Revista Científica UNAR (ISSN 1982-4920), Araras (SP), v.23, n.1, p.01-12, 2023.
DOI: 10.18762/1982-4920.20230001

A IMPORTÂNCIA DE BOAS PRÁTICAS E A GESTÃO DE SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES.

Daiane Isabele de Lima Basilio, André Castro Rizo

RESUMO

O seguinte artigo tem como objetivo realizar um estudo de caso com base em um acompanhamento anual de uma organização de grande porte que possui diversas unidades de trabalho pelo Brasil e uma matriz que mantém o datacenter com os servidores principais de todas as unidades e a relação que ela estabelece com a gestão da segurança da informação e homogeneidade nos processos relacionados a acesso, manipulação de dados e treinamento. Então com base nesses apontamentos serão identificadas as falhas de segurança da informação encontradas no relacionamento de prestador de serviços e cliente, e propor soluções voltadas à gestão da segurança da informação para os problemas evidenciados durante o estudo de caso.

Palavras-chave: Gestão de Segurança da informação; Processos; Homogeneidade;

Abstract

The objective of the following article is to conduct a case study based on an annual monitoring of a large organization that operates multiple work units across Brazil, with a central headquarters maintaining the data center housing the primary servers for all units. This study examines the relationship between the organization and its information security management, as well as the standardization of processes related to access control, data handling, and training. Based on the findings, the study will identify information security vulnerabilities present in the service provider-client relationship and propose solutions aimed at enhancing information security management to address the issues uncovered during the case study.

Keywords: Information Security Management; Processes; Standardization;

1. INTRODUÇÃO

Grandes, médias ou até mesmo pequenas organizações dificilmente trabalham sozinhas, geralmente é prestado um serviço, contratado um serviço ou a organização possui várias unidades de trabalho que podem estar espalhadas em diferentes regiões do país. Portanto quando a gestão da segurança da informação

não depende apenas de um local ou uma equipe, a organização fica mais exposta e propensa a ter processos diferentes e recursos alocados de formas distintas em cada unidade de trabalho, o que pode ocasionar falhas na segurança da informação e consequentemente prejuízos financeiros e morais para a empresa, além de existir a possibilidade de questões processuais relacionadas a Lei Geral de Proteção de Dados atualmente vigente no Brasil.

Entende-se como segurança da informação processos, normas e ações que tem como objetivo manter os dados/informações íntegros, autênticos, confidenciais e disponíveis.

> Segurança da Informação é a proteção da informação contra vários tipos de ameaças, com a finalidade de garantir a continuidade do negócio, minimizando seus riscos e maximizando o retorno sobre os investimentos. A Segurança da Informação é obtida através da adoção de um conjunto de controles adequados, que devem ser estabelecidos, implantados, monitorados, analisados e melhorados constantemente, a fim de garantir que os objetivos estratégicos do negócio e da segurança da informação sejam atendidos (ABN NBR ISO/IEC 27002, p.10, 2005).

Esse estudo tem como objetivo avaliar falhas na implementação de plano de segurança da informação em uma determinada organização nacional que possui cerca de 56 filiais por todo o país, clientes e prestadores de serviço que contenham acesso direto a manipulação de dados. As falhas apresentadas nesse trabalho não serão diretamente ligadas a pessoas ou infraestrutura das organizações, mas sim sobre a necessidade de ter processos homogêneos e o alcance total de todos os envolvidos na implementação do plano de segurança da informação, baseando-se no acompanhamento do dia a dia de uma organização que cumpre todos os recursos citados no início desse parágrafo.

Quando se fala em processos homogêneos tem-se como objetivo exemplificar que determinada empresa possui um datacenter e mantém um processo estruturado de segurança da informação com restrição de acessos, tempo mínimo para redefinição de senha, plano de contingência com hierarquia de responsáveis bem definidas sendo seguidas pelos seus colaboradores, que se seguidos corretamente podem mitigar riscos e reduzir vulnerabilidades. Porém se essa empresa possui um prestador de serviços com acesso aos servidores desse datacenter, mesmo que esse

acesso seja remoto, e o prestador de serviços de desenvolvimento de software não segue o mesmo plano ou não possui as mesmas restrições estabelecidas no plano de segurança, a eficácia desse plano adotado pela empresa, se realizada uma análise de risco é possível seja reduzida pela metade, ou seja, para que um processo realmente reduza riscos ele deve ser adotado por todas as partes envolvidas sem exceções quando se trata do mesmo projeto/produto.

