UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE GRADUAÇÃO
CENTRO MULTIDISCIPLINAR DE ANGICOS
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

ROBERTA KAROLINE DE SOUZA BEZERRA

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO - UM ESTUDO DE CASO NA UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO

ANGICOS/RN
2019

ROBERTA KAROLINE DE SOUZA BEZERRA

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO - UM ESTUDO DE CASO NA UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO

Monografia apresentada à Universidade Federal Rural do Semi-Árido como requisito para obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Profa. Me. Luana Dantas Chagas

ANGICOS/RN

2019

B574p Bezerra, Roberta Karoline de Souza.
Políticas de Segurança da Informação - Um estudo de caso na Universidade Federal Rural do Semi-Árido / Roberta Karoline de Souza Bezerra. - 2019.
67 f. : il.

Orientadora: Luana Dantas Chagas.
Monografia (graduação) - Universidade Federal Rural do Semi-árido, Curso de Sistemas de Informação, 2019.

1. Informação. 2. Segurança. 3. Política de Segurança. 4. UFERSA. I. Chagas, Luana Dantas, orient. II. Título.

ROBERTA KAROLINE DE SOUZA BEZERRA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – UM ESTUDO DE CASO NA UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO

Trabalho de Conclusão de Curso apresentado à Universidade Federal Rural do Semi-Árido como requisito para obtenção do título de Bacharel em Sistemas de Informação.

Defendida em: 20 / 03 / 2019 .

BANCA EXAMINADORA

Luana Dantas Chagas

Luana Dantas Chagas, Profa. Ma. (UFERSA)

Orientadora-Presidente

Joêmia Leilane Gomes de Medeiros

Joêmia Leilane Gomes de Medeiros, Profa. Dra. (UFERSA)

Membro Examinadora

Adriana Mara Guimarães de Farias

Adriana Mara Guimarães de Faria, Profa. Ma. (UFERSA)

Membro Examinadora

AGRADECIMENTOS

Gostaria de agradecer aos meu pais, Maria Izabel e Roberto Marzo, pela educação que me foi dada e por toda a dedicação que desde pequena me foi destinada.

Toda minha gratidão aos meus professores por todo o conhecimento que me foi passado, pelos conselhos e orientações. Em especial a Sairo Raoni, que além de professor se tornou um grande amigo pessoal e sempre me incentivou a não desistir. Gostaria de agradecer também a professora Luana Dantas por toda paciência, dedicação e confiança que me foi depositada. A professora Welliana Benevides e Alessandra Soares por todas as conversas, conselhos e palavras de incentivo em meio aos meus momentos de desmotivação. Vocês são grandes exemplos para mim, não só de pessoas, como também de profissionais excepcionais.

Obrigada aos meus amigos pelos momentos de diversão, companheirismo e amizade. Em especial ao meu grande amigo Antunes França e a minha querida companheira Amanda Miranda, pois sem o apoio de vocês, eu não conseguiria ter chegado até aqui. Obrigada por toda paciência que tiveram em sempre me lembrar do quanto eu sou capaz nas diversas vezes em que não me senti assim. Obrigada por me incentivarem diariamente e não me deixarem desistir.

“Basta ser sincero e desejar profundo,
você será capaz de sacudir o mundo.”
Raul Seixas

RESUMO

A política de segurança da informação é um documento orientador dentro de uma organização. Por intermédio desta política, é possível identificar desde estratégias gerais de segurança até a implementação de procedimentos e operações adotadas no dia a dia de uma organização. Devido a importância que a PoSIC possui, é possível encontrá-la nos mais diversos âmbitos, inclusive nas instituições de ensino superior, já que as mesmas lidam diariamente com inúmeros dados importantes de docentes, discentes e técnicos. Diante disso, esse trabalho objetivou realizar um estudo sobre a PoSIC da Universidade Federal Rural do Semi-Árido (UFERSA). Nesse estudo, foi verificada a política da instituição considerando os documentos disponibilizados ao público por meio de página oficial, bem como por meio de entrevista com o setor responsável por manter essa política. Foi possível identificar que a mesma trouxe, por meio da sua implementação, benefícios para a instituição, entre eles, a redução de ataques maliciosos e a efetivação de algumas medidas de segurança.

Palavras-chave: informação, segurança, política de segurança, UFERSA.

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	*Associação Brasileira de Normas Técnicas*
APF	*Administração Pública Federal*
CERT.br	*Centro de Estudos, Resposta e Tratamento de incidentes de Segurança*
CGD	*Comitê de Governança Digital*
CGTI	*Comitê Gestor de Tecnologia da Informação*
CID	*Confidencialidade, Integridade e Disponibilidade*
CONSUNI	*Conselho Universitário*
DoS	*Denial of Service*
EaD	*Ensino a Distância*
ENADE	*Exame Nacional de Desempenho dos Estudantes*
ESAM	*Escola Superior de Agricultura de Mossoró*
GSI/PR	*Gabinete de Segurança Institucional da Presidência da República*
IFES	*Instituições Federais do Ensino Superior*
INDA	*Instituto Nacional de Desenvolvimento Agrário*
MEC	*Ministério da Educação*
PNSI	*Política Nacional de Segurança da Informação*
PoSIC	*Política de Segurança da Informação e Comunicação*
SI	*Segurança da Informação*
SUTIC	*Superintendência de Tecnologia da Informação e Comunicação*
TCU	*Tribunal de Contas da União*
TI	*Tecnologia da Informação*
UCL	*University College London*
UFERSA	*Universidade Federal Rural do Semi-Árido*

SUMÁRIO

1 INTRODUÇÃO

Nos dias de hoje, uma grande quantidade de informações é armazenada em dispositivos digitais. Muitas delas são importantes e sigilosas, tornando indispensável tomar medidas que visem garantia de segurança. Isso acontece principalmente em empresas e organizações, que possuem informações importantes que podem ser cruciais para o seu sucesso ou fracasso. Diante desse contexto, o acesso de terceiros a informações privadas pode causar diversos problemas.

No que se refere a segurança das informações privadas, no meio computacional, Stallings e Brown (2014) relatam que o objetivo da segurança é procurar proteger recursos e informações sigilosas do acesso de elementos não autorizados e também da manipulação e utilização não autorizada dessas informações, sejam essas ações intencionais ou não.

A necessidade de proteção pode variar de acordo com os objetivos de cada organização ou dos possíveis riscos e ameaças aos quais a mesma esteja exposta. Dentre esses riscos, é possível apontar destruição de informações, o roubo ou desvio de dados, a revelação de informações, a falsificação ou modificação de informações e a interrupção de serviços.

Para Howard (1997), a segurança da informação é a responsável por prevenir que atacantes alcancem os seus objetivos por meio do uso ou acesso não autorizado a máquinas e redes. Ainda de acordo com o autor, essa prevenção se dá com a aplicação de recursos, políticas e mecanismos que visam assegurar a segurança das informações das organizações da melhor forma possível.

Dentre esses recursos estão inclusas as políticas de segurança que visam assegurar a segurança de informações garantindo três propriedades: confidencialidade, integridade e disponibilidade. De acordo com Lopes (2012), a política de segurança da informação é um documento que indica o apoio e o compromisso da gestão à segurança da informação, bem como, determina o cargo que a segurança da informação possui para atingir e apoiar a visão e a missão da organização. Guimarães, Lins e da Oliveira (2006) dizem que é muito importante restringir o acesso lógico e físico aos computadores, especialmente nos locais que partilhem de algum meio de comunicação público ou em ambientes computacionais

compartilhados. Deste modo, é possível perceber o quão é essencial a aplicação de políticas de segurança e medidas preventivas em diversos âmbitos, incluindo no âmbito das instituições de ensino federal, para que assim exista uma salvaguarda das informações da organização.

A utilização de dados em sistemas está cada vez mais comum entre as organizações e não seria diferente em relação as universidades, que realizam o processamento e compartilhamento desses dados através de sistemas e redes de computadores, o que ajuda a tornar o seu trabalho mais prático e eficaz. Diante desse contexto, o objetivo deste trabalho é realizar um estudo de caso sobre a política de segurança da informação da Universidade Federal Rural do Semi-Árido.

1.1 Justificativa

Com a popularização das tecnologias, cada vez mais usuários se rendem aos meios tecnológicos e desta maneira, a utilização de informações digitais vem se tornando cada vez mais comum nos dias atuais. As informações digitais são importantes pois acabam trazendo bastante praticidade através do seu uso, já que por meio de um computador é possível armazenar uma grande quantidade de informações, além de geri-las e encontrá-las bem mais facilmente. Marciano (2006) coloca a informação como um recurso transformador não só para as organizações e a sociedade, mas também para o indivíduo. Então, tendo em vista a proporção da importância da informação, é essencial protegê-la e garantir a sua salvaguarda através da segurança da informação.

Apesar da adoção de políticas e mecanismos de proteção para as informações, é possível encontrar diversos relatos de ataques. De acordo com Jessen e Hoepers (2005), o CERT.br afirma que vírus, fraudes, ferramentas automatizadas de ataques, vulnerabilidades frequentes, códigos maliciosos explorando essas vulnerabilidades em curto espaço de tempo e ataques de força bruta são as principais ameaças à segurança de informações.

Landim (2015) relata que em janeiro de 2014 ocorreu uma situação na qual um trojan – *malware* que abre portas de rede sem a autorização de um usuário – voltado a furtar informações de dados bancários de usuários estava sendo disfarçado como

uma atualização de um popular aplicativo de mensagens e enviado por e-mails, convidando os usuários a realizarem esta nova atualização. Já Gusmão (2014) diz que em maio do mesmo ano, a empresa de comércio eletrônico eBay foi vítima de ataque cibernético, onde informações pessoais dos usuários, como endereços de entrega, telefones e e-mails, foram vazadas. Isso acarretou no comprometimento de um banco de dados repleto de senhas criptografadas, sendo necessário que a empresa solicitasse a troca de senha dos seus 112 milhões de usuários.

Na mídia, Lima, Tadini e Capelas (2018) noticiaram que em 28 de setembro de 2018 foi revelado pelo Facebook uma falha de segurança, onde invasores passaram a possuir acesso às contas dos usuários da rede social. A falha aconteceu através da função “Ver Como” do Facebook, função esta que permitia que os usuários tivessem a visualização do seu perfil a partir da visão de quem não era seu amigo na rede social. Porém, devido a falha ocorrida na função, quando utilizada pelos invasores, eles conseguiam ter acesso aos perfis dos usuários da mesma maneira que os próprios proprietários das contas. Este acontecimento acabou acarretando em 50 milhões de usuários afetados.

Estatísticas coletadas pelo Centro de Estudos, Resposta e Tratamento de incidentes de Segurança (CERT.br) no Brasil (CERT.br, 2017) mostram que, ao longo do ano de 2017, foram reportados 833.775 incidentes. Dentre esses, 53,16% foram de ataques do tipo scan; 21,41%, foram do tipo *Denial of Service* ou DoS; ataques web possuem uma porcentagem de 7,29%; logo após estão os ataques de fraude com 7,11%; 5,41% para os ataques do tipo *worm*; ataques de invasão com 0,05% e 0,57% de outros tipos de ataques que não se enquadram nas categorias anteriores.

