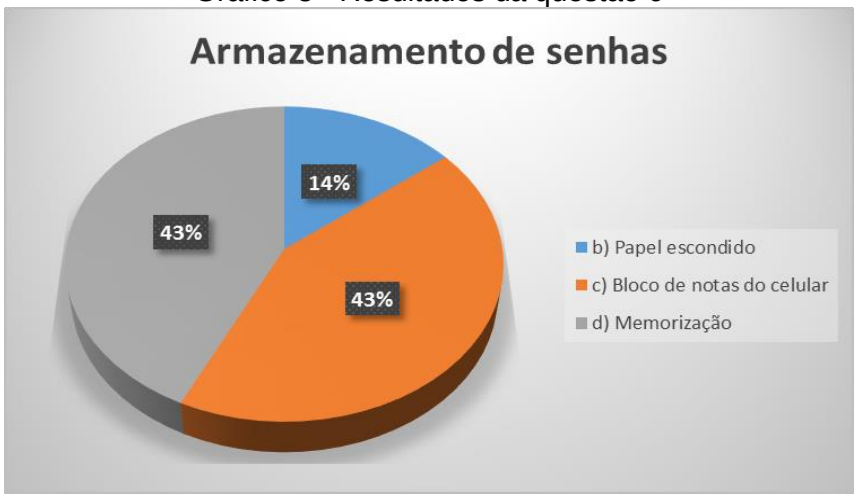
Gráfico 7 - Resultados da questão 5

Fonte: elaboração própria.

Apenas 57% dos funcionários utilizam senhas consideradas seguras no contexto atual, utilizar senhas que possuem apenas números e lembram coisas, lugares e momentos que viveu, podem se tornar vulnerabilidades para ataques de força bruta ou até mesmo ser facilmente notadas por pessoas fisicamente próximas que o veem digitando a senha.

Questão 6 – Interpelados sobre como armazenam suas senhas e quais métodos utilizam, responderam:

Gráfico 8 - Resultados da questão 6

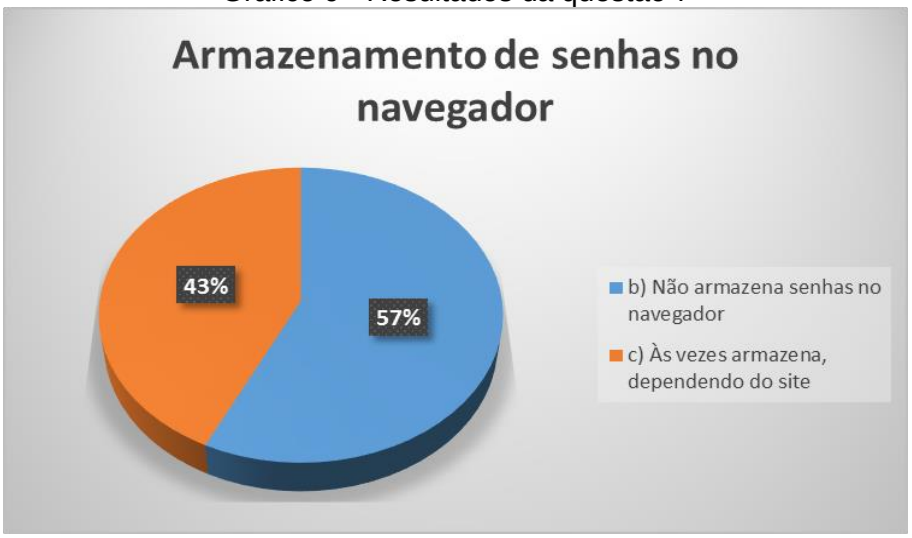


Fonte: elaboração própria

Como resultado, 43% dos funcionários memorizam as senhas na cabeça [o que pode incidir na perda das senhas por esquecimento], o restante anota no papel ou no celular, que também não é seguro devido à facilidade de acesso por outras pessoas. Nenhum deles utiliza software de gerenciamento de senhas, o qual é considerado como o mais seguro atualmente, uma vez que todas as senhas são armazenadas num arquivo criptografado que só abre com a chave-mestra de acesso.

Questão 7 – Os funcionários foram indagados quanto ao armazenamento de senhas no navegador, quando é oferecido que sejam memorizadas para o próximo acesso:

Gráfico 9 - Resultados da questão 7



Fonte: elaboração própria

43% dos funcionários armazenam senhas no navegador dependendo dos sites. O armazenamento de senhas pode se tornar um risco devido ao fato delas estarem salvas, as quais podem ser exibidas nas configurações de senhas salvas do navegador. Também há um arquivo, dentro da pasta do navegador, onde elas ficam armazenadas, porém podem ser acessadas caso alguém entre em seu *login* do sistema operacional, mesmo que o arquivo seja criptografado.

Questão 8 – Problematizados quanto aos avisos de atualização que são exibidos sobre os *softwares* do computador, responderam da seguinte maneira:

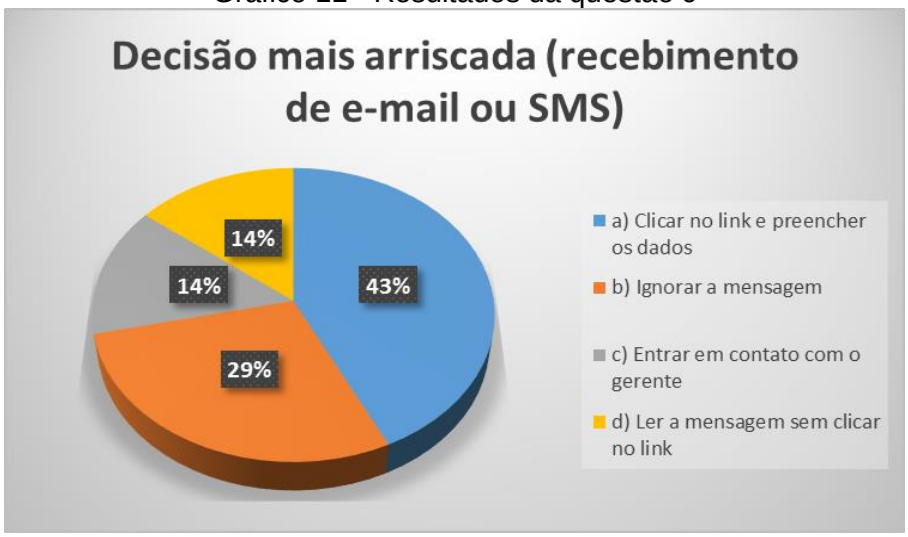
Gráfico 10 - Resultados da questão 8

Fonte: elaboração própria

Tendo em vista que 43% dos funcionários permanece inerte quanto à atualização dos computadores que utilizam no ambiente de trabalho, pode-se afirmar que há uma vulnerabilidade nessa questão, uma vez que boa parte dessas atualizações incidem em falhas de segurança dos *softwares*, que são sanadas assim que os programas são atualizados.

Questão 9 – Perguntados sobre qual seria a decisão mais arriscada ao receber um *e-mail* ou SMS do banco sobre multa e cancelamento do cartão, onde haveria um *link* no corpo da mensagem, foi informado o seguinte:

Gráfico 11 - Resultados da questão 9

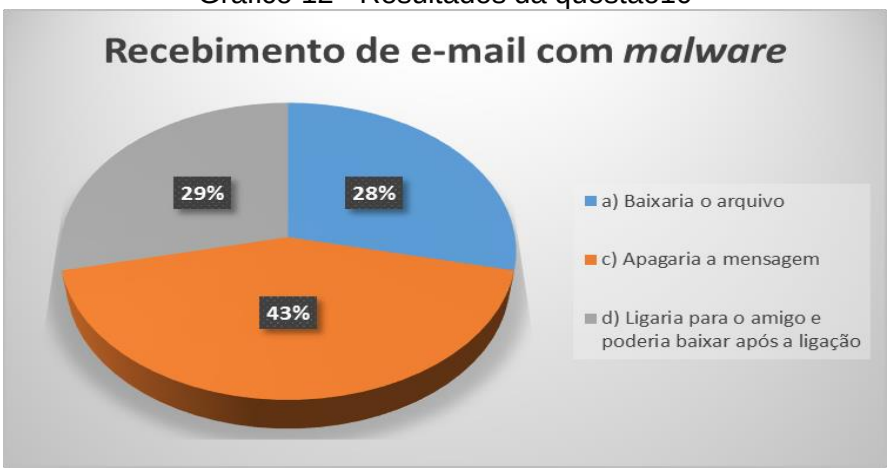


Fonte: elaboração própria.

Clicar num *link* de *e-mail* ou SMS com certeza seria a decisão mais arriscada, os bancos não costumam passar essas informações dessa maneira, isto poderia desencadear um ataque cibernético. Sendo assim, 43% dos funcionários sabem qual a postura mais arriscada quando recebem possíveis ataques de *phishing* através de e-mail ou SMS.

Questão 10 – Questionados sobre a decisão diante do recebimento de um *e-mail* com anexo malicioso (*malware*), diante de uma história de alguém se passando por um amigo, responderam o seguinte:

Gráfico 12 - Resultados da questão10



Fonte: elaboração própria.

28% dos funcionários baixariam arquivos de *malware* contidos em e-mail, 29% poderiam se tornar potenciais vítimas e 43% tomariam a postura correta diante da situação. O arquivo de extensão “.exe” nitidamente é malicioso, uma vez que não existem vídeos com este tipo de extensão, nem seria necessário ligar para o amigo

e confirmar, uma vez que ele poderia se confundir com outra ocasião e confirmar uma informação que não procede dele.