5 REFERENCIAL TEÓRICO

A seguir serão demonstrados alguns conceitos relevantes para um melhor entendimento do trabalho

2.1 ABNT NBR ISSO/IEC 27002

Para gerir processos e atender uma gestão baseada em pontos concisos será utilizada como referência a norma ABNT NBR ISO/IEC 27002, ela aparecerá em diversas partes do trabalho principalmente para referenciar modos de trabalho e gestão da segurança da informação com partes externas, terceirizados e riscos gerados a partir desses relacionamentos na organização.

> Convém que a segurança dos recursos de processamento da informação e da informação da organização não seja reduzida pela introdução de produtos ou de serviços oriundos de partes externas. Convém que qualquer acesso de recurso de processamento da informação da organização e ao processamento e comunicação da organização por partes externas seja controlado. Convém que seja feita uma análise/avaliação dos riscos envolvidos para determinar as possíveis implicações na segurança e os controles necessários, onde existir uma necessidade de negócio para trabalhar com partes externas, que possa requerer acesso aos recursos de processamento da informação e a informação da organização, ou na obtenção e fornecimento de um produto e serviço de uma parte externa ou para ela. Convém que os controles sejam acordados e definidos por meio de um acordo com a parte externa. (ISO/IEC 27002, p. 15, 2005)

2.2 Gestão da Política da Informação

Portanto em continuidade com a norma citada acima, outros autores como Nassif e Rezende (p.113, 2017) informam que: “Bons gestores sabem que, em todos os momentos, precisam estar cientes de que uma boa política de gestão da informação

deve englobar vários aspectos clássicos, mas, dentre eles, deve-se levar em conta a segurança da informação.” Com isso conclui-se que não é viável tratar a gestão e a segurança da informação de forma separada, sendo as duas formas complementos de trabalho e essenciais para o bom funcionamento da organização, padronização de processos e a homogeneidade da Segurança da Informação.

2.3 Boas Práticas de Segurança da Informação

Então partindo da premissa que a segurança da informação deve existir e estar acoplada com a gestão da informação cabe definir quais as melhores práticas para que isso seja feito e quais áreas serão afetadas com essas mudanças. De acordo com Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.BR a política de segurança deve ser compartilhada e trabalhada para todos os envolvidos em três tópicos, conscientização, treinamento, aconselhamento técnico e de políticas, com o intuito de “compartilhar o conhecimento e incentivar a adoção de boas práticas”.

Para considerar as boas práticas e padronização de processos como algo cultural e natural entre os colaboradores é necessário que parte disso contenha uma boa gestão de pessoas, segundo Ventura e Nassif (p. 224, 2016) “uma má concepção de trabalho ou uma gestão inadequada impede o alinhamento dos indivíduos com o objetivo, com a estratégica da organização e, principalmente, o acesso a todo conhecimento que as mesmas possuem”. Sob essa perspectiva é indispensável pensar que a seleção de pessoas, criar um ambiente de pertencimento e que as políticas de segurança da informação estejam visíveis e ao alcance de todos é o passo inicial para garantir o cumprimento de processos e a homogeneidade deles.

2.4 Lei Geral de Proteção de Dados

A Lei Geral de proteção de dados atualmente válida em meio nacional, não apenas adverte sobre o tratamento irregular de dados, as responsabilidades atribuídas as organizações, operador e controlador de dados como sugere na seção II Art. 50 a aplicação de boas práticas.

> Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as

> normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (BRASIL, 2018, Art. 50)

5 METODOLOGIA

Com o intuito de obter um conhecimento mais profundo e sólido sobre o tema de gestão de segurança da informação e homogeneidade processual proposta nesse trabalho foi realizada uma pesquisa bibliográfica exploratória baseada em artigos científicos na internet, livros técnicos, sites, sempre em busca dos pontos mais relevantes para o desenvolvimento do artigo**.**

O recurso utilizado para esse artigo será um estudo de caso baseado em uma organização nacional de grande porte com data center próprio, que possui mais de 56 unidades de trabalho espalhadas pelo país, com exportação internacional e relacionamento com diversos mercados ao redor do mundo, a mesma possui uma equipe especializada e com uma documentação de segurança da informação já estabelecida e vigente, mas que devido as várias ramificações organizacionais os processos mesmo que iguais têm sido trabalhados de forma independente assim como as restrições de acesso podem variar de acordo com o departamento, mesmo que esses departamentos trabalhem com os mesmo fornecedores e clientes.

Portanto com base em situações vivenciadas em rotinas de trabalho em um ano com uma relação fornecedor/cliente que requer acesso a servidores, bancos de dados, processos de alterações de banco de dados e acesso a dados confidenciais e até mesmo segredos industriais, serão apontados os momentos e processos em que a segurança da informação se mostra fragmentada e independente, visando propor soluções para a redução dos problemas apontados e retornando para a base inicial da proposta de estabelecer processos homogêneos e seguros.

Para compreensão geral e aplicação da possível solução dos problemas encontrados serão primeiramente apresentados os processos de segurança estabelecidos pela empresa que de alguma forma visão assegurar a segurança da informação e proteção de dados. Cada tópico abaixo representa um processo e as suas medidas preventivas para manter a segurança da informação nos acessos, tráfego de rede e manipulação de dados da organização.

- Para acesso a aplicação de controle e lançamento de dados diários utilizada pela organização é necessário que seja assinado um termo de responsabilidade de uso da rede interna da organização assim como responsabilidade ao tratamento dos dados que ficarão de fácil acesso para todos. A partir disso é liberado um usuário e senha de VPN (transmissão de dados seguros e anônimos em uma conexão de rede privada) com liberação de token e o mesmo usuário e senha para acesso de uma plataforma que permite o acesso remoto aos servidores.
- O acesso remoto aos servidores para os prestadores de serviços é liberado de acordo com uma solicitação formalizada via e-mail pela gerência de cada departamento que utiliza o software fornecido pelo prestador de serviços.
- Toda mudança (correção de bugs, atualização de versão do software, aumento de tabelas, implementação de logs) que possa afetar o ambiente de produção deve ser comunicada a equipe de servidores, agendada a data de execução, documentada com o fim de comprovar quais mudanças irão ocorrer a partir dessa alteração, passar por testes de qualidade e gerencia no ambiente de homologação e ser apresentada previamente para um comitê que envolve toda equipe de branco de dados e infraestrutura da organização para que possa ser disponibilizada em produção.
- O acesso ao servidor e banco de produção deve ser restrito apenas para a equipe de segurança da informação e equipe de servidores da organização, sendo que usuários externos estão expressamente proibidos de terem esse acesso.

Os pontos apresentados acima parecem ser eficientes e possibilitarem que a os dados manipulados estejam seguros, pois de acordo com eles a organização trabalhou nos pontos de responsabilização pela manipulação e acesso as informações a partir do documento assinado, obrigatoriedade de uso de VPN que consiste na criação de rede segura e privada entre o dispositivo do prestador de serviços e da organização, além da dupla autenticação com um token pelo celular. Porém essas medidas possuem falhas de segurança no acesso sendo que apesar

do usuário da VPN ser nominal, a plataforma de acesso remoto ao servidor permite que existam diversos acessos de maquinas diferentes e IP's (protocolo de rede) diferentes e de uma VPN diferente, então o acesso pode ocorrer da seguinte forma: um determinado usuário acessa sua VPN, porém pode entrar com o acesso do usuário de outro usuário na plataforma de acesso remoto de servidores mesmo que o usuário que esse outro usuário esteja conectado na mesma plataforma, ou seja, não é feita uma validação de compatibilidade de acesso e nem a restrição de acessos mútuos, o que permite que existam diversos acessos sem a garantia do uso único/ nominal.