Os ataques atingem inclusive instituições de ensino. Segundo Tadeu (2018), uma grande quantidade de ataques cibernéticos em larga proporção a instituições de ensino marcou o ano de 2017 tanto no Brasil, como no exterior. O centro universitário Uninovafapi, instituição privada da cidade de Teresina - Piauí, foi uma das instituições que possuiu um caso de grande repercussão. Alvo de um ataque de ransomware (sequestro e resgate de dados), a mesma teve cerca de 30 mil dados pessoais de alunos e professores sequestrado. Em junho de 2017, a *University College London* (UCL) foi mais um alvo, onde funcionários e estudantes tiveram seus arquivos bloqueados por outro vírus de resgate.

Tadeu (2018) diz que o relatório produzido pela Cisco sobre segurança cibernética relata que a regularidade de manifestação global de ataques de ransomware a instituições de ensino já possui mais registros do que a qualquer outra indústria. Uma das razões para isso é o baixo nível de maturidade em tecnologia da informação (TI) e em segurança da informação (SI) que as instituições acadêmicas possuem, o que acaba tornando a área educacional um alvo cada vez mais preferencial para os ciberataques. Tal fato ressalta a importância do estudo das políticas de segurança da informação no meio acadêmico.

Os diversos exemplos existentes de falhas ocorridas na segurança computacional e as suas consequências ressaltam e reforçam a importância de possuir uma política de segurança da informação, adotando estratégias que busquem proteger os sistemas das organizações, inclusive de instituições de ensino. Nesse trabalho, será realizado um estudo sobre a política de segurança da informação no âmbito das Universidades Federal Rural do Semi-Árido.

1.2 Objetivo geral

Este trabalho tem por finalidade realizar um estudo sobre a política de segurança da informação da Universidade Federal Rural do Semi-Árido, a fim de identificar desde estratégias gerais de segurança até implementação de procedimentos.

1.2.1 Objetivos específicos

- Realizar pesquisa bibliográfica sobre políticas de segurança da informação;
- Identificar políticas governamentais e normas sobre segurança da informação;
- Identificar a política de segurança da informação da UFERSA por meio das informações disponibilizadas ao público;

- Identificar a política de segurança da informação da UFERSA por meio de entrevista com setor responsável.

1.3 Estrutura do trabalho

Este trabalho está dividido em quatro capítulos. Além do Capítulo 1, já apresentado, o trabalho é estruturado da seguinte maneira:

- No Capítulo 2 será introduzido fundamentos da segurança da informação, contemplando tipos de ameaças, vulnerabilidades, normas, políticas de segurança e segurança da informação nas instituições federais.
- No Capítulo 3 será apresentado o estudo realizado sobre a política de segurança da informação da Universidade Federal Rural do Semi-Árido.
- Por fim, o Capítulo 4 apresenta as considerações finais do trabalho.

2. SEGURANÇA DA INFORMAÇÃO

Todo e qualquer dado ou conteúdo valioso com capacidade de transferência e/ou armazenamento, seja para alguma organização ou para algum indivíduo, pode ser entendido como informação. No nosso atual período, as informações digitais tornaram-se um recurso bastante significativo e valioso, pois elas dizem muito sobre a organização e as pessoas nela envolvidas. Esses dados e conteúdos são, principalmente, provenientes dos sistemas de informação.

De acordo com Rezende (2005), pode ser nomeado como um sistema de informação genérico todo e qualquer sistema que de alguma maneira gere informação ou possua armazenamento de dados. Podendo colaborar consideravelmente com a solução de vários problemas organizacionais, os sistemas de informação têm como seu objetivo principal o auxílio no processo da tomada de decisão nas organizações onde o mesmo está inserido, tornando sua presença significativa para as organizações.

Os sistemas de informação trazem diversos benefícios como o auxílio na inteligência organizacional, eficiência, segurança, controle das operações e informações, entre outros. Para tal, são compostos por cinco recursos principais, são eles: pessoas, *hardware*, *software*, dados e redes. Todos os sistemas de informação operam desses recursos para realizar atividades de entrada, processamento, saída, armazenamento e controle que transformam recursos de dados em produtos de informação. Dada a importância das informações, é fundamental que elas sejam adequadamente protegidas da melhor forma possível.

Existem diversos fatores que podem acabar interferindo ou afetando de alguma forma a segurança dessas informações. Alguns deles podem acontecer devido ao ambiente em que os dados se encontram, já outros é possível que ocorram devido ao comportamento do usuário – como, por exemplo, quando o usuário não utiliza de senha em seus dispositivos. Além desses fatores, ainda existem usuários maliciosos que objetivam atingir diretamente informações através da destruição, do roubo ou da modificação das mesmas. A fim de lidar com esses fatores, há a área de segurança da informação.

De acordo com Fontes (2017), a segurança da informação se dá através de um grupo de procedimentos, orientações, políticas, normas e algumas outras ações que possuem como objetivo a proteção do recurso informação, o que permite a organização tenha sucesso na missão almejada. Uma informação incorreta ou mesmo a falta dela pode vir a ocasionar em perdas para a organização que causem danos ao seu funcionamento, desta forma, a segurança da informação é responsável por buscar a diminuição desses riscos.

De acordo com Pfleeger e Pfleeger (2011), existem três propriedades da segurança que precisam ser garantidas, são elas: a confidencialidade, a integridade e a disponibilidade. Essas propriedades são conhecidas como a tríade CID. A disponibilidade se trata da competência que um sistema possui de preservar o direito de que qualquer parte autorizada possa utilizar de um determinado recurso quando for necessário. A integridade refere-se à capacidade de proteger as informações para garantir que elas só possam ser modificadas por quem possui autorização para tal. Já a confidencialidade busca garantir que apenas sistemas ou usuários autorizados tenham acesso a informações protegidas.

Tratando-se ainda da confidencialidade, para Pfleeger e Pfleeger (2011) ela abrange apenas a visualização dos dados, o que não necessariamente dá a habilidade de alterá-los. Uma comunicação em rede, por exemplo, pode ser interrompida de algum modo e a qualquer momento por um usuário malicioso, também conhecido como “*hacker*”. Porém, caso os participantes estejam utilizando algum mecanismo para proteger a sua confidencialidade, o *hacker* não terá acesso ao seu conteúdo. Ou seja, ele pode conseguir interceptar mensagens, mas não vai conseguir visualizar o seu conteúdo, o que é de grande relevância já que evitaria a quebra de sigilo das comunicações, assim como a utilização maliciosa de informações confidenciais. Há, no entanto, uma certa dificuldade em garantir as propriedades da tríade CID devido a algumas vulnerabilidades e ameaças que podem acabar colocando-as em risco.

2.1 Ameaças

Uma forma de diminuir os riscos de não garantir segurança da informação é entender sobre as vulnerabilidades e ameaças que a cercam. Pfleeger e Pfleeger (2011) colocam a vulnerabilidade como fraquezas existentes na segurança do sistema, ou seja, “brechas” que facilitam invasões. Por exemplo, um sistema operacional ou um *software* desatualizado, que não contenha alguma atualização de segurança. Então, é importante que o usuário consiga maneiras de neutralizar essas vulnerabilidades de forma a impossibilitar as ameaças e minimizar a probabilidade de ataques.

Tratando-se das ameaças, Pfleeger e Pfleeger (2011) as definem como quaisquer situações que podem afetar negativamente as informações ou o sistema, e que elas podem ser classificadas entre: ameaças não-humanas ou ameaças humanas. Componentes defeituosos, quedas de energia elétrica, incêndios e raios são exemplos de ameaças não-humanas. Já as ameaças humanas são divididas ainda entre não-maliciosas e mal-intencionadas.

Quando falamos em ameaças não-maliciosas tratamos de acidentes como, por exemplo, encaminhar um arquivo para um contato errado sem perceber, clicar em uma opção errada no momento em que se abre uma janela de diálogo causando a exclusão de um arquivo, deixar cair um copo de água sobre um computador, entre outros. A maioria dos danos à segurança, no entanto, ocorre devido a usuários mal-intencionados, também conhecidos como *hackers* ou invasores. Nesse tipo de situação, tais ações são chamadas de ataques.

Existem diversos tipos de ataques, que geralmente é por onde os usuários maliciosos buscam roubar informações. Dentre esses diversos tipos, é possível observar que existem 4 tipos principais, são eles: o ataque de força bruta, o de engenharia social, os do tipo *Denial of Service* e os ataques de invasão.

O ataque de força bruta requer paciência, pois consiste em testar cada possibilidade de chave existente dentro de um espaço possível de chaves, até que a decriptação com uma delas resulte em um texto claro válido. Para a obtenção do sucesso em um ataque de força bruta, geralmente é necessário testar pelo menos a metade de todas as possibilidades de chaves existentes. Segundo Basta, Basta e

Brown (2014), se o atacante dispuser do tempo necessário, é possível extrair até as senhas mais difíceis usando de todas as possíveis combinações de caracteres especiais, letras e números. Como envolve testar as mais diversas possibilidades, os ataques de força bruta podem ser bastante demorados. Há diversos fatores que podem influenciar na velocidade desse tipo de ataque. O mais importante desses é a extensão da senha, em que quanto maior a palavra-chave, maior será o tempo gasto para a determinação dela. Como esse tipo de ataque necessita de uma grande quantidade de tentativas, é possível detectá-lo e impedi-lo ao bloquear o acesso após um determinado número de tentativas falhas. Se o número de tentativas de permitidas antes do bloqueio for adequadamente pequeno, é provável que o ataque falhará.

Se tratando do ataque através do método da engenharia social, Basta, Basta e Brown (2014) citam que este método pode ser utilizado por um *hacker* com o intuito da obtenção de dados. Esta é uma técnica que se aproveita da confiança e da natureza humana das pessoas para extrair informações importantes. A engenharia social dispõe de muitas técnicas, como o "*phishing*", onde são utilizados falsos e-mails para se passar por organizações verdadeiras e capturar informações de usuários.

Já os ataques do tipo *Denial of Service*, que também podem ser chamados de DoS, são notificações de ataques de negação de serviço, onde um conjunto de computadores ou mesmo um computador só é utilizado pelo atacante para derrubar e tirar de operação uma rede, um computador ou um serviço. Para realizar esse tipo de ataque, o autor do mesmo envia diversas notificações ou requisições para a máquina que deseja derrubar, o que faz com que a mesma chegue ao ponto de não conseguir lidar com todas elas. Isso acaba deixando o computador tão sobrecarregado que ele passa a negar o serviço. Por isso, os ataques do tipo DoS também são conhecidos como ataques de negação de serviço.

Por fim, o ataque de invasão refere-se a ações bem-sucedidas que resultem no acesso não autorizado a uma rede ou a um computador. Um exemplo desse tipo de ataque seria uma clássica invasão de redes, onde o *hacker* se aproveitaria de alguma vulnerabilidade encontrada no serviço de rede ou mesmo no sistema operacional para desta maneira conseguir obter o acesso não autorizado a máquina.

Além desses quatro tipos de ataques já citados, ainda é possível encontrar ataques outros tipos. Por exemplo, ataques do tipo *scan*, que são notificações de

varreduras em redes de computadores com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados pelos mesmos. Há também ataques do tipo web, que são casos particulares de ataque onde se é visado especificamente o comprometimento de servidores web ou desfigurações de páginas na internet. Há ataques de fraude, que englobando também as tentativas falhas, tratam-se de incidentes em que ocorre uma tentativa de obter vantagem em cima de alguma vítima, como por exemplo, quando um atacante rouba dados de alguma vítima para realizar compras em seu nome. Outro exemplo são os ataques do tipo *worm*, que são notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede, entre outros.