Questão 11 – Indagados sobre decisões diante envolvendo páginas de *sites* falsas, responderam:

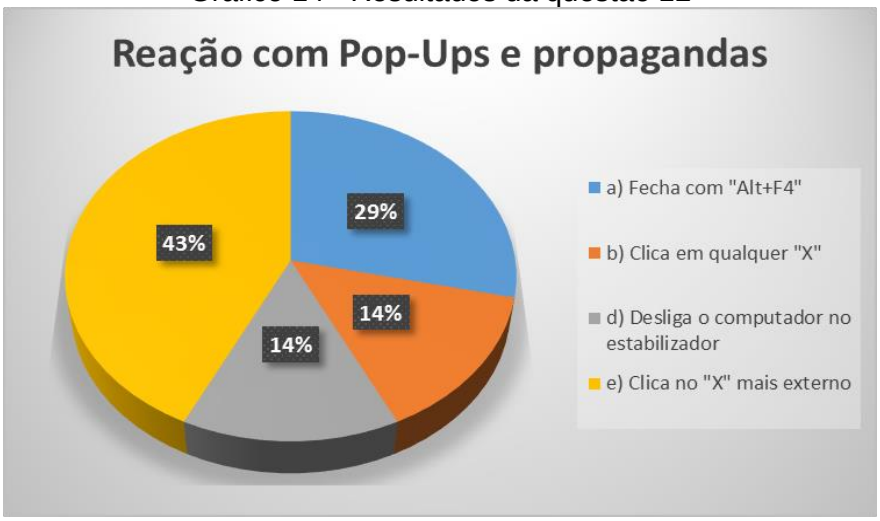
Gráfico 13 - Resultados da questão 11

Fonte: elaboração própria.

28% não saberiam lidar com possíveis sites de *phishing,* dos quais geralmente não possuam certificados SSL. Já existem recursos utilizados para fazer a página criada se tornar mais relevante que a original nas pesquisas do Google, fazendo com que ela venha a aparecer primeiro na lista de pesquisa.

Questão 12 – Ao serem interpelados quanto a pop-ups que aparecem de forma inesperada ao navegarem pela *internet*, informaram que tomariam a seguinte postura:

Gráfico 14 - Resultados da questão 12

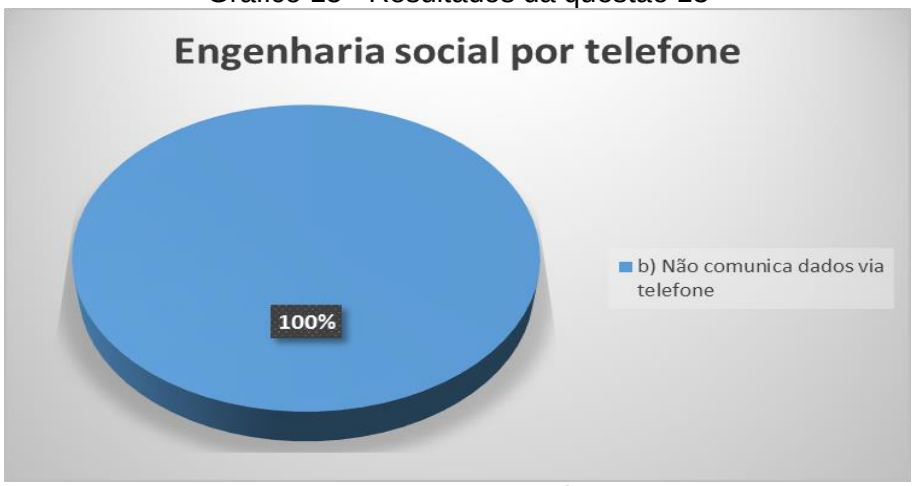


Fonte: elaboração própria.

28% não saberiam como fechar propagandas e pop-ups indesejados. Se a propaganda aparecer numa janela nova, é interessante fechar com “Alt+F4”. Porém, se estiver dentro da página, o “X” mais externo pode ser o mais seguro.

Questão 13 – Recebimento de ligação via celular que incide numa engenharia social:

Gráfico 15 - Resultados da questão 13

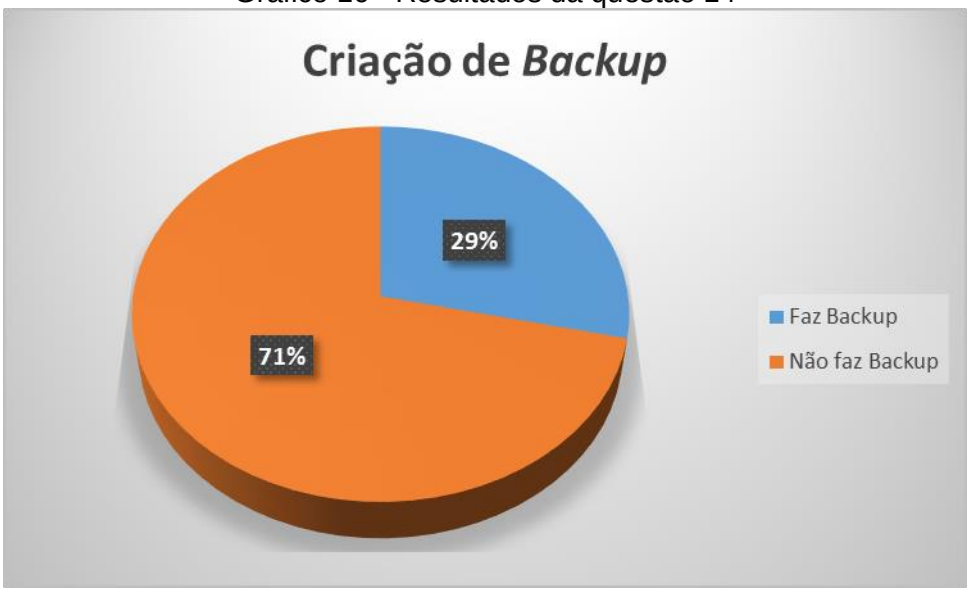


Fonte: elaboração própria.

Nenhum dos funcionários comunicaria dados via telefone às instituições, o que demonstra que estão conscientizados quanto ao assunto.

Questão 14 – Nesta questão foram abordados sobre o uso de *backup* de seus arquivos, obtendo os resultados demonstrados a seguir:

Gráfico 16 - Resultados da questão 14



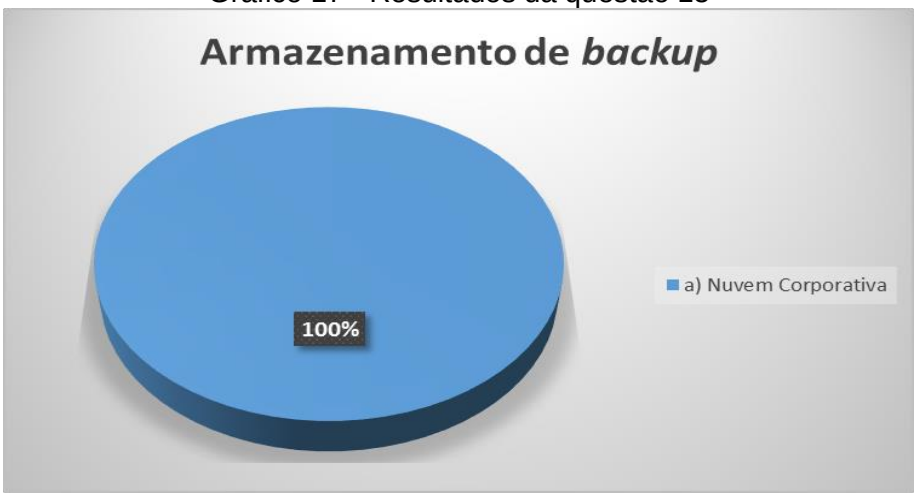
Fonte: elaboração própria.

71% dos funcionários não possuem cópias de arquivos em dispositivos externos (*backup*). Isto é uma falha grave e muito comum quando os funcionários não são conscientizados sobre o tratamento da informação, em caso de danos a

hardwares ou mesmo infecção por vírus, poderão perder seus dados e terão que trabalhar dobrado para elaborar novamente os que vinham sendo utilizados, sendo que alguns poderão ser perdidos definitivamente.

Questão 15 e 16 – Dos que utilizam *backup,* ficou demonstrado como e com que frequência armazenam suas cópias de dados:

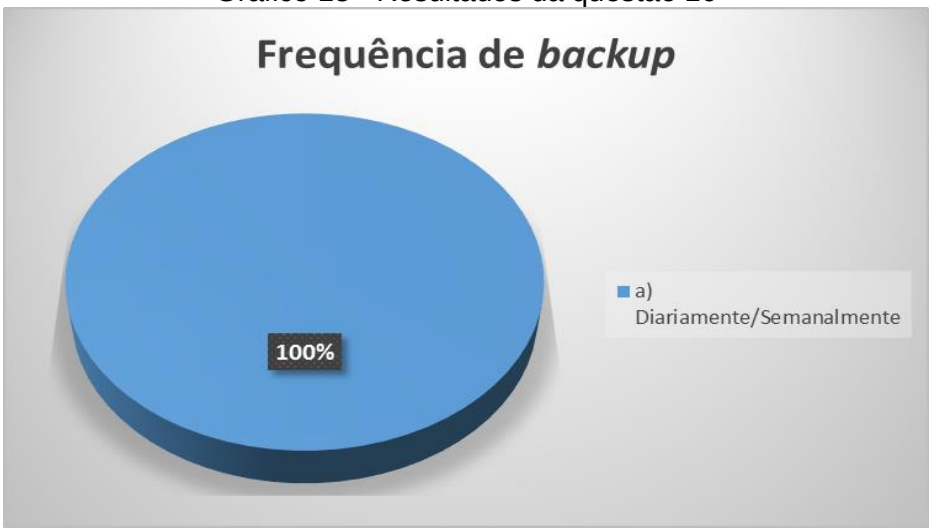
Gráfico 17 - Resultados da questão 15



Fonte: elaboração própria.

Dos 29% que fazem *backup,* todos utilizam a nuvem corporativa e o fazem diariamente/semanalmente, o que se considera o ideal neste caso. A nuvem corporativa tem essa finalidade e possui procedimentos para o tratamento das informações armazenadas ali. A frequência com que os *backups* são feitos pode definir quanto tempo de trabalho poderão perder em caso de incidentes.

