UNIVERSIDADE DO SUL DE SANTA CATARINA

PAULO ROBERTO ZANCHIN DE PAULA

A IMPORTÂNICA DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO PARA A CONTINUIDADE DOS NEGÓCIOS.

Palhoça

2020

PAULO ROBERTO ZANCHIN DE PAULA

A IMPORTÂNICA DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO PARA A CONTINUIDADE DOS NEGÓCIOS.

Relatório apresentado ao Curso **Tecnólogo em Gestão da Tecnologia da Informação,** da Universidade do Sul de Santa Catarina, como requisito parcial à aprovação na unidade de aprendizagem de Estudo de Caso.

Orientador: Prof. Roberto Fabiano Fernandes

Palhoça

2020

PAULO ROBERTO ZANCHIN DE PAULA

A IMPORTÂNICA DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO PARA A CONTINUIDADE DOS NEGÓCIOS:

Este trabalho de pesquisa na modalidade de Estudo de Caso foi julgado adequado à obtenção do grau de Tecnólogo em Gestão da Tecnologia da Informação e aprovado, em sua forma final, pelo Curso Superior de Tecnologia em Gestão da Tecnologia da Informação, da Universidade do Sul de Santa Catarina.

Palhoça, 31 de maio de 2020.

Prof. e orientador Roberto Fabiano Fernandes
Universidade do Sul de Santa Catarina

AGRADECIMENTOS

A minha amada e querida esposa Gisele que sempre me incentivou e acreditou em mim, aos meus filhos Bernardo e Antonia, sempre muito pacientes, sorridentes, me enchendo de força e a Deus, Àquele que me da força e proteção.

RESUMO

Este estudo de caso tem por objetivo discorrer sobre a importância nas organizações da criação, adoção e manutenção de políticas de segurança da informação.
A justificativa para este estudo é a importância, cada vez mais latente, da proteção do ativo mais valoroso de uma organização, a informação.

Para alcançar este propósito, este estudo de caso recorre ao método descritivo e através de uma abordagem qualitativa em uma organização multinacional, que a mais de 20 anos atua no Brasil no ramo do agronegócio, com diversas filiais pelo país e contando com 1.500 colaboradores, pretende demonstrar de forma clara e objetiva a importância para uma organização na adesão de políticas que objetivam garantir a privacidade, a integridade e a disponibilidade dos dados.

Palavras-chave: Tecnologia. Políticas de segurança da Informação. Privacidade de dados.

SUMÁRIO

1 INTRODUÇÃO

Com o surgimento de novas tecnologias, sejam elas aplicativos, redes sociais, dispositivos de hardwares, em uma velocidade incrível, o trabalho de proteger e garantir a integridade dos dados em uma organização, seja ela do tamanho que for, é cada vez mais um grande e dispendioso trabalho para as equipes de Tecnologia da Informação.

Profissionais de segurança de dados precisam ser, além de técnicos, gestores de processos para garantir que a informação sempre estará disponível de forma rápida e íntegra. Para isso a implementação, a manutenção e aprimoramento de políticas de segurança da informação é vital e indispensável.

Como lidar com colaboradores que entram e saem da organização? Como tratar e mitigar vulnerabilidades em softwares utilizados na empresa? Como monitorar e gerenciar centenas ou até mesmo milhares de dispositivos conectados à rede corporativa da organização? As respostas para estas e outras muitas perguntas devem estar inseridas dentro das políticas para a segurança de dados dentro de uma organização. E para que essas políticas tenham a eficácia desejada e esperada por todos é preciso que processos sejam bem planejados e executados, e que uma boa comunicação aconteça entre os colaboradores, fazendo que todos tenham ciência da importância de cuidar de toda e qualquer informação dentro da organização.

2 TEMA

A importância dada a informação pelas organizações aumenta significativamente a cada ano, em especial na última década. Com o fluxo cada vez maior e mais detalhado de informações, bem como com a valorização dos dados obtidos, tratados e armazenados, a criação de políticas de segurança da informação vem ganhando força e importância no contexto de uma organização, independente do seu tamanho, da abrangência ou ramo de atividade em que atua no mercado nacional. “A informação é um recurso essencial para toda a organização, independentemente de seu porte e do seu segmento de atuação no mercado.” (Fontes, 2006, p 1).