A neutralização de ameaças e vulnerabilidades especificamente ajudam a proteger o sistema de danos. Mas além disso, também é necessário estabelecer e adotar políticas de segurança na organização, para assim conseguir prevenir, amenizar e lidar com esses tipos de problemas.

2.2 Políticas de segurança da informação

Para o Estado brasileiro, um significativo recurso que vem crescendo bastante em qualquer atividade e setor é a informação. De acordo com o Ministério do Planejamento, Desenvolvimento e Gestão (2019) o principal ativo das instituições, sejam elas privadas ou públicas, são as informações, independentemente do seu formato. E, estando os sistemas que suportam essas informações cada vez mais expostos a riscos, a aplicação de políticas de segurança acaba sendo cada vez mais indispensável no âmbito das organizações.

Para a ABNT (2013), a política, em uma definição geral, trata-se de uma regra universal inclusa em uma organização, que determina os limites e as ações necessárias para atingir os objetivos e as metas organizacionais. No contexto da segurança, é o documento que irá estabelecer os limites, as normas, as diretrizes e o direcionamento que a organização almeja para os controles que irão ser implementados na proteção da informação.

Segundo Monteiro (2009), o significado de uma política deve ser constituído com base na assimilação da missão da organização, sem deixar de considerar os

requisitos legais e normativos que a regem. Ainda de acordo com o autor, a Política de Segurança da Informação e Comunicação (PoSIC) é um documento que precisará ser lido por todos que compõem a organização, sendo necessário que o documento esteja compreensível e de entendimento claro.

Tratando-se das boas práticas da segurança da informação, Fontes (2012) disserta que é de fundamental importância que qualquer organização possua a sua Política de Segurança da Informação e Comunicação, pois dessa maneira o método de segurança da informação poderá ser produzido, implantado e mantido.

De acordo com Lopes (2012), a política de segurança da informação é um documento orientador dentro de uma organização. Tal política pode ser dividida em três classes, são elas: as políticas de alto nível, as políticas de baixo nível e as metapolíticas. As políticas de alto nível envolvem os procedimentos aceitáveis de uma política juntamente com os seus objetivos gerais, tudo através de planos globais de alto nível. As políticas de baixo nível tratam-se da ação de métodos de segurança da informação que são escolhidos e definidos em meio a diversas condições e alternativas. Essas políticas orientam e definem as decisões atuais e futuras da segurança da informação, tal como, a definição de diretrizes para senhas. Já as metapolíticas, que também são chamadas por alguns autores de “políticas para as políticas”, referem-se a diretrizes organizacionais para a manutenção e a elaboração das políticas. São exemplos de diretrizes de metapolíticas o momento em que a política deve ser realizada e quem seria o encarregado por constituí-las.

Lopes (2012) diz ainda que existem três estruturas fundamentais para as políticas de segurança, que são: as políticas individuais, a política completa e a política completa modular. As políticas individuais são políticas de segurança independentes e separadas para cada um dos sistemas e tecnologias utilizados na organização. Já na política completa, que é considerada por alguns autores como a mais comum, é englobado em um só documento todas as tecnologias que foram utilizadas. Esse documento, que é gerido, controlado e definido pela organização, oferecerá orientações gerais para os sistemas como um todo que são empregados pela organização. Já a política completa modular, colocada pelos autores como a estrutura mais eficaz para as políticas de segurança, atua como a política completa, mas inclui ainda apêndices modulares que proporciona detalhes característicos a respeito de cada tecnologia. Esses detalhes englobam diferenças, observações, restrições e

funcionalidades particulares relativas ao uso das tecnologias que não são cobertos de maneira apropriada pelo documento da política base.

As políticas de segurança dentre os seus níveis de classes e estruturas podem ainda basear-se em algumas normas para guiar as orientações que serão colocadas em seus documentos.

2.2.1 Normas

A ISO/IEC 17799:2000 é uma norma internacional de segurança da informação, resultante de esforços nessa área de começaram com o governo britânico, em 1987. Essa norma possui um alto número de requerimentos e controles que precisam ser atendidos para assegurar a segurança das informações das organizações na qual a mesma procura cobrir os mais diversos tópicos da área de segurança. Foi buscando o exemplo da ISO/IEC 17799:2000, que diversos países, inclusive o Brasil, desenvolveram normas nacionais de segurança.

Em setembro de 2001, a ABNT (2005) homologou a versão brasileira da norma (que foi atualizada em 2005), onde a mesma possui como objetivo determinar diretrizes e princípios gerais para implementar, iniciar, melhorar e manter a gestão de segurança da informação em uma determinada organização. Inspirada na norma ISO/IEC 17799:2000, esta norma é denominada de NBR ISO/IEC 17799:2005.

Conforme a norma NBR ISO/IEC 17799:2005, a política de segurança deve apresentar algumas características como, por exemplo, dispor de um apoio e orientação da direção para a segurança da informação conforme as leis e regulamentações relevantes, cláusulas contratuais e requisitos da própria organização. Outra característica é que a política de segurança precisa ser aprovada pela diretoria, divulgada e publicada de maneira em que abranja a todos os colaboradores. A norma determina que a direção deve designar uma política clara, composta pelos objetivos do negócio e que apresente apoio e comprometimento para com a segurança da informação através da manutenção. A norma coloca ainda que as políticas de segurança devem dispor as consequências das violações. Outra indicação é a definição de responsabilidades gerais e específicas e a revisão regular

da política de segurança com garantia de que, em caso de alteração, a mesma seja revista.

De acordo com Martins e Santos (2005), a norma NBR ISO/IEC 17799:2005 diz que a política de segurança deverá conter alguns tópicos: a propriedade da informação, a classificação da informação, o controle de acesso, a gerência de usuários e senhas, a segurança física, o desenvolvimento de sistemas ou compra de sistemas e o plano de continuidade de negócios.

A propriedade de informação indica que deve ser estabelecida uma pessoa para realizar a definição de qual nível de acesso as informações será permitido acesso e quem terá autorização para possuir este acesso.

A classificação da informação determina que o gestor será o responsável por categorizar a informação em relação aos princípios das propriedades da informação, que são: a integridade, confidencialidade e disponibilidade.

O controle de acesso coloca que toda solicitação de acesso deve ser documentada e que é necessário esquivar-se da segregação de função, de tal maneira que um mesmo usuário não deverá possuir o acesso à liberação de pagamento e geração do mesmo.

A gerência de usuários e senhas diz que as senhas devem estar de acordo com os critérios de qualidade, portanto, deverão ser senhas fortes que possuam uma alteração periódica. Além disso, as senhas precisam ser individuais e únicas, sendo de total responsabilidade do próprio usuário.

A segurança física diz respeito aos acessos a âmbitos de servidores, que só poderão ser consentidos após uma autorização. A entrada e a saída de pessoas e equipamentos devem ser monitoradas, para que assim possa ser mantido um controle.

No desenvolvimento de sistemas ou compra de sistemas/softwares é de fundamental relevância que seja estabelecida uma sistemática interna com destaque na parte dos requisitos de segurança, já que a segurança é fundamental em qualquer tipo de sistema.

Por fim, o plano de continuidade de negócios sugere a geração de padrões e controles que exibem características quanto ao plano de contingência e continuidade

dos negócios. Martins e Santos (2005) relatam que este tópico é tido como um dos tópicos mais importantes na política de segurança de acordo com a norma.

O governo federal também estabelece algumas normas, a fim de auxiliar na gestão de segurança da informação e comunicações e nas suas políticas de segurança da informação. Tais diretrizes devem ser consideradas pelas entidades e órgãos da Administração Pública Federal (APF), tomando-as como base para suas próprias normas.

Em 26 de dezembro de 2018, o governo federal lançou uma nova Política Nacional de Segurança da Informação (PNSI) com a publicação do Decreto nº 9.637. Baseado em uma visão sistêmica e abrangente, o decreto atualiza as normas incluídas no Decreto 3.505/2000, a fim de fortificar ainda mais a cultura da segurança da informação na sociedade em geral. A criação do documento foi coordenada pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e buscou atualizar e retificar as diretrizes e os princípios que guiam a atuação dos gestores públicos federais.

Instituída no âmbito da Administração Pública Federal, a Política Nacional de Segurança da Informação atual ressalta a importância da educação como um eixo fundamental para o auxílio da cultura em segurança da informação, possuindo entre as suas metas o estímulo do progresso contínuo da qualificação dos indivíduos envoltos com esta área. Além disto, ela também enfatiza o auxílio a pesquisas científicas buscando, assim, dar o suporte necessário a inovação e ao desenvolvimento tecnológico, tal como a promoção da cooperação e integração entre o setor empresarial, a sociedade, o poder público e as instituições acadêmicas.

De acordo com o Ministério da Economia (2018), Ciro Avelino, o secretário adjunto de Tecnologia da Informação e Comunicação do Ministério de Planejamento, Desenvolvimento e Gestão, disse que o trabalho administrado pelo Gabinete de Segurança Institucional renova diretrizes e princípios indispensáveis de segurança que nortearão ações estratégicas para acrescentar e tornar ainda maior a proteção da privacidade, dos dados pessoais dos usuários e do acesso às informações dos cidadãos. Isso tudo ocorre através da Política Nacional de Segurança da Informação (PNSI), que tem a finalidade de assegurar atributos como a confidencialidade, a autenticidade, a disponibilidade e a integridade da informação a nível nacional, através

da segurança física, da proteção de dados organizacionais, da defesa e da segurança cibernética.

A PNSI retrata uma evolução não só para a administração pública federal, mas sim para toda a sociedade brasileira. Ela aprova diretrizes, normas, estratégias e recomendações com o intuito de garantir a segurança da informação. Além disso, a mesma também implementa e elabora programas sobre a segurança da informação que são destinados a capacitar e conscientizar os servidores públicos federais e da sociedade; estabelece critérios que permitam o monitoramento e a avaliação da execução da PNSI acompanha a evolução doutrinária e tecnológica, tanto em âmbito nacional como internacional e apoia a elaboração dos planos nacionais que são vinculados à Estratégia Nacional de Segurança da Informação. A PNSI busca ainda estabelecer os requisitos mínimos de segurança que são necessários para a utilização de produtos que incorporem recursos de segurança da informação, de maneira que assegure a confidencialidade, disponibilidade, autenticidade e integridade da informação.

Tendo em vista que as políticas de segurança tendem a determinar diretrizes em um nível mais estratégico, é importante pensar sobre práticas que devem ser adotadas a fim de garantir as determinações das políticas. Tais práticas tratam-se de medidas de segurança.

2.2.2 Medidas de segurança

Sabendo que as informações ficam cada vez mais vulneráveis a riscos de segurança graças ao contexto globalizado em que se encontra o âmbito tecnológico, as medidas de segurança são aplicadas com o objetivo de atenuar as vulnerabilidades e diminuir a probabilidade de que hajam ações de ameaças e consequentemente incidentes de segurança.

