MATHEUS TONETO ALVES

WANDERSON RODRIGUES ALVES

UM ESTUDO DE CASO SOBRE COMO GARANTIR A SEGURANÇA DA INFORMAÇÃO DURANTE O HOME OFFICE

JI-PARANÁ

2021

MATHEUS TONETO ALVES

WANDERSON RODRIGUES ALVES

UM ESTUDO DE CASO SOBRE COMO GARANTIR A SEGURANÇA DA INFORMAÇÃO DURANTE O HOME OFFICE

Trabalho de Conclusão de Curso apresentada à Banca Examinadora do Centro Universitário São Lucas, como requisito de aprovação para obtenção do Título de Bacharel em Sistemas de Informação.

Orientador: Prof. Thyago Bohrer Borges

JI-PARANÁ

2021

Dados Internacionais de Catalogação na Publicação - CIP

A474e Alves, Matheus Toneto.

Um estudo de caso sobre como garantir a segurança da informação durante o home office. / Matheus Toneto Alves ; Wanderson Rodrigues Alves. – Ji-Paraná, 2021.
69 p., il.

Monografia (Curso de Sistemas de Informação) – Centro Universitário São Lucas Ji-Paraná, 2021.

Orientador: Prof. Me. Thyago Bohrer Borges

1. Gestão da segurança da informação. 2. Segurança da informação. 3. Tecnologia da informação. 4. Segurança Cibernética. 5. Segurança Digital. 6. COVID-19 – Pandemia. I. Alves, Wanderson Rodrigues. II. Borges, Thyago Bohrer. III. Título.

CDU 004.056

Ficha Catalográfica Elaborada pelo Bibliotecário Giordani Nunes da Silva CRB 11/1125

SÃO LUCAS
EDUCACIONAL

ATA DE TRABALHO DE CONCLUSÃO DE CURSO

ATA Nº 03/2020 DE TRABALHO DE CONCLUSÃO DE CURSO

No vigésimo terceiro dia do mês de junho de 2021, no horário das 18h às reuniram-se o(a) Orientador(a) professor(a) Me. Thyago Bohrer Borges e os(as) professores(as) Prof. Me. Ana Flavia Moreira Camargo e Prof. Esp. José Rodolfo Milazzotto Olivas para comporem Banca Examinadora de Trabalho de Conclusão de Curso, sob a presidência do(a) primeiro(a), para analisarem a apresentação do trabalho **"Um Estudo de Caso sobre como garantir a segurança da informação durante o Home Office"**. Após arguições e apreciação sobre o trabalho exposto foi atribuída à menção como nota do Trabalho de Conclusão de Curso dos(a) acadêmicos(a): Matheus Toneto Alves e Wanderson Rodrigues Alves

Obs: Trabalho de Conclusão de Curso (X) aprovado ou ( )reprovado com nota total de 8,0 (oito) pontos, sendo atribuídos o valor 8,0
(oito) ao trabalho escrito e 8,0(oito) à apresentação oral.

MATHEUS TONETO ALVES E WANDERSON RODRIGUES ALVES

Prof. Me. Thyago Bohrer Borges
Orientador

Prof. Esp. José Rodolffo Milazzotto Olivas

Prof. Me. Ana Flavia Moreira Camargo

Prof. Me. Thyago Bohrer Borges
Coord. Sistemas de Informação

RESUMO

Este trabalho apresenta um estudo de caso sobre como garantir a segurança da informação durante o home office em uma instituição financeira analisando as práticas relacionado a segurança da informação.

A segurança da informação está dividida em duas categorias, nela temos: Segurança Cibernética e Segurança Digital. A segurança cibernética é uma forma de proteger as pessoas e empresas contra-ataques de criminosos, que se aproveitam das vulnerabilidades digitais para invadir, roubar e manipular dados ou arquivos.

Vivemos hoje na era digital, onde se tem todas as informações na palma da mão, com comodidade e benefícios que também trouxeram riscos, por isso é de suma importância conhecemos e entendemos sobre a segurança da informação.

Segurança Digital é onde se define medidas e ferramentas para a proteção das informações do negócio e seus servidores. Tornando-se relevante em todos as circunstâncias principalmente em home office, haja visto a necessidade do mesmo causada pela pandemia da COVID-19 trazendo consigo muitas incertezas e consequentemente maior vulnerabilidade.

Tendo a segurança da informação como sua aliada, as empresas podem proteger dados e informações de clientes, garantindo assim a continuidade de seus serviços trazendo segurança aos dados aplicados em cada instituição mesmo em home office.

Palavras-chave: Gestão da segurança da informação, Segurança da informação, Tecnologia da informação, Segurança Cibernética, Segurança Digital. COVID-19, Pandemia.

SUMÁRIO

1. INTRODUÇÃO

O home office tornou-se uma realidade para diversos seguimentos no brasil, devido a pandemia causada pela COVID-19. Geralmente, em suas casas, os colaboradores não disponibilizam dos mesmos recursos de suas empresas, desta forma a segurança da informação tornou-se uma preocupação ainda maior.

Em virtude da pandemia, em muitos casos, o home office precisou ser adaptado às pressas. Sem planejamento adequado o trabalho remoto foi iniciado e deste então muitas empresas têm se planejado e estruturado de diversas formas para se adaptar aos riscos e preocupações relacionados à segurança da informação, portanto, não é surpresa que empresas tenham defasagem na segurança da informação por um período curto.

O contexto pandêmico vem trazendo para a realidade brasileira muitas situações imprevisíveis as quais muitas gestões não se prepararam, desta forma é comum existir brechas e vulnerabilidade na segurança digital com relação ao home office. Tomadas de decisões precisam ser corretas para essa nova realidade.

2. OBJETIVOS

2.1. OBJETIVO GERAL

Apresentar de forma direta os conceitos e características da segurança da informação, e da mesma forma home office. Porque o contexto da pandemia, causado pela COVID-19, tem relação e acelerados estas práticas.

2.2. OBJETIVOS ESPECÍFICOS

- Apresentar características das normativas sobre o assunto;
- Elaborar um estudo de caso em uma instituição financeira, cooperativa de crédito, observado as práticas elaboradas para a segurança da informação adotadas em home office;
- Verificar o controle de segurança da informação e infraestrutura de Tecnologia da Informação, tendo como embasamento teórico a proposta da norma ABNT

NBR ISO/IEC 27002 – Código de Prática para a Gestão da Segurança da Informação.

2.3. JUSTIFICATIVA

Trabalhar de casa tem sido uma alternativa mais segura neste momento, por conta da Covid-19. No entanto, essa ação exige cuidados redobrados com a segurança. Se estando em home office é necessário cuidado ao manipular dados pessoais de outras pessoas e ser conservador com os seus próprios dados pessoais.

Seja causado pela pandemia ou não o home office tende a crescer nos próximos anos. Por isso, o fundamental é que cuidem da segurança da informação para que o trabalho remoto seja de fato vantajoso para empresas e pessoas.

Execute atividades com muita atenção, para que pessoas mal-intencionadas não induzem você a passar informações sensíveis ou executar alguma tarefa da qual possa ser tirado proveito.

2.4. REFERENCIAL TEÓRICO

O referencial tem o objetivo de apresentar os conceitos e ideias que foram estabelecidos para o trabalho com base em estudos de caso e pesquisa bibliográfica, dando sustentação ao tema.

No que se diz sobre o estudo de caso, a coleta de dados foi através de questionário de Segurança da Informação e entrevistas individuais com os colaboradores e gestor da área de tecnologia da informação.

3. SEGURANÇA DA INFORMAÇÃO E DIRETRIZES RELACIONAIS

Neste capítulo consta princípios e conceitos relacionados à segurança da informação, mostrando de forma clara e objetiva aspectos e elementos relacionados a este assunto que se faz influenciar a segurança da informação.

3.1. O CONCEITO DA INFORMAÇÃO

A informação pode ser definida como qualquer conteúdo ou dado que tenha valor para a organização em um determinado contexto. Ela pode ser de uso restrito, exposta ao público para consulta ou aquisição, armazenada, utilizada e transmitida, e de natureza interna ou externa.

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades. (Norma Brasileira Regulamentadora nº 17799:2005)

Avançando mais ainda para a compreensão desse conceito, precisamos também entender as diferenças entre dados, informação e conhecimento, elementos igualmente importantes e que fazem parte do ambiente de Segurança da Informação.

Dados representa um ou mais significados, mas, isoladamente, eles não conseguem transmitir uma mensagem ou representar algum tipo de significado. Na prática, eles constituem a matéria-prima da informação, ou seja, é a informação ainda não tratada

Depois que os dados são processados, organizados e tratados é que se pode afirmar algo em relação a eles. Nesse momento, temos o que chamamos de informação. Diferentemente dos dados, elas possuem significado e são passíveis de análise para tomada de decisões. Dessa forma, podemos dizer que a informação nada mais é do que um conjunto de dados que foram tratados e processados e que produziu um resultado com significado.

Se a informação é o dado trabalhado, podemos afirmar que o conhecimento é a informação trabalhada. É o resultado de um esforço dedicado à compreensão do significado da informação. Vale realçar que o conhecimento se constitui das relações e da interpretação das informações.

> A informação recebe o título de ativo intangível, ou seja, o uso indevido ou divulgação não autorizada pode gerar danos e envolver ilícitos que vão desde quebra de sigilo profissional, a vazamento de informação confidencial de uma instituição ou exposição da vida íntima ou privacidade de uma pessoa. (PINHEIRO, 2010, p. 82)

“Informação não é conhecimento. A única fonte do conhecimento é a experiência.” *Albert Einstein.*

3.2. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação tem o objetivo de preservar as características da informação relativas à sua confidencialidade, a integridade e a disponibilidade.

- Disponibilidade – propriedade que a informação apresenta, de estar disponível e utilizável numa eventual requisição de uma entidade autorizada ABNT (2006).
- Integridade – propriedade que a informação apresenta, de estar completa e fiel ao estado original ABNT (2006).
- Confidencialidade – propriedade que a informação apresenta, de estar disponível apenas para àqueles que estão autorizados a obtê-la ABNT (2006).

Peixoto (2006) indicou três princípios fundamentais para a segurança da informação: (1) Disponibilidade: propriedade que a informação apresenta, de estar disponível e utilizável em eventual requisição de uma entidade autorizada; (2) Integridade: propriedade que a informação apresenta, de estar completa e fiel ao estado original; (3) Confidencialidade: propriedade que a informação apresenta, de estar disponível apenas para àqueles que estão autorizados a obtê-la.

> [...] o princípio da integridade é respeitado quando a informação acessada está completa, sem alterações e, portanto, confiável. Ou seja, quando a informação é alterada ou chegada de forma incorreta ao seu destino, isto faz com que a integridade se quebre (OLIVEIRA; MOURO; ARAÚJO, 2012, p. 3).

Galvão (2015), confidencialidade representa a garantia que a informação estará acessível somente para a pessoa autorizada. Se uma pessoa sem autorização tem conhecimento, ocorre uma violação de privacidade.

Palma (2016) diz que, a integridade é um pilar essencial para os processos de negócio onde informações corrompidas geram grandes problemas, ou também, necessidade de correção e retrabalho quando tratadas em tempo. a informações e ativos associados quando necessário.

Galvão (2015), disponibilidade é a garantia de que, quando as pessoas autorizadas solicitarem alguma informação, estas estejam disponíveis.

3.3. SEGURANÇA DA INFORMAÇÃO

Para um melhor entendimento, é necessária primeiramente entender alguns conceitos básicos como: ameaças, vulnerabilidades, ativos, ataques, métodos de segurança e ciclo de vida da informação.

Segundo a norma NBR ISO/IEC 27002 (ABNT, 2013), “a segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de hardware e software”.

De acordo com a norma ABNT NBR ISO/IEC 17799, Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Sequencialmente, a norma regulamentadora define segurança da informação como a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

“o processo de proteger a informação das ameaças para garantir a sua integridade, disponibilidade e confidencialidade”. (Beal, 2005, p. 71).

> Segurança da informação tem como objetivo a proteção dos sistemas contra a alteração e invasão dos dados por pessoas não autorizadas. Ela deve prevenir, detectar, deter e documentar qualquer ameaça aos seus dados e processamento haja vista que uma informação incorreta ou a falta dela pode ocasionar grandes perdas que comprometam o funcionamento da organização e seu retorno. (FONTES, 2006, p. 02).

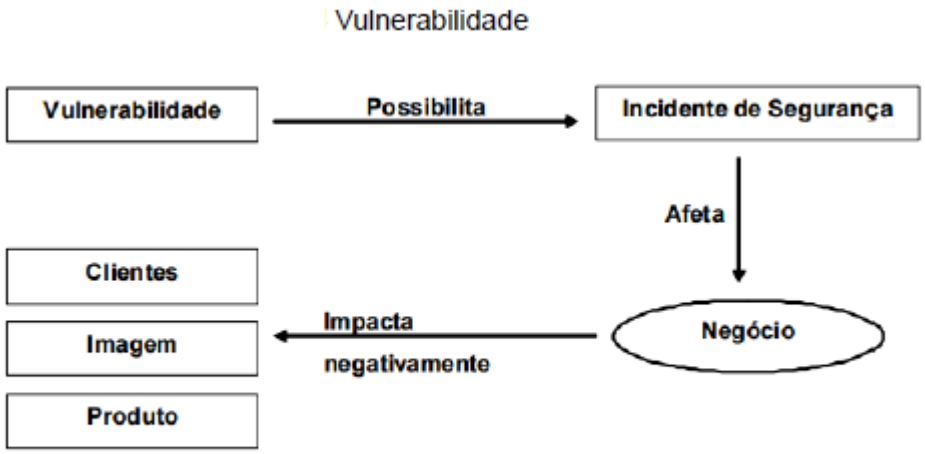
Acima de tudo, segurança da informação diz respeito a como as pessoas usam as informações que chegam até elas, nada pode escapar do ecossistema de proteção criado para preservar a confidencialidade da informação.

Entender por ameaça todo e qualquer fator que pode causar algum incidente ou problema que possa prejudicar a organização de alguma forma. (GALVÃO, 2015).

Sêmola (2003), as ameaças são agentes ou condições que afetam as informações e seus ativos, explorando as vulnerabilidades, gerando incidentes de perda de confidencialidade e impactos aos negócios da empresa.