A segurança da informação deve estar ligada diretamente aos objetivos do negócio. A proteção destes dados contra a divulgação indevida, seja ela intencional ou não intencional, contra a modificação não autorizada, a destruição não desejada, ou a negação de serviço deve ser definida através de políticas e procedimentos. Cada vez mais as organizações dependem da informação, e esta, precisa ser integra, inviolável e sempre estar disponível.

“A segurança da informação pode ser considerada um ativo crítico e fundamental; zelar por ela, portanto, é de fundamental importância para as organizações” (Kolbe Júnior, 2017, p.123).

Nesse contexto, este trabalho tem como tema a importância de políticas de segurança da informação para a continuidade dos negócios.

Imaginamos uma organização onde cada setor, ou até mesmo cada indivíduo, guarda a sua informação de maneira que melhor lhe convém! O risco desta informação ser perdida, alterada, copiada é muito grande, ou quase certo! Como a organização pode garantir a integridade, a disponibilidade, a confidencialidade dessa informação sem políticas que garantam a segurança dessas informações?

“Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes” ABNT NBR ISO/IEC 27002:2013 (2013, p 8).

Através deste trabalho, pretende-se sugerir: Como identificar melhores políticas de segurança da informação para a organização?

“A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada” (Sêmola, 2001, p.18)

Cada organização tem suas particularidades, seus processos e características, o “como fazer” bem distintos das demais organizações. Essas particularidades decorrem das pessoas que ali trabalham. E essas diferenças fazem com que os profissionais de segurança da informação atentem para os detalhes.

“Ao estabelecer uma política para a segurança da informação, a administração provê as diretivas e o apoio para a organização. Essa política deve ser escrita em conformidade com os requisitos do negócio, bem como com as leis e os regulamentos relevantes.” (Hintzbergen; Smulders; Baars, 2018, p. 67)

Este estudo tem como justificativa demostrar a real importância na adoção e manutenção de políticas de segurança da informação. No contexto de uma organização, é preciso conscientizar a todos da responsabilidade da preservação dos dados, a criticidade e a importância que estes têm para a continuidade dos negócios em uma organização.

3 OBJETIVOS

3.1 OBJETIVO GERAL

Identificar aspectos da política de segurança da informação a serem aplicados em organizações do agronegócio.

1.1 OBJETIVOS ESPECÍFICOS

Analisar o contexto atual da organização em relação a proteção de dados.

Examinar o contexto atual da organização em relação a políticas de segurança da informação.

Investigar quais as melhores práticas para a implementação de políticas de segurança da informação na organização.

Caracterizar elementos de segurança da informação apropriados para o contexto da organização.

4 PROCEDIMENTOS METODOLÓGICOS

4.1 CAMPO DE ESTUDO

Este trabalho é uma pesquisa na forma de estudo de caso descritivo com uma abordagem qualitativa.

O âmbito desta pesquisa contempla um estudo de caso sobre Políticas de Segurança da Informação, exemplificando com bases teóricas o que uma organização necessita fazer para garantir a integridade e a inviolabilidade da sua informação.

O campo de pesquisa é uma organização privada multinacional, com sua sede no Brasil na cidade de Porto Alegre, RS. É atuante em todo o território nacional no setor do agronegócio, possui mais de 1.500 funcionários no país com seis filiais distribuídas pelo Brasil.

4.2 INSTRUMENTOS DE COLETA DE DADOS

Como instrumento de coleta de dados, foi utilizado um questionário, tendo como público alvo os gestores da organização. As áreas foram escolhidas levando em conta a sua estratégia e importância dentro da organização.