Conforme Pfleeger e Pfleeger (2011), muitas formas de medidas protetivas estão à disposição dos usuários. Algumas são caras e mais difíceis de implementar e utilizar, enquanto outras possuem um custo menor e são mais simples. Independente disso, a escolha desse critério irá depender da situação e do que desejasse proteger. Fechaduras, cercas e paredes são exemplos de tipos de proteções físicas, que têm

como objetivo impossibilitar ataques que buscam acesso físico a recursos. Outra classe é a de proteções administrativas ou processuais, que aconselham ações de pessoas por meio de contratos, políticas, direitos autorais, acordos, procedimentos, regulamentos, diretrizes, leis, entre outros. Proteções técnicas buscam evitar ameaças relacionadas à tecnologia por meio de protocolos de redes, sistemas de detecção de intrusão, *firewalls*, senhas, etc.

A criptografia é mais uma das medidas de segurança que podem ser utilizadas pelas organizações, De acordo com Nakamura e De Geus (2007), ela possui um importante papel na segurança computacional, pois é responsável por permitir trocas seguras de mensagens e informações pela rede. Portanto, ela também é de fundamental importância para a segurança das organizações e dos usuários. A criptografia utiliza algoritmos baseados em funções matemáticas para disfarçar mensagens, tornando-as ilegíveis. Denominada de encriptação, esta ação transforma o texto claro em um texto cifrado, de forma que o usuário só volta a possuir a mensagem em sua forma original após o processo de decriptação.

Buscando possuir domínio sobre o acesso, a medida preventiva de controles de acesso realiza uma espécie de fiscalização, na qual primeiramente existe um processo de identificação, que de acordo com Rezende (1998), é onde o usuário irá convencer ao sistema ou ao órgão responsável por esse controle de quem ele é. Por exemplo, utilizando um nome de usuário, um e-mail, etc. Após essa identificação, vem o processo de autenticação, que se trata do usuário provar que ele é exatamente quem ele está dizendo ser, podendo ocorrer através de uma senha, de uma biometria, etc.

A prevenção e a detecção de danos também se encontram entre as medidas de segurança. Declarando que existem algumas formas de se lidar com os danos, Pfleeger e Pfleeger (2011) atribuem uma grande importância na detecção do ataque logo que ele acontece, pois isso permitirá que seja tomada uma reação imediata, desta maneira evitando futuros maiores estragos. Já a prevenção de danos possibilita que as vulnerabilidades sejam eliminadas.

Além da segurança dos dados e informações, a segurança das redes de computadores também está inclusa na segurança da informação e a sua preservação é de fundamental importância. Essa necessidade é maior ainda considerando a expansão da Internet, que aumenta o leque de vulnerabilidades e ataques, trazendo

grandes desafios para serem enfrentados como as infecções por vírus e as invasões *hackers*.

Organizações que trabalham com informações online devem considerar bastante a segurança das redes. Para tal, devem considerar diversas medidas de segurança, entre elas: uma combinação de múltiplas camadas de defesa, o monitoramento de acesso, o uso de *software* antivírus e antimalware, a análise comportamental (que torna capaz a detecção de intrusos enquanto a mesma ocorre), a segurança em nível de aplicativo, etc. Todas essas formas buscam proteger de alguma maneira a usabilidade e a integridade das informações e conexões.

2.2.3 Segurança da informação em Instituições Federais

A segurança da informação e as políticas de segurança da informação são de fundamental importância nas instituições federais. De acordo com o Ministério do Planejamento, Desenvolvimento e Gestão (2019), uma considerável quantidade de informações é utilizada pelas entidades e órgãos da Administração Pública Federal na busca por gerar de maneira eficiente a prestação de serviço público ao cidadão, e da mesma forma utilizando-as também para a tomada estratégica de decisões.

Nesse contexto, o órgão do Ministério do Planejamento, Desenvolvimento e Gestão (2019) indica que na gestão de segurança da informação e comunicações, é importante incluir metas e diretrizes referentes ao assunto na elaboração do plano estratégico de cada elemento e entidade de Administração Pública Federal. Assim, é possível motivar e impulsionar a criação de uma cultura de segurança da informação.

Por meio da Secretaria de Fiscalização de Tecnologia da Informação, o Tribunal de Contas da União (TCU) (2008) proferiu uma situação crítica dos processos de segurança da informação dos órgãos da Administração Pública Federal (APF). De acordo com os dados demonstrados foi possível observar que, dos órgãos que foram pesquisados, 64% não teriam instituído sua Política de Segurança da Informação e Comunicação (PoSIC). A partir disso, é possível identificar a necessidade de informar aos órgãos sobre a Política de Segurança da Informação e Comunicação e sobre a necessidade em aplicar a PoSIC nas instituições.

Então, tendo sido decretada pelo Ministro Chefe do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) (2009), a norma 03/IN01/DSIC/GSIPR possui a finalidade de determinar critérios, diretrizes e procedimentos para a elaboração, divulgação, institucionalização e atualização da PoSIC nas entidades e órgãos da Administração Pública Federal. De acordo com Rios, Teixeira Filho e Rios (2017) nessa norma estão inclusas orientações de possibilidades para elaboração da Política de Segurança da Informação e Comunicação, além também da sugestão de itens a serem contemplados. Entretanto, esta norma é uma recomendação, portanto, a sua implementação não é uma característica apenas de um determinado órgão da APF e isto pode acabar condicionando a uma disseminação de vários modelos diferentes de PoSIC, o que acarreta na necessidade de um cuidado redobrado na criação do documento para um segmento específico da Administração Pública Federal.

Rios, Teixeira Filho e Rios (2017) relatam que mesmo com trabalhos do governo federal que acarretem na implantação de Política de Segurança da Informação e Comunicação, algumas Instituições Federais do Ensino Superior (IFES) ainda não dispõem esse documento em caráter institucionalizado. Conforme o Tribunal de Contas da União (2015) das 98 Instituições Federais do Ensino Superior que participaram do Levantamento de Governança de TI que foi realizado pela Secretaria de Fiscalização de Tecnologia da Informação, apenas 47 dessas instituições afirmaram possuir a PoSIC, porém, somente 34 instituições alegaram a utilização de maneira integral. Todavia, 13 instituições declararam estar ainda na fase de finalização, enquanto outras 51 instituições afirmaram não dispor ainda de uma PoSIC.

As organizações precisam ser conduzidas para a composição e implantação de uma PoSIC no processo de segurança da informação, assim, devem descrever os métodos que são indispensáveis para a proteção de seus recursos de informação contra a exposição inadequada (sendo ela intencional ou não), a destruição não autorizada, a modificação não desejada ou a negação de serviço.

De acordo com o Decreto 3.505/2000 (2000), a própria Constituição Federal estabelece o uso de Política de Segurança da Informação e Comunicação nas entidades e órgãos da Administração Pública Federal. Tal qual Araújo (2012), o Brasil não possui apenas uma Lei que atue sobre a segurança da informação, contudo, no

grupo de sua legislação, é possível que diversas sejam aplicadas buscando preservar a segurança dos seus ativos nos órgãos da Administração Pública Federal.

A Administração Pública Federal, através dos seus diversos instrumentos normativos, vem mostrando a sua precaução quando se trata da segurança da informação. A lei 8.159/1991, por exemplo, afirma que é obrigação do poder público tratar da gestão documental e especialmente da preservação dos documentos de arquivos, como utensílio de suporte à cultura, à administração, ao desenvolvimento científico. O Decreto de número 4.553/2002 é mais um exemplo, já que o mesmo trata da garantia de proteção das informações, dos documentos, dos dados e dos materiais sigilosos relevantes da segurança do Estado e da sociedade no âmbito da Administração Pública Federal.

O Decreto 3.505/2000 (2000) foi estabelecido pelo governo federal brasileiro em 13 de junho de 2000, graças a preocupação do próprio governo em conservar a proteção da informação das instituições e organizações vinculadas aos órgãos da Administração Pública Federal. Este decreto tem como objetivo estabelecer a Política de Segurança da Informação nas entidades e órgãos da APF. O mesmo ainda busca eliminar a dependência externa e relação a equipamentos, dispositivos, sistemas e atividades vinculadas à segurança dos sistemas de informação; promover ações necessárias à implementação e manutenção da segurança da informação; estabelecer normas jurídicas necessárias à efetiva implementação da SI; promover a capacitação de recursos humanos para o desenvolvimento de competência científico tecnológica em segurança da informação. Além disto, o decreto ainda preza pelas diretrizes, princípios e regras gerais são os deveres de uma Política de Segurança da Informação e Comunicação e a mesma precisa ser institucionalizada para ser aplicada em todo o órgão.

3. A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA UFERSA

Como uma instituição pública federal de ensino superior brasileira, a Universidade Federal Rural do Semi-Árido teve início a partir da Prefeitura Municipal de Mossoró-RN, que proporcionou a criação da Escola Superior de Agricultura de Mossoró (ESAM) através do Decreto 03/67, de 18 de abril de 1967. A mesma foi inaugurada no dia 22 de dezembro de 1967 e teve como seu mantenedor o Instituto Nacional de Desenvolvimento Agrário (INDA). Em 1969, a instituição foi incorporada como autarquia em regime especial à Rede Federal de Ensino Superior por meio do Decreto 1036, de 21 de outubro de 1969. Por intermédio da Lei Nº 11.155, que foi publicada no dia 1º de agosto de 2005, a instituição passou a figurar como Universidade.

A UFERSA possui quatro campi, que são localizados nas cidades de Mossoró, Angicos, Pau dos Ferros e Caraúbas. A reitoria está localizada na cidade de Mossoró, onde fica o campus sede. Atualmente a instituição oferta cursos de graduação, pós-graduação e de Ensino a Distância (EaD). Tendo 26 cursos de pós-graduação disponíveis, entre eles: pós-graduação em ciência da computação, em engenharia elétrica, em produção animal, em direito, em ecologia e conservação, em ciência e engenharia de materiais, entre outros. Para o EaD, são oferecidos 4 tipos diferentes de cursos, são eles: licenciatura em matemática, licenciatura em computação, licenciatura em física e licenciatura em química. Quanto aos cursos de graduação, na unidade de Mossoró estão disponíveis 22 tipos de cursos, entre eles: ciência e tecnologia, administração, agronomia, ciência da computação, engenharia florestal, medicina, engenharia de petróleo, ciências contábeis, direito, biotecnologia, etc. No campus de Angicos, há 6 tipos de cursos de graduação, como por exemplo: sistemas de informação, engenharia civil, pedagogia, dentre outros. No campus de Caraúbas existem 7 cursos, alguns deles são: letras inglês, engenharia mecânica, letras português, letras libras e outros. E por fim, no campus de Pau dos Ferros também são ofertados 7 cursos de graduação como, por exemplo: arquitetura e urbanismo, engenharia ambiental sanitária, engenharia de software, tecnologia da informação, etc.

A UFERSA é uma instituição de grande importância para o estado do Rio Grande do Norte. Tendo sido eleita a sétima melhor universidade do país e a segunda

melhor universidade do Rio Grande do Norte no ano de 2011 pelo MEC, a mesma, destaca-se pela qualidade do ensino que oferta.

Tal qual outras instituições federais, a UFERSA faz uso de sistemas de informações para conduzir suas atividades. Em seus sistemas, opera com dados que envolvem uma grande quantidade de servidores e alunos. Assim, é de grande importância adotar políticas de segurança da informação.