Galvão (2015), fraqueza e fragilidade estão relacionadas ao ativo da empresa e pode m ser compreendidos como vulnerabilidade na estrutura organizacional, facilitando uma ameaça causando um incidente.

Sêmola (2003), afirma que vulnerabilidades são fragilidades presentes ou associadas a ativos que manipulam e/ou processam dados. Elas não provocam incidentes, por serem dados passivos, necessitando de um agente causador ou condição favorável, vazamento ou incêndio.



Fonte: LAUREANO (2005).

A Figura mostra que a vulnerabilidade tem relação direta com os negócios da organização, afetando seus ativos, e impactando negativamente o vínculo com os clientes, imagem da companhia e seus produtos.

Ativos são elementos que fazem parte dos processos de manipulação e processamento da informação. Pode m ser definidos como ativos: a própria informação, meio que é armazenada, pessoa, tecnologia, sistemas, equipamentos utilizados para manusear, transporta, descarta e que possua valor.

Sêmola (2003), ativo é tudo que compõe os processos que manipulam e processam as informações, sua informação, o meio em que ela é armazenada, onde ela é manuseada, transportada e descartada.

Para Galvão (2015), ativo significa qualquer parte que componha a organização, sendo ela, uma pessoa, sistema, tecnologia e todos que são ou não responsáveis por um processo ou por uma área específica da empresa.

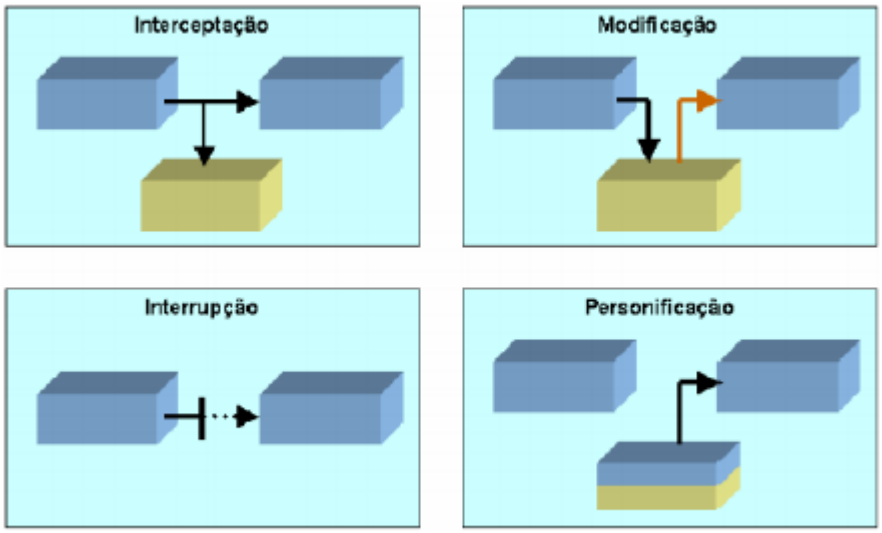
> Os ataques podem ser definidos como um problema de segurança, tal que, um agente busca obter algum tipo de retorno, atingindo um ativo de valor. Seu retorno pode ser financeiro ou não (ALBURQUERQUE; RIBEIRO, 2002, p. 04).

De acordo com Oliveira (2001), o ataque é a coleta dos dados e informações sobre seu alvo. O atacante tentará o máximo de informações sobre seu alvo.

O fato de um sistema estar sendo atacado, não significa que seus dados e seus dados serão afetados. Segundo Laureano (2005), um ataque só terá sucesso dependendo da vulnerabilidade do sistema e das medidas de proteção que ele possui.

Pode ser classificado como formas de ataques: Vírus, Trojans ou Cavalo de Tróia, Worms, Engenharia social, phishing... Quando um ataque ocorre, o fluxo normal de transmissão dos dados é alterado. Este fluxo normal pode ser alterado por mecanismos de ataques, bem como: interrupção, interceptação, modificação e personificação.

Tipos de Ataques



Fonte: LAUREANO (2005).

Laureano (2015), interrupção é quando a informação ficará indisponível, não é mais possível acessá-la, interrompendo o fluxo normal da mensagem ao destino. Interceptação é quando informações sigilosas poderão ser visualizadas por pessoas sem autorização. Modificação incide na alteração das informações por pessoas não autorizadas, violação da integridade da mensagem. Personificação define-se como uma pessoa que acessa as informações ou a transmite se passando por pessoas autênticas, violação da autenticidade.

Sêmola (2003), os mecanismos de segurança da informação são práticas, procedimentos e mecanismos usados para a proteção das informações e seus ativos, prevenindo contra as ameaças e impedindo que estas explorem vulnerabilidades.

Algumas medidas de segurança são consideradas controles que podem ter as seguintes características: preventivas, detectáveis e corretivas.

Medidas preventivas, segundo Sêmola (2003), são medidas cujo objetivo são evitar incidentes que possam acontecer. Visam manter a segurança já implementada que estabeleçam a conduta e a ética da segurança da organização. Como exemplos, podem-se citar as políticas de segurança, procedimentos e normas, palestras de conscientização de usuários, ferramentas como firewall e antivírus.

Medidas detectáveis são medidas que visam identificar condições ou indivíduos causadores de ameaças, a fim de evitar que as ameaças explorem vulnerabilidades. Pode-se citar como exemplos, a análise de risco, IDS (Intrusion Detection System), câmeras de vigilância e alarmes.

Medidas corretivas são ações voltadas à correção de uma estrutura tecnológica e humana, para que se adaptem às condições de segurança estabelecidas pela organização ou voltadas à redução dos impactos. Exemplos de medidas corretivas são backups, plano de continuidade operacional e plano de recuperação de desastres.

Os mecanismos de segurança da informação envolvem controles físicos e lógicos referentes ao software, hardware e humanos.

Santana (2013), controles físicos definem-se como um conjunto de medidas capaz de controlar acesso das pessoas. Realizado por restrições de acesso e registro que servem como barreira adicional ao acesso lógico. Alguns exemplos de controles físicos são: portas blindadas, detectores de metal, catracas com leitura biométrica, fechaduras com senhas. Controles lógicos podem ser definidos como barreiras que impedem ou limitam acesso à informação em meio eletrônico, tal como, criptografia, assinatura digital, tipos de autenticação, firewalls e autenticação.

4. PRÁTICAS PARA A GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Neste momento apresentará as principais diretrizes e princípios para manter e melhorar a gestão de segurança da informação em uma organização.

4.1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Uma Política de Segurança da Informação é uma das mais importantes medidas a serem tomadas, já que será a base de princípios que seguidos pela gestão. Para Fontes (2010), uma política de segurança tem como objetivo definir o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente de tecnologia da organização e que são os

princípios fundamentais de como a organização exige que a informação seja utilizada, além de que se aplica a todos os usuários que utilizam as informações da organização. Conforme a própria norma ABNT NBR ISO/IEC 17799, convêm que o documento de política de segurança da informação declare o comprometimento da direção e estabeleça o enfoque da organização para gerenciar a segurança da informação. Convêm que o documento da política contenha declarações relativas a:

- definição da segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação.
- declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhadas ao negócio.
- estrutura para estabelecer os objetivos de controle e os controles, incluindo uma estrutura de gerenciamento de risco.
- definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo registro dos incidentes de segurança da informação. Este documento deve ser acessível e compreensível para o leitor em foco.

4.2. ANÁLISE, AVALIAÇÃO E TRATAMENTO DE RISCOS

Risco é a probabilidade de que as vulnerabilidades sejam exploradas pelas ameaças existentes, danificando ou ocasionando perdas aos ativos e acarretando prejuízos aos negócios da empresa, conforme a CERT BR.

Para a norma ABNT (2005), espera-se que as análises/avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base em critérios para aceitação dos riscos e dos objetivos relevantes para a organização. Convém que os resultados determinem ações para o gerenciamento dos riscos de segurança da informação e para a implantação dos devidos controles. O processo de avaliar riscos precisa ser um processo contínuo de forma a cobrir todo o ambiente organizacional.

Convém também, que a análise/avaliação de riscos de segurança da informação tenha seu escopo definido e inclua os relacionamentos com as análises de outras áreas, se necessário. Exemplos de análise/avaliação de riscos são discutidas no ISO/IEC TR 13335-3 (Guidelines for the management of TI security: Techniques for the management of TI secutiry).

Segundo ABNT (2005), antes de considerar o tratamento de um risco, a organização deve definir os critérios para determinar se os riscos podem ser ou não aceitos. O risco é aceito se ele é baixo ou se seu custo do tratamento não é economicamente viável para a organização.

Para cada um dos riscos identificados, uma decisão sobre o tratamento do risco precisa ser tomada. Algumas opções incluem:

- aplicar controles apropriados para reduzir os riscos;
- conhecer e objetivamente aceitar o risco, se for o caso;
- evitar riscos, não possibilitando ações que poderiam causar outros riscos;
- transferir os riscos associados para outras partes, por exemplo, seguradoras ou fornecedores.

Para aqueles riscos aceitos, onde necessitam de tratamento e aplicações de controles apropriados, estes controles devem assegurar que os riscos sejam reduzidos a um nível aceitável, levando-se em conta:

- os requisitos e restrições das legislações vigentes;
- objetivos do negócio;
- os requisitos e restrições operacionais;
- custo de implementação e operação;
- necessidade de balancear o investimento na implementação e operação, contra a probabilidade de danos que resultem em falhas de segurança da informação.

Deve-se lembrar que nenhum conjunto de controles pode garantir a segurança completa, e que uma ação de gestão deve existir para monitorar, avaliar e melhorar a eficiência e eficácia dos controles de segurança da informação, sendo que estas ações devem sempre está alinhada ao negócio da organização.

4.3. CONTROLE DE ACESSOS

Para a ABNT (2005), o acesso à informação, aos recursos de processamento das informações e aos processos de negócios deve ser controlado com base nos requisitos de negócio e na segurança da informação. Portanto, deve ser assegurado o acesso de usuário autorizado e prevenido o acesso não autorizado a sistemas de informação. Para isso, deve haver procedimentos que englobem desde o cadastro inicial de um novo usuário até o cancelamento final do seu registro, garantindo assim que já não possuem mais acesso a sistemas de informação e serviços.

Os usuários sempre devem estar conscientes de suas responsabilidades, particularmente no que se refere ao uso de senhas e de segurança dos equipamentos de usuários. Nesse sentido, sugere-se ainda a adoção da “política de mesa e tela limpa”, para reduzir o risco de acessos não autorizados ou danos a documentos, papéis, mídias e recursos de processamento da informação que estejam ao alcance de qualquer um.

Boa parte das organizações possui controle total para limitar o acesso ao conteúdo de seus funcionários. Através dos conhecidos e mais utilizados firewall para proteção. Um firewall é uma espécie de filtro projetado para bloquear ou admitir determinados tipos de tráfico na rede. Por exemplo, pode bloquear sites entendidos como impróprios, ou que não se adéquam aos objetivos da empresa.

Define quais informações o usuário tem acesso, quais dados ele pode visualizar, alterar ou excluir. Autorização e controle de acesso é uma forma de dividir responsabilidades. A informação dentro de uma empresa deve ser classificada e disponibilizada de acordo com a necessidade de cada usuário. A autenticação é o mecanismo de controlar quem pode e quem não pode visualizar determinada informação.

Pelo fato de o controle de acesso ser dependente da identificação do usuário, a autorização de uso é frequentemente integrada com os mecanismos de autenticação, conforme Masahiro (2009).

4.4. CONFORMIDADE

A norma ABNT ISSO/IEC 17799, relata que a Conformidade deva garantir e evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.

Para isso, é conveniente contratar, caso necessário, consultoria especializada, bem como analisar criticamente a segurança dos sistemas de informação a intervalos regulares, verificando, sobretudo, sua conformidade e aderência a requisitos legais e regulamentares.

Em resumo, nota-se claramente ao longo de toda a norma, que a característica predominante é a prevenção, evitando-se a todo o custo, a adoção de medidas de caráter reativo. Mesmo as que forem reativas, como por exemplo, a execução de um plano de continuidade de negócios, são previamente planejadas para que, no momento oportuno e se necessárias, sejam devidamente implementadas.

Segundo Peixoto (2006), um teste de conformidade tem como principal objetivo, permitir a percepção relativa ao grau de conformidade que a organização possui em relação aos controles sugeridos pelo código de conduta de gestão de segurança da informação definidos pela norma ABNT NBR ISO/IEC 17799.

5. A SEGURANÇA DE INFORMAÇÃO NAS INSTITUIÇÕES FINANCEIRAS

No capítulo são apresentadas definições, aspectos das instituições financeiras, além de fazer uma análise da segurança da informação.

5.1. INSTITUIÇÕES FINANCEIRAS

Segundo Fortuna (2008), as instituições financeiras no Brasil estão divididas em dois tipos, monetárias e não monetárias, sendo a primeira mais conhecida até mesmo pela natureza e múltiplas funções, onde os Bancos Comerciais têm papel de destaque constituindo a base do sistema monetário, devido muito aos serviços prestados.

Ainda de acordo com Fortuna (2008), instituições financeiras monetárias são aquelas que possuem depósito à vista e, portanto, multiplicam a moeda, dentre elas destacam-se:

- Bancos Comerciais;
- Caixas Econômicas;
- Bancos Cooperativos;
- Cooperativas de Crédito.

5.2. SEGURANÇA DA INFORMAÇÃO DAS INSTITUIÇÕES FINANCEIRAS

Para Fortuna (2008), a Tecnologia da Informação (TI) se apresenta como um vetor de diferenciação, competitividade e eficiência em qualquer negócio. Na esfera financeira não é diferente, em diversas atividades, mas principalmente nos processos de negócios e na criação de diversos serviços que necessitam de canais de comunicação entre a financeira e os clientes, tais como Home Banking ou do Mobile Bank.

O desenvolvimento de um planejamento de T.I tem a importância fundamental nos bancos e cooperativas de crédito, pois possui um grande potencial para alavancar as atividades de negócios. Estas instituições implementam novos serviços com o objetivo de aumentar a eficiência dos negócios através da melhoria da administração de transações comerciais e informações geradas por essas. O desenvolvimento contínuo em Tecnologia da Informação proporciona a criação de novas áreas de negócios e novos produtos.