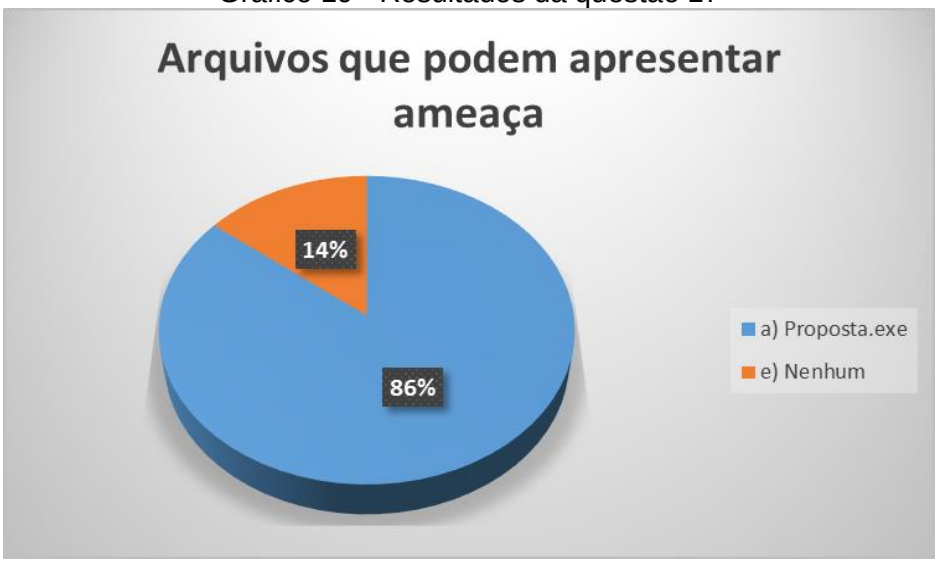
Gráfico 18 - Resultados da questão 16



Fonte: elaboração própria.

Questão 17 – Perguntados se saberiam identificar um arquivo de extensão maliciosa prestes a ser baixado, responderam:

Gráfico 19 - Resultados da questão 17



Fonte: elaboração própria.

Apenas 14% não saberia identificar um arquivo com extensão maliciosa, arquivos executáveis [.exe], quando de origem desconhecida, costumam ser tipificados como *malwares.*

Questão 18 – Conexão de dispositivos USB vindos de pessoas de fora da organização:

Gráfico 20 - Resultados da questão 18.

Fonte: elaboração própria.

Nenhum dos funcionários aceitaria conectar dispositivos externos de fornecedores em seus computadores, isso é considerado muito bom, pois evita uma série de arquivos maliciosos que podem estar inseridos em pendrives de pessoas desconhecidas.

Encerrados os preenchimentos dos questionários, foi verificado que a necessidade de conscientização existe e a palestra de conscientização seria muito

proveitosa no contexto de segurança da informação desse setor do órgão, uma vez que boa parte dos funcionários precisa tomar conhecimento de alguns métodos para se prevenir e tomar decisões que evitem situações prejudiciais às informações que estão sob sua responsabilidade. Os entrevistados estavam aptos a participar da palestra de conscientização e visualização das cartilhas acerca de assuntos relacionados a boas práticas de segurança da informação.

3.2 Palestra de conscientização dos usuários de rede

Ao iniciar a palestra, foi apresentada uma motivação e razões para se executar esse tipo de trabalho, em seguida, demonstrados, em nível prático, os riscos a que estão expostos quando navegam pela Internet e utilizam dispositivos eletrônicos, bem como se prevenir das ameaças expostas em sites e mídias removíveis.

Os assuntos da palestra foram abordados com base nas principais falhas dos funcionários, constatadas no questionário, e nas cartilhas que foram divulgadas no órgão, as quais estão inclusas no apêndice desta monografia. Foi verificado que boa parte dos funcionários estava vulnerável a ataques de *phishing, malware,* engenharia social, *spams*, *ransomware* e outros tipos de fraudes. Para isso a conscientização foi criada com abordagens sobre: boas práticas no uso de computadores, boas práticas na elaboração de senhas, navegação segura na internet, como evitar engenharia social, qual a necessidade de fazer *backup* dos arquivos e como fazê-lo.

Foram mencionadas algumas boas práticas no uso de computadores que mitigam uma série de vulnerabilidades:

- Bloquear o computador, para exigir *login* quando sair da estação de trabalho - ao colocar nessa tela, é necessário inserir o *login* e senha de usuário, o que se faz importante, para evitar uma ação de um desconhecido ou anônimo no seu computador. Esta prática dificulta a ação de uma pessoa mal-intencionada que pode estar tentando acessar os arquivos, uma vez que precisa da senha de acesso.
- Atualizar os softwares do sistema operacional – é importante que se mantenham os *softwares* atualizados, o que geralmente é informado por notificações do sistema operacional, nesse momento

é essencial a ação do usuário, atualizando o sistema ou comunicando ao setor de TI para que o faça. Esta medida é motivada pela segurança, pois boa parte das atualizações está voltada para alterações em vulnerabilidades ou falhas nos *softwares* que foram descobertas ou exploradas por *Hackers.*

- Cuidados com dispositivos USB – é comum a ocorrência de incidentes através de dispositivos de Pendrives e HDs Externos, onde arquivos maliciosos se infiltram nos computadores dos usuários, que são infectados e tendem a se propagar pela rede. É interessante evitar que se conectem dispositivos desse tipo, porém, caso seja de extrema importância, se faz necessário executar uma varredura com antivírus antes de se transferir qualquer arquivo para o computador.

Em seguida foram abordadas boas práticas para elaboração de senhas:

- Ao elaborar senhas é aconselhável combinar palavras e números, com caracteres especiais, maiúsculas e minúsculas, evitando usar os dados pessoais. Esta medida diminui as possibilidades de quebra de senhas por força bruta.
- Para gerenciar as senhas, é importante utilizar um software de gerenciamento de senhas ou memorizar na cabeça, porém a memorização incide na possibilidade de esquecimento de senhas, o que prejudicaria o andamento de atividades diárias.
- Evitar armazenamento de senhas no navegador, pois pode se tornar uma vulnerabilidade desnecessária no momento em que é possível visualizá-las através das opções de senhas armazenadas no navegador, sem qualquer necessidade de inserção de login e senha.

Navegação segura na Internet:

- É importante evitar popups e propagandas, uma vez que são muito utilizados para redirecionar para sites que são alvos de ataques cibernéticos, ou baixar arquivos maliciosos. Aconselha-se que

essas propagandas sejam fechadas com “Alt+F4” ou clicando no ícone de “X” mais externo do pop-up, para que não clique em um ícone falso de fechar e nem seja alvo do possível ataque.

- Evita-se clicar em links de e-mails, afim de evitar ataques de *phishing*, pois podem redirecionar para outros domínios (falsos), que buscam coletar seus dados para arquivar em bancos de dados de pessoas maliciosas, geralmente se passam por instituições de alta credibilidade na sociedade.
- Evita-se baixar anexos de e-mails, principalmente arquivos com extensão .cmd, .bat, .scr, .exe e .zip. Estes tipos são comuns em ataques de *malwares*, os quais agem sorrateiramente no sistema operacional, podendo afetar os princípios da confidencialidade, integridade e disponibilidade dos dados.
- Verificar certificados SSL em sites, principalmente os que envolvem operações financeiras ou dados pessoais. O símbolo do cadeado verde fechado ou o “https” ao início do endereço, demonstram a segurança da transmissão de informações reconhecida pelo navegador de internet, os quais criptografam as informações durante as transmissões, evitando que os dados tramitem de forma clara, mas de forma segura.

Foi enfatizado o valor das informações das quais os funcionários do setor licitação possuem, da importância e responsabilidade de cada um quanto à produção, manipulação e preservação dos dados que estão sob sua posse. Em seguida, expostas as ações que os cibercriminosos costumam utilizar para fazer uma engenharia social, onde buscam fazer contatos pessoais persuasivos se aproveitando de algumas características comuns no ser humano: vontade de ser útil, de ser amigável, de agilizar as tarefas e de ajudar o próximo. Os quais usam estas informações para manipular pessoas, obter senhas, maiores acessos aos sistemas e dados pessoais de funcionários.

Por último, foi mencionada a importância do uso de *backup*. Para isso, coube ressaltar a vantagem de se ter os dados salvos, uma vez que podem ser perdidos através de um incidente, os quais facilmente são recuperados quando existe uma cópia deles salva em outro dispositivo. Esse tipo de método garante a

disponibilidade dos dados e deve ser feito frequentemente, se possível diariamente, sendo mais seguro criptografá-los e transferi-los à nuvem corporativa como forma de *backup*.

A introdução com motivação e o apoio do chefe do setor foram fundamentais para o envolvimento de todos no processo de garantia de uma melhoria na segurança das informações daquele setor. A linguagem de alto nível utilizada na palestra facilitou a comunicação entre o palestrante e os funcionários, garantindo a concentração de todos durante sua execução. O tempo também foi adequado, pois foi possível abordar os assuntos de forma mais direta, evitando que se tornasse um conteúdo maçante e enfadonho. Outro ponto importante foi o compartilhamento de experiências vividas pelos funcionários ao longo da carreira, onde os mais inexperientes puderam consolidar o conteúdo demonstrado através de exemplos práticos citados pelos mais experientes, inclusive o chefe que também participou da pesquisa e da palestra. Um ponto a melhorar na palestra seria a inserção de vídeos práticos e notícias de jornais com casos reais, afim de trazer ainda mais demonstrações sobre a responsabilidade de cada um.