Nesse trabalho, objetivou-se realizar um estudo sobre a política de segurança da informação da UFERSA, a fim de identificar desde diretrizes de alto nível até os procedimentos e operações adotadas no dia a dia. Para tal, foi empregada uma pesquisa descritiva. Como indica Gil (2010), este tipo de pesquisa envolve levantamento bibliográfico, estudo de experiências práticas com o estudo de caso pesquisado e análise de exemplos que estimulem a compreensão. A identificação da política de segurança da UFERSA se deu considerando dois olhares: pelas informações disponibilizadas pela instituição por meio de sua página oficial na Internet e pelo setor da instituição responsável por manter a política de segurança da informação.

3.1 Política de segurança da informação da UFERSA conforme o Conselho Universitário

A Política de Segurança da Informação e Comunicação da Universidade Federal Rural do Semi-Árido foi estabelecida pelo Conselho Universitário (CONSUNI) (2017) através da Resolução CONSUNI/UFERSA 015/2017, de 15 de dezembro de 2017. Para a criação do documento, levou-se em consideração a legislação, as normas vigentes no país e os seus regulamentos.

A política de segurança da informação da Universidade Federal Rural do Semi-Árido possui 4 princípios, são eles:

- Que as regras de proteção dos ativos de informação e comunicação sejam concisas, precisas e de fácil entendimento;
- Que haja clareza no trato da informação;

- Que seja assegurado o direito coletivo e pessoal à particularidade e a confidencialidade da correspondência e das comunicações restritas, sem que apresente comprometimento dos ativos de informação e comunicação;
- Que seja assegurada a segurança dos dados, informações e conhecimentos sigilosos produzidos na UFERSA.

A política de segurança da informação da UFERSA é dividida entre diretrizes e estratégias gerais, tratamento dos ativos, controle de acesso, auditoria e conformidade, gestão de continuidade, gestão de risco, competências e responsabilidades, penalidades e composição e atualização.

As diretrizes e estratégias gerais afirmam que todos os ativos de comunicação e informação precisam ser protegidos e são classificados como parte do patrimônio da UFERSA. Para a proteção dos ativos de informação e comunicação da UFERSA é estabelecido que a universidade deve implementar estratégias de recuperação de incidentes, sejam acidentais ou propositais. É estabelecido também que deve haver o tratamento e a classificação das informações que estão presentes nos ativos de comunicação e informação da UFERSA conforme o seu respectivo grau de sigilo, sendo as normas, regras e padrões de segurança estabelecidos os mesmos para todos os setores da Instituição. Essa diretriz ainda indica que ativos de informação e comunicação podem ser submetidos a auditoria e monitoração, de modo que os registros que foram obtidos nesses processos poderão ser manuseados para identificação de violações.

No o tratamento dos ativos, a PoSIC da UFERSA determina que é preciso levar em conta 3 aspectos, são eles: que é necessário que todo ativo custodiado ou de propriedade da universidade seja inventariado e assegurado de acordo com as diretrizes determinadas nesta política e nas demais regulamentações em vigor; que todo ativo de informação custodiado ou de propriedade da universidade necessitará ser classificado, de forma implícita ou explícita, em relação aos aspectos de disponibilidade, autenticidade, integridade, confidencialidade e não-repúdio; e que todo ativo custodiado ou de propriedade da instituição só poderá ser cedido por intermédio de uma autorização formal.

No tocante ao controle de acesso, é preciso garantir o controle do acesso físico e lógico aos ativos. Para tal, a política de segurança determina que devem ser considerados quatro aspectos:

- O uso dos ativos necessitará ser consentido pelo gestor imediato do solicitante, através de uma solicitação a repartição responsável pelo ativo;
- É indispensável que toda a utilização dos ativos seja monitorada e limitada ao mínimo que será preciso para a realização das atividades de cada usuário;
- Sempre que acontecer a mudança de atribuições, admissão ou desligamento de servidor da universidade, a chefia imediata referente terá a responsabilidade de realizar uma notificação a repartição responsável pelos ativos que foram usados pelo membro. A repartição encarregada pelos ativos terá que providenciar os ajustes que forem precisos dos privilégios de acesso, do respectivo servidor e aos ativos em questão;
- Todo o ambiente precisa ser classificado e protegido através de medidas adequadas de segurança conforme o sigilo dos ativos que são armazenados no local e a sua criticidade.

Já para a auditoria e conformidade, a política de segurança da informação considera que quando possível, a utilização de todo ativo deverá produzir trilhas de auditoria que precisarão ser guardadas para efeito de análise baseada nas diretrizes relatadas nesta política e as demais regulamentações em vigor; e que o uso de todo ativo estará sujeito a auditoria e monitoramento de modo que, quando possível, deverá ser examinado em procura de indícios de descumprimento desta política e das demais regulamentações que estejam em vigor.

Com relação a gestão de continuidade, estão inclusos treinamentos, testes, backup, plano de contingência e a documentação de procedimentos. Para esta parte, é preciso considerar 5 aspectos:

- Deverá ser definida a gestão de continuidade no ambiente da UFERSA, com o propósito de diminuir os impactos de falhas acidentais dos ativos que suportam as operações da universidade;
- É preciso determinar um plano de contingência para o restabelecimento dos procedimentos críticos que foram suspensos por falhas;

- Todo ativo, eletrônico ou não, deve ser armazenado de forma segura e adequada;
- Deve haver uma cópia de segurança para todo ativo eletrônico de informação e comunicação da instituição;
- É necessário que toda cópia de segurança seja conservada, sempre que possível, em um local considerado seguro e diferente do local onde está localizado o respectivo ativo de informação.

A gestão de risco envolve o inventariamento dos ativos, avaliação, tratamento, análise, comunicação, aceitação e monitoramento dos riscos. Para tal, são considerados três aspectos: deverão ser avaliados e, caso seja possível, minimizados os riscos relacionados aos ativos; toda ação de segurança da informação precisará ser realizada segundo a avaliação da criticidade dos ativos; e deverá haver o acatamento da legislação vigente na universidade em toda ação de segurança da informação.

No que tange a competências e responsabilidade, a política de segurança da instituição diz que a segurança da informação juntamente com as suas posturas, hábitos, responsabilidades, éticas e cuidados com os ativos de informação, também serão responsabilidade de cada usuário e de todas as repartições da UFERSA e não somente de profissionais e/ou da área de tecnologia da informação e comunicação. Na ocorrência de qualquer transgressão da política de segurança da informação, deve-se realizar notificação a Superintendência de Tecnologia da Informação e Comunicação (SUTIC), repartição principal de execução e averiguação da PoSIC da UFERSA. No caso de recursos a algum julgamento de infrações da PoSIC, a responsabilidade da entidade recursal é o CONSUNI.

Relacionado as penalidades, a política da UFERSA diz que a violação ou o descumprimento da mesma e dos demais procedimentos e normas definidas referentes a ela, acarretará em penalidades, obedecidos aos ritos legais e em conformidade com o regimento geral da instituição. Visto que a violação reflita como afronta à legislação vigente no país, definindo contravenção ou crime, é imposto que a administração superior realize as providências necessárias para que se cumpram as leis.

Por fim, em relação a composição e atualização da PoSIC, é estabelecido que a política é composta além da Resolução CONSUNI/UFERSA Nº 015/2017, das demais normas, portarias, instruções, decisões, regulamentações e outros documentos legalmente elaborados a que ela se concerne, homologados ou emitidos pelo CONSUNI. A política deve ser revisada quando houver necessidade, ou no mínimo, de 3 em 3 anos.

As principais diretrizes da Política de Segurança da Informação e Comunicação da Universidade Federal Rural do Semi-Árido, de forma resumida, são apresentadas no Quadro 1.

Quadro 1 – Principais diretrizes da PoSIC da UFERSA

PRINCÍPIOS	• **Fácil entendimento** das regras de segurança; • **Transparência** no trato da informação; • **Garantia** ao sigilo da correspondência; • **Proteção** de dados.
DIRETRIZES E ESTRATÉGIAS GERAIS	• Informações são **patrimônios**; • Estratégias de **recuperação**; • **Classificação e tratamento** das informações; • **Normas e padrões de segurança** gerais; • Informações são sujeitas a **monitoria e auditoria**.
TRATAMENTO DOS ATIVOS	• **Asseguração** dos ativos de acordo com as diretrizes; • **Classificação** segundo a Tríade CID; • Ativos **cedidos** somente sob autorização.
CONTROLE DE ACESSO	• **Autorização** do uso dos ativos pelo setor; • **Controle** do uso dos ativos; • **Admissão, mudança das atribuições, desligamento de servidor** são responsabilidades da chefia; • **Mecanismos de segurança**.
AUDITORIA E CONFORMIDADE	• **Trilhas de auditoria** devem ser geradas; • **Análise** da utilização dos ativos.
GESTÃO DE CONTINUIDADE	• Objetiva minimizar **impacto de falha**; • **Plano de contingência**; • **Salvaguarda** de ativos armazenados; • **Cópia de segurança** para ativos eletrônicos; • **Locais diferentes** para armazenamento da cópia de segurança.

GESTÃO DE RISCO	• **Minimização de riscos**; • **Respeito a legislação vigente** na instituição.
COMPETÊNCIAS E RESPONSABILIDADES	• A **responsabilidade** com os ativos é dever de todos os usuários e setores da instituição; • **Comunicação** de incidentes e **identificação** de ameaças aos setores da SUTIC, CGTI e CGD; • **Suprimentos de recursos** para a SUTIC; • **A sugestão de instrumentos e o julgamento de infrações** deverão ser realizados pelo CGTI E CGD; • O CONSUNI é a entidade que orienta ao **julgamento de infrações**.
PENALIDADES	Penalidades serão aplicadas caso haja o **descumprimento ou violação** da PoSIC.
COMPOSIÇÃO E ATUALIZAÇÃO	A **revisão** desta política deverá ocorrer sempre que necessário, ou no mínimo, a cada 3 anos.

Fonte: Autoria Própria

3.2 Política de segurança da informação da UFERSA conforme Superintendência de Tecnologia da Informação e Comunicação

A política de segurança da informação da UFERSA, estabelecida pela CONSUNI, estabelece diretrizes abrangentes, sem muitos detalhes de quais procedimentos adotar no dia a dia da instituição. Diante desse contexto, para compreender ainda mais como é mantida a política de segurança de informação da instituição, foi realizada uma entrevista com o responsável da Superintendência de Tecnologia da Informação e Comunicação, o servidor Kleber Jacinto, Diretor de Segurança da Informação. A SUTIC é a unidade administrativa vinculada à Reitoria responsável por implantar, planejar e manter as atividades relacionadas à Tecnologia da Informação e Comunicação da UFERSA.

No primeiro questionamento da entrevista foi perguntado acerca da importância da política de segurança da informação para UFERSA. Como resposta, foi explicado pelo servidor era necessário considerar dois aspectos, são eles: o institucional e o da comunidade. Do ponto de vista institucional, ele explica que a universidade entende sim a importância e a necessidade da política de segurança da informação. Relata

que, inclusive, a universidade já entendia essa importância desde o tempo em que dados eram guardados apenas em papel, logo, a segurança já é algo que orgânico na instituição.

Uma vez que a informação transita em algum momento nos computadores em praticamente todos os serviços que a universidade oferece a comunidade, o servidor relata que é essencial manter uma boa relação de segurança com esses dados e informações e também é de extrema importância para que assim sejam minimizados os riscos de que, por exemplo, alguns desses dados acabem extrapolando os muros da universidade, o que não seria do interesse de ninguém.