Quadro 1 – Instrumento de coleta de dados

Instrumento de coleta de dados	**Universo pesquisado**	**Finalidade do Instrumento**
Questionário	Entrevista realizada com gerentes e diretores das seguintes áreas: Tecnologia da Informação – Sistemas; Tecnologia da Informação – Infraestrutura; Auditoria e *Compliance*; Crédito e Cobrança; Desenvolvimento e Pesquisa; Projetos Industriais, Marketing; Contabilidade; Fiscal, Gerencia Comercial, Diretoria Administrativa e Recursos Humanos.	Averiguar o nível de conhecimento dos entrevistados com relação à segurança da informação. Identificar pontos e processos para adequar as políticas de segurança da informação, com a realidade de organização. Analisar o nível de conhecimento dos gestores sobre as políticas de segurança da informação da empresa.

Fonte: CAVALCANTI e MOREIRA (2008).

5 APRESENTAÇÃO E ANÁLISE DA REALIDADE OBSERVADA

5.1 ESTRUTURA DA ORGANIZAÇÃO

A empresa XYZ, chegou ao Brasil em outubro de 1997, trazendo consigo ares conservadores, típicos de empresas familiares, européias atuantes no agronegócio. Ao longo dos mais de 20 anos de atuação no Brasil, a XYZ cresceu de forma sólida e rápida principalmente nos últimos 10 anos. Esse crescimento se deu não só no número de colaboradores, mas também no número de filiais e no aumento da fatia do mercado de fertilizantes no país. A empresa tem sua sede nacional em Porto Alegre, possui ainda escritórios comerciais em diversos estados da federação e três unidades fabris em três estados diferentes, contando com mais de 1.500 colaboradores, destes aproximadamente 50% exercendo suas atividades de forma externa.

O parque tecnológico é composto por uma estrutura mista entre ambiente virtualizado e ambiente físico, com um data center primário e um site backup, oitocentos e cinquenta estações de trabalho, setenta e cinco impressoras em rede, noventa switches, onze firewalls e cento e vinte e seis servidores com vinte e oito sistemas e dezesseis banco de dados. Para dar suporte e apoio a esta estrutura a empresa tem em seu quadro dezenove colaboradores na área de Tecnologia da Informação, dividida em Sistemas e Infraestrutura.

5.2 DESCRIÇÃO E ANÁLISE DA REALIDADE OBSERVADA

Com a finalidade de expor de maneira clara e de fácil compreensão para todos os leitores, descrevo aqui uma análise da realidade observada na empresa XYZ sobre o espectro da implantação, manutenção e atualização de Políticas de Segurança da Informação. Para tal entendimento e posterior descrição neste trabalho, foi aplicado um questionário em gestores de doze áreas da empresa, a saber: Tecnologia da Informação Sistemas, Tecnologia da Informação Infraestrutura, Crédito e Cobrança, Controle de Gestão, Auditoria, Pesquisa e Desenvolvimento, Marketing, Contabilidade, Fiscal, Gerencia Comercial, Projetos Industriais, Diretoria Administrativa Financeira.

O tempo médio de casa dos colaboradores que responderam ao questionário é de sete anos e quatro meses, e o tempo médio de experiência na função exercida é de dez anos e seis meses.

As perguntas deste questionário foram construídas com base nas obras dos autores Willian Caprino, Jule Hintzbergen, André Smulders, Hans Baars, Edison Fontes, Kolbe Jú-

nior e na norma da ABNT NBR ISO/IEC 27002:2013 que estão devidamente identificadas na revisão de literatura.

Com base nas respostas obtidas é possível analisar o grau de percepção sobre a importância da proteção da informação dentro da organização por parte dos gestores, onde 80% deles afirmam que a preocupação com segurança de dados é percebida por todos, alguns citando inclusive um dos valores da empresa, a Segurança. Os 20% restantes afirmam que sentem a preocupação com a segurança dos dados, mas vêem claramente espaço para mudanças neste assunto.

Com uma média de experiência na função superior a 10 anos, o que nos indica um bom conhecimento dos processos da empresa, os gestores chamam a atenção e reconhecem o esforço da organização em proteger um ativo muito valioso como a informação, reconhecendo este ativo com um dos pilares para o fortalecimento e crescimento da empresa. É percebido por mais de 70% dos gestores uma evolução nos processos e políticas que visam a segurança das informações.