A inserção de imagens e curtos textos na apresentação também foi positiva, garantindo a facilidade no entendimento e remetendo as falas do palestrante ao essencial de cada assunto. O que fez com que os funcionários dessem mais atenção quanto ao assunto e refletissem a importância de adotar boas práticas para o uso seguro da informação, levando em conta situações das quais já passaram por dificuldades devido à falta de adoção de certos procedimentos, que facilitariam a recuperação dos seus dados e agilizariam o serviço durante o expediente. Isto os fez questionarem diversas situações, inclusive na vida pessoal, sobre como poderiam evitar que acontecessem e quais atitudes poderiam mudar para melhorar.

A apresentação da palestra permitiu que o chefe do setor determinasse que o uso de *pen drive* fosse extinto, os usuários de rede do setor tiveram de se adaptar ao uso da nuvem corporativa, a apresentação da palestra permitiu que os funcionários entendessem os motivos e evitassem resistências quanto à determinação que foi dada. Outro fato observado foi o registro de chamados técnicos dos próprios funcionários ao setor de Tecnologia da Informação, solicitando que seus sistemas fossem atualizados. Fatos considerados como resultados positivos da palestra.

3.3 Questionário após a palestra

Após a avaliação inicial de conhecimento sobre segurança da informação e apresentação da palestra de conscientização, os pesquisados responderam a um novo questionário. Desta vez o objetivo foi avaliar os resultados após a conscientização dos usuários, identificando se os resultados foram positivos ou negativos. A elaboração de questões sobre ataques de *phishing, malware,* engenharia social, *spams, ramsonware* e outros tipos de fraudes, buscou verificar se o aprendizado foi assimilado pelos funcionários do setor de licitações do órgão público estudado. Este questionário buscou conceitos da área de segurança da informação, bem como aplicações do uso dos métodos explanados na palestra de conscientização. Os funcionários tiveram até quatro dias para responder aos questionários.

As questões estão embasadas nas necessidades de informação apresentadas nas respostas do questionário preliminar, conforme a descrição das questões a seguir:

Questão 1 – Envolve o conceito de *backup* de dados, que se trata de uma cópia dos dados em dispositivos de armazenamento externos à máquina local, é importante mencionar que fazer uma cópia dos arquivos no mesmo dispositivo não é *backup*, portanto a alternativa correta é a letra a). Esta questão foi elaborada devido ao fato de a maioria dos funcionários não utilizarem *backup* de seus dados e alguns nem sabiam do que se tratava;

Questão 2 – Avalia uma situação em que seria necessária a utilização do *backup,* o qual é muito útil quando há perdas ou corrupções de dados, muito comuns em ataques de *malware* e *ramsonware,* desta forma a alternativa correta é a letra a). A questão foi necessária para que os funcionários reconhecessem a importância de se efetuar esse método para preservação dos dados e quando devem utilizá-lo;

Questão 3 – Menciona alguns conceitos sobre *backup,* onde a alternativa incorreta é a c), que afirmava que a responsabilidade pela execução de *backup* é exclusiva do setor de TI. A responsabilidade principal é do usuário, uma vez que sabe quais são seus arquivos mais utilizados e qual sua necessidade. A inserção da questão foi elaborada pela necessidade de reconhecimento do usuário quanto à sua responsabilidade sobre o uso de *backup*;

Questão 4 – Aborda sobre formas de elaborar senhas, combinar palavras, números, caracteres especiais, maiúsculas e minúsculas tem sido a forma mais segura de se elaborar senhas atualmente, uma vez que dificulta vulnerabilidades a ataques de força bruta, portanto a alternativa correta é a d). A questão foi inserida porque quase metade dos funcionários utiliza senhas elaboradas apenas por números, coisas, lugares ou momentos que viveram;

Questão 5 – Discorre sobre formas de armazenar senhas, apesar de memorizar as senhas na cabeça ser a mais segura quanto a vazamento de senhas, pode-se perdê-la por esquecimento. Grandes quantidades de senhas devem ser armazenadas em programas de gerenciamento de senhas com criptografia, pois necessitam apenas de uma senha-mestra e são armazenadas em arquivos criptografados, desta forma a alternativa correta é a e). Esta questão foi inserida devido aos maus hábitos dos funcionários em armazenar suas senhas;

Questão 6 – Envolve conceitos sobre senhas, dos quais é incorreto afirmar que há segurança ao anotar senhas em papéis, independentemente de estarem em armários ou gavetas, sendo assim a alternativa incorreta é a a). Esta questão foi inserida devido aos maus hábitos dos funcionários em armazenar suas senhas;

Questão 7 – Contextualiza um caso de *phishing,* que geralmente se trata de uma página de *internet* redirecionada por um *link* contido em e-*mail* de autor desconhecido, a alternativa correta é a b). A importância de se criar esta questão ficou evidente pelo fato de que a maioria dos funcionários não sabia identificar o que era mais arriscado a se fazer quando se recebe um falso e-mail ou SMS, contendo *link*, de um autor desconhecido;

Questão 8 – Descreve a importância de se manter o computador atualizado, o que otimiza o desempenho e corrige falhas de segurança dos *softwares*, a alternativa correta é a b). Esta questão foi inserida porque foi constatado no questionário preliminar que quase metade dos funcionários ficava inerte quanto a atualizações do sistema operacional, o que pode prejudicar a manutenção da segurança da informação;

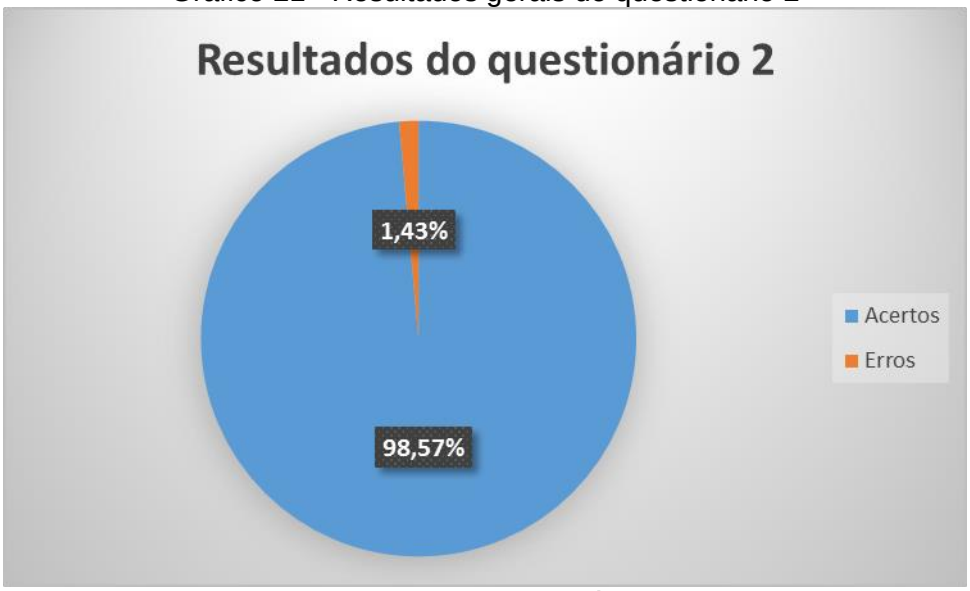
Questão 9 – Aborda sobre uma situação com envio de *malware* por anexo de e-mail, arquivos com extensão .scr possuem extensão de *screensavers,* .exe são executáveis, .bat são arquivos de *script* com comandos prontos. Arquivos .doc são documentos de texto e erros na digitação do nome do arquivo não tem significância

relevante, portanto a alternativa correta é a c). Esta questão teve ênfase na baixa porcentagem que não soube identificar arquivos de extensão maliciosa, possibilitando o aprofundamento em mencionar outros tipos de extensão e ênfase em cada tipo e função dessas extensões comumente utilizadas em *malwares*;

Questão 10 – Envolve melhores práticas para se fechar pop-ups e propagandas. Caso a propaganda esteja numa janela nova, é interessante fechar com “Alt+F4”, porém, se estiver dentro da página, o “X” mais externo pode ser o mais seguro, consequentemente a alternativa correta é a letra a). Sua relevância teve propósito no comportamento apresentado por alguns no questionário preliminar, onde alguns não sabiam qual a melhor maneira de se evitar problemas maiores com o aparecimento de propagandas e pop-ups indesejáveis.

Seguem os resultados gerais do questionário 2:

Gráfico 21 - Resultados gerais do questionário 2



Fonte: elaboração própria

- A eficiência dos pesquisados atingiu o nível de 98,57% de precisão nas respostas, demonstrando que os funcionários entenderam o assunto e que sabem agir sob certas situações que podem demonstrar risco aos seus dados;
- O resultado demonstrou que houve grande proveito da palestra ora apresentada, pois o aproveitamento foi de quase 100% de acertos.

3.4 Conclusões do estudo

Com os resultados deste questionário, a apresentação da palestra conscientização de usuários nos permitiu concluir que o método foi positivo e é muito proveitoso para mitigar as chances dos usuários de rede estarem vulneráveis a ataques de *phishing, malware,* engenharia social, *spams*, *ransomware* e outros tipos de fraudes. Também foi importante para demonstrar aos usuários de rede que eles possuem a responsabilidade de cuidar de seus dados, senhas e informações privilegiadas.

É possível afirmar que os funcionários que participaram da pesquisa adquiriram um conhecimento mínimo necessário na área de segurança da informação e sabem identificar situações que são comuns em certos tipos de ataques cibernéticos, o que reduz os riscos de incidentes relativos às informações sob sua posse, evidenciando que houve melhorias no contexto de segurança da informação do setor pesquisado.

Por último, é relevante mencionar a importância de se manter a constância desse tipo de trabalho, tendo em vista que os usuários de rede tinham recebido instruções há pouco tempo e conseguiram assimilar o conteúdo, porém alguns meses após o trabalho, o resultado tenderia a ser um pouco diferente. Esta pesquisa não pôde ser mais aprofundada devido ao curto tempo em que foi efetuada, caso contrário poderíamos obter resultados mais consolidados mediante um intervalo maior entre a palestra de conscientização e o segundo questionário, o que traz a expectativa de uma nova pesquisa envolvendo os funcionários daquele setor, afim de verificar se as observações permanecem em nível elevado ou se há necessidade de manutenção do que foi apresentado na palestra de conscientização.