Já em relação ao aspecto da comunidade, ele diz que tem certeza de que a comunidade inteira não tem ciência da importância da política de segurança da informação.

Na sequência, o servidor foi indagado a respeito de como a instituição lidava com a segurança da informação no período de 2005 a 2017, já que somente em 15 de dezembro de 2017 foi estabelecida a PoSIC através da Resolução CONSUNI/UFERSA Nº 015/2017. O servidor relatou que a política de segurança é a formalização de um conjunto de boas práticas e recomendações legais, logo, é um documento formalizado. Ele fala que apesar do fato da política só ter sido colocada no papel recentemente, as boas práticas de segurança já vinham sendo seguidas pela instituição desde sempre. Então, o fato de não existir esse documento antes de 2017 não significa que a UFERSA já não utilizava dessas boas práticas de segurança antes. A diferença é somente que antes essas boas práticas não eram documentadas, porém sempre existiram.

Na terceira pergunta, foi questionado quais as práticas que a UFERSA adota para garantir a segurança dos ativos de informação e comunicação da instituição. O entrevistado explicou que não faz sentido adotar uma política que seja tecnicamente correta, mas que não seja aderente a vida do usuário. Então, na busca pela agregação destas coisas, a universidade vem adotando algumas práticas de gestão, em especial, de catalogação específica de equipamentos, instalação de softwares de monitoramento e outras ações deste tipo.

Na sequência, foi questionado a respeito de quais procedimentos são adotados pela UFERSA para garantir a recuperação de informações na ocorrência de incidentes. O servidor explicou que hoje há uma política de backup na universidade que é o principal mecanismo utilizado para a recuperação de dados, em que há

backups de hardware e software. Ele exemplifica dizendo que a instituição possui cópias do mesmo hardware onde hoje funcionam os sistemas acadêmico, então, se por acaso o servidor onde está sendo utilizado o sistema acadêmico parar, eles possuem plena condição de migrar para outro hardware sem nenhum problema. O servidor explicou ainda que no caso da ocorrência de uma ação ainda mais catastrófica, como por exemplo, um incêndio na central de dados, eles possuem um backup externo dos mesmos dados em outro local separado. O servidor acrescentou ainda que a universidade está em fase de testes para a migração de alguns desses locais externos para os campi do interior, para que deste modo, possam ter o mesmo backup do campus central também nos campi do interior.

O quinto questionamento feito refere-se à determinação na PoSIC da UFERSA da utilização de classificação dos aspectos de confidencialidade, integridade, autenticidade e disponibilidade, indagando de qual maneira é adotada essa classificação nos processos de segurança da instituição. O sr. Kleber Jacinto relatou que este artigo é baseado no normativo anterior que se trata da classificação de informações que foi implementado pela Política de Informação ao Cidadão, criada entre 2012 e 2013. Então, esta classificação foi feita pela PoSIC, porém ela está de acordo com os parâmetros que foram anteriormente descritos. Logo, aquilo que é tido como confidencial, é respeitado pela PoSIC sem ter o seu conceito alterado.

No sexto questionamento foi perguntado a respeito de quais práticas a UFERSA adota para buscar garantir o controle físico e lógico dos seus ativos. Foi explicado pelo servidor que o físico e o lógico tratam-se de dois “mundos” bem diferentes. Ele diz que, no físico, está incluso desde a funcionária responsável pela limpeza trancar a sala até ter câmeras de segurança em todo o perímetro da universidade, com uma empresa de segurança ativa, que passa mensagens e vistoria. Nesse contexto ainda há elementos mais relacionados diretamente a TI como, por exemplo, a utilização de equipamentos com cabo de aço que possuem presilhas ou de equipamentos configuráveis fora da instituição ou fora da rede da instituição. Do ponto de vista físico, o servidor relata que a UFERSA já dispõe de tudo que foi listado.

Já do ponto de vista lógico, há um outro cenário completamente diferente. Além dos backups que a instituição possui, o servidor relata que a instituição possui também políticas de senhas fortes para os usuários, políticas de separação de dados que usuários podem acessar e dados que não devem ser acessados por ninguém até mesmo em sistemas que são coletivos, como por exemplo, o acadêmico. Por exemplo,

embora docentes e discentes tenham acesso ao mesmo núcleo de dados, através de senhas e perfis diferentes são disponibilizados acessos diferentes. Então, do ponto de vista lógico, existe uma série de outras infraestruturas que permitem claramente que ocorra essa separação, assim, buscando dentro do possível, garantir que esses dados não vão ser fragilizados de alguma maneira.

Em seguida, o servidor foi indagado a respeito da utilização de auditorias, se desde a implementação da PoSIC da UFERSA já ocorreu a necessidade de alguma auditoria e se sim, qual a motivação do processo e quais os resultados. O servidor relatou que não poderia dizer o que motivou, pelo fato de que muitas dessas auditorias são sigilosas, mas disse que sim, já houveram diversas. Ele informou que algumas auditorias possuíram motivos autênticos, enquanto outras não têm uma motivação direta. Por exemplo, se a suspeita que houve alguma tentativa de acesso a conta de um docente ou se alguém tentou roubar a senha de algum docente é possível realizar uma auditoria. No que se refere aos resultados, o sr. Kleber Jacinto explanou que alguns desses procedimentos são meramente de controle interno. Por exemplo, se um usuário teve a senha roubada, ele entende que o sistema foi utilizado por alguma outra pessoa de maneira indevida. Portanto, será aberto um processo administrativo e o relatório de auditoria estará contido neste processo dizendo se houve um mal-uso ou não do sistema. A partir disso é que serão tomadas as decisões com base nas normas da instituição e as leis do país.

Na oitava pergunta foi questionado se a UFERSA dispõe de um plano de contingência no caso de ocorrer algum incidente e se sim, o que esse plano determina de modo geral. O entrevistado explanou que para a existência de um plano de contingência existe um nível de formalização e que hoje a universidade não dispõe desta formalização. Para 2019, a SUTIC tem como meta formalizar um plano de contingência.

O servidor acrescenta que, embora não se tenha um plano de contingência, há boas práticas que são adotadas. Ele relata que já houveram algumas situações onde foi preciso acionar essas boas práticas como, por exemplo, em falta de energia por 72 horas ou queima do condicionador de ar do datacenter. O sr. Kleber Jacinto explica que o principal elemento dessas boas práticas é ter profissionais que dentro das suas atribuições já sabem o que fazer nesse tipo de situação. Outro ponto importante é contar com os elementos de backup: de dados, de hardware, de software, de rede. Desta maneira, os profissionais acionam esses elementos de backup quando

necessário. Então, os profissionais e os elementos de backup são os dois principais fundamentos da forma que UFERSA tem de responder a qualquer incidente de grande porte.

Posteriormente foi questionado a respeito de uma das medidas de segurança que está determinada na PoSIC da UFERSA que é a de ter cópias de dados mantidas em local diferente de onde se encontra o ativo de informação. Assim, perguntou-se se a universidade conseguiu implementar essa medida e de que maneira foi feito isso. O servidor explicou que hoje, além do datacenter da instituição que possui vários discos, existem também backups dentro do próprio data center. Desta maneira, tem-se um banco de dados em produção e tem mais uma cópia desse banco. Além disso, também há cópias externas desse banco em datacenters isolados no campus. Então, hoje a instituição já tem e implementa esses backups externos. Ele disse ainda que a meta para 2019 é levar essa mesma prática para pelo menos um dos campi do interior.

O décimo questionamento feito refere-se ao conhecimento dos usuários em relação a política de segurança da informação da UFERSA. Foi perguntado se a universidade promove treinamentos quanto a sua política de segurança e de que maneira a mesma é divulgada. Quando questionado sobre, o Sr. Kleber Jacinto explanou que ainda não houve a necessidade de tratamentos formais, como por exemplo, a elaboração de um curso sobre a PoSIC da instituição. Ele relatou que o que é feito é uma conversa com os setores quando necessário. Porém, o mesmo explana que a medida em que as normas operacionais do dia a dia forem surgindo, é possível que eles precisem implementar outras técnicas para fazer com que essa informação chegue mais diretamente a todos os setores.

Na décima primeira questão foi perguntado a respeito dos ataques maliciosos, se a UFERSA já sofreu algum ataque contra os seus ativos e caso sim, foi pedido para relatar algum. Foi explicitado pelo Diretor de Segurança da Informação da SUTIC que a universidade sofre diversas tentativas de ataques por dia. O mesmo disse que hoje, todas as universidades do Brasil, até mesmo as mais distantes, contam com links tecnicamente muito bons, estáveis e com uma grande largura de banda e isso acaba tornando as universidades bastantes visadas, ou seja, uma espécie de alvo entre os *hackers.* Ele exemplifica dizendo que o link da UFERSA campus Mossoró possui 1GB de banda e, por isso, torna-se atrativo para um *hacker* que ao possuir domínio sobre algumas máquinas de dentro da instituição pode utilizar essa banda para tarefas que

lhe beneficiem. Há ainda o fator de que, para alguns, invadir uma universidade é motivo de status dentro de suas comunidades.

Ainda sobre essa questão, o Sr. Kleber Jacinto disse que já houveram situações em que usuários maliciosos obtiveram sucesso em suas tentativas. Por exemplo, a universidade já foi atingida tendo o serviço de e-mail de um servidor sido utilizado para enviar spans. Não houve nenhum comprometimento de dados institucionais, pois a máquina utilizada não os continha. Porém, o invasor causou problemas para a universidade pois o spam partia de um IP da instituição e, quando os servidores internacionais de e-mail começam a verificar a quem pertencia este IP, eles começaram a bloquear coisas do domínio dele, no caso, a UFERSA. O servidor relata ainda que a última ocorrência de ataque malicioso bem-sucedido foi entre 2015 e 2016, antes da implantação da PoSIC da UFERSA.

No décimo segundo questionamento foi indagado a respeito das medidas de correções adotadas na ocorrência de ataques maliciosos e dos prejuízos que foram causados a instituição por causa deles. O Diretor de Segurança da Informação relatou que até então não houve nenhum prejuízo relacionado a dano de dados, dano de hardware e coisas desse tipo que são a principal preocupação da universidade. Porém, alguns desses ataques acarretaram em um prejuízo de imagem para a instituição. Já em relação as correções adotadas, a universidade disponibiliza de uma equipe de resposta a incidentes de segurança, a mesma dispõe das boas práticas, porém ainda não foi formalizada e a formalização desta equipe é também meta para o ano de 2019.

Na pergunta seguinte foi questionado se na UFERSA ocorre incidentes não maliciosos, que são causados devido a descuido ou falta de conhecimento do usuário. Sobre isto, o entrevistado explanou que qualquer sistema que lide com pessoas está sujeito a este tipo de acontecimento e que muitas vezes o usuário faz algo sem entender os impactos que aquela ação pode vir a causar no sistema ou na instituição. Ele relata ainda que embora a SUTIC possua o amparo técnico e legal para indicar uma punição ao usuário, eles geralmente não fazem isso por realmente entender que a pessoa não agiu de má fé.

Na sequência foi questionado se a UFERSA dispõe de estatísticas relativas a segurança da informação, o que elas indicam e quais as medidas tomadas com base nelas. O Sr. Kleber Jacinto declarou que a universidade não dispõe de estatísticas formais e nem de um relatório específico para isso. Entretanto, possui uma série de

indicadores do dia a dia, como gráficos dos últimos 6 meses, gráficos de tráfegos, estatísticas de tráfegos, estatísticas de uso dos sistemas, entre outros.