> A tecnologia da informação apoia todas as etapas de um processo de inteligência competitiva, desde a fase de identificação das necessidades de informação, passando pela coleta, análise e disseminação, até a avaliação dos produtos entregues. Ela organiza o fluxo de informação e auxilia nos principais objetivos do Sistema de Inteligência competitiva: alerta possíveis oportunidades e ameaças, apoiar o processo de tomada de decisão estratégica, avaliar e monitor os concorrentes, a indústria e as tendencias políticas e sociais e apoiar o planejamento e o processo estratégico. (GOMES, 2001, p. 83).

Os negócios financeiros são arriscados pela sua própria natureza. Entretanto, conhecer os riscos com a maior precisão possível é um dos pilares de um sistema de controles internos eficiente, permitindo uma pronta ação no sentido de evitá-los ou minimizá-los.

A expressão risco, engloba inúmeras incertezas, é qualquer evento que possa afetar os objetivos das organizações. conforme evidência Damodaran (2009), pode-se analisar o risco como oportunidade, pois o risco pode propiciar retorno positivo quando bem administrado. O autor afirma que o risco oferece oportunidades ao mesmo tempo em que nos expõe a resultados talvez indesejáveis.

No que se refere à gestão de riscos, o Comitê de Supervisão Bancária da Basileia, no seu material de Princípios Fundamentais para uma Supervisão Bancária

Efetiva (2006), considera que a inadequada avaliação de riscos contribuiu decisivamente para os problemas de controles internos de algumas organizações bancárias e às perdas relacionadas.

> Em que pese as instituições financeiras e cooperativas de crédito sempre despenderam atenção majoritária para dos riscos de mercado, contudo a globalização e a dependência das novas tecnologias, deixaram o sistema financeiro notoriamente exposto ao risco operacional (MOOSA, 2007, p. 167-200).

Crouhy, Galai e Mark (2008) definem risco operacional como eventos externos, ou deficiências em controlos internos ou sistemas de informação resultando numa perda, quer seja antecipada ou completamente inesperada.

Como origem dos eventos de risco operacional, Santos (2011) aponta o ser humano como a principal ameaça a qualquer tipo de informação, visto que o seu processamento se inicia e se finaliza no usuário do sistema informacional.

Brink (2002) lista os erros mais comuns cometidos pelas pessoas que comprometem a segurança da informação: equívoco, omissão, distração ou negligência de funcionários ou terceiros contratados e de comportamentos fraudulentos (adulterações de controles, descumprimento intencional das normas, vazamento de informações privilegiadas, desvio de valores, divulgação de informações erradas).

Contudo ressalta-se que todos os envolvidos no processo são responsáveis pela segurança da informação, se tratando do aspecto pessoal, a responsabilidade é dos colaboradores da instituição bem como dos usuários.

> Pois, de nada vale a melhor capacitação técnica senão conscientizar o usuário, o profissional, o cidadão, destas tecnologias, e de que a segurança da informação é consequentemente, a segurança cibernética, é um problema de todos. Assim sendo, esta conscientização deve ser iniciada desde o ensino fundamental, criando uma cultura orientada a esta abordagem, pois é inegável que a cada dia a iniciação digital se dá em idades mais precoces. (CANONGIA, 2009, p. 46).

Sêmola (2006) destaca ainda como fator de risco as vulnerabilidades físicas como as barreiras de controle de acesso, por exemplo, bem como as vulnerabilidades tecnológicas, vindas de configurações ou parametrizações inadequadas de sistemas ou firewall.

Consoante a isso Brink (2002), destaca que os riscos decorrentes do sistema, originam-se da descontinuidade das atividades apoiadas por serviços tecnológicos, salientando a sobrecarga de sistemas de processamento de dados (risco de overloads), incapacidade dos sistemas de prover informações confiáveis e suficientes, incompatibilidade e/ou indisponibilidade de informações, falta de meios seguros de acesso aos sistemas, obsolescência dos sistemas e equipamentos, falhas de hardware, ausências de backup e de legalização do software, inadequação de sistemas operacionais/aplicativos e outros.

Neto e Silveira (2017) enfatizam que a segurança da informação envolve cumulativamente a segurança física, que está voltada aos locais nos quais se encontram as informações, ou seja, refere-se a necessidade de proteger equipamentos e programas dentro de um local adequado a eles, bem como a segurança lógica que baseia-se na forma de utilização dos recursos nas diversas atividades cotidianas da instituição que se encontra de posse deles, e pôr fim a segurança humana, pois todos esses recursos são utilizados por pessoas, de modo que elas devem entender seu papel na manutenção das informações dentro de parâmetros de segurança e confiabilidade.

Rocha (2008) destaca a necessidade de mudança na cultura empresarial do Brasil. A segurança da informação somente será efetivada quando se compreender que as informações constituem o patrimônio da empresa.

As inovações tecnológicas proporcionam trocas informacionais e conhecimentos, na comercialização eletrônica de bens e serviços, e ainda na transmissão de dados sensíveis. Diante destes cenários a preocupação da cooperativa, está pautada em atender as necessidades e preferências dos cooperados, criando canais confiáveis que melhorem a vida e o dia a dia das pessoas.

Atualmente todo cooperado pode gerenciar sua vida financeira com apenas poucos cliques. A grande maioria das instituições financeiras e cooperativas de crédito, permitem que seus clientes e cooperados tenham acesso a empréstimos, financiamentos, aplicações financeiras, pagamentos de boletos e transações financeiras por meio de um aplicativo instalado em seus smartphones, ou pelo acesso via Internet Banking.

> Aumenta o grau de liberdade com que os homens podem atuar no mundo social e material. Permitem executar largas cadeias de processamento, diversos inputs e obtendo um número indefinido de produtos. Sendo sociais

> em sua produção, permite que desde um único ponto se possa intervir em uma vasta rede sendo sociais em sua produção, permite que desde um único ponto se possa intervir em uma vasta rede com múltiplas consequências no mundo social e material. (GONZALEZ, 2006, p. 52).

No mundo conectado, segurança dever ser um pilar estratégico. A segurança da informação dever ser uma das maiores preocupações das empresas, especialmente nesse ramo, vez que a perda de dados pode comprometer seus lucros, seus resultados, sua confiabilidade no mercado. (TORRES, 2014).

> A segurança da informação, por muitos, é vista como a proteção de dados oferecidos ou recebidos por alguém, porém, é preciso compreender que esta significa muito mais do que isso, pois engloba o desenvolvimento de medidas e práticas que façam com que esses dados sejam resguardados mesmo dentro da empresa, já que mesmo ali existem usuários não autorizados a utilizar essas informações e, caso tenham acesso a elas, poderão fazer um uso inadequado, fornecendo-as a quem não tenha direito a isso. (OLIVEIRA; MOURA; ARAÚJO, 2012, p. 02).

A consultoria de TI é responsável por fazer uma checagem e avaliação dos riscos do ambiente de trabalho dos sistemas de informação que suportam os processos de negócio. A atividade tem como intuito ajudar a organização por meio da identificação e avaliação de exposições ao risco que sejam significativas, bem como contribuir para o avanço dos mecanismos de gestão de risco e de controle dos sistemas de informação. (ISACA, 2010).

Dentro da realidade apresentada pela cooperativa de crédito, uma auditoria poderia ocorrer em duas áreas distintas conforme leciona Neto e Solonca (2007). Auditoria de segurança de informações e auditoria de aplicativos.

Os autores ainda explicam que uma auditoria da segurança da informação visa mitigar vulnerabilidades em ambientes informatizados, ela avalia a política de segurança da informação e os controles relacionados a aspectos de segurança e de controles que influenciam o bom funcionamento dos sistemas da organização. Tais controles estão listados a seguir:

- Avaliação da política de segurança;
- Controles de acesso lógico;
- Controles de acesso físico;
- Controles ambientais;
- Plano de contingência e continuidade de serviços;

- Controles organizacionais;
- Controles de mudanças;
- Controle de operação dos sistemas;
- Backups dos bancos de dados;
- Controles sobre computadores;
- Controles sobre ambiente cliente-servidor.

Já uma auditoria de aplicativos, está direcionada para a segurança e o controle de aplicativos específicos, incluindo aspectos que fazem parte da área que o aplicativo atende. A auditoria de aplicativos compreende: - Controles sobre o desenvolvimento de sistemas e aplicativos;

- Controles de entrada, processamento e saída de dados;
- Controles sobre o conteúdo e funcionamento do aplicativo com relação à área por ele atendida.

De acordo com o Tribunal de Contas da União a segurança da informação é obtida:

I. Estabelecendo requisitos de segurança: É fundamental que a organização identifique seus requisitos de segurança. Fontes principais:

- Análise de Risco dos Ativos de Informação.
- Normas internas (PSI, classificação da informação).
- Legislação vigente, estatutos, regulamentação e cláusulas contratuais (requisitos legais).
- Conjunto particular (no contexto da organização) de princípios, objetivos e requisitos para o processamento da informação (objetivos de negócio).

II. Estabelecendo controles: Uma vez identificado os requisitos de segurança, podem ser selecionados e implementados controles que visam satisfazer esses requisitos.

Existirão situações em que a implementação de controles não será capaz de eliminar as vulnerabilidades identificadas, contudo poderá ser suficiente para reduzir

os seus respectivos impactos ou probabilidade de ocorrência a um nível de risco aceitável.

Controles compensatórios também devem ser identificados. Exemplo: funções devem ser segregadas para evitar fraudes e erros, contudo isso pode não ser possível para organizações pequenas e, nesse caso, outra maneira de se alcançar o mesmo objetivo de controle poderá ser necessário (ex.: utilização de trilhas de auditoria para monitoramento de acessos e atividades por outra pessoa). Implementação de controles por meio de:

- Políticas.
- Práticas.
- Procedimentos.
- Pessoas.
- Estruturas organizacionais.
- Ferramentas de software.

III. Política de Segurança da Informação (PSI): tem por objetivo prover à administração uma direção e apoio para a segurança da informação, bem como estabelecer os princípios adotados pela organização para a distribuição, proteção, administração e supervisão dos recursos de informação.

O grande pilar de sustentação do ambiente informatizado é preservar os princípios básicos de segurança: integridade, disponibilidade, confidencialidade.

Para se construir um comportamento de segurança da informação em uma organização, será preciso interagir os elementos pertinentes à Ciência da Informação, e que esses elementos alimentam uma trajetória que se inicia com a necessidade de informação, passa pela busca informacional e termina com o comportamento informacional. (Almeida et. Al, 2013, p. 181)

6. HOME OFFICE

Em continuidade, abordaremos agora os princípios e conceitos relacionados ao home office, descrevendo um pouco sobre suas principais seguranças e sua importância visto que tendo um plano de continuidade e os seguindo, as chances de

os colaboradores terem suas ferramentas de trabalho invadidas por Hackers, seja ela qual for, são reduzidas.

6.1. PRINCÍPIOS E CONCEITOS

Empresas que selecionam e treinam de forma adequada seus colaboradores para trabalharem de home office, apresentam grandes ganhos em um cenário onde se trabalhar de forma remota faz-se necessário.

> O termo home office, utilizado nas organizações do Brasil, significa trabalho em domicílio. O trabalho em home office é uma modalidade do chamado teletrabalho, em que o funcionário realiza suas atividades laborais fora da organização, podendo exercê-las de maneira integral ou não, com o uso de ferramentas tecnológicas que o conectam a ela. A Sobratt (Sociedade Brasileira de Teletrabalho e Tele atividades). (REGIANE, 2017, p. 29).

> Uma das forças motrizes identificadas para a implantação e melhoria do trabalho em home office é a disponibilidade de tecnologia. As atuais ferramentas tecnológicas agilizam cada vez mais a gestão do trabalho em home office (e: telefonia, computadores pessoais, rede interligadas com a empresa, softwares como organizadores de tarefas, calendários, gerenciadores de projetos, vídeo conferência etc.) e fazem com que a comunicação e a interação entre as partes aconteçam de qualquer lugar onde estejam os funcionários. (REGIANE, 2017, p. 31).

6.2. MANTENDO A SEGURANÇA

6.2.1. Engenharia Social

A engenharia social consiste na utilização de técnicas de manipulação para pessoas executarem ações ou divulgarem informações confidenciais. O engenheiro social faz com que pessoas quebrem procedimentos e normas de segurança, seja através de telefonemas, e-mails, sites ou através de pessoas.

Os ataques de engenharia social são divididos em dois tipos, que são eles: baseados em humanos (no-tech hacking) e baseados em tecnologia que requerem o uso de equipamentos eletrônicos para se chegar ao objetivo, sendo utilizado e-mail, telefone, redes sociais, sites, mensagens instantâneas, entre outros para composição de técnicas como: phishing, vishing, spyware, malware, entre outras.

> Eles são charmosos, educado e agradam facilmente, traços sociais necessários para estabelecer a afinidade e confiança. Um engenheiro social experiente pode ter acesso a praticamente qualquer informação alvo usando as estratégias e táticas da sua habilidade (MITNICK; SIMON 2003, p. 18)

6.2.2. Phishing

O termo phishing é originado da palavra inglesa fishing, que significa pescar, ou seja, é a conduta daquele que pesca informações sobre o usuário de computador. É um tipo de fraude eletrônica, onde o golpista busca obter informações pessoais do usuário como senhas, dados financeiros, números de cartões de crédito e outros dados pessoais. No início a palavra phishing era utilizada para definir a fraude que consistia no desvio de e-mail não solicitado pela vítima, que era estimulada a acessar sites fraudulentos. Os sites tinham a intenção de permitir o acesso às informações eletrônicas da pessoa que lhe acessava, como por exemplo, número da conta bancária, cartão de crédito, senhas, e-mails e outras informações pessoais.

> São diferentes os modos pelos quais os cibercriminosos agem, mas em linhas gerais, a conduta consiste na captação ilícita mediante especulações ou processos fraudulentos onde o internauta é induzido a acreditar que necessita fornecer dados que posteriormente são utilizados por quadrilhas ou pessoa mal-intencionada. (BERONALDO E MARIANA, 2020, p. 09).