CONCLUSÃO

O objetivo geral deste estudo foi analisar o contexto de Segurança da Informação de um setor de licitações num Órgão Público, avaliando o comportamento dos funcionários diante de situações hipotéticas, conscientizar os usuários de rede mediante palestra, orientando sobre boas práticas para preservar a segurança das informações e verificar os resultados obtidos pela conscientização através de questionário. Demonstrar, através do estudo de caso, se o método de conscientização afetou o tratamento com as informações manipuladas pelo setor.

Através do estudo de caso ficou nítido que a conscientização efetuada teve efeitos positivos no setor estudado, onde os funcionários adquiriram noções de tratamento com informações e boas práticas no uso de computadores, navegação na internet e uso de e-mail. Desta forma, o estudo almejou contribuir para um ambiente de trabalho mais seguro no intuito de preservar as informações que pertencem àquele setor.

Tendo em vista a norma que direciona esta pesquisa, é importante citar o que consta no tópico 7.2.2. da NBR ISO/IEC 27002:2013, que fala sobre conscientização, educação e treinamento em segurança da informação, onde convém que

> todos os funcionários da organização e, onde pertinente, partes externas devem recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções. (ASSOCIAÇÃO, 2013, p. 20)

Somente a palestra de conscientização e a divulgação de cartilhas não são o suficiente para garantir que os funcionários estão seguros quanto à utilização das informações, cabe ressaltar que outras ferramentas são importantes para se consolidar um Sistema de Gestão de Segurança da Informação (SGSI), como documentos de apoio às decisões e estratégias do setor de Tecnologia da Informação para um melhor aproveitamento do uso da informação, como a criação de uma Política de Segurança da Informação, Normas de Segurança da Informação (uso de internet, e-mail, senha de acesso), Termo de Uso da Rede Corporativa. Estas medidas garantem um comprometimento maior da alta direção com as medidas de segurança da informação, como também enfatiza ainda mais a responsabilidade [formal] de cada funcionário sobre o uso e tratamento de informações atinentes aos serviços relativos ao órgão.

Também são importantes as criações de comitês e grupos para a execução, fiscalização e implementação de medidas novas. Onde cada membro que os compõe teria sua finalidade fundamental dentro do ambiente corporativo, direcionando as decisões que competem a cada um e promovendo ações necessárias para implementação e manutenção da segurança da informação. Tais medidas de planejamento, ações, fiscalizações e ajustes, consolidam o ciclo PDCA, que exige a continuidade das atividades para que o SGSI seja implementado de maneira eficiente.

Cabe ainda mencionar o trabalho fundamental do setor de Tecnologia da Informação em implementar soluções de segurança no ambiente de infraestrutura de TI de forma física e lógica. É crucial a restrição de acesso a locais sensíveis, exigência de senhas a informações privilegiadas, controle de entrada e saída de pessoal e material, etc. A visão holística e coordenada voltada para os riscos de segurança da informação da organização deve ser considerada para que seja implementado um conjunto de controles de segurança da informação detalhado, embasado na estrutura global de um sistema de gestão coerente (ASSOCIAÇÂO, 2013).

Sendo assim, com a formalização das medidas de segurança da informação através de políticas, termos e normas, os programas de treinamento, educação e conscientização se aprimoram ainda mais, pois as diretrizes elaboradas podem ser melhor exploradas durante a execução das palestras, alinhando a conscientização dos funcionários às medidas implementadas pela alta direção. O conjunto de ações físicas e lógicas de infraestrutura combinado com usuários conscientizados garante um Sistema de Gestão de Segurança da Informação mais bem aprimorado.

REFERÊNCIAS

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

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

AVAST. **Malware – O que é malware e como removê-lo.** Disponível em: <https://www.avast.com/pt-br/c-malware>. Acesso em 30/08/17 às 14:30h.

BASTOS, Alberto; CAUBIT, Rosângela. **ISO 27001 e 27002 Uma Visão Prática.** Porto Alegre: Modulo, 2009.

BEAL, A. **Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações.** São Paulo: Atlas S.A., 2008.

BRAGA, P. **Técnicas de Engenharia Social.** Artigo – Universidade Federal do Rio de Janeiro – Instituto de Matemática, Rio de Janeiro, 2010. Disponível em: < https://securityinformationnews.files.wordpress.com/2014/02/tecnicas_de_engenharia_social.pdf >. Acesso às 19:00h do dia 21 de agosto de 2017.

BRASIL. Presidência da República. Decreto nº 3.505, de 13 de junho de 2000. **Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.** Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm>. Acesso em 23/08/17, às 10:30h.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008. **Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.** Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 13 de junho de 2008ª, n. 115 – Seção 1.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. **Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.** Diário Oficial [da] República Federativa do Brasil, Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 23/08/17 às 11h.

CENTRO DE ESTUDOS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. **Cartilha de Ataques na Internet.** Disponível em: <https://cartilha.cert.br/ataques/>. Acesso em 30/08/17, às 10:15h.

CENTRO DE ESTUDOS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. **Cartilha de Códigos Maliciosos.** Disponível em: <https://cartilha.cert.br/malware/>. Acesso em 30/08/17, às 10:15h.

CENTRO DE ESTUDOS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. **Cartilha de Golpes na Internet.** Disponível em: <https://cartilha.cert.br/golpes/>. Acesso em 30/08/17, às 10:15h.

CENTRO DE ESTUDOS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. **Cartilha de Segurança de computadores.** Disponível em: <https://cartilha.cert.br/computadores/>. Acesso em 30/08/17, às 10:15h.

CENTRO DE ESTUDOS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. **Cartilha de Segurança na Internet.** Disponível em: <https://cartilha.cert.br/seguranca/>. Acesso em 30/08/17, às 10:15h.

CENTRO DE ESTUDOS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. **Cartilha de Spam.** Disponível em: <https://cartilha.cert.br/spam/>. Acesso em 30/08/17, às 10:15h.

CENTRO DE ESTUDOS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. **Cartilha de Uso seguro da Internet.** Disponível em: <https://cartilha.cert.br/uso-seguro/>. Acesso em 30/08/17, às 10:15h.

CENTRO DE ESTUDOS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. **Estatísticas dos incidentes reportados ao CERT.br.** Disponível em: <https://www.cartilha.cert.br/stats/incidentes>. Acesso em 30/08/17, às 10h.

CENTRO DE ESTUDOS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT. **Incidentes reportados ao Cert.br – Janeiro a dezembro de 2016.** Disponível em: <br.https://www.cartilha.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html>. Acesso em 30/08/17 às 14h.

CENTRO DE ESTUDOS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT. **Spams reportados ao Cert.br por ano.** Disponível em: <https://www.cartilha.cert.br/stats/spam>. Acesso em 30/08/17 às 14h.

CÔRTE, K. **Segurança da Informação Baseada no Valor da Informação e nos Pilares Tecnologia, Pessoas e Processos.** 2014, 212p. Tese (Doutorado em Ciencia da Informação) – Universidade de Brasília – Faculdade de Ciência da Informação, Brasília.

DAWEL, D. **A Segurança da Informação nas Empresas**. Rio de Janeiro: Ciência Moderna, 2005.

DIAS, C. **Segurança e Auditoria da Tecnologia da Informação.** Rio de Janeiro: Axcel Books do Brasil, 2000.

FONTES, E. **Vivendo a Segurança da Informação.** São Paulo: Brasiliano & Associados, 2000.

FRÓIO, L. R. **Um Modelo Faseado de Gestão da Segurança da Informação.** 2008, 146p. Dissertação (Mestrado em Ciência da Informação) – Universidade de Brasília – Faculdade de Tecnologia, Brasília.

GABINETE DE SEGURANÇA INSTITUCIONAL. **Organograma do Gabinete de Segurança Institucional da Presidência da República.** Disponível em: <http://www.gsi.gov.br/sobre/estrutura>. Acesso em 18/08/17 às 10:35h.

GIL, A. C. **Métodos e Técnicas de Pesquisa Social** - 6ª Ed. São Paulo: 2008.

HARRIS, S. **All-In-One CISPP, Exam Guide Sixth Edition**. Estados Unidos: McGraw-Hill Companies, 2013.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELETROTECHNICAL COMISSION – ISO/IEC 27000:2014 – **Information Technology** - Security Techniques - Information Security Management Systems - Overview and Vocabulary – Suíça, 2014.

ISO. **Standards catalogue – 03.100.70 – Management systems**. Disponível em: <https://www.iso.org/ics/03.100.70/x/>, acesso em: 30/08/2017 às 21:38h.

EPTV. **Após ciberataque, Hospital de Câncer de Barretos estima 5 dias para normalizar atendimentos em todo o país.** Disponível em: <http://g1.globo.com/sp/ribeirao-preto-franca/noticia/apos-ciberataque-hospital-de-cancer-de-barretos-estima-5-dias-para-normalizar-atendimentos-em-todo-o-pais.ghtml>. Acesso em 04/09/2017 às 10:15h.

HANNA, W. **Hackers invadem sites do governo do DF e publicam ataques a Michel Temer.** Disponível em: <http://g1.globo.com/distrito-federal/noticia/hackers-invadem-sites-do-governo-do-df-e-postam-ataques-a-michel-temer.ghtml>. Acesso em 04/09/2017 às 10:15h.

KASPERSKY. **Você é ciberesperto?.** Disponível em: <https://www.kaspersky.com.br/blog/cyber-savvy-quiz/>. Acesso em 25/08/17 às 10h.

KHARAZ, A. et al. **UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware.** Disponível em: <https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_kharraz.pdf> acesso em 31/08/17 às 10:35h.