Por fim, foi perguntado ao entrevistado o que ele achava que deveria ser melhorado na política de segurança da informação da UFERSA. O mesmo explanou que a mudança mais significativa a ser feita hoje na PoSIC da UFERSA seria que o CONSUNI concedesse a um outro setor ou a uma outra entidade o poder de aprovação das normas. O servidor explica, dizendo que algumas normas que necessitam de aprovação, são normas operacionais e normas do dia a dia, portanto, são documentos que deveriam ser estudados e publicados com muita agilidade e o fato de incluir este documento na pauta do Conselho Universitário acaba fazendo com que seja perdida essa agilidade. Tendo em vista que o CONSUNI tem uma agenda bastante lotada, a aprovação de uma norma pelo mesmo leva em média de 1 ano e meio a 2 anos. O Diretor de Segurança da Informação da SUTIC ressalta ainda que o Comitê de Governança Digital tem decisões tão importantes a tomar quanto o CONSUNI, logo, conceder o poder de aprovação a este setor, por exemplo, tornaria tudo muito mais ágil, já que o mesmo se reúne com mais frequência, tem uma agenda menos lotada e uma maior disponibilidade dos seus membros.

4 CONSIDERAÇÕES FINAIS

Ao estudarmos política de segurança da informação, percebemos que o tema é de bastante relevância dentro do âmbito atual em que se encontram as tecnologias. Observamos que a aplicação da mesma pode acarretar em vantagens para as entidades e organizações pois, desta maneira, será possível obter uma segurança maior relacionada aos seus ativos de informação. A PoSIC busca, por intermédio das suas orientações, proteger a confidencialidade, a integridade e a disponibilidade das informações, tanto através de medidas de segurança e orientações elaboradas de acordo com as necessidades da organização, como por meio da implementação de orientações baseadas em leis e normas governamentais. Mediante os benefícios que a PoSIC traz, é possível diminuir bastante as vulnerabilidades e as ameaças ao qual softwares, sistemas e ativos de informação são expostos diariamente.

A política de segurança da informação é de fundamental importância nos mais variados âmbitos e nas instituições de ensino superior não seria diferente, já que as mesmas adotaram os sistemas de informação e lidam diariamente com diversos dados. Sabendo disso, a pesquisa realizada buscou identificar desde as estratégias gerais de segurança até a implementação de procedimentos em relação a política de segurança da informação da Universidade Federal Rural do Semi-Árido.

O presente trabalho contou com uma pesquisa descritiva, com estudo e a análise das informações que estão disponíveis ao público, por meio de página oficial na Internet, sobre a PoSIC da instituição e com a realização de uma entrevista com o Sr. Kleber Jacinto, Diretor de Segurança da Informação da SUTIC, para identificar a Política de Segurança da Informação da UFERSA.

Através do estudo realizado neste trabalho foi possívei perceber que Universidade Federal Rural do Semi-Árido ainda precisa melhorar a sua PoSIC em alguns aspectos, como por exemplo, no aspecto da formalização, já que a mesma possui alguns planos que atualmente são realizados somente através das boas práticas e que ainda não são documentados. Entretanto, é visível os benefícios que a implantação da Política de Segurança da Informação e Comunicação trouxe para a instituição, entre eles, a redução de ataques maliciosos, medidas de contingência na ocorrência de ataques e a efetivação de algumas medidas de segurança.

Portanto, o estudo realizado neste trabalho demonstrou a importância da informação no âmbito tecnológico, a relevância da segurança da informação e das políticas de segurança da informação e o valioso benefício que a PoSIC pode trazer para as organizações através da sua implantação.

4.1 Trabalhos futuros

A Política de Segurança da Informação e Comunicação da UFERSA possui suas normas e diretrizes, que determinam o que pode ou não ser feito na instituição no que se refere a segurança. Dessa forma, sendo um documento orientador para a instituição. No decorrer deste trabalho, foram identificadas questões que podem melhorar o estudo realizado e, portanto, são consideradas como possíveis trabalhos futuros. São elas:

- Realizar um trabalho que ressalte a importância de retirar a responsabilidade de aprovação das normas de cima do CONSUNI na resolução CONSUNI/UFERSA 015/2017 e mostrar a praticidade que a resolução obteria ao passar essa responsabilidade de aprovação para um outro setor, como por exemplo, o Comitê de Governança Digital;
- Verificar a Política de Segurança da Informação e Comunicação da UFERSA do ponto de vista dos usuários, afim de identificar vulnerabilidades;

REFERÊNCIAS

ARAÚJO, Wagner Junqueira de. Leis, decretos e normas sobre Gestão da Segurança da Informação nos órgãos da Administração Pública Federal. **Informação & Sociedade: Estudos**, v. 22, 2012.

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT) – **Tecnologia da Informação - Código de Prática para Gestão da Segurança da Informação: NBR ISO/IEC 17799:2005** Rio de Janeiro: ABNT, 2005.

BASTA, A.; BASTA, N.; BROWN, M. **Segurança de computadores e teste de invasão.** 2. ed. São Paulo: Cengage Learning, 2014.

CONSELHO UNIVERSITÁRIO. Política de segurança da informação e comunicação. **Consuni/UFERSA,** 15 dez. 2017. Disponível em: <https://documentos.ufersa.edu.br/wp-content/uploads/sites/79/2018/01/RESOLUCAO_CONSUNI_015_2017-1.pdf>. Acessado em: 21 fev. 2019.

Decreto nº 3.505 de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Casa Civil, Subchefia para Assuntos Jurídicos, 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm>. Acessado em 21 fev. 2019.

Estatística dos índices reportados ao cert.br. **Cert.br**, jan./dez. 2017. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 11 fev. 2019.

FONTES, Edison. **Políticas e normas para segurança da informação**. Rio de janeiro: Brasport, 2012.

FONTES, Edison Luiz Gonçalves. **Segurança da informação**. Editora Saraiva, 2017.

GIL, A. C. **Como Elaborar Projetos de Pesquisa.** 5. ed. São Paulo: Atlas, 2010.

GUIMARAES, Alexandre Guedes; LINS, Rafael Dueire; DA OLIVEIRA, Raimundo Correa. **Segurança em Redes Privadas Virtuais-VPNs**. Brasport, 2006.

GUSMÃO, G. **As 17 maiores falhas de segurança de 2014.** Exame Abril. 2014. Disponível em: <https://exame.abril.com.br/tecnologia/as-17-maiores-falhas-de-seguranca-de-2014/>. Acesso em: 04 de fev. 2019.

HOWARD, J. D. **An analysis of security incidents on the internet: 1989-1995**. 1997. Tese de Doutorado – Carnegie Mellon University, Pittsburgh, Pennsylvania, EUA.

Incidentes reportados ao cert.br. **Cert.br**, jan./dez. 2017. Disponível em: <https://www.cert.br/stats/incidentes/2017-jan-dec/tipos-ataque.html>. Acesso em: 11 fev. 2019.

JESSEN, K. S.; HOEPERS, C. **A Evolução dos Problemas de Segurança e Formas de Proteção.** Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. 2005. Disponível em: <https://www.cert.br/docs/palestras/certbr-usp2005.pdf>. Acesso em 05 de fev. 2019.

LANDIM, W. **Os 12 principais incidentes com segurança da informação em 2014.** TecMundo. 2015. Disponível em: <https://www.tecmundo.com.br/seguranca/73110-12-principais-incidentes-seguranca-informacao-2014.htm>. Acesso em: 06 de fev. 2019.

LIMA, Mariana; TADINI, Giovanna Wolf; CAPELAS, Bruno. Falha de segurança no Facebook atinge 50 milhões de usuários. **Link Estadão**, São Paulo, 29 set. 2018. Disponível em: <https://link.estadao.com.br/noticias/empresas,hackers-vazam-dados-de-50-milhoes-de-usuarios-diz-facebook,70002523613 >. Acesso em: 9 fev. 2019.

LOPES, Isabel Maria. **Adopção de políticas de segurança de sistemas de informação na administração pública local em Portugal**. 2012.

MARCIANO, João Luiz Pereira. **Segurança da informação: uma abordagem social**. 2006. 212 f. Tese (Doutorado em Ciência da Informação) - Universidade de Brasília, Brasília, 2006.

MARTINS, Alaíde Barbosa; SANTOS, Celso Alberto Saibel. Uma Metodologia para implantação de um Sistema de Gestão de Segurança da Informação. **JISTEM-Journal of Information Systems and Technology Management (Online)**, v. 2, n. 2, p. 121-136, 2005.

Ministério da Economia. Governo federal lança nova Política Nacional de Segurança da Informação. **Planejamento, desenvolvimento e gestão**, 28 dez. 2018. Disponível em: <http://www.planejamento.gov.br/noticias/governo-federal-lanca-nova-politica-nacional-de-seguranca-da-informacao>. Acesso em: 1 fev. 2019.

Ministério do Planejamento, Desenvolvimento e Gestão. Segurança da informação. **Governo digital**, 2019. Disponível em: <https://www.governodigital.gov.br/transformacao/compras/orientacoes/seguranca-da-informacao>. Acesso em: 1 fev. 2019.

MONTEIRO, Iná Lúcia Cipriano de Oliveira. **Proposta de um Guia para elaboração de políticas de segurança da informação e comunicação em órgãos da APF**. Dissertação (Mestrado) - Universidade de Brasília. Brasília-DF, 2009.

NAKAMURA, Emilio Tissato; DE GEUS, Paulo Lício. **Segurança de redes em ambientes cooperativos**. Novatec Editora, 2007.

PFLEEGER, C. P.; PFLEEGER, S. L. **Analyzing computer security: a threat / vulnerability / countermeasure approach.** Upper Saddle River, NJ: Prentice Hall, 2011.

Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Norma Complementar nº 03/IN01/DSIC/GSI/PR**. Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. Brasília, DF, GSI/PR, 2009. 5p. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf >. Acessado em: 20 fev. 2019.

REZENDE, Denis Alcides. **Engenharia de Software e Sistemas de Informação**. 3. ed. Rio de Janeiro, Brasport, 2005.

REZENDE, Pedro Antonio Dourado. Criptografia e Segurança na Informática. **Apostila-Capítulos**, v. 1, n. 2, p. 3, 1998.

RIOS, Orlivaldo Kléber Lima; TEIXEIRA FILHO, José Gilson de Almeida; RIOS, Vânia Patrícia da Silva. Gestão de segurança da informação: práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação. **NAVUS-Revista de Gestão e Tecnologia**, v. 7, n. 2, p. 49-65, 2017.

STALLINGS, William; BROWN, Lawrie. **Segurança de computadores: princípios e práticas**. 2014.

TADEU, Erivelton. Educação, o novo alvo preferencial dos cibercriminosos. **Revista ensino superior,** 2 mai. 2018. Disponível em: <http://www.revistaensinosuperior.com.br/informacoes-cibercriminosos/>. Acesso em: 11 fev. 2019.

Tribunal de Contas da União. **Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal**. Brasília: TCU, Secretaria de Fiscalização e Tecnologia da Informação. Sumário Executivo, 2008. 48 p. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2515176.PDF>. Acessado em: 20 fev. 2019.