A visão dos gestores sobre a segurança da informação dentro da organização é positiva, "*noto que a empresa vem investindo cada vez mais no tema", "Vejo esforços e tenho a sensação de segurança",* " *é uma das prioridades*", foram respostas recorrentes, o que demostra uma forte percepção por partes dos gestores. Ainda nesse tema alguns gestores lembraram que *"falta priorização. As pessoas têm liberdade de compartilhar dados por diferentes plataformas, utilizando equipamentos da empresa"* e que *"muitos dados transacionais e gerenciais circulam via e-mail ou outras plataformas fora do ambiente seguro e controlado da empresa, gerando potencial risco de uso indevido da informação"*.

Quando questionados sobre a orientação dada pela empresa a cada colaborador sobre o assunto segurança da informação, todos lembram dos informativos quinzenais enviados a todos por e-mail, fixados em murais e divulgados em outras ferramentas de comunicação interna da empresa. O código de ética da empresa foi citado em 75% das respostas, nele consta um capítulo inteiro sobre a segurança da informação, com referências não só aos colaboradores, mas também aos terceiros e fornecedores. A integração dada aos novos colaboradores conta com um pequeno, mas valioso, parágrafo sobre a responsabilidade de cada um com os recursos tecnológicos disponibilizados pela organização.

Ter uma definição clara do que proteger e dar as orientações necessárias de forma simples e periódica, reforçando a importância e o engajamento de cada colaborador para a proteção dos dados é uma prática importante e que vem trazendo bons resultados para a organização. A definição de perfis de acesso à rede, de acesso à internet e a outros recursos tecnológicos é outro processo implementado com sucesso e bem aceito por todos. A adoção da política de perfis de acesso é vista como necessária por todos, apesar de alguns citarem que: "*as*

vezes atrapalha um pouco nos processos do dia a dia, mas são necessários para a segurança".

A metade dos gestores afirmam que a "*preocupação maior da empresa deve ser com a informação que circula, ou tem origem nos colaboradores que trabalham de forma externa"*. Eles também vêem como o ponto mais fraco no elo da segurança da informação estes colaboradores.

Sobre a responsabilidade dos gestores quanto a segurança da informação, todos foram unânimes em reconhecer a importâncias das políticas e processos voltados a proteção dos dados, porém apenas 20% deles reconheceram que precisam do auxílio dos seus subordinados, e 90% citaram que são *"os responsáveis pelo reforço na divulgação das informações."*

O grande fluxo de informações para muitos colaboradores é uma preocupação de 30% dos gestores, sendo que 20% deles citaram que não existe uma política para disciplinar este volume de informações , que segundo eles, é desnecessário.

Como fator direcionador para investimentos, a continuidade dos negócios é a mais citadas dentre os gestores, pois afirmam que *"a continuidade dos negócios deve ser sempre o principal driver de todas as ações na empresa"* também citam que *"tendo em vista o grau de impacto negativo que danos na informação podem causar para a continuidade dos negócios da empresa".*

Temos 80% dos gestores afirmando que investimentos em proteção dos dados é fator determinante para a continuidade dos negócios, superando aspectos como imagem da empresa, conformidades regulatórias e saúde financeira.

Para 90% dos gestores, a evolução na segurança da informação é notória com o passar do tempo, e deste total, 50% afirmam que ainda a muito para melhorar, principalmente para os colaboradores externos. Outros 25% citaram que "*a evolução em controles de acesso é notória, mas ainda é pouco se comparados com outras empresas do mesmo porte."*

6 PROPOSTA DE SOLUÇÃO DA SITUAÇÃO-PROBLEMA

A seguir apresento proposta de solução da situação, baseado na realidade observada junto aos gestores da organização.