LUIZ, G. **Sistemas do GDF sofrem 12 invasões e 52 mil tentativas de 'ataque' em 2016.** Disponível em: <http://g1.globo.com/distrito-federal/noticia/sistemas-do-

gdf-sofrem-12-invasoes-e-52-mil-tentativas-de-ataque-em-2016.ghtml>. Acesso em 04/09/2017 às 16:40h.

MARCIANO, J. L. **O Enfoque Social da Segurança da Informação.** 2006, 88-98p. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília – Faculdade de Tecnologia, Brasília.

MITNICK, K. **The Art of Deception**. Estados Unidos: John Wiley & Sons, 2002.

NORTON. **Malware – Como eles atacam.** Disponível em: <https://br.norton.com/security_response/malware.jsp>. Acesso em 30/08/17 às 14:00h.

PEIXOTO, J. **Funcionária de empresa cedeu dados para hacker sem desconfiar de fraude;** Disponível em: <http://g1.globo.com/mg/grande-minas/noticia/funcionaria-de-empresa-cedeu-dados-para-hacker-sem-desconfiar-de-fraude.ghtml>. Acesso em 04/09/2017 às 13:30h.

PMI. **A Guide to the Project Management Body of Knowledge (PMBOK Guide)**. Pennsylvania: PMI, 2004.

PRESSE, F. **Ataque de hackers 'sem precedentes' provoca alerta no mundo.** Disponível em: <http://g1.globo.com/tecnologia/noticia/ataque-de-hackers-sem-precedentes-provoca-alerta-no-mundo.ghtml>, acesso em 31/08/17, às 10:05h.

SÊMOLA, M. **Gestão da Segurança da Informação Uma Visão Executiva.** Rio de Janeiro: Elsevier, 2003.

VIANA, E. W. **Análise do Comportamento Informacional na Gestão da Segurança Cibernética da Administração Pública Federal.** 2015, 115p. Dissertação (Mestrado em Ciência da Informação) – Universidade de Brasília – Faculdade de Ciência da Informação, Brasília.

VIEIRA, L. **Análise de malware em forense computacional.** Disponível em: <https://www.vivaolinux.com.br/artigo/Analise-de-Malware-em-Forense-Computacional>. Acesso em 18/08/17 às 11:00h.

APÊNDICE A – Questionário Preliminar À Palestra

Curso de Pós-Graduação *lato sensu* em Redes de Computadores com Ênfase em Segurança

Questionário

Prezado(a) Senhor(a), sou aluno do curso de pós-graduação *lato sensu* em Redes de Computadores com Ênfase em Segurança do Centro Universitário de Brasília, e solicito sua participação no presente questionário. O trabalho se desenvolve no contexto tecnológico da Segurança da Informação, onde o foco da pesquisa é avaliar a importância, necessidade e benefícios da conscientização de usuários de rede atuantes na Administração Pública Federal.

A Segurança da Informação é uma das atividades na área tecnológica que vem recebendo grande ênfase, principalmente após alguns ataques cibernéticos que tem afetado empresas e órgãos públicos de diversas maneiras, o que prejudica até mesmo o cidadão. A conscientização se faz necessária, uma vez que o fator humano influencia diretamente na produção, manipulação e divulgação de dados, sejam eles corporativos ou pessoais.

A pesquisa é faseada em três atividades:

1ª fase: Questionário.

2ª fase: Palestra de conscientização.

3ª fase: Questionário.

Estima-se que serão necessários 15 minutos para respondê-lo.

Desde já agradeço a atenção e cooperação em fazer parte desta pesquisa!

Cordialmente,

Ricardo Bruno Breustedt

Aluno do curso de Pós-Graduação do Instituto CEUB de Pesquisa e Desenvolvimento – UniCEUB.

Gilberto Netto

Orientador – Professor Doutor - Instituto CEUB de Pesquisa e Desenvolvimento – UniCEUB.

1) Idade:
   a) ( ) Até 20 anos.
   b) ( ) Até 30 anos.
   c) ( ) Até 40 anos.
   d) ( ) Acima de 40 anos.

2) Escolaridade:
   a) ( ) Fundamental incompleto.
   b) ( ) Fundamental completo.
   c) ( ) Médio incompleto.
   d) ( ) Médio completo.
   e) ( ) Superior incompleto.
   f) ( ) Superior completo.

3) Já fez qualquer tipo de curso na área de tecnologia ou segurança da informação?
   a) ( ) Sim.
   b) ( ) Não.

4) Você está trabalhando e há uma urgência para resolver fora da sua sala enquanto elabora um documento no computador, tendo em vista a necessidade de ir resolver o problema com rapidez, o que você faz?
   a) ( ) Deixo o computador como está e vou rapidamente ao local resolver o problema, afinal é urgente.
   b) ( ) Passo minha senha de *login* a outra pessoa para que ela termine o meu documento, enquanto resolvo a urgência.
   c) ( ) Bloqueio a tela do computador, para que seja solicitado *login/*senha quando voltar, enquanto resolvo a urgência.
   d) ( ) Ignoro a urgência, pois estou elaborando um documento.

5) Ao elaborar uma senha para uso de *e-mails* ou sistemas, qual o critério que você utiliza?
   a) ( ) Senhas sequenciais como “123456” ou “abcdef” para facilitar na hora de memorizar.
   b) ( ) Números de telefone, datas de nascimento, CPF, dados pessoais, etc.
   c) ( ) Substantivos que lembram coisas que gosto, lugares que visitei ou momentos que vivi.
   d) ( ) Combinação de palavras e números, com caracteres especiais, maiúsculas e minúsculas.

6) Os sistemas utilizados no trabalho exigem várias senhas, alguns inclusive exigem combinações complicadas, o que dificulta sua memorização. Qual método você utiliza para guardar suas senhas?
   a) ( ) Utilizo um *software* de gerenciamento de senhas.
   b) ( ) Anoto num papel e escondo em gavetas, armários ou lugares em que as pessoas não costumam mexer.
   c) ( ) Salvo no bloco de notas do meu celular pessoal.
   d) ( ) Memorizo todas as senhas em minha cabeça.
   e) ( ) Utilizo uma única senha para vários sistemas.

7) Ao inserir seu *login* e senha num *site*, o navegador oferece que sejam salvos os dados para que ele se complete automaticamente da próxima vez. Sabendo que, geralmente, somente você utiliza esse computador, salvaria os dados de *login*?
   a) ( ) Sim, assim agiliza meu acesso às contas que utilizo nos sistemas.
   b) ( ) Não, nunca permito que o navegador memorize minhas senhas.
   c) ( ) Às vezes, depende do *site*.

8) O sistema operacional do seu computador do trabalho adverte que são necessárias atualizações nos *softwares* do computador, qual sua postura diante da advertência?
   a) ( ) Ignoro, pois o computador está funcionando e não precisa que seus programas sejam atualizados.
   b) ( ) Peço ao setor de Tecnologia da Informação que atualize assim que possível.
   c) ( ) Aguardo até que o setor de Tecnologia da Informação venha até minha área de trabalho, independente do tempo que levar, para então atualizar meu sistema.
   d) ( ) Não faço nada, nem aciono o setor de Tecnologia da Informação, pois não quero alterar o sistema do computador que utilizo no trabalho.

9) Você recebeu um *e-mail* ou SMS do banco, informando que seus dados precisam ser atualizados afim de evitar multa e cancelamento do cartão, contendo um *link* no corpo da mensagem, qual seria a **DECISÃO MAIS ARRISCADA** nesse caso?
   a) ( ) Clicar no *link* e preencher os dados para evitar mal maior.
   b) ( ) Ignorar a mensagem e excluir o *e-mail*/SMS.
   c) ( ) Entrar em contato com o gerente do banco para que confirme o que foi enviado, e responder caso ele confirme.
   d) ( ) Ler a mensagem, porém sem clicar no *link.*

10) Você recebeu um *e-mail* de um velho amigo e verificou que seu endereço eletrônico era diferente do usual, porém no corpo da mensagem ele descreve que criou o *e-mail* recentemente e também afirma que está encaminhando como anexo um vídeo de uma viagem que vocês fizeram com o nome de “Viagem.exe”, que postura tomaria diante dessa situação?
   a) ( ) Baixaria o arquivo anexo ao *e-mail* e buscaria assistir assim que tivesse tempo disponível.
   b) ( ) Compartilharia após fazer o *download* do arquivo com os contatos mais próximos.
   c) ( ) Apagaria a mensagem.
   d) ( ) Ligaria para o amigo para questionar se enviou algum *e-mail* daquele endereço eletrônico recentemente.

11) Ao pesquisar um site, que você utiliza diariamente, em que é necessário efetuar *login* ou fornecer dados, o navegador de internet informa que o certificado de segurança do *site* não é confiável, o que não costumava acontecer em dias anteriores, o que você faz?
   a) ( ) Adiciono a exceção de segurança para entrar no *site*, pois esse tipo de aviso é irrelevante.
   b) ( ) Confirmo para que continue, adicionando a exceção de segurança, pois todos os dias busco esse mesmo site através de ferramentas de pesquisa como o *Google*.

c) ( ) Verifico se o endereço do *site* está correto e, tento digitá-lo no navegador, para ter certeza de que é o *site* que utilizo diariamente, para só então confirmar a exceção de segurança, pois confio em seus mantenedores.
d) ( ) Saio do *site,* pois não confio em *sites* sem certificado de segurança.

12) Ao navegar na *internet*, foi verificado que uma janela *pop-up* de repente se abriu com a seguinte mensagem: “Seu acesso foi premiado por ser o visitante de número 1.000.000 do nosso *site,* clique no *link* abaixo para receber seu prêmio”. Qual seria sua ação diante desta situação?
a) ( ) Busco fechar a tela com o atalho “Alt+F4”.
b) ( ) Clico em qualquer “X” que aparecer, principalmente o mais centralizado, se houver mais de um.
c) ( ) Clico no *link* para saber como receber meu prêmio.
d) ( ) Desligo o computador no estabilizador.
e) ( ) Clico no “X” mais externo à figura da propaganda.