Tribunal de Contas da União. **Levantamento de Governança de TI 2014**. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2015. 94 p. Disponível em: <http://portal3.tcu.gov.br/portal/pls/portal/docs/2705176.PDF>. Acessado em: 20 fev. 2019.

APÊNDICES

APÊNDICE A – Roteiro para entrevista sobre a política segurança da informação

UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE GRADUAÇÃO
CENTRO MULTIDISCIPLINAR DE ANGICOS
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

Essa entrevista refere-se ao trabalho de conclusão de curso de Roberta Karoline de Souza Bezerra, aluna do curso de Sistemas de Informação da UFERSA – Campus Angicos, cujo o trabalho desenvolvido é “Políticas de Segurança da Informação – Um estudo de caso na Universidade Federal Rural do Semi-Árido”.

1) As políticas de segurança da informação (PoSIC) sempre são veiculadas como fatores de grande importância para uma organização. Qual a importância da política de segurança da informação para a UFERSA?

2) A PoSIC da UFERSA foi estabelecida na Resolução CONSUNI/UFERSA Nº 015/2017, de 15 de dezembro de 2017. No entanto, a UFERSA existe desde o ano de 2005. Como a instituição lidou com a segurança da informação no período de 2005 a 2017?

3) A PoSIC da UFERSA determina que os ativos de informação e comunicação são patrimônios da instituição. De maneira geral, quais práticas a UFERSA adota para garantir a segurança desse patrimônio?

4) No Art 6º da PoSIC é determinado que a instituição deve adotar estratégias para a recuperação da informação, mesmo quando esta for prejudicada por desastres naturais. Quais procedimentos a UFERSA adota para garantir a recuperação de informações na ocorrência de incidentes?

5) A PoSIC da UFERSA indica a utilização de classificação para aspectos de confidencialidade, integridade, autenticidade e disponibilidade. Como funciona essa classificação e como ela é adotada nos procedimentos de segurança da instituição?

6) Quais práticas a UFERSA adota para garantir o controle físico e lógico dos seus ativos?

7) A PoSIC da UFERSA indica o uso de auditorias. Desde sua implementação, já ocorreu necessidade de alguma auditoria? Se sim, o que motivou o processo e quais foram os resultados?

8) A UFERSA dispõe de um plano de contingência no caso de ocorrer algum incidente? Se sim, poderia me explicar, de modo geral, o que esse plano determina?

9) Uma das medidas de segurança determinada na PoSIC da UFERSA é ter cópias de dados mantidas em local diferente de onde se encontra o ativo da informação. A UFERSA conseguiu implementar essa medida? Como?

10) Para que uma política de segurança da informação seja eficaz é importante que todos os usuários a conheçam e adotem. A UFERSA promove treinamentos quanto sua política de segurança? Como ela é divulgada?

11) A UFERSA já sofreu algum tipo de ataque malicioso contra seus ativos? Caso sim, poderia relatar alguns deles?

12) Na ocorrência de ataques maliciosos, quais foram as medidas de correção adotadas? Houve algum prejuízo para a instituição?

13) Na UFERSA ocorre problemas de incidentes não maliciosos, em que o incidente acontece, por exemplo, devido a descuido ou falta de conhecimento do usuário?

14) A UFERSA dispõe de estatísticas relativas à segurança da informação? Se sim, o que elas indicam e quais medidas serão tomadas a partir delas?

15) O que o senhor acha que deveria ser melhorado na política de segurança de informação da UFERSA?

APÊNDICE B – Entrevista com o Diretor de Segurança da Informação da SUTIC

Pergunta: As políticas de segurança da informação (PoSIC) sempre são veiculadas como fatores de grande importância para uma organização. Qual a importância da política de segurança da informação para a UFERSA?

Resposta: *Do ponto de vista da resposta a gente precisa pensar em dois aspectos: aspecto institucional e aspecto da comunidade. Muitas das ações da instituição da UFERSA ou de outra instituição do porte da UFERSA, as vezes elas acontecem ainda que a comunidade não entenda que elas são necessárias, porque a gente tem os pilares do ensino, pesquisa e extensão muito fortes, mas para dar suporte a essas três infraestruturas, a instituição tem uma série de outros serviços atrelados e nesse é que a comunidade enxerga esses outros serviços atrelados. E até nisso a política de segurança é também importante, porque hoje praticamente em todos os serviços que a universidade oferece a comunidade, ela em algum momento transita em computadores. Ou por redes de computadores, ou está armazenado em um computador, ou está lá no computador do restaurante universitário que é o dado que o aluno almoçou e depois é coletado e trazido para a central, ou é o dado de nota acadêmica do aluno, enfim, toda vida acadêmica do aluno no ensino, na pesquisa ou na extensão, está de alguma forma armazenada em computadores e tramita em redes da instituição ou fora da instituição. Se você não manter uma boa relação de segurança com esses elementos, você corre um sério risco de fazer com que alguns desses dados extrapole os muros da universidade, o que não é do interesse de ninguém. Porque que disse que a gente precisa separar isso em duas visões: a instituição ela entende muito bem essa necessidade, porque já entendia que isso era verdade no tempo que era no papel, então já é algo que orgânico, faz parte da instituição ter esse cuidado com o tratamento institucional, mas para quem chega na instituição como aluno passa um período e vai embora, nem sempre há tempo do aluno ter essa visão de que "ah, a instituição realmente tem essa preocupação", isso fica transparente pra ele. E isso é bom, porque se isso fica transparente para o cliente final é porque a gente está fazendo a coisa bem de alguma forma. Então, se toda nossa comunidade tem ciência de que a política é importante? Tenho certeza que não. Seria interessante ter mais campanhas educativas? Sim, a gente vem fazendo isso com alguma frequência. Isso chega a todo mundo? Não tenho certeza. Será que o meu aluno lá da medicina que não tem, em tese, conexão nenhuma com tecnologia,*

ele entende de tal coisa? Ele entende que tal dia o Facebook estava bloqueado ou ele entende porque tal dia ele tentou mandar uma mensagem para mil pessoas e não foi essa mensagem e ele recebeu uma notificação dizendo que não podia, será que ele entendeu a motivação disso? Não sei se ele entendeu, não tenho certeza. A organização, a instituição, ela entende a importância. A comunidade inteira entende a importância? Acho que não, mas recebe os efeitos da instituição ter esse entendimento.

Pergunta: A PoSIC da UFERSA foi estabelecida na Resolução CONSUNI/UFERSA Nº 015/2017, de 15 de dezembro de 2017. No entanto, a UFERSA existe desde o ano de 2005. Como a instituição lidou com a segurança da informação no período de 2005 a 2017?

Resposta: *Na verdade, a política de segurança é a formalização de um conjunto de boas práticas e recomendações legais. É um documento onde a instituição chega e diz: olhe, eu sei que isso é importante, isso é importante para minha comunidade e em virtude disso nós vamos passar a ter como regra. Isso não significa em absoluto, na UFERSA ou em qualquer outro local, de que não haja boas práticas de segurança. Então, se você perguntar a qualquer setor da instituição, a pessoas que trabalham a mais tempo, de 2005 pra cá ou anterior de 2005, e dizer assim "um dado de um aluno que você imprime, você joga em qualquer canto o papel ou você destrói?", a maior parte do setor vai dizer "não, eu destruo." E isso se quer está na nossa política formal, que um documento impresso precisa ser destruído. Mas isso já faz parte da cultura organizacional, então assim, apesar da formalização, apesar de que colocar a política no papel tenha sido um evento recente, as boas práticas de segurança são seguidas desde sempre. Seja no setor de TI explicitamente, onde você fala em segurança da informação e todo mundo lembra de TI automaticamente, mas também nos setores que lidam com dados de alunos desde sempre. Registro acadêmico, Pró-Reitoria de assuntos acadêmicos, Pró-Reitoria de extensão, Pró-Reitoria de pesquisa, etc. Tem a questão de proteção de projetos de docentes e tal. Então a instituição sempre levou muito a sério isso, a gente só não tinha todos esses eventos documentados, essas boas práticas documentadas e instaladas em um documento. A diferença é só essa. Mas as boas práticas sempre existiram.*

Pergunta: A PoSIC da UFERSA determina que os ativos de informação e comunicação são patrimônios da instituição. De maneira geral, quais práticas a UFERSA adota para garantir a segurança desse patrimônio?

Resposta: *Todo bem institucional, não só de informática, mas cadeira, mesa, armários, ar-condicionado e tudo mais, todos os bens institucionais são patrimoniados, eles são patrimônios da união. Então há inventários temporários, tanto inventário global da instituição, como inventário de tecnologia da informação, que verifica a integridade daqueles bens, a funcionalidade daquele bem, se um bem foi alocado em um certo setor e não está funcionando por um certo motivo, se não está funcionando, o porque não está funcionando e coisa desse tipo. Então, sobre o bem físico isso já é feito desde sempre também, independentemente de política isso já acontece. Do ponto de vista de gestão tecnológica, de tecnologia da informação propriamente dita, a gente vem passando por um processo de mudança da forma como a instituição encara isso e muito reflete a existência da política de segurança. Na verdade, desde que a instituição formatou sua rede e formatou a maneira como ia lidar com informática, nunca houve um processo rigoroso no sentido de, por exemplo, atrelar tal máquina a tal usuário, então eu posso chegar, ligar esse computador aqui e utilizar ele normalmente, sem senha e tudo mais, sempre houve uma relação de confiança. Mas isso quando a instituição era pequena, quando era ESAM eu não estava nem na instituição ainda nessa época e tudo, isso a gente está falando de 20 anos atrás, de 25 anos atrás, você tinha um número pequeno de computadores, uma rede pequena, um número de pessoas menor ainda que usava, então era fácil manter essa relação de confiança e a instituição cresceu mantendo essa relação e hoje a gente chegou num ponto que já não é mais sustentável somente essa relação de confiança, ainda existe, porque afinal de contas é um servidor público que está ali tratando, então a gente entende que o servidor público vai tratar o bem público com atenção, com cuidado. A mesma coisa se refere ao aluno, a gente entende que o aluno entende que aquele bem é um bem que é patrimônio dele também, afinal de contas foi pago pelos impostos dele, mas a gente sabe que hoje essa relação de confiança já não é suficiente para manter. Então a gente vem adotando algumas práticas de gestão, em especial, de catalogação específica de equipamentos, instalação de softwares de monitoramento e outras ações deste tipo, para a gente*

encontrar o melhor formato de ir substituindo essa relação de confiança, por uma relação técnica. Sem, com tudo, causar algum tipo de aflição, algum tipo de preocupação com o usuário final. Porque não adianta a gente adotar uma política que seja tecnicamente correta, mas que não seja aderente a vida do usuário, isso não faz sentido. Então a gente precisa agregar esses dois cenários para a coisa poder dar certo.

Pergunta: No Art 6º da PoSIC é determinado que a instituição deve adotar estratégias para a recuperação da informação, mesmo quando esta for prejudicada por desastres naturais. Quais procedimentos a UFERSA adota para garantir a recuperação de informações na ocorrência de incidentes?

Resposta: *Hoje nós temos uma política de backup, que é o principal mecanismo para recuperação de dados. Você ter uma cópia daquilo ali para quando precisar. Então hoje a gente tem backups de hadware e backups de software. O mesmo hardware onde hoje funcionam os sistemas acadêmicos, por