6.2.3. VPN

“Virtual Private Network” ou Rede Privada Virtual, é uma rede privada construída sobre a infraestrutura de uma rede pública, normalmente a Internet. Ou seja, ao invés de se utilizar links dedicados ou redes de pacotes para conectar redes remotas, utiliza-se a infraestrutura da Internet.

O conceito de VPN surgiu da necessidade de se utilizar redes de comunicação não confiáveis para trafegar informações de forma segura. As redes públicas são consideradas não confiáveis, tendo em vista que os dados que nelas trafegam estão sujeitos a interceptação e captura. Em contrapartida, estas redes públicas tendem a ter um custo de utilização inferior aos necessários para o estabelecimento de redes proprietárias, envolvendo a contratação de circuitos exclusivos e independentes.

> Para executar suas tarefas em outro lugar que não seja no escritório, o funcionário necessita de algumas tecnologias a sua disposição, como: um computador, acesso à internet, seja por wifi, bluetooth ou por roteamento de algum dispositivo eletrônico como celular, e ainda utilização de um software de acesso via VPN (VIRTUAL PRIVATE NETWORK) para conseguir conectar-se ao ambiente e as páginas internas da empresa. (REGIANI, 2017, p. 24).

A criptografia é implementada por um conjunto de métodos de tratamento e transformação dos dados que serão transmitidos pela rede pública. Um conjunto de regras é aplicado sobre os dados, empregando uma sequência de bits (chave) como padrão a ser utilizado na criptografia. Partindo dos dados que serão transmitidos, o objetivo é criar uma sequência de dados que não possa ser entendida por terceiros, que não façam parte da VPN, sendo que apenas o verdadeiro destinatário dos dados deve ser capaz de recuperar os dados originais fazendo uso de uma chave.

São chamadas de Chave Simétrica e de Chave Assimétrica as tecnologias utilizadas para criptografar dados.

- Chave Simétrica ou Chave Privada: É a técnica de criptografia onde é utilizada a mesma chave para criptografar e descriptografar os dados. Sendo assim, a manutenção da chave em segredo é fundamental para a eficiência do processo.

- Chave Assimétrica ou Chave Pública: É a técnica de criptografia onde as chaves utilizadas para criptografar e descriptografar são diferentes, sendo, no entanto relacionadas. A chave utilizada para criptografar os dados é formada por duas partes, sendo uma pública e outra privada, da mesma forma que a chave utilizada para descriptografar

6.2.4. Proteger Senhas

Donald Norman (1990), em seu livro "Design of Everyday Things", chama a atenção para a dificuldade que a maioria das pessoas encontra ao precisar lembrar de códigos secretos ou senhas. Especificamente no caso de códigos secretos, ou senhas, é importante que sejam mantidos em segredo, uma vez que protegem informações confidenciais. Algumas senhas ainda devem ser periodicamente alteradas. Como pode alguém, lembrar de tantas senhas? Ao que tudo indica, não é possível. De que maneira, então, as pessoas administram a situação?

Do ponto de vista da Segurança da Informação, uma boa senha deveria ser segura, o que foi definido por algumas diretrizes publicadas pelo Departamento de

Defesa Americano (DoD), em 1985. Além de várias recomendações técnicas para a implementação e gerenciamento de senhas, o documento do DoD forneceu recomendações sobre como os indivíduos deveriam selecionar e administrar suas senhas. Essas recomendações deram origem às seguintes regras (Smith, 2002):

1. Cada senha escolhida deve ser nova e diferente, já que o uso de uma única senha para vários sistemas pode dar aos invasores uma grande vantagem ao interceptar uma só senha;

2. Senhas devem ser memorizadas. Se uma senha é registrada em papel, este deve ser armazenado em local seguro;

3. Senhas devem ser compostas de pelo menos seis caracteres, provavelmente mais, dependendo do tamanho do conjunto de caracteres usados, i.e. se contêm apenas números, números e letras, ou se contêm uma combinação de números, letras e outros caracteres do teclado como, por exemplo, "*", "%", "$", "#", "@", e outros;

4. Senhas devem ser substituídas periodicamente;

5. Senhas devem conter uma mistura de letras (tanto maiúsculas quanto minúsculas), dígitos e caracteres de pontuação.

6.2.5. Atualizações de Sistemas

As atualizações nem sempre são vistas com bons olhos pelos usuários das mais variadas tecnologias que utilizamos com tanta frequência atualmente. Parece óbvio, mas as atualizações são muito importantes para manter um funcionamento estável e seguro dos softwares e aplicações que usamos diariamente.

Não é nenhum segredo que as atualizações trazem, dentre outras coisas, diversas correções para estabilidade e, principalmente, vulnerabilidades. Com o passar do tempo, muitas ameaças surgem em todo tipo de ambiente, como sistemas operacionais, navegadores e softwares, e são justamente as atualizações, as responsáveis por corrigir e manter seu funcionamento com segurança.

Conforme Sans Institute (2017), um dos grandes problemas em manter o software antivírus atualizado é que sempre os desenvolvedores de malwares estão um passo à frente das empresas de segurança, pois o próprio conceito tradicional das ferramentas de antivírus é a criação de vacinas baseadas em amostras de vírus existentes. Dessa maneira, a ameaça após ser criada e divulgada na internet precisa ser identificada, analisada através de engenharia reversa e a empresa de segurança precisa elaborar uma vacina baseada nos resultados. Somente após esse processo ela disponibiliza essa vacina para que seus softwares clientes façam o processo de atualização.

6.2.6. Nuvem

A palavra nuvem sugere uma ideia de ambiente desconhecido, o qual podemos ver somente seu início e fim. Por este motivo está foi muito bem empregada na nomenclatura deste novo modelo, onde toda a infraestrutura e recursos computacionais ficam “escondidos”, tendo o usuário o acesso apenas a uma interface padrão através da qual é disponibilizado todo o conjunto de variadas aplicações e serviços.

A nuvem é representada pela internet, isto é, a infraestrutura de comunicação composta por um conjunto de hardwares, softwares, interfaces, redes de telecomunicação, dispositivos de controle e de armazenamento que permitem a entrega da computação como serviço. Para tornar este modelo possível, é necessário reunir todas as aplicações e dados dos usuários em grandes centros de armazenamento, conhecidos como data centers.

O fornecedor de nuvem precisa também fornecer evidências de que os esquemas de criptografia utilizados foram projetados e testados por especialistas experientes. "Acidentes com criptografia pode fazer o dado inutilizável e mesmo a criptografia normal pode comprometer a disponibilidade" (GARTNER, 2009).

Enfim, a computação na nuvem representa um novo modelo de serviço capaz de fornecer todo o tipo de processamento, infraestrutura e armazenamento de dados

através da internet (tanto como componentes separados ou uma plataforma completa) baseado na necessidade do usuário

6.2.7. Tratamentos de Dados, Informações Sensíveis

> Sem dúvida, as tecnologias contribuíram para grandes avanços em todos os campos da ciência e foram o principal fator para a automatização das formas de trabalho, anteriormente realizadas majoritariamente de forma presencial, consecutiva e manual. Entretanto, essas alterações trouxeram algumas consequências para o mundo do trabalho, com a geração de empregos, e, logo para a vida do trabalhador. (Brynjolfsson e McAfee, 2014, p. 63)

> A tecnologia tem avançado rapidamente, e a boa notícia é que isso aumenta de modo radical a capacidade da economia. No entanto, o progresso tecnológico não beneficia todo mundo automaticamente em uma sociedade. Em especial, as rendas têm se tornando ainda mais desiguais, assim como as oportunidades de emprego. (Brynjolfsson e McAfee, 2014 p. 65).

Os indivíduos que conseguiram ter acesso as novas tecnologias e se adaptarem as mudanças tendem a ter mais oportunidades em relação aos outros que não o fizeram. Ainda segundo os autores, o aumento por mão de obra qualificada está relacionado aos avanços das tecnologias, pois “exigiu da força de trabalho níveis de habilidades mais altos e radicalmente diferentes”. Para tanto, os trabalhadores buscam novas formas de se manterem competitivos para o mercado de trabalho, capacitando-se em diferentes níveis que exigem o conhecimento tecnológico.

6.2.8. Acessos Remoto

Segundo o site NDC, desde 2005, o trabalho remoto cresceu 173%, segundo pesquisa recente da consultoria Global Workplace Analytics. Esse número pode ser ainda maior, após a pandemia do coronavírus, quando muitos empregadores se viram forçados a enviar sua força de trabalho para casa para prevenir a propagação da Covid-19. Isso significa implementar soluções que facilitem o trabalho remoto, educar seus funcionários sobre como usá-las e implementar uma política que garanta a produtividade e segurança da informação no caminho. Assim, enquanto é possível garantir produtividade no home office, a segurança da informação surge como uma das maiores preocupações da empresa que adotam a modalidade de trabalho. Mas,

como assegurar que as informações e dados sigilosos da organização não caiam nas mãos de agentes maliciosos?

Para ajudar nessa questão, mostraremos, a seguir, como é possível reduzir proativamente o risco de violação de dados no acesso remoto e ainda proteger os ativos intelectuais da organização! Acompanhe

- Políticas de acesso remoto fracas
- Falta de visibilidade da atividade do usuário
- Falhas na autenticação de identidade do usuário
- Tentativas oportunistas de phishing

6.2.9. Redes Abertas

Quando se falamos em trabalho home office ficamos sempre com um pé atras das consequências que podemos deixar, por isso tomar o máximo de cuidado ao fazer alguma coisa para não poder prejudicar a sua empresa. E um dos cuidados é nunca acessar o computador da empresa numa rede WIFI de modo aberta, porque pode ocorrer a perda dos seus dados, onde a mesma rede fica sem proteção alguma contra hackers.

> As redes de computadores podem ser classificadas quanto a sua abrangência geográfica. Os tipos de redes de computadores quanto a sua abrangência geográfica são PAN, LAN, MAN e WAN. (GOMES, 2012, p. 18)

Citei algumas redes wi-fi sempre buscar a melhor que encaixa para seu dia a dia com alta segurança profissional.

6.2.10. Dispositivos Portáteis, Mídias Locais

> Salve os arquivos de trabalho em um dispositivo extra, como pendrives, hd’s externos e cartões de memória. Nesse período de trabalho remoto, é preciso reduzir os intervalos entre um backup e outro. A recomendação para esse tipo de procedimento é diária. Em caso de um incidente de Ransomware, por exemplo, a restauração dos arquivos afetados deve ser resolvida com mais facilidade, excluindo os arquivos que bloqueados substituindo pelos que estão salvos no backup. (SUPERINTENDIA DE TIC | UFRJ, 2020, p. 17).

HD externo, todo dia deixa uma programação para ao término do seu dia sendo ele na empresa ou home office para fazer um backup de segurança dos seus dados que você utilizou no dia, importante passo, lembrando de sempre você guardar esse HD em um local seguro, além de guardar importante colocar uma senha de padrão alto também para ter uma segurança maior.

7. ESTUDOS DE CASO COMO ESTRATÉGIA DE PESQUISA NA ÁREA DE SEGURANÇA DA INFORMAÇÃO

Fernandes (2010), a característica exploratória dos estudos de casos é importante para analisar gestão de segurança da informação em organizações.

7.1. ESTUDO DE CASO

A pesquisa baseada em estudo de caso reflete sobre nossa realidade atual causado pela pandemia da COVID-19, relacionada dentro do ambiente de trabalho em home office. Variáveis e fatores são observados nesse contexto, além de suas relações, na busca por evidências que mostrem ou descrevam uma determinada situação, conforme indicado por Gomes (2006).

Segundo Fernandes (2010), o estudo de caso pode além de servir de pressupostos a generalizações, também descrever uma determinada configuração de ambiente.

7.2. ESTUDO DE CASO REALIZADO NA INSTITUIÇÃO FINANCEIRA BSC

Este estudo de caso teve como objetivo principal observar, analisar e descrever a segurança da informação para os colaboradores em home office de uma instituição financeira, utilizando tópicos relativos das políticas de segurança da informação, infraestrutura de tecnologia da informação (TI) e práticas de gestão da segurança da informação. Estes tópicos foram escolhidos levando em consideração que grande parte dos controles de segurança da informação estão especificados em ABNT (2005) e ABNT (2006). A instituição financeira BSC foi assim denominada para que não fossem expostas informações confidenciais, vulnerabilidades, dentre outros aspectos.

Conforme o avança da pandemia causa pelo coronavírus se deu o entendimento deste estudo como essencial e os meios utilizados para esta pesquisa foram:

- **Observação direta** – Por meio de análise diária na unidade administrativa, e contatos realizados pelos colaboradores em home office;
- **Entrevistas** – Com o questionário que se encontra no anexo, foi realizado a entrevista com o responsável pelas ações da equipe de tecnologia da informação e segurança da informação, com o objetivo de coletar dados acerca da segurança da informação na instituição BSC, assim como a coleta de depoimentos dos colaboradores.

As entrevistas focadas em segurança da informação e infraestrutura, foram realizadas com um gerente de TI, Colaborador de TI responsável pela Infraestrutura trabalhando in loco e colaborador de TI responsável pela política de segurança trabalhando em home office. O questionário verificador de conformidade com a norma ABNT (2005) foi aplicado aos colaboradores mais aptos, in loco e home office. Segue tabela indicando os participantes que foram entrevistados em cada questionário.