13) Você recebe uma ligação de um número de celular dizendo que recebeu um seguro de vida do banco em que possui conta corrente, através de um sorteio do qual você não tinha conhecimento que havia ocorrido. Entretanto a atendente que está ao telefone seguiu todos os procedimentos naturais de uma ligação corporativa, se identificando, informando que está sendo gravado e solicitando seus dados (nome, CPF, número da conta corrente e senha do cartão) para confirmação de que você é realmente o dono da conta, caso contrário ela afirma que não poderá autorizar a concessão. Supondo que você tenha interesse em adquirir um seguro de vida, o que você faz?
a) ( ) Aceito a proposta e informo meus dados, afim de dar agilidade ao seguro.
b) ( ) Não informo, pois não comunico meus dados via telefone, somente pessoalmente.
c) ( ) Aceito a proposta, porém solicito que me conceda um *e-mail* para informar meus dados, pois prefiro digitar.
d) ( ) Não informo, mas se a atendente insistir, posso mudar de ideia para não perder a oportunidade.

14) Você costuma fazer *backup* (cópia) de seus arquivos do computador do trabalho?
a) ( ) Sim
b) ( ) Não

15) Se sua resposta na questão 14 foi “sim”, qual seria o dispositivo mais utilizado para armazenamento de seus dados?
a) ( ) Nuvem corporativa
b) ( ) Pendrive
c) ( ) HD Externo

d) ( ) CD
e) ( ) Outros

16) Se sua resposta na questão 14 foi “sim”, com que frequência você faz esse *backup* novamente?
a) ( ) Diariamente/Semanalmente
b) ( ) Mensalmente
c) ( ) Semestral
d) ( ) Anualmente

17) Você está operando um pregão eletrônico no computador do trabalho e o fornecedor envia um arquivo contendo propostas anexas, qual dos arquivos abaixo poderia apresentar uma ameaça ao seu sistema operacional?
a) ( ) Proposta.exe
b) ( ) Proposta.JPG
c) ( ) Propsta.PDF
d) ( ) Proposta.PDF
e) ( ) Nenhuma das anteriores

18) Supondo que um fornecedor venha à sua sala hoje e informe que tem as propostas de uma licitação (através de pregão eletrônico) que ele está participando em seu órgão armazenadas num *pendrive,* afirmando que as trouxe para transferir ao seu computador, qual a melhor decisão a ser tomada?
a) ( ) Conectar ao computador e transferir.
b) ( ) Chamar alguém do setor de Tecnologia da Informação para vasculhar o *pendrive* com antivírus antes de transferir qualquer arquivo.
c) ( ) Copiar os arquivos e pedir ao fornecedor que também envie seus anexos através do site de pregão eletrônico.
d) ( ) Não copiar os arquivos e orientar que o fornecedor envie os anexos através do site de pregão eletrônico.

APÊNDICE B – Questionário Após A Palestra

Curso de Pós-Graduação *lato sensu* em Redes de Computadores com Ênfase em Segurança

Questionário – parte 2

Caro(a) Sr,(a), Esta é a fase final da pesquisa, obrigado por colaborar!

Considerando o que foi ministrado na palestra, responda as questões que seguem abaixo, assinalando com um “X” a opção correta.

1) O que é um *backup* de dados?
   a) ( ) Cópia de dados de um dispositivo de armazenamento a outro para tornar possível a sua restauração em caso de perda dos dados originais.
   b) ( ) Atualização dos *softwares* do computador.
   c) ( ) Cópia de dados de um dispositivo de armazenamento para o mesmo dispositivo em que foram produzidos, para tornar possível a sua restauração em caso de perda dos dados originais.
   d) ( ) Configuração dos dados dos sistemas que estão sendo utilizados no computador.

2) Qual das situações abaixo descreve o cenário ideal para o uso de *backups* de dados?:
   a) ( ) Para recuperar eventuais perdas ou corrupção de dados.
   b) ( ) Para evitar contaminações por vírus.
   c) ( ) Para garantir que o disco permaneça desfragmentado.
   d) ( ) Para atualizar o navegador de internet.

3) Ainda sobre backup, marque a alternativa **INCORRETA**:
   a) ( ) Uma das maneiras de fazer o *backup* é copiando os arquivos do computador em HDs externos.
   b) ( ) O backup diário é uma boa prática, tendo em vista que em caso de perdas de dados, recupera-se os dados para o dia anterior.
   c) ( ) A execução do *backup* é de responsabilidade exclusiva do setor de Tecnologia da Informação.
   d) ( ) Uma das maneiras de fazer o *backup* é copiando os arquivos do computador para a nuvem corporativa

4) Qual a maneira mais segura de elaborar uma senha?
   a) ( ) Senhas sequenciais como “123456” ou “abcdef” para facilitar na hora de memorizar.
   b) ( ) Números de telefone, datas de nascimento, CPF, dados pessoais, etc.
   c) ( ) Substantivos que lembram coisas que gosto, lugares que visitei ou momentos que vivi.

d) ( ) Combinar palavras e números, com caracteres especiais, maiúsculas e minúsculas.

5) De acordo com o que foi ministrado na palestra, qual a maneira mais adequada de armazenar grandes quantidades de senhas complexas?
   a) ( ) Enviar por e-mail para minha caixa de entrada.
   b) ( ) Anotar num papel e esconder em gavetas, armários ou lugares em que as pessoas não costumam mexer.
   c) ( ) Salvar no bloco de notas do meu celular pessoal.
   d) ( ) Memorizar todas as senhas em minha cabeça.
   e) ( ) Utilizar um *software* de gerenciamento de senhas.

6) Sobre o uso de senhas, marque a alternativa **INCORRETA**:
   a) ( ) É muito seguro anotar senhas em papéis, desde que permaneçam guardadas em armários, gavetas ou lugares onde outras pessoas não costumam mexer.
   b) ( ) O armazenamento de senhas no navegador pode se tornar uma vulnerabilidade que facilita o acesso às senhas por pessoas que possam tentar invadir o computador.
   c) ( ) Guardar as senhas na própria memória é muito seguro, porém incide no risco de um possível esquecimento das mesmas, o que pode acarretar na sua perda.
   d) ( ) Para uma grande quantidade de senhas complexas, uma boa solução é o uso de programas de gerenciamento de senhas com criptografia.

7) *Phishing* é a criação de páginas de *internet* falsas, com o objetivo de coletar dados de usuários, como *logins*, senhas e dados pessoais. Qual dos cenários abaixo descreve uma situação de *phishing?*
   a) ( ) Propagação de vírus através de pen-drive.
   b) ( ) Ao clicar num *link* contido num e-mail de autor desconhecido, é direcionado a uma página de *internet,* geralmente similar à de uma instituição de confiança, que propõe o preenchimento de um formulário e envio de dados.
   c) ( ) Ao abrir a caixa de entrada de e-mail, verificar várias propagandas repetidas do mesmo usuário, sobre coisas que talvez nem interessem ao dono do e-mail.
   d) ( ) Propagação de vírus na rede corporativa.

8) Qual a importância de se manter o computador atualizado?
   a) ( ) Não há necessidade de se manter o computador atualizado.
   b) ( ) As atualizações de programas do computador e do sistema operacional otimizam o desempenho e corrigem falhas de segurança dos programas, mitigando possíveis vulnerabilidades no sistema.
   c) ( ) Faz com que o computador fique totalmente imune a vírus.

d) ( ) Servem apenas para deixar a aparência do sistema operacional mais atraente.

9) Ataques de *malware* são comumente enviados através de anexos de e-mails. Para evitar um ataque desse tipo e, supondo que seja um anexo de e-mail, qual dos arquivos abaixo provavelmente **não** apresentaria um risco ao seu sistema?
   a) ( ) Licitacao.bat
   b) ( ) Licitacao.exe
   c) ( ) Licitacco.doc
   d) ( ) Licitacao.scr

10) Qual a melhor prática para se fechar pop-ups e propagandas indesejadas?
   a) ( ) Se for uma janela separada, fechar com “Alt+F4”, caso contrário, clicar no ícone de “X” mais externo do pop-up.
   b) ( ) Clicar em qualquer ícone de “X”, mesmo que esteja mais centralizado do que outros.
   c) ( ) Apertar a tecla “Enter” até que o pop-up ou propaganda seja fechado.
   d) ( ) Clicar em “OK” e “Seguinte” até que acabem as propagandas.

APÊNDICE C – Slides da Palestra de Conscientização

Palestra de conscientização

Segurança da Informação

Ricardo Bruno Breustedt

Sumário

- 1. Introdução
- 2. Desenvolvimento:
  - Boas práticas no uso de computadores
  - Elaboração de senhas
  - Navegação segura na Internet
  - Evitando engenharia social
  - Backups
- 3. Conclusão

Introdução

Ao pensarmos nas atividades executadas diariamente nas instituições, é possível notar que tudo gira em torno de informações.

Documentos, processos, protocolos, sistemas e dados pessoais giram em torno dessas informações, as quais são manipuladas por integrantes dos órgãos públicos.

Introdução

Agora reflita um pouco sobre todas as informações que estão sob sua posse atualmente. Imagine as seguintes situações e como você se sentiria se alguma delas ocorresse com as informações relativas à sua função:

- Todos seus arquivos elaborados e dados pessoais estão expostos para uma pessoa de fora da instituição;
- Todos seus arquivos elaborados e dados pessoais foram alterados e salvos por cima dos antigos sem o seu consentimento ou conhecimento;
- Todos seus arquivos foram apagados sem prévio aviso e você não tem mais acesso a eles

Desenvolvimento

Boas práticas no uso de computadores

1- Colocar o computador na tela de *login* quando sair da estação de trabalho.