6.1 PROPOSTA DE MELHORIA PARA A REALIDADE ESTUDADA

A partir das respostas dadas pelos gestores da organização, onde sua ampla maioria não tem domínio técnico sobre Tecnologia da Informação e menos ainda sobre Segurança da Informação, fica claro que a organização precisa fomentar a compreensão da dimensão das dificuldades e dos enormes desafios envolvidos para proteger um grande fluxo de informação que envolve um grande número de usuários. A organização possui gestores com boa experiencia em sua área de atuação, orientados de forma superficial pela organização sobre o assunto Segurança da Informação. Tal orientação é transmitida periodicamente, mas sem um levantamento do real entendimento por parte dos colaboradores da mensagem transmitida.

A revisão de processos administrativos referentes ao fluxo de informações gerenciais deve ser revista, uma vez que é motivo de preocupação por parte dos gestores. Tal revisão deve levar em conta a real necessidade do grande número de pessoas envolvidas no recebimento de informações tão sensíveis e importantes. Além disso é necessário a determinação de padronização de softwares para a transmissão das informações gerenciais. É preciso estabelecer regras bem definidas para uso de softwares de compartilhamento e envio de dados, levando em conta que a organização precisa saber: qual, quando, de quem e para quem a informação foi transmitida ou compartilhada.

A revisão de processos e das políticas com relação ao fluxo de informações entre colaboradores da empresa e terceiros precisa ser constantemente medida e atualizada, levando em consideração aspectos legais.

A utilização de dispositivos de armazenamento externo como *HD's* externos e *PenDrivers* ainda não foi definida por nenhuma política, deixando uma falha de segurança preocupante e mencionada pelos gestores.

6.2 RESULTADOS ESPERADOS

Espera-se atingir uma melhora significativa com a segurança e com integridade dos dados gerados, gerenciados e guardados pela organização. A evolução e melhoria nos processos também é aguardada, uma vez que todas as áreas, em conjunto com o setor de tecnologia da informação, terão a oportunidade de refinarem seus processos, diminuindo o tempo

de execução dos mesmos, eliminando o fluxo de informações à colaboradores que não necessitam de tais informações, trazendo assim mais segurança e confiabilidade para o processo. A adoção de softwares líderes de mercado para gerenciar o compartilhamento de informações dará maior credibilidade junto a fornecedores e parceiros, segurança para a organização e estará em conformidade com aspectos legais.

6.3 VIABILIDADE DA PROPOSTA

A revisão de políticas e dos processos não despenderá recursos financeiros, pois é plenamente possível de ser realizada pelos colaboradores e gestores da organização. Essa revisão depende exclusivamente da conscientização por parte da direção da real necessidade de atualização e manutenção das políticas de segurança.

Medir, junto aos colaboradores, de que maneira as ferramentas de comunicação interna da empresa auxiliam na conscientização da real importância e do necessário engajamento sobre segurança da informação, é outro fator importantíssimo e totalmente viável financeiramente.

A criação de grupos de trabalho homogêneos para discutir as alterações e atualizações dos processos visando uma maior segurança é a chave para a revitalização de algumas políticas de segurança, sempre tendo em mente e muito bem definidos os envolvidos, os responsáveis, bem como a determinação de período para a elaboração desses projetos.

Uma vez que a direção entenda perfeitamente os riscos atuais, e os ganhos em segurança da informação com a adoção de softwares *DLP's - Data Loss Prevention* - do inglês Prevenção de Perda de Dados, o custo com esse software será muito bem aceito.

7 CONSIDERAÇÕES FINAIS

Mudanças em comportamentos sempre são difíceis, onerosas e demandam um certo tempo para aceitação e colaboração de todos. Com mudanças em processos que envolvem segurança de dados não seria diferente. Sem dúvida o grande desavio para as organizações está na mudança de hábitos.

Ao realizar um levantamento junto aos principais setores da organização, contando com a participação de gestores experientes, foi possível identificar aspectos que contribuem com o horizonte planejado pelo setor de Tecnologia da Informação. O entendimento da necessidade, cada vez maior, da criação de processos que envolvam a proteção, a integridade e o gerenciamento da informação circulante na empresa é notado e sentido por todos.