A liberação de dados perante a solicitação da gerência da área é uma forma de controle, porém não requer nenhum documento comprobatório de ligação do colaborador do prestador de serviços com a necessidade do acesso ao servidor e quais recursos serão utilizados, o que pode permitir que um colaborador do departamento de recursos humanos receba um acesso mesmo que a sua função não tenha necessidade ou relação com esse acesso.

E os processos de gestão de mudanças são configurados como qualquer alteração no ambiente de produção que possam gerar baixo ou alto risco, esses processos são os que mais sofrem alterações e possuem procedimentos diversos de acordo com o departamento, apesar de todos os colaboradores da equipe de servidores trabalharem no mesmo local físico, mesma equipe e sob a mesma gestão de segurança da informação, cada um trabalha da forma que entende para atender esse processo gerando os seguintes cenários:

1. Para o primeiro departamento é necessário cumprir todos os requisitos citados anteriormente, qualquer alteração em produção até mesmo uma resolução de bug deve passar por todo o processo de comitê, evidencia de resultados, documentação, homologação e aprovação da área responsável.
2. Para o segundo departamento é necessário que mudanças estruturais de banco de dados passem por comitê, evidencia de resultados, documentação e homologação e aprovação da área responsável.
3. Para o terceiro departamento mudanças estruturais de banco de dados necessitam apenas de documentação da solicitação, homologação e aprovação da área responsável.

Concluindo, o último item de segurança apresentado trabalha com a restrição de acesso ao servidor de produção e ao banco de dados de produção apenas para a equipe de servidores e segurança da informação se enquadra como uma medida preventiva por parte da equipe para que nem todos os usuários possam executar ações permanente, irreversíveis ou de grande prejuízo para a organização, porém isso é algo que apesar de estar dentro da política de segurança e ser conhecido por todos também tem sido trabalhado como exceção, pois ao longo do estudo de caso identificamos que um usuário da empresa prestadora de serviços possuía acesso a todos os servidores com a possibilidade de executar updates, queries de leitura, desligar o IIS (plataforma de gerenciamento de software que possibilita pausar e desligar uma aplicação hospedada no servidor), subir a aplicação e até mesmo desligar o servidor pelo acesso remoto.

Para validar se essa liberação de acesso poderia ocorrer para qualquer gerente de projetos ou responsável pelo produto, foi feito contato com a organização solicitando acesso para um segundo usuário com essas características (gerente de projetos) e o acesso foi negado, pois o colaborador do mesmo departamento reforçou que “o acesso aos servidores e banco de produção são restritos a equipe da organização e que qualquer alteração que impacte o ambiente deve passar pelo processo de GMUD mesmo que seja um pequeno ajuste em produção”.

5 RESULTADOS E DISCUSSÃO

A primeira tratativa para solucionar as falhas de segurança levantadas seria, limitar em apenas um acesso ao software de acesso remoto aos servidores de forma que ao tentar mais de um acesso simultâneo seja essa informação seja guardada em logs de acesso, para melhor rastreio do porquê de existirem acessos simultâneos de um mesmo usuário por máquinas diferentes, se o acesso é único e não deve ser compartilhado, e como segundo passo inserir uma validação de 2 fatores em que por meio de um token ou autorização remota o usuário possa validar a autenticidade de seu acesso.

Então, sendo os pontos acima evidenciados como uma atenção necessária para estabelecer processos seguros em uma relação de cliente/fornecedor ou

simplesmente acesso de terceiros pela norma ABNT NBR ISO/IEC 27002 que visa orientar sobre o tema.