Participantes	Ocupação	Questionário
1	Gerente de T. I	Política de segurança e infra
2	Colaborador de T.I política de segurança	Política de segurança
3	Colaborador de T. I infraestrutura	Infraestrutura
4	Gerentes, analistas, colaboradores	Conformidades

7.3. A INSTITUIÇÃO FINANCEIRA BSC

A BSC, é uma instituição financeira cooperativa onde não se tem clientes e sim donos, homens e mulheres que acreditam e promovem a justiça financeira, onde as decisões são tomadas de forma democrática. Definindo-se com:

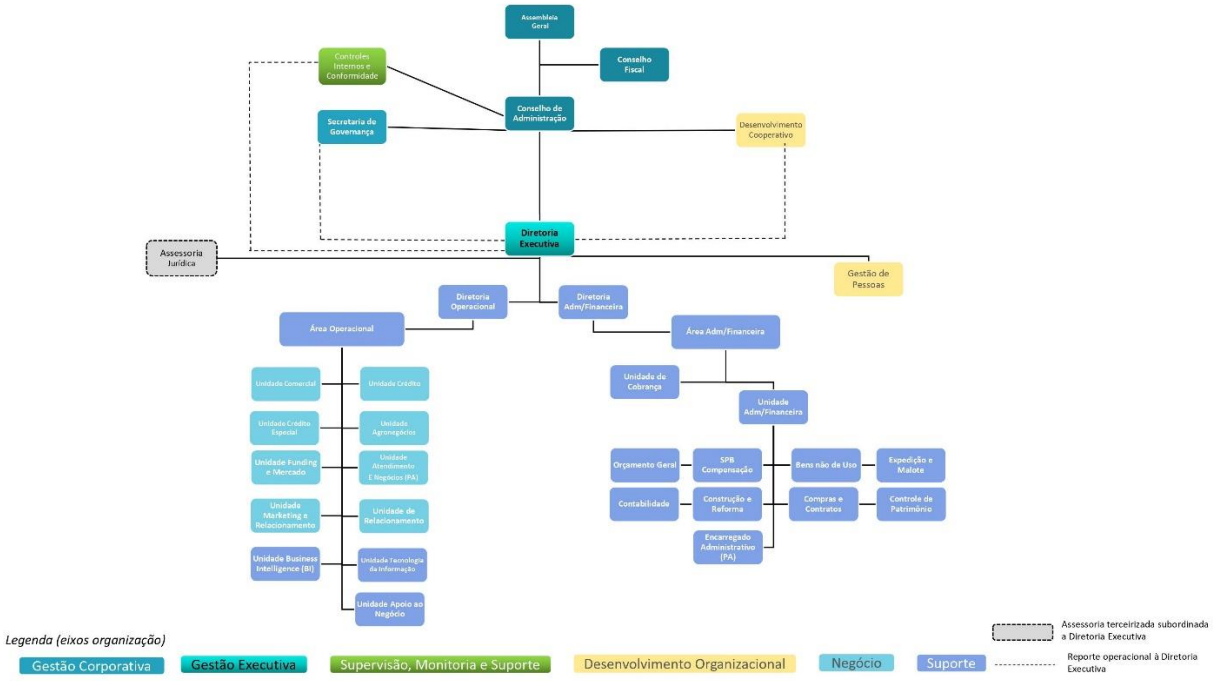
- **Propósito** - Conectar pessoas para promover justiça financeira e prosperidade.
- **Missão** - Promover soluções e experiências inovadoras e sustentáveis por meio de cooperação.
- **Visão** - Ser referência em cooperativismo, promovendo o desenvolvimento econômico e social das pessoas e comunidade.

Tendo como principal objetivo fazer cumprir uma gestão democrática, participativa e, principalmente, representativa. Junto aos seus valores: Respeito e

Valorização das Pessoas; Cooperativismo e Sustentabilidade; Ética e Integridade; Excelência e Eficiência; Liderança Responsável; Inovação e Simplicidade.

7.3.1. Gestão e Estrutura Organizacional

Uma instituição financeira baseada no cooperativismo, tem suas decisões tomadas pelos conselheiros, estes que representam os associados/cooperados. Segue um fluxograma para um melhor entendimento de suas estrutura e ramificação:



Os processos relacionais a TI da BCS estão ligados ao operacional, tendo assim em mente que o departamento de tecnologia está, de maneira direta, presente na forma final dos produtos ou serviços entregues aos cooperados.

7.4. A SEGURANÇA DA INFORMAÇÃO NA INSTITUIÇÃO

A segurança da informação na BCS apresenta um nível elevado de maturidade, pois existe uma preocupação evidente por parte de todos os envolvidos nas atividades da instituição. Existe uma política de segurança bem elaborada e alinhada ao código de conduta de ética dos funcionários e colaboradores. A sua elaboração teve a participação de todas as áreas que constituem a instituição e com o apoio do conselho administrativo e diretoria executiva. Este último de extrema importância pois já foi professor desta instituição de ensino, formado neste mesmo curso dando assim

suporte para tratar dos assuntos relacionados a TI. Além de tais, é de suma importância realçar as informações dos analistas “Grande parte dos requisitos de conformidade, são de exigências de órgãos reguladores, BACEN, código civil, diretos do consumidor por exemplo. eles são assegurados pela política de segurança da instituição”.

A BSC possui um planejamento estratégico de tecnologia que estabelece o direcionamento, ações e os recursos da área de TI para um período estipulado de 12 meses, alinhado ao planejamento estratégico institucional geral. Este planejamento é aprovado pelo conselho administrativo, diretoria executiva e sua fiscalização cabe ao conselho fiscal. Conforme palavras do gerente de TI “Ao chegar em março de 2020 já estávamos com o orçamento aprovado e suas aplicações elaboradas. Foi quando se iniciou a pandemia no nosso estado, fazendo com que os recursos fossem direcionados para outros pontos, mas de maneira positiva pois precisamos corrigir falhas que surgiram com o home office”.

A instituição vem investindo cada vez mais na segurança da informação e se preocupando com a parte dos colaboradores que se encontram em home office, parte de seus recursos financeiros estão sendo destinados na conscientização de seus colaboradores acerca da segurança da informação e na utilização correta de seus sistemas. Os treinamentos existentes visam à divulgação da Política de Segurança, através de treinamentos específicos e palestras online. Existe não só cursos de segurança da informação em sua plataforma de aprendizagem virtual, mas também vários outros visando a organização e a segurança de dados. Esta plataforma está disponível para todos os colaboradores, inclusive estagiários. Conforme palavras do estagiário de TI “A instituição tem nos proporcionado todos os tipos de aprendizado, não só o trabalho elaborado aqui, mas também com cursos e treinamentos para a segurança da informação, até por que cada documento, dado e informação, aqui é importante e devemos tratados de maneira correta”. E o colaborador de T. I responsável pela infraestrutura acrescenta “A instituição não peca na formação e nas cobranças dessas aos seus colaboradores, para se ter uma ideia umas das exigências é o curso CONDUTA EM REDES SOCIAIS, nele você aprende a cuidar da segurança da informação quando usar suas redes sociais e isso é um grande diferencial, principalmente se for pensar nos colaboradores em home office”

O gerenciamento e monitoramento é realiza através de uma gestão de políticas que controla e registra quaisquer tentativas de acesso direto e indireto de usuários (autorizados ou não) ocorridos nos recursos de infraestrutura (servidores, redes, entre outros ativos de T I). A utilização deste recurso é para que ocorrências sejam registradas a fim de detectar eventuais ações que indiquem falhas de segurança em processos. As informações coletadas são organizadas levando-se em consideração o grau de importância das ameaças, assim sendo tratadas por prioridade para garantir a integridade das informações.

Estas políticas estão divididas por setores e níveis de cargos, sendo que os gerentes têm uma maior liberdade sobre seu ativo. Outro ponto importante a se realçar são as camadas de criptografias e política de segurança diferenciada para os colaboradores em home office, devido ao fato de ser uma rede doméstica a BSC tem a preocupação com o trefego de informações realizados por estes. Conforme palavras do colaborador de TI “Com o imprevisto início da pandemia tivemos que agir rápido com a configuração de VPN, claro que já tínhamos equipamentos preparados para atender essa demanda, porém nunca havíamos feito teste para algo nessa escala, então tivemos sim uma grande preocupação.” Já o gerente de tecnologia da informação declara “Com o início da pandemia e os colaboradores em home office precisaríamos de algum software que nos ajudasse a melhorar o monitoramento dos ativos, o Kaspersky Business nos trouxe esse recurso. Além de ser um ótimo antivírus, alguns recursos nos trouxeram mais segurança, a localização e bloqueios de acesso as máquinas em caso de roubo são alguns desses recursos, isso ajudou a melhorar o nível de segurança já estabelecido pelo active directory”. O colaborador de T.I responsável pela política de segurança continua “Temos uma política no antivírus diferenciado para os colaboradores em home office, recursos como bluetooth e entradas usb são vulneráveis demais para estarem disponíveis fora da instituição”.

O departamento de tecnologia junto ao controle interno da cooperativa tem como responsabilidade tratar e solucionar qualquer evento adverso que comprometa ativos tecnológicos, pessoas, patrimônio ou processos de negócio, que possam causar prejuízo. Todos os colaboradores têm a responsabilidade de notificar vulnerabilidades e eventos que possam causar impacto aos ativos da instituição ao

ambiente de segurança da informação. E este tratar, monitorar e acompanhar adequadamente trata-se de aspectos que envolvam incidentes de segurança. O colaborador de T. I designado a cuidar da infraestrutura entrevistado ressalta que “Não estou aqui somente para dar suporte aos colaboradores, minha função é muito além de ensinar o pacote office (risos). Estamos monitorando cada ativo, cada computador tem que estar nas conformidades pois qualquer vulnerabilidade pode nos custar muito, para a instituição e seus associados”

Lembrando que os níveis de acesso aos acervos digitais, nos servidores locais ou em nuvem fazem parte da política de segurança. O acesso a pastas contendo imagens, vídeo, áudio, documentos, entre outros, é considerado restrito a cada departamento e assim estabelecendo as conformidade e interesses de cada departamento.

Todos os assuntos relativos a incidentes de segurança, tratamento da informação, responsabilidades de cada colaborador, ameaças, riscos, vulnerabilidades, fraudes, e aspectos relacionados à segurança da informação, são abordados em vários cursos internos promovidos pela própria instituição, obrigatórios a todos os colaboradores e que tem reciclagem a cada 12 meses, este é um processo de conscientização em segurança da informação.

Além destes recursos a instituição dispara duas vezes na semana um informativo de segurança da informação por e-mail e ao final do mês uma cartilha atualizada com todas as informações já disponibilizadas, a instituição dá um maior foco para os colaboradores que estão em home office, neles são apontados temas como: não passe informações por telefone; aplicar os níveis de seguranças para e-mail; engenharia social; Phishing; segurança mobile; aletas de segurança do antivírus. Esta cartilha está disponível no anexo II deste trabalho.

Conforme palavras do gerente de TI “A Microsoft disponibiliza vários recursos de segurança para utilizar de maneira correto os recursos do office 365, devido os colaboradores em home office foi implementado vários níveis de segurança no outlook. autenticação de dois fatores e níveis de confidencialidade ao envio de e-mail, fora alguns desse recursos implementados que hoje são obrigatórios”. E o colaborador

de T.I responsável pela política de segurança completa “Os dispositivos mobiles utilizados pela BSC acompanha a instalação do antivírus para manter os níveis de segurança assim como é feito nos computadores.”

Na segurança física e do ambiente, a BSC possui uma gestão dos recursos de segurança bancária e patrimonial, dentre os principais recursos de segurança destacam-se:

- **Vigilância Ostensiva:** atividade exercida no interior das instalações com o objetivo de resguardar a integridade física individual de colaboradores e cooperados, proteger o patrimônio da empresa e imagem da BSC.
- **Sistema de alarme:** implantados sistemas de alarme anti-assalto anti-incêndio e anti-intrusão.
- **Porta Giratória Detector de Metais:** recomendado às instituições financeiras, pelo Ministério da Justiça.
- **Sistema de Circuito Fechado:** proporciona observação eletrônica, dos ambientes internos da unidade, gravando e, quando necessário, transmitindo as imagens a uma central de monitoramento.
- **Leitora Biométrica:** recurso utilizado para dar acesso a portal com níveis de segurança restritos.
- **Fragmentadora de papéis:** evita ações de engenharia social.
- **Sistema de Caixas-fortes e Cofres:** propicia, de forma adequada, a guarda e a proteção de valores e de bens sob a responsabilidade das unidades.

O fornecimento de energia elétrica também é entendido como elemento de infraestrutura de TI. Para assim, de modo planejado, atenderem de forma adequada às necessidades dos serviços de tecnologia. O datacenter está localizado em uma sala climatizada de acordo com as especificações do fabricante de todos os equipamentos ali localizados, nesta sala contem termômetros onde se é feito o monitoramento deles na sala de suporte.

Na unidade administrativa dispõe de um gerador de energia que é acionado no momento da falta de energia elétrica da rede pública. Além do gerador existe uma rede paralela abastecida pelo nobreak, proporcionando assim redundância no fornecimento de energia, possibilitando a continuidade dos serviços oferecidos.

Esta rede paralela alimentada pelo nobreak está disponível também para as 17 agencias que compõe o grupo. Além delas foram disponibilizados aos colaboradores em home office estações de nobreak se necessário. Conforme palavras do colaborador de TI responsável pela infraestrutura “Com a migração de muitos colaboradores para o home office, tivemos que disponibilizar parte dos recursos em novas máquinas, estão sendo adquiridos vários notebooks robustos para atender demandas elencadas a estes colaboradores, além disso um hardware de grande desempenho e que possua qualidade da bateria é uma das nossas grandes preocupações”

A BSC através do ambiente de tecnologia possui um plano de contingência e recuperação de desastres de forma a manter a continuidade dos serviços essenciais à realização dos negócios, conforme afirmado pelo gerente de tecnologia em resposta a este assunto “Dentro do plano de contingência inclui-se nosso sistema de backup, tudo aquilo que não está em nuvem vem sendo replicado em tempo real para uma cópia exata do nosso datacenter montado em outra localidade”. E para finalizar discorre sobre o assunto um dos colaboradores de T.I “Uma das políticas de segurança aplicadas para os colaboradores em home office é que eles só podem salvar arquivos nos servidores, locais ou em nuvem. As políticas do active directory não os permitem salvar arquivos em seus computadores, assim caso roubados não se tem arquivos locais.”

7.5. AVALIAÇÃO DOS CONTROLES DE SEGURANÇA DA INFORMAÇÃO NA BSC

Foi formulado um questionário verificador de conformidade com a norma ABNT NBR ISO/IEC 17799 e ABNT NBR ISO/IEC 27002, presente no anexo deste trabalho com base em Praticando a Segurança da Informação em Edison Fontes (2010).

Com base nos resultados obtidos através da aplicação do questionário, contata-se que a Política de Segurança da Informação e demais controles e regulamentos é baseada na ABNT NBR ISO/IEC 27002. Avaliaram-se os objetivos de controle de segurança da informação presentes na instituição financeira BSC em relação ao seu atendimento. As respostas apresentadas abaixo como sim significam

que os controles são atendidos, parcialmente significa que alguns controles são atendidos e não significa que nenhum controle é atendido.