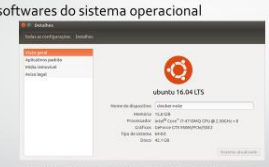
Fonte: http://ts.news.softpedia-static.com/images/news2/ubuntu-16-04-stupendously-hot-charmander-concept-looks-amazing-ulip644-9.jpg

Esta prática dificulta a ação de uma pessoa mal-intencionada que pode estar tentando acessar os arquivos aos quais você tem acesso, uma vez que precisa da senha de login.

Desenvolvimento

Boas práticas no uso de computadores

2- Atualizar os softwares do sistema operacional



Fonte: http://www.cleuber.com.br/wp-content/uploads/2016/04/sistemas604.png

Esta medida é motivada pela segurança, pois boa parte das atualizações está voltada para alterações em vulnerabilidades ou falhas nos *softwares* que foram descobertas ou exploradas por *Hackers*.

Desenvolvimento

Boas práticas no uso de computadores

3- Cuidados com dispositivos USB

Fonte: http://www.itworldcanada.com/wp-content/uploads/2016/05/FEATURE-USB-stick-Virus-THINKSTOCK-628x250.jpg

É interessante evitar que se conectem dispositivos desse tipo, porém, caso seja de extrema importância, se faz necessário executar uma varredura com antivírus antes de se transferir qualquer arquivo para o computador.

Desenvolvimento

Elaboração de senhas

1- Combinar palavras e números, com caracteres especiais, maiúsculas e minúsculas, evitando usar dados pessoais

flavio_arana

Ar@ntesF4K3#!

Esta medida diminui as possibilidades de quebra de senhas por força bruta.

Desenvolvimento

Elaboração de senhas

2- Para gerenciar as senhas, é importante utilizar um software de gerenciamento de senhas com criptografia ou memorizar na cabeça.

Fonte: https://opensource.com/sites/default/files/keepassx_newentry.png

É importante observar que a memorização incide na possibilidade de esquecimento de senhas, o que prejudicaria o acesso de sistemas.

Desenvolvimento
Elaboração de senhas

3- Evitar armazenamento de senhas no navegador, pois pode se tornar uma vulnerabilidade desnecessária no momento em que é possível visualizá-las através das opções de senhas armazenadas no navegador, sem qualquer necessidade de inserção de login e senha.

Desenvolvimento
Uso seguro da internet

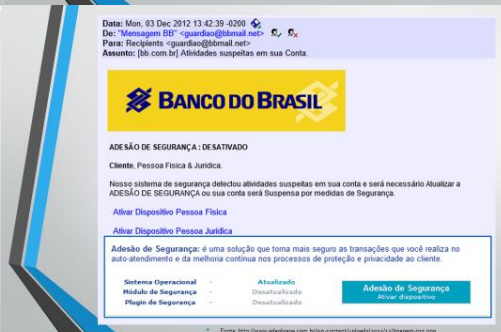
1- É importante evitar popups e propagandas.

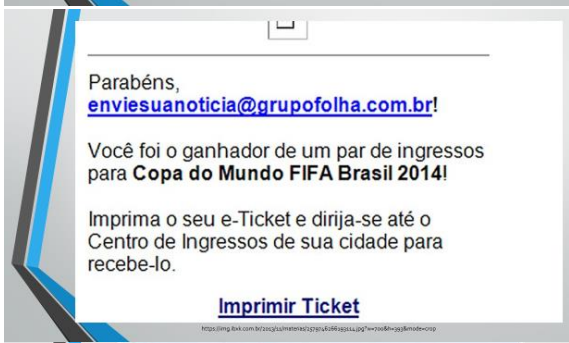
Muito utilizados para redirecionamento de sites ou baixar arquivos maliciosos. Aconselha-se que essas propagandas sejam fechadas com "Alt+F4" ou clicando no ícone de "X" mais externo do pop-up, para que não clique em um ícone falso de fechar e nem seja alvo do possível ataque.

Desenvolvimento
Uso seguro da Internet

2- Evita-se clicar em links de e-mails.

A finalidade é evitar ataques de phishing, pois podem redirecionar para outros domínios (falsos), que buscam coletar seus dados para arquivar em bancos de dados de pessoas maliciosas, geralmente se passam por instituições de alta credibilidade na sociedade.

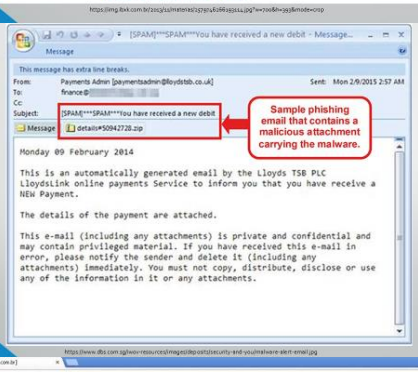




Desenvolvimento
Uso seguro da Internet

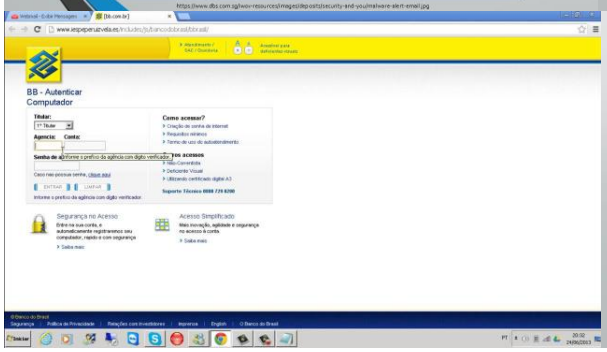
3- Evita-se baixar anexos de e-mails, principalmente arquivos com extensão .cmd, .bat, .scr, .exe e .zip.

Estes tipos são comuns em ataques de *malwares*, os quais agem sorrateiramente no sistema operacional, podendo afetar os princípios da confidencialidade, integridade e disponibilidade dos dados.



Desenvolvimento
Uso seguro da internet

4- Verificar ortografia de link e certificados SSL em sites, principalmente os que envolvem operações financeiras ou dados pessoais.



Desenvolvimento
Engenharia Social

Engenheiros sociais buscam informações através de pessoas mediante **contatos pessoais persuasivos** e se aproveitam das características do ser humano: vontade de ser útil, de ser amigável e de ajudar o próximo. Os quais usam estas informações para obter senhas, maiores acessos aos sistemas e dados pessoais de funcionários.

Desenvolvimento

Engenharia Social

É importante se considerar os seguintes atributos das informações ao ser abordado por alguém:

- o valor das informações;
- a importância; e
- responsabilidade de cada um.

Essa pessoa, por mais amigável que pareça, precisa saber desse tipo de informação?

Desenvolvimento

Backup

Cópia de arquivos em dispositivos externos à maquina local.

Mantém seus dados salvos e garante a disponibilidade de seus arquivos, caso haja perda daqueles que você utiliza diariamente.

Conclusão

Retirada de Dúvidas

APÊNDICE D – Cartilhas de Conscientização Divulgadas

Boas práticas no uso de computadores

1- Colocar o computador na tela de *login* quando sair da estação de trabalho.

Esta prática dificulta a ação de uma pessoa mal-intencionada que pode estar tentando acessar os arquivos aos quais você tem acesso, uma vez que precisa da senha de login.

2- Atualizar os softwares do sistema operacional

Esta medida é motivada pela segurança, pois boa parte das atualizações está voltada para alterações em vulnerabilidades ou falhas nos *softwares* que foram descobertas ou exploradas por *Hackers*.

3- Cuidados com dispositivos USB

É interessante evitar que se conectem dispositivos desse tipo, porém, caso seja de extrema importância, se faz necessário executar uma varredura com antivírus antes de se transferir qualquer arquivo para o computador.

Elaboração de senhas

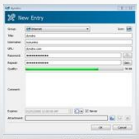
1- Combinar palavras e números, com caracteres especiais, maiúsculas e minúsculas, evitando usar dados pessoais

flavio_arana

Ar@naFak3#!

Esta medida diminui as possibilidades de quebra de senhas por força bruta.

2- Para gerenciar as senhas, é importante utilizar um software de gerenciamento de senhas com criptografia ou memorizar na cabeça.



É importante observar que a memorização incide na possibilidade de esquecimento de senhas, o que prejudicaria o acesso de sistemas.

3- Evitar armazenamento de senhas no navegador, pois pode se tornar uma vulnerabilidade desnecessária no momento em que é possível visualizá-las através das opções de senhas armazenadas no navegador, sem qualquer necessidade de inserção de login e senha.

Uso seguro da Internet

1- É importante evitar popups e propagandas.

Muito utilizados para redirecionamento de sites ou baixar arquivos maliciosos. Aconselha-se que essas propagandas sejam fechadas com "Alt+F4" ou clicando no ícone de "X" mais externo do pop-up, para que não clique em um ícone falso de fechar e nem seja alvo do possível ataque.

2- Evita-se clicar em links de e-mails.

A finalidade é evitar ataques de phishing, pois podem redirecionar para outros domínios (falsos), que buscam coletar seus dados para arquivar em bancos de dados de pessoas maliciosas, geralmente se passam por instituições de alta credibilidade na sociedade.

3- Evita-se baixar anexos de e-mails, principalmente arquivos com extensão .cmd, .bat, .scr, .exe e .zip.

Estes tipos são comuns em ataques de *malwares*, os quais agem sorrateiramente no sistema operacional, podendo afetar os princípios da confidencialidade, integridade e disponibilidade dos dados.

4- Verificar ortografia de link e certificados SSL em sites, principalmente os que envolvem operações financeiras ou dados pessoais.

Fonte: http://i1.ytimg.com/vi/aaaaaaag-c8/aaaaaaa/backup.jpg

BACKUP

1- O que é?

Cópia de arquivos em dispositivos externos à maquina local.

2- Por que fazer backup?

Porque mantém seus dados salvos e garante a disponibilidade de seus arquivos, caso haja perda daqueles que você utiliza diariamente, seja por descuido ou por algum fator externo.

3- Quando devo fazer backup de meus arquivos?

Se possível, diariamente. Cada dia que deixa de fazer backup pode se tornar um dia a menos de trabalho salvo, caso perca seus dados.