> Convém que a segurança dos recursos de processamento da informação e da informação da organização não seja reduzida pela introdução de produtos ou de serviços oriundos de partes externas. Convém que qualquer acesso de recurso de processamento da informação da organização e ao processamento e comunicação da organização por partes externas seja controlado. Convém que seja feita uma análise/avaliação dos riscos envolvidos para determinar as possíveis implicações na segurança e os controles necessários, onde existir uma necessidade de negócio para trabalhar com partes externas, que possa requerer acesso aos recursos de processamento da informação e a informação da organização, ou na obtenção e fornecimento de um produto e serviço de uma parte externa ou para ela. Convém que os controles sejam acordados e definidos por meio de um acordo com a parte externa. (ISO/IEC 27002, p 15, 2005)

E para que a liberação de acesso seja condizente com a necessidade, cargo e responsabilidade do usuário que está solicitando é necessário que a organização tenha um documento padrão em que além das políticas de uso da rede interna da organização, tenha também os campos de informação sobre o que gerou a necessidade de acesso a rede interna, seu posicionamento na estrutura organizacional e quais serão suas principais atividades dentro da rede interna, pois a partir disso as limitações de acesso para esses usuários serão mais assertivas e será mais fácil de identificar comportamentos anormais ou que possam gerar qualquer risco para organização.

De acordo com autores como Nassif e Rezende (p.113, 2017) informam que: “Bons gestores sabem que, em todos os momentos, precisam estar cientes de que uma boa política de gestão da informação deve englobar vários aspectos clássicos, mas, dentre eles, deve-se levar em conta a segurança da informação.” Portanto é importante reforçar que a gerência deve se atentar com as solicitações feitas por ela, e entender sobre a responsabilidade que é liberar acesso a dados confidenciais para terceiros e o impacto que isso pode gerar a organização, então todos os gestores e não somente os gestores da área da tecnologia da informação devem estar em conformidade com as regras estabelecidas, principalmente quando tratamos de

organizações que possuem redes internas e um datacenter próprio como a observada nesse estudo de caso.

Sobre os processos de gestão de mudanças, foi identificado que 1 processo obteve 3 formas diferentes de execução de trabalho do mesmo processo, fazendo com que a segurança dessas alterações estejam fragilizadas, e comprovam a necessidade de que para considerar as boas práticas e padronização de processos como algo cultural e natural entre os colaboradores é necessário que parte disso contenha uma boa gestão de pessoas, segundo Ventura e Nassif (p. 224, 2016) “uma má concepção de trabalho ou uma gestão inadequada impede o alinhamento dos indivíduos com o objetivo, com a estratégica da organização e, principalmente, o acesso a todo conhecimento que as mesmas possuem”. O trecho pontuado evidencia a necessidade de clareza nos processos estabelecidos pela organização, facilidade ao acesso de documentos e uma boa documentação entre gestão e operação. Porém também é necessário que exista o acompanhamento de perto de processos delicados como esse, e até mesmo auditorias internas que possam medir a aderência dos colaboradores a política de segurança da informação existente.

É recomendado que sejam feitas auditorias internas de forma regular e imparcial por parte do avaliador, com a finalidade de tomar nota e levantar os principais pontos divergentes entre prática e teoria da política de segurança da informação vigente na organização, com base nela será possível reavaliar os processos já existentes, melhorar os treinamentos fornecidos aos colaboradores e também revisitar os direitos e deveres de todos os envolvidos nos processos não conformes e no controle de segurança e proteção de dados.

De acordo com Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.BR a política de segurança deve ser compartilhada e trabalhada para todos os envolvidos em três tópicos, conscientização, treinamento, aconselhamento técnico e de políticas, com o intuito de “compartilhar o conhecimento e incentivar a adoção de boas práticas”. Ou seja, a equipe que executa o mesmo processo de formas diferentes de acordo com a afinidade ou percepção própria precisa repassar pelas etapas de treinamento de segurança da informação, ser supervisionada e passar por testes que messam a eficácia dos treinamentos

aplicados, assim a equipe ficará alinhada e terá menor possibilidade de colocar em risco a segurança da informação por erros decorrentes de procedimentos internos.

Então com base na última situação apresentada na metodologia, é possível concluir que o maior impasse da empresa é como aplicar as políticas de segurança da informação já existentes na prática do dia a dia de todos os colaboradores, pois em determinados departamentos existem colaboradores dedicados e dispostos a cumprirem com todos os requisitos de segurança e outros que agem pela própria vontade colocando o coleguismo e a proximidade com o solicitante frente as políticas instituídas pela empresa.