Objetivo do Controle	Atendimento ao objetivo
Política de Segurança da Informação	Parcialmente
Fatores Críticos de Sucesso	Sim
Infraestrutura de segurança da informação	Sim
Gestão de Ativos	Sim
Segurança Física e do Ambiente	Sim
Controle de Acesso	Sim
Gestão de Incidentes de Segurança	Sim
Gestão da Continuidade do Negócio	Sim
Conformidade	Sim

7.6. ANÁLISE DOS RESULTADOS

Conforme a análise sobre a segurança da informação, todos tem o seu papel nesta instituição, que se inicia na leitura da documentação de segurança de TI, e da área que vai atuar, alinhados com o manual do colaborador e suas obrigatoriedades indo até as empresas prestadoras de serviços que assim como os demais fazem o seu papel para resguardar todas as informações de maneira correta.

Os cuidados tidos com os colaboradores em home office é visto de uma maneira admirável, novas tecnologias e recursos foram aplicadas para atender as necessidades desses, de maneira que as atividades desenvolvidas pelos mesmos não sofram danos ou preocupações de fraudes caudas por ataques cibernéticos.

Ficou constatado que existe ali um sistema de solicitação de suporte que abrange diversas áreas da instituição, nele é possível solicitar uma demanda para o departamento de tecnologia ou para o financeiro. Apesar da ideia ser boa, um sistema integralizado entre departamentos, foi constatado algumas falhas principalmente de segurança, alguns colaboradores conseguem enxergar alçadas mais restritas interdepartamentais.

Enquanto esse estudo de caso se seguia a gestão de tecnologia junto ao controle interno buscavam software que poderiam sanar essa falha na segurança da informação e resguardas a privacidade de dados de cada departamento. A ideia é um sistema que possa continuar integralizado entre todos os departamentos, mas que seja algo moderno e seguro, onde se possa demonstrar as prioridades de chamados e relatórios para sanar incidentes recorrentes buscando agilidade e qualidade nos

atendimentos aos colaboradores que tem o objetivo de resolver questões relacionadas aos cooperados.

7.6.1. Instrumento de Pesquisa – Respostas dos Questionários

Os dados e informações deste questionário serão utilizados para a pesquisa acadêmica do curso de bacharelado em Sistemas de Informação do Centro Universitário São Lucas de Ji-Paraná. As informações serão apresentadas sem a identificação dos entrevistados assim como a instituição, com o objetivo de analisar a gestão de segurança da informação dos colaboradores em loco e home office.
Respostas aos questionários relativos à política de segurança da informação, gestão da segurança da informação, infraestrutura de tecnologia da informação e home office.

Política de Segurança da Informação e Gestão de Segurança da Informação
Entrevistado: Gerente de TI

1. **A instituição financeira possui uma política de segurança da informação? Ela considera as visões de todos os envolvidos?**
   R: Sim

2. **Qual o intervalo de tempo que a política de segurança da informação é revisada? Este intervalo de tempo é definido ou ocorre quando mudanças significativas na instituição?**
   R: Revisada Anualmente ou a qualquer tempo conforme necessidade

3. **Existe uma conscientização da importância da política de segurança da informação por parte dos colaboradores? Como isto é mensurado?**
   R: Sim, enviado regularmente informativos sobre o tema, e dado treinamento a novos colaboradores

4. **A política de segurança da informação define os papéis e responsabilidades pela segurança da informação?**
   R: Sim

5. **Quando da formulação do planejamento estratégico da organização, a segurança da informação é considerada?**
   R: Sim

6. **A diretoria da instituição considera a gestão da segurança da informação como questão crítica para a organização?**
   R: Sim

7. **As decisões relacionadas com a segurança da informação são tomadas exclusivamente pela área de TI ou em conjunto com a equipe responsável pelas decisões estratégicas da organização?**
   R: Em com conjunto com a equipe

8. **O acesso às informações preserva os critérios de confidencialidade, integridade e disponibilidade?**
   R: Sim

9. **Como é feita a identificação dos riscos? Eles são previstos através de um plano de contingência?**
   R: São medidos os riscos, reduzindo sempre a níveis aceitáveis onde não terão alto impacto. Sim são previstos em planos de contingência

10. **Existem controles e requisitos de segurança da informação quando dos contratos com terceiros?**
    R: Sim, inclusive sobre tratamento de dados pessoais

7.6.2. Infraestrutura de Tecnologia da Informação (TI) e Gestão de Segurança da Informação

1. **Como é vista a infraestrutura de TI na organização? Há compreensivo, pela instituição, a influência da infraestrutura de TI no cumprimento da missão?**
   R: Ela é vista como o ponto central da organização, sendo que ela tem total influencia no desempenho das metas

2. **A diretoria vê a infraestrutura de TI como elemento estratégico da instituição? Como a diretoria trata dos investimentos em infraestrutura de TI pela organização?**
   R: Sim, porém trata com cautela os investimentos

3. **Como as falhas em elementos da infraestrutura afetam a confiabilidade da organização? Qual a relação entre eficiência da instituição e sua infraestrutura de TI?**
   R: As falhas deixam os colaboradores e clientes insatisfeitos, consequentemente as falhas reduzem a produtividade e afastam negócios

4. **O fornecimento de energia elétrica é visto como elementos de infraestrutura de TI?**
   R: Com certeza

5. **Quais controles de acesso físico aos ambientes restritos e ambientes de TI na instituição?**
   R: Separação por vários ambientes, sendo necessário passar 3 níveis de acesso

6. **Os equipamentos de uso individual, tais como notebook e desktops, são vistos como ativos da infraestrutura de TI?**
   R: Sim

7. **Como é realizado o processo de armazenamento e recuperação de dados utilizados pela instituição?**
   R: utilizando sites distintos, utilizando tecnologias de disaster recovery

8. **O monitoramento do correto funcionamento dos equipamentos da infraestrutura de TI é feito? Os resultados do monitoramento são usados para melhoria da infraestrutura de TI?**
   R: Sim

7.6.3. Home Office

1. **Quais as maiores dificuldades enfrentadas pela equipe de T.I ao aderir o home office no início da pandemia?**
   R: Implantação de VPN

2. **Existem vantagem ou desvantagens na infraestrutura com os colaboradores em Home office?**
   R: No atual cenário não, inclusive alguns colaboradores são mais produtivos em home office

3. **Relacionado a proteção de dados, quais as maiores preocupações trabalhando em home office?**
   R: roubo de equipamento somente

4. **Como funciona o home office na instituição, os colaboradores utilizam dispositivos pessoais?**
   R: Não

5. **Como pode ser realizado a proteção dos logins? Quais camadas de proteção podem evitar uma brecha de segurança?**
   R: Criptografia da conexão

6. **Para os colaboradores que estão em home office, existe uma política de segurança diferente comparada aos que estão in loco?**
   R: Sim

7. **Engenharia social é um risco para os colaboradores em home office?**
   R: Sim

8. **A instituição pratica meios de deixar os colaboradores informados sobre os ricos? Existem práticas, medidas a serem adotadas para garantir a segurança da informação?**
   R: Sim

9. **Ferramentas para segurança das informações é essencial. Firewall, Antivírus, Web Filter, IDS/IPS, Proxy, VPN. quais as dificuldades para aplicação em home office?**
   R: Sim totalmente essencial, e todas aplicadas independente do ambiente

7.6.4. QUESTIONÁRIO VERIFICADOR DE CONFORMIDADE COM A NORMA ABNT NBR ISO/IEC 17799 e ABNT NBR ISO/IEC 27002

Para a resposta de cada questão o padrão de avaliação utilizado será o seguinte:
0 – Não se aplica.
1 – Resposta – Não.
2 – Solução em Planejamento inicial.
3 – Está planejada a implantação da solução.
4 – Parcialmente implementada. Ainda não confiável.
5 – Está funcionando bem.
6 – Sim

Política de Segurança da informação

1. Existe um documento de política de segurança definindo a filosofia, as diretrizes da organização em relação ao uso e proteção da informação?
   R: 6

2. Existem outros regulamentos que complementam e detalham como os objetivos descritos na política de segurança da informação podem e devem ser alcançados?
   R: 6

3. Existe um processo que garanta a atualidade dos regulamentos de segurança?
   R: 4

4. É garantido que todos os usuários de informação conhecem os regulamentos de segurança de informação existentes?

R: 6

5. A política de segurança da informação está coerente com o código de ética e demais políticas corporativas?
   R: 6

6. A política de segurança da informação está de acordo com a legislação do país?
   R: 6

Fatores críticos de sucesso

1. Quando do planejamento das ações de negócio da organização existe o envolvimento da área de segurança da informação?
   R: 5

2. O executivo da área de segurança da informação participa de comitê que analisa os requisitos necessários para a implementação dos futuros produtos e serviços da organização?
   R: 6

3. Existe definido o orçamento e demais recursos para o processo de gestão da segurança da informação?
   R: 6

4. A direção da organização valida periodicamente o direcionamento e prioridades da implementação dos controles de segurança da informação?
   R: 6

Infraestrutura de segurança da informação

1. Existe uma estrutura organizacional com a responsabilidade de coordenar o processo de segurança da informação?
   R: 4

2. Foi dado conhecimento a todos os usuários da informação da existência da área responsável pelo processo de segurança da informação?
   R: 6

3. A área de segurança da informação tem definido formalmente suas responsabilidades, escopo de atuação, estrutura de recursos e plano de ação?
   R: 6

Gestão de Ativos

1. Existe uma política de classificação da informação que define os níveis de sigilo e indica para cada um deles como deve ser tratada a informação?
   R: 6

2. O gestor da informação é o responsável pela liberação do acesso à informação pelo usuário?
   R: 6

3. Existe procedimento definido para o descarte de equipamentos garantindo que as informações serão devidamente apagadas antes do ativo ser liberado?
   R: 4

Segurança em recursos humanos

1. Existe um processo de conscientização e treinamento de usuários em segurança da informação?
   R: 6

2. Todo tipo de usuário participa do treinamento em segurança da informação?
   R: 6

3. Todo usuário antes de iniciar suas atividades profissionais na organização recebe orientações em relação à segurança da informação e toma conhecimento dos regulamentos existentes?
   R: 6

4. Cada usuário formaliza o seu conhecimento dos regulamentos através de assinatura de um documento?
   R: 6

Segurança física e do ambiente

1. Cada pessoa tem autorização de acesso físico apenas aos ambientes que necessita acessar para desempenhar as funções profissionais na organização?
   R: 6

2. O acesso físico das áreas é controlado, impedindo que pessoas não autorizadas acessem ambientes em que não estão autorizadas?
   R: 6

3. O acesso físico de cada pessoa fica registrada, permitindo uma auditoria?
   R: 6

4. Existe o monitoramento e gravação de imagens dos principais pontos de acesso ao ambiente físico, pontos de vigilância e do perímetro do terreno?
   R: 6

5. As imagens são armazenadas durante um período previamente estabelecido, podendo ser recuperadas neste período?
   R: 6

6. As imagens são guardadas em um local protegido adequadamente de forma que não seja possível o roubo delas com o objetivo de desaparecimento de provas?
   R: 6

7. As pessoas são avisadas de que o ambiente é monitorado e gravado?
   R: 4

8. Existe um processo contínuo garantindo a efetividade das medidas de controles existentes?
   R: 5

9. Existe um controle de para a saída e entrada de material?
   R: 6

10. Sempre que possível é utilizado material retardante a fogo, que dificulta o início e a propagação do incêndio?
    R: 6

11. Existe sinalização de emergência indicando as saídas e saídas de emergência?
    R: 6

Gerenciamento das operações e comunicações

1. Existe documentação dos processos e procedimento relativos aos recursos de informação?
   R: 6

2. Foi analisada a questão da segregação de função e está garantido que este controle está implementado?
   R: 5

3. É proibida a execução no ambiente de produção de programas em teste ou em situação de homologação?
   R: 5

4. Antes da passagem de programas para a produção é feito um processo de teste e homologação para garantir que o que será implantado em agências possui uma qualidade e uma efetividade adequada?

R: 6

5. Todo o processo de passagem de programa para o ambiente de produção pode ser auditado?
   R: 6

6. Os serviços prestados por terceiros são monitorados e gerenciados de maneira que possa ser feita uma avaliação desse prestador de serviço?
   R: 6

Controle de acesso

1. A identificação do usuário é única e individual para qualquer tipo de usuário?
   R: 6

2. Existe a garantia da não existência de identificações genéricas?
   R: 6
3. Quando a autenticação é feita através de senha, essa senha é secreta e de conhecimento exclusivamente do usuário?
   R: 6

4. É declarado nas políticas que o usuário é responsável pelo acesso realizado com a sua identificação e autenticação?
   R: 6

5. Todo acesso realizado ou tentativa, ao ambiente computacional é gravado e guardado durante um tempo definido pela segurança da informação?
   R: 6

6. A informação é apenas liberada para o usuário após a autorização do gestor da informação?
   R: 6

7. O processo de liberação de acesso da informação para o usuário é formalizado e registrado, permitindo auditoria?
   R: 6

8. Existe um processo automático que retire os acessos do usuário quando ele é transferido para outra área da organização?
   R: 1

9. Existe um processo automático que retire a identificação do usuário quando ele encerra seu relacionamento profissional com a organização?
   R: 1

10. Quando do uso de senhas, o arquivo de senhas é criptografado?
    R: 6

Aquisição, desenvolvimento e manutenção de sistemas

1. É utilizada uma metodologia de desenvolvimento de sistemas, e essa metodologia é de conhecimento de todos os desenvolvedores (funcionários e terceiros)?
   R: 6

2. Existe na metodologia desenvolvimento de sistemas uma etapa para a especificação dos requisitos de segurança da informação antes do desenho lógico da solução?
   R: 6

3. Existem pelo menos três ambientes computacionais: de desenvolvimento, de teste e produção?
   R: 6

4. Quando da aquisição de sistemas são considerados vários aspectos da solução, inclusive o grau de certeza da continuidade do fornecedor no mercado de tecnologia?