Com o estudo realizado junto aos gestores, foi possível identificar aspectos bem marcantes com relação a políticas de segurança da informação, dentre os quais podemos citar: políticas de senhas, políticas de acesso à rede interna entre outras.

Com uma comunicação periódica aos colaboradores sobre o que está acontecendo em relação à segurança da informação, apresentado dicas e cuidados que devem ser adotados por todos, o grau de conscientização e participação dos colaboradores com a segurança da informação aumenta com o passar do tempo. Este resultado é fruto da colaboração da direção com a área de Tecnologia da Informação.

O processo de proteger um bem tão valioso para a organização, nos tempos atuais é grandioso, difícil e requer muito trabalho e esforços diários por parte da equipe técnica e de gestão da tecnologia da informação. Quando a organização tem clareza da necessidade de fomentar políticas para a proteção dos dados, todo o processo de proteção ganha um incentivo e torna-se mais viável de ser administrado no dia a dia.

Muito importante é poder concluir que a organização tem ciência das dificuldades de proteger dados, ainda mais com a alta velocidade de transformação das tecnologias, e está empenhada em investir e incentivar sempre para a melhoria das políticas de segurança da informação.

REFERÊNCIAS

ABNT NBR ISO/IEC 27002:2013, 8 p.

CABRAL, Carlos e CAPRINO, Willian. **Trilhas em segurança da informação**. Rio de Janeiro: Brasport, 2015.

FONTES, Edison. **Políticas e normas para a segurança da informação**. Rio de Janeiro: Brasport, 2006. 1 p.

HINTZBERGEN, Jule; SMULDERS, André; BAARS, Hans. **Fundamentos de segurança da informação - Com base na ISO 27001 e na ISO 27002**. Rio de Janeiro: Brasport, 2018. 67 p.

KOLBE JUNIOR, Armando. **Sistemas de Segurança da informação na era conhecimento**. Curitiba: InterSaberes, 2017. 123 p.

NETTO, Abner da Silva; DA SILVEIRA, Antonio Pinheiro. **Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas**. Univ. Municipal de São Caetano do Sul – IMES. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752007000300007 >. Acesso em: 18 de mai. 2020.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva**. Rio de Janeiro: Campus, 2001. 18 p.

WEIDMAN, Georia. **Testes de Invasão. Uma Introdução prática ao hacking**. São Paulo: Novatec, 2015.

APÊNDICE

Este questionário faz parte do estudo de caso para o curso de Gestão em Tecnologia da Informação. - UNISUL.

Definições:
Dados = Toda informação, física ou digital, independente da forma como é armazenada, tratada e divulgada.

As perguntas deste questionário foram construídas com base nas obras dos autores Willian Caprino, Jule Hintzbergen, André Smulders, Hans Baars, Edison Fontes, Kolbe Júnior e na norma da ABNT NBR ISO/IEC 27002:2013 que estão devidamente identificadas na revisão de literatura.

Perguntas:

1 – Há quanto tempo você trabalha na empresa?

2 – Qual o seu tempo de experiência na atividade/função que você exerce hoje na empresa?

3 – Como você vê a segurança da informação dentro da organização?

4 – A empresa orienta você periodicamente sobre ações para a proteção de dados?

5 – Você conhece o posicionamento da empresa em relação aos funcionários e prestadores de serviço no que diz respeito à proteção de dados?

6 – Você tem conhecimento das Políticas de Segurança da Informação da organização?

7 – Dos fatores direcionadores para o investimento em segurança da informação, na sua opinião, qual o mais relevante? Justifique:

7.1 – Conformidade com políticas internas;

7.2 – Condições econômicas;

7.3 – Continuidade dos negócios / recuperação de desastres;

7.4 – Imagem da empresa;

7.5 – Conformidade regulatória.

8 – Qual a sua responsabilidade em relação aos dados da empresa?

9 – Relacione a sua percepção, quanto à segurança da informação, levando em consideração o início do seu trabalho na empresa até o momento atual.