O seguinte trecho de Ventura e Nassif (p.230, 2016) “Outro ponto claro para os gestores é que se o resultado não acontece e se há um descompasso nas informações e nas ações é por falta de atitude dos colaboradores e não por incoerências provenientes da dinâmica do trabalho” reforça que, a falha nos resultados e no não seguimento das regras pode estar ligado diretamente aos colaboradores envolvidos e não apenas a dinâmica de trabalho, sendo nesses casos necessária a aplicação de medidas punitivas a fim de reforçar a seriedade dos pontos tratados.

> Muitos sistemas de informação não foram projetados para serem seguros, uma vez que a Segurança da informação não pode ser alcançada apenas por meios técnicos. Segurança da Informação deve estar apoiada por uma gestão e por procedimentos apropriados. Os mecanismos de controle devem ser detalhadamente implementados. A implantação deve acontecer de cima para baixo (arquitetura Top-Down), atingindo desde a mais alta direção, passando por todos os funcionários e abrangendo clientes, fornecedores e acionistas. Uma consultoria externa especializada pode ser útil no momento de sua implantação (LAHTI e PETERSON, 2006 apud TRRES, ANHESINE e AZZOLINI JUNIOR, p.17, 2010).

5 CONSIDERAÇÕES FINAIS

Todos os pontos destacados ao longo do estudo de caso são falhas que facilmente seriam solucionadas com uma boa comunicação entre gestão e operação, entretanto como se tratam de processos estabelecidos há um tempo e colaboradores que trabalham há ano na organização, todas as medidas citadas ao longo dos

resultados e discussão como, informar de forma clara os processos de segurança da informação, ter gestores da área de tecnologia alinhados com gestores da segurança da informação, melhor definição de responsabilidades para evitar o acesso indevido a determinadas informações, auditorias internas a fim de medir a eficácia da equipe no cumprimentos das políticas estabelecidas e punições adequadas ao não cumprimento das normas internas, podem e devem ser adotados a fim de minimizar os riscos proeminentes à falta de padrão e furos de segurança estabelecidos pela forma de trabalho dos colaboradores

REFERÊNCIAS

BR, Cert. **Sobre o CERT.br**. 2022. Disponível em: https://www.cert.br/sobre/. Acesso em: 26 nov. 2022.

Brasil. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 15 jun. 2023.

BRASIL. ABN NBR ISO/IEC 27002. **Tecnologia da Informação - Técnicas de Segurança - Código de Prática Para Segurança da Informação**.

LAHTI, C. B.; PETERSON, R. Sarbanes-Oxley: Conformidade TI usando COBIT e ferramentas open source. Rio de Janeiro: Alta Books, 2006.

NASSIF, M. E.; RESENDE, W. da C. Gestão da informação e do conhecimento e suas relações com segurança da informação, tecnologias da informação e compartilhamento. **Ciência da Informação**, *[S. l.]*, v. 45, n. 3, 2018. DOI:

10.18225/ci.inf.v45i3.4052. Disponível em: https://revista.ibict.br/ciinf/article/view/4052. Acesso em: 9 dez. 2022.

TORRES, Marcelo Teixeira; ANHESINE, Marcelo Wilson; AZZOLINI JÚNIOR, Walther. A GESTÃO DA SEGURANÇA DA INFORMAÇÃO E SEU ALINHAMENTO ESTRATÉGICO NA ORGANIZAÇÃO. **Revista Fatec**, São Paulo, v. 1, n. 7, p. 11-21, jan. 2010. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/40/37. Acesso em: 12 nov. 2022.

VENTURA, Rita de Cássia Martins de Oliveira; NASSIF, Mônica Erichsen. GESTÃO DE PESSOAS E SUAS RELAÇÕES COM O COMPARTILHAMENTO DA INFORMAÇÃO NO CONTEXTO ORGANIZACIONAL. **Inf. & Soc**, João Pessoa, v. 3, n. 26, p. 221-234, dez. 2016. Disponível em: https://brapci.inf.br/index.php/res/download/95944. Acesso em: 26 nov. 2022.