R: 6

5. Existem cópias de segurança suficientes para recuperação do ambiente de desenvolvimento de sistemas?
   R: 6

Gestão de incidentes de segurança

1. Existe um processo estruturado para o tratamento de incidentes de segurança da informação?
   R: 5

2. A prioridade de ações a ser feita em consequência de ocorrência de incidentes de segurança da informação considera o negócio da organização?
   R: 6

3. O processo de tratamento de incidentes de segurança da informação gera informações que possibilitam um melhor planejamento para a proteção do ambiente de tecnologia?
   R: 6

4. Existe um canal de comunicação entre o usuário possa registrar a ocorrência de um incidente, além de acompanhar a pesquisa destes incidentes e conclusões definidas pela organização?
   R: 6

Gestão da continuidade do negócio

1. Existe um plano de continuidade de negócio para ser seguido quando da ocorrência de um desastre que indisponibilize recursos de informação?
   R: 6

2. É realizada periodicamente uma avaliação de risco com foco nas ameaças que podem indisponibilizar recursos de informação e podem parar ou degradar em muito o desempenho da realização do negócio?
   R: 4

3. Existe um manual atualizado que define os procedimentos a serem feitos quando da ocorrência de uma situação de contingência?
   R: 4

4. Todos os envolvidos foram treinados considerando as orientações formalizadas no manual do plano de continuidade de negócio?
   R: 4

5. São realizados testes periódicos para a utilização do plano de continuidade de negócio?
   R: 4

6. Existem cópias de segurança considerando aspectos de operação, de auditoria, guardadas de forma segura, suficientes para uma recuperação da informação?
   R: 6

Conformidade

1. Existe de forma explícita o conjunto de legislação, regulamentos de segmentos de negócio e requisitos éticos que a organização é obrigada a seguir?
   R: 6

2. Esse conjunto de requisitos é de conhecimento dos usuários que tratam a informação da organização para desenvolver sistemas, proteger a mesma e definir procedimentos de recuperação dos recursos da informação?
   R: 6

3. A área jurídica interage fortemente com a área de segurança da informação com a área de tecnologia da informação, com o objetivo de garantir a conformidade da organização com a legislação e demais regulamentos?
   R: 4

4. Existe processo que defina e formalize os requisitos necessários para que possam ser realizados procedimentos de auditoria e de performance computacional?
   R: 4

7.7. CONSIDERAÇÕES FINAIS

Neste trabalho foi relatado o cenário de gestão da segurança da informação e seus cuidados com os colaboradores em home office da instituição financeira BSC, os dados foram levantados por meio de estudo de caso proposto.

Estudos de caso, semelhante ao realizado neste trabalho relativo à gestão da segurança da informação na instituição BSC, podem inclusive ser utilizados para preparar e orientar organizações, para que estejam em conformidade com os requisitos, políticas de segurança da informação aos quais estão sujeitas. Assim sendo, pode-se utilizar estudos como este como forma de preparação para auditorias, com o intuito de identificar eventuais falhas e adequações necessárias.

8. CONCLUSÃO

Através deste trabalho de conclusão de curso e do estudo de caso utilizado, foi possível realizar uma avaliação da instituição financeira BSC quanto à sua gestão de segurança da informação, práticas de segurança da informação e suas aplicações em home office, observando as normas e legislações a que está sujeita.

Através da sua política de segurança bem definida e de acesso a todos os colaboradores, a gestão da segurança da informação nesta instituição é uma questão já bem desenvolvida onde existe um bom mecanismo para divulgação e conscientização desta política, cursos, palestras, reuniões e informativos auxiliam no processo de conscientização.

Pôde-se se observar que a administração da BSC através de seu planejamento estratégico, políticas orçamentárias, orçamento direcionado aos recursos de TI, segurança da informação e infraestrutura de tecnologia consideram as questões relacionadas de suma importância para o crescimento do negócio e da instituição.

Visto que todos os seus processos são organizados e bem divididos pela equipe para evitar que falhas aconteçam, mas ainda se da a necessidade de melhoria no fluxo de suporte e direcionamento de chamados, questão esta que já está sendo corrigida conforme mencionado anteriormente. Outras questões bem desenvolvidas e com a segurança bem aplicadas são os contratos de prestadores de serviços terceirizados. É de grande admiração a conscientização dos colaboradores referente a segurança da informação, in loco ou em home office.

Para finalizar se dá a importância e a preocupação evidente da administração com questões relativas à segurança do pessoal e ambiente, com o objetivo de prover a segurança dos seus cooperados, colaboradores e ativos de TI, por uma gestão de segurança bancária e patrimonial. A instituição dispõe de um plano bem definido de análise de riscos, contingência e recuperação de desastres.

8.1. TRABALHOS FUTUROS

A proposta de continuação para este trabalho seria realizar um mesmo estudo proposto neste trabalho em organizações financeiras e confrontar os resultados obtidos com os resultados deste.

9. REFERÊNCIAS

ABNT. **Associação Brasileira de Normas Técnicas**. ABNT NBR ISO/IEC 17799. ABNT, Rio de Janeiro, (2005).

ABNT. **Associação Brasileira de Normas Técnicas**. ABNT NBR ISO/IEC 27002. ABNT, Rio de Janeiro, (2007).

ALBURQUERQUE, Ricardo; RIBEIRO, Bruno. **Segurança no desenvolvimento de Software**. Rio de Janeiro: Editora Campus Ltda, 2002.

ALMEIDA, M.B., CARNEIRO, Luciana Emirena Santos. **Gestão da Informação e do Conhecimento no âmbito das práticas de Segurança da Informação: O fator humano nas organizações**. Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação, Florianópolis, v. 18.

ANTONIO, MARCOS. **Engenharia Social um perigo Eminente**. Disponível em < https://www.academia.edu/38720641/ENGENHARIA_SOCIAL_Um_Perigo_Eminente> Acesso em: 26 de maio 2021.

AURORA DA SILVA, CLAUDETE. **Gestão da segurança da informação: um olhar a partir da Ciência da Informação**. Disponível em < http://tede.bibliotecadigital.puccampinas.edu.br:8080/jspui/bitstream/tede/819/1/Claudete%20Aurora%20da%20Silva.pdf> Acesso em: 25 de maio 2021.

BEAL, Adriana, Segurança da Informação: **Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações**. 1. ed. São Paulo: Atlas, 2005.

BERONALDA, MARIANA. **Phishing de internet, como criminalizar? Aspectos tecnicose Juridicos dessa ameaça virtual**. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=6840f4a1c1d16484> Acesso em: 26 de maio 2021.

BRINK,G. J. Operational risk: **the new challenge for bank**. 1. Ed. Nova York: Palgrave, 2002.

CANONGIA, Claudia; **MANDARINO, Rafael. Segurança Cibernética: o desafio da nova sociedade da informação**. Parcerias estratégicas, Brasília, v.14.

CANONGIA, Claudia; MANDARINO, **Rafael. Segurança Cibernética: o desafio da nova sociedade da informação**. Parcerias estratégicas, Brasília.

CROUHY, Michel; GALAI, Dan; MARK, Robert. **Fundamentos da Gestão de Risco**. Rio de Janeiro: Qualitymark Editora, 2008.

CROUHY, Michel; GALAI, Dan; MARK, Robert. Gerenciamento de Risco – **Abordagem Conceitual e Prática**. São Paulo: QualityMark Editora, 2004.

DAMODARAN, A. **Gestão estratégica do risco: uma referência para a tomada de riscos empresariais**. Porto Alegre: Artmed, 2009.

ELIANE, C. (Org.). **Racismo e anti-racismo na educação: repensando nossa escola**. São Paulo: Selo Negro, 2001.

FONTES, Edison. **Segurança da Informação: O Usuário faz a diferença**. São Paulo: Saraiva, 2006.

FONTES, Edison. **Praticando a segurança da informação**. Rio de Janeiro: Brasport, 2010.

FORTUNA, Eduardo. **Mercado Financeiro – Produtos e serviços**. Rio de Janeiro: Quality mark 2008.

GALVÃO, Michele da Costa. **Fundamentos em Segurança da Informação**. São Paulo: Person Education do Brasil, 2015.

GOMES, Nilma Lino. **Educação cidadã, etnia e raça: o trato pedagógico da diversidade**. In:

GOMES, CLEBER CALDANA. **Instalador e reparador de redes de computadores**. Disponível em < http://pronatec.ifpr.edu.br/wp-content/uploads/2012/07/irrc1.pdf>. Acesso em: 25 de maio 2021.

GONZALEZ DE GOMEZ, Maria Nélida. **Mudanças das relações entre conhecimento, linguagem e informação**: reflexão epistemológica, consequências políticas. In:

LAUREANO, Marcos Aurelio, **Pchek.Gestão de Segurança da Informação**, 2005.

Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em: 31 de março de 2021.

MELLO, ALVARO. **O trabalho em qualquer lugar e a qualquer hora**. Disponível em: <https://www.crasp.gov.br/centro/conteudo/old/uploads/17_11_2004_TELETRABALHO_O_TRABALHO_EM_QUALQUER_LUGAR_E_A_QUALQUER_HORA.pdf> Acesso em: 25 de maio 2021.

MOOSA, I. A. **Operational Risk: A Survey. New York University Salomnn Center, Financial Markets, Institutions & Instruments**, v. 16.

NETO, Abílio Bueno; SOLONCA, Davi. **Auditoria de Sistemas Informatizados**. 3ª edição; Palhoça: Unisul Virtual, 2007.

NETTO, Abner da Silva; SILVEIRA, **Marco Antônio Pereira da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias** empresas. Revista de Gestão da Tecnologia e Sistemas de Informação. Vol. 4. Disponível em: < https://www.researchgate.net/publication/26543807_Gestao_Da_Seguranca_Da_Informacao_Fatores_Que_Influenciam_Sua_Adocao_Em_Pequenas_E_Medias_Empresas> Acessado em 13 de maio de 2021.

ORRICO, Evelyn Dill; GONZALEZ DE GOMEZ, Maria Nélida (Ed.). **Políticas de memória e informação: reflexos na organização do conhecimento**. Disponível em: < http://revista.ibict.br/inclusao/article/view/1513/1709> Acessado em 13 de maio de 2021.

OLIVEIRA, Wilson José de. **Segurança da Informação: Técnicas e Soluções**. Florianópolis: Visual Books Ltda, 2001.

OLIVEIRA, Gabriella Domingos de; MOURA, Rafaela Caroline Gaudêncio de; ARAÚJO, Francisco de Assis Norberto Galdino de. **Gestão da segurança da**

informação: perspectivas baseadas na tecnologia da informação. In: Encontro Regional de Estudantes de Biblioteconomia, Documentação, Ciência e Gestão da Informação, 15, 2012, Juazeiro do Norte. Disponível em: <https://periodicos.ufpb.br/ojs/index.php/pbcib/issue/view/1610>. Acesso em: 15 de abril de 2021.

PEIXOTO, Mário César Pintaudi. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro, Brasport, 2006.

PINHEIRO, Patrícia Peck. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2010.

SANTOS, Alfredo Luiz dos. Gerenciamento de identidades: **Segurança da Informação**. Rio de Janeiro: Brasport, 2007.

SANTANA, Raimundo Alexandrino de. **Os Firewalls e a segurança na internet**, 2013. Disponível em: <https://pt.slideshare.net/alexandrino1/tcc-firewalls-e-a-segurana-na-internet>. Acesso em: 15 de abril de 2021.

SALVATICO, REGIANI**. A carreira de profissionais de TI em sistemas home office**. Disponível em <https://tede2.pucsp.br/bitstream/handle/20000/2/Regiani%20Salv%C3%A1tico%20Pereira%20da%20Silva.pdf > Acesso em: 25 de maio 2021.

SERGIO MARCONDES, JOSÉ. **Engenharia social: O que é? Conceitos, Técnicas e como se proteger**. Disponível em < https://gestaodesegurancaprivada.com.br/engenharia-social-o-que-e-conceitos/> Acesso em: 25 de maio 2021.

SÊMOLA, Marcos. **Gestão da Segurança da Informação, uma visão Executiva**. Rio de Janeiro: Elsevier, 2003.

SÊMOLA, M. **você já fez uma análise de riscos de verdade**? Rio de Janeiro, n.41, jun. 2002. Disponível em: <

http://www.semola.com.br/disco/Coluna_IDGNow_41.pdf>. Acessado em 12 de maio de 2021.

TRABALHO REMOTO DOMICILIAR, **GUIA DE ORIENTACAO E BOA PRÁTICAS**. Disponível em <https://tic.ufrj.br/wp-content/uploads/2020/03/Cartilha-de-Trabalho-Remoto-Seguro-1.pdf> Acesso em: 26 de maio 2021.

TCU. **Boas Práticas em Segurança da Informação**. 4. ed. Brasília: TCU, 2012. Disponível em < https://portal.tcu.gov.br/biblioteca-digital/cartilha-de-boas-praticas-em-seguranca-da-informacao-4-edicao.htm> acessado em 11 de maio de 2021.

MITNICK, K. D.; SIMON, W. L. A Arte de Enganar: ataques de hackers – controlando o fator humano na segurança da Informação. São Paulo: Makron, 2003.

Smith, R.E. (2002). The strong password dilemma. Authentication: From Passwords to Public Keys. Chapter 6. Addison-Wesley

SANS INSTITUTE. Issues with Keeping AntiVirus Software Up to Date. Disponível em:<https://www.sans.org/reading-room/whitepapers/malicious/issues-keeping-antivirussoftware-date-34>. acessado em 11 de maio de 2021

ANEXO I
CARTILHA DE SEGURANÇA DA INFORMAÇÃO

Encontre aqui orientações para manter os seus dados e dos nossos cooperados sempre protegidos.

INTRODUÇÃO

Nas próximas páginas, você vai encontrar informações importantes sobre:

- Lei Geral de Proteção de Dados Pessoais (LGPD);
- Melhores práticas no tratamento de dados pessoais;
- Orientação de segurança para home office;

- Como proteger seus dados;
- Informações pessoais em redes sociais;
- Utilização de dispositivos móveis;
- Evitando ataques de engenharia social; e
- Dicas para evitar Phishing.

Consulte este documento sempre que precisar.

- **LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)**A Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018, regula e impõe uma profunda transformação na forma pela qual as empresas no Brasil utilizam ou tratam dados pessoais. Ela visa garantir que as pessoas tenham mais privacidade e controle sobre seus dados, e que seja evitado o mal-uso deles por terceiros. Entenda um pouco mais sobre a LGPD:
- A Lei Geral de Proteção de Dados Pessoais (LGPD) foi criada para regulamentar o tratamento dos dados pessoais e fazer com que a privacidade das pessoas seja respeitada. Com a LGPD, os dados pessoais só poderão necessidade, transparência, segurança, não discriminação etc.;
- Todos os processos que tratam dados pessoais devem estar em conformidade com a LGPD. Portanto, além de tomar cuidado com os seus dados, você também deve tomar cuidado com os dados de outras pessoas que de alguma forma são tratados por você, principalmente, evitando seu vazamento;
- Tratamento é qualquer ação que seja executada com os dados pessoais, como um simples registro ou acesso de dados de colaborador (como RG, CPF, endereço, biometria etc.), armazenamento, transferência, classificação eliminação, ou qualquer outra manipulação de dados pessoais. Sendo assim, é importante estar atento, pois a LGPD impactará várias áreas, como RH, Marketing, administrativo, TI, dentre outras. E além dos meios digitais, isso também vale para meios físicos, como formulários em papel, documentos, registros manuais de portarias para acesso em condomínio etc.;
- A LGPD demanda uma mudança de atitude para a forma de como tratamos os dados pessoais e isso terá impacto nos processos do negócio. Quem não cumprir a Lei, pode ter a atividade de coleta de dados suspensa, a ampla divulgação da infração para a imprensa e até mesmo a possibilidade de receber

multa. E não se trata apenas de estar em conformidade com a Lei, mas também de manter a conformidade ao longo do tempo. Portanto, todos nós devemos conhecer os princípios da LGPD, pois, de alguma forma, utilizamos dados de cooperados e/ou dos colaboradores em nossas atividades.

MELHORES PRÁTICAS NO TRATAMENTO DE DADOS PESSOAIS

É necessário cuidado ao manipular dados pessoais de outras pessoas e ser conservador com os seus próprios dados pessoais. Seguem dicas de melhores práticas para o tratamento de dados pessoais:

- Ao compartilhar seus dados em aplicativos e serviços online, procure saber todas as finalidades da utilização e evite o uso por pessoas não autorizadas;
- Ao utilizarmos redes sociais, estamos disponibilizando nossos dados pessoais. Por isso, tenha cuidado com quais dados você compartilha;
- Limite o acesso às suas informações pessoais às pessoas que, de fato, precisam delas para a execução de suas atividades;
- Se precisar divulgar dados pessoais, verifique antes a identidade da pessoa que solicita e a real necessidade de passar essa informação;
- Sempre questione se, para a aquisição de determinado produto ou serviço, você precisa realmente informar todos os dados solicitados;
- Cuidado com mensagens aparentemente legítimas e verdadeiras que são utilizadas para capturar dados de usuários;
- Seja cuidadoso(a) com o que você compartilha. Quanto mais informações pessoais você revela online, mais vulnerável você fica a roubo de identidade e golpes;
- Proteja sua privacidade. Leia a política de privacidade de sites onde você está compartilhando conteúdo e saiba como sua informação poderá ser usada;
- Pense a longo prazo. Uma vez que uma informação é compartilhada na Internet, talvez nunca mais possa ser deletada;
- Bloqueie sua estação de trabalho sempre que for se ausentar;
- Não armazene dados pessoais sensíveis localmente em sua estação de trabalho, como por exemplo, origem racial ou étnica, convicção religiosa,

opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político;

- Não utilize o verso de fotocópias com dados pessoais ou informações sensíveis como folhas de rascunho;
- Se for necessário armazenar dados pessoais fisicamente, guarde-os em armários com portas fechadas à chave, ou em local seguro e de acesso restrito; e
- Tenha cautela ao descartar documentos com informações pessoais ou dados sensíveis. É importante fazer esse descarte após utilização de um triturador ou fragmentadora de papel.

ORIENTAÇÕES DE SEGURANÇA PARA HOME OFFICE

Trabalhar de casa tem sido uma alternativa mais segura neste momento, por conta da Covid-19. No entanto, essa ação exige cuidados redobrados com a segurança. Se você está em home office, siga essas dicas e saiba como manter suas seguras mesmo longe da organização:

- Utilize somente sua rede residencial ou móvel para o trabalho remoto. Não realize o acesso remoto por meio de rede wi-fi pública ou de vizinhos.
- Se possível, configure uma senha forte para seu wi-fi; E, principalmente, assegure que seu roteador não está configurado com a senha padrão do fabricante;
- Sempre que possível, utilize dispositivos corporativos que já possuam as configurações e atualizações de segurança da organização para a realização do acesso remoto, ao invés de dispositivos pessoais;
- Não é permitido o acesso aos equipamentos e sistemas de informações da empresa por pessoas não autorizadas;
- Não realize o acesso remoto por meio de máquinas instaladas em locais públicos (Coworking, Lan House, Cyber café e outros locais do gênero);
- Bloqueie seu computador sempre que se ausentar da estação de trabalho;
- Mantenha as estações de trabalho, dispositivos móveis e os computadores portáteis atualizados com todos os patches de correção e de segurança fornecidos pelo fabricante, devidamente aplicados;

- Evite usar opções de preenchimento automático de dados como “Lembre-se de mim”;
- Se suspeitar de comprometimento da sua senha de acesso, troque-a imediatamente;
- Não discuta informações confidenciais em locais públicos ou de circulação de pessoas não ligadas à empresa;
- Utilize o acesso via VPN somente para execução de atividades que requeiram esse tipo de acesso;
- Esteja atento caso receba ligações de alguma pessoa se identificando como colaborador, solicitando informações sensíveis, pedindo que seja informada alguma senha padrão, a execução de algum procedimento como alteração de perfil ou concessão de acesso, pois pode ser uma pessoa mal-intencionada se passando por um colaborador; e
- Nunca forneça informações sensíveis, pessoais ou da empresa, por telefone ou outros meios, quando a iniciativa do contato não for sua.

COMO PROTEGER SEUS DADOS

Você sabe criar senhas fortes, seguras e difíceis de adivinhar? Com essas dicas simples, você aprende a fazer isso e deixa seus dados mais protegidos. Dá uma olhada:

- Crie senhas fortes e difíceis de decifrar por pessoas mal-intencionadas;
- Sua senha é pessoal, inequívoca e intransferível. Jamais revele-a a terceiros, nem mesmo para um colaborador ou alguém de sua confiança;
- Evite gravar senhas para preenchimento automático em sistemas e browsers;
- Não guarde sua senha em agenda, gaveta ou próxima ao monitor;
- Mude suas senhas regularmente ou ao suspeitar de quebra de sigilo;
- Não utilize as mesmas senhas para acesso aos sistemas da instituição e sistemas pessoais;
- Ao criar uma senha, evite usar palavras curtas, data de nascimento, telefone ou sequências (exemplo: “123456”, “qwerty”, “asdfghjkl” etc.). Para montar uma senha forte, use letras maiúsculas e minúsculas, números e símbolos;
- Ninguém está autorizado a solicitar sua senha em nome da instituição;

- Desconfie e não clique em links desconhecidos recebidos pelo WhatsApp, telegrama, SMS e outros;
- Verifique as configurações de privacidade das suas redes sociais e seja sempre cauteloso com o que você posta publicamente; e
- Evite compartilhar suas informações pessoais, como número de telefone ou data de aniversário. Estas informações são peças-chave para verificação de identidade e conta, e podem ser utilizadas por pessoas mal-intencionadas.

INFORMAÇÕES PESSOAIS EM REDES SOCIAIS

O número de pessoas que utilizam redes sociais é altíssimo e, com isso, há constante aumento de vazamentos de informações pessoais de usuários. Por exemplo, mais de 540 milhões de usuários do Facebook já tiveram seus dados expostos em servidores na nuvem, sem qualquer tipo de senha de acesso. É importante citar, ainda, que os dados pessoais são importantes ativos de marketing, pois as empresas podem saber detalhes dos gostos e preferências. O principal valor desses dados é, certamente, conseguir prestar serviços cada vez mais personalizados, conforme os anseios, desejos individuais. Por isso, é preciso cuidado ao compartilhar dados pessoais em redes sociais.

Seguem algumas dicas para utilizar as redes sociais e manter cautela com seus dados pessoais:

- Seja cuidadoso com o que você posta e compartilha nas redes sociais. É ótimo quando somos lembrados, mas também pode ser muito perigoso;
- Leia e conheça a política de privacidade de sites de mídias sociais, pois é assim que você ficar sabendo como seus dados serão utilizados;
- Evite compartilhar sua vida e rotina, pois pessoas mal-intencionadas podem utilizar suas informações pessoais para prática de crimes diversos;
- Altere e limite o compartilhamento de dados nas suas redes sociais por meio das configurações de privacidade;
- Bloqueie propagandas baseadas nas suas informações pessoais, alterando as configurações de uso de dados por anunciantes na plataforma;

- Evite fazer check-in nas redes sociais, indicando o local que você está no momento. Quando você faz isso, a sua localização é compartilhada também com pessoas mal-intencionadas;
- Desative a sincronização dos aplicativos de redes sociais com os contatos do seu celular. Essa permissão é opcional e deve ser negada;
- Apague seu histórico periodicamente. Redes sociais armazenam suas ações como acessos, curtidas, pesquisas, comentários, páginas acessadas etc. Em caso de vazamento de contas, pessoas desconhecidas podem ter acesso a todo seu histórico. Além disso, também é indicado apagar o cache e cookies regularmente, limitando o acesso às suas ações em navegadores da Internet, utilizadas por empresas para venda de anúncios direcionados;
- Não permita o reconhecimento facial. Apesar de interessante, é arriscado. Afinal, seu rosto fica armazenado no banco de dados e pode ser encontrado em imagens diversas da Internet, sendo veiculado fora da rede social.

UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS

Assim como seu computador, o seu dispositivo móvel também pode ser usado para a prática de atividades maliciosas, como furto de dados, envio de spam e propagação de códigos maliciosos.

Confira dicas de segurança para utilização de dispositivos moveis:

- Instale um software antimalware antes de instalar qualquer aplicativo, principalmente aqueles desenvolvidos por terceiros;
- Mantenha o sistema operacional e os aplicativos sempre atualizados;
- Fique atento às notícias do fabricante, principalmente sobre segurança;
- Seja cuidadoso ao instalar aplicações desenvolvidas por terceiros, como complementos, extensões e plug-ins. Procure por fontes confiáveis e bem avaliados pelos usuários, e verifique se as permissões necessárias para a execução são coerentes com a destinação da aplicação;
- Tenha cautela ao usar aplicativos baseados em geolocalização, pois isto pode comprometer a sua privacidade;
- Evite utilizar reder wi-fi públicas;

- Mantenha interfaces de comunicação como bluetooth e wi-fi desabilitadas, e somente as habilite quando for necessário;
- Configure a conexão bluetooth para que seu dispositivo não seja encontrado por outros dispositivos;
- Sempre que possível, mantenha as informações de dados pessoais sensíveis em formato criptografado;
- Fique de olho no seu dispositivo móvel, principalmente em locais de risco. Procure não o deixar sobre a mesa e tenha cuidado em ambientes públicos;
- Use conexão segura sempre que a comunicação envolver dados confidenciais;
- Cadastre uma senha de acesso que seja forte e bem elaborada, combinando números, símbolos e letras maiúsculas e minúsculas;
- Configure-o, se possível, para que os dados sejam apagados após algumas tentativas de desbloqueio sem sucesso. Use esta opção com cautela, principalmente se você tem filhos e eles “brincam” com o seu dispositivo;
- Ao se desfazer do seu dispositivo móvel, apague todas as informações nele contidas e restaure a opção de fábrica.

EVITANDO ATAQUES DE ENGENHARIA SOCIAL

Engenharia social é a habilidade de um cibercriminoso conseguir acesso à informação confidenciais de uma empresa por meio da persuasão. Execute suas atividades com muita atenção, para que pessoas mal-intencionadas não induzem você a passar informações sensíveis ou executar alguma tarefa da qual possa ser tirado proveito.

Para evitar golpes de Engenharia Social, siga essas importantes recomendações de segurança:

- Caso receba uma ligação de alguém se identificando como colaborador da instituição, solicitando informações sensíveis ou pedindo alguma senha padrão, por exemplo, fique atento! Pode ser uma pessoa mal-intencionada se passando por um colaborador;
- Evite fazer cadastros na Internet, especialmente fornecendo seus dados pessoais;

- Nunca forneça informações sensíveis, pessoais ou da empresa, por telefone ou outros meios, quando a iniciativa do contato não for sua;
- Use as ferramentas oficiais da instituição, como a Central de Suporte e Serviços (Top Desk), Microsoft Teams e Outlook para conversar com outros colaboradores. Por meio delas podemos identificar e validar o solicitante;
- Seja cuidadoso com o que você posta na Internet, principalmente nas redes sociais. Essas informações podem ser usadas por malfeitores para confirmar os seus dados cadastrais e responder perguntas de segurança; e
- Evite expor assuntos relacionados ao seu trabalho em público ou em redes sociais. Use o bom senso sempre!

DICAS PARA EVITAR PHISHING

Phishing é um processo fraudulento utilizado para adquirir informações de usuários, ou até mesmo infectá-los. É a forma mais comum de ataque cibernético e tem uma taxa de sucesso relativamente alta. Seguem dicas para não cair em Phishing:

- Pense bem antes de clicar em links, sejam eles de sites ou e-mails, e nunca clique naqueles que pareçam suspeitos;
- Antes de clicar em algum link, posicione o ponteiro do mouse em cima desse link para que seja exibido o verdadeiro endereço web, depois verifique se este direciona a um site confiável e com boa reputação;
- Nunca abra arquivos anexos suspeitos recebidos por e-mail;
- Se você desconfiar de um e-mail recebido, mesmo que seja de alguém conhecido, cuidado: pode ser um e-mail falso;
- Tenha um cuidado especial com mensagens que solicitam “ação imediata” ou que ameacem você a perder algo caso não responda à mensagem, como, por exemplo, atualizar o aplicativo bancário para não ter a conta bloqueada;
- Evite fornecer informações pessoais por telefone, principalmente em ligações não solicitadas;
- Se algum e-mail parecer ser Phishing, provavelmente é. Não teste sua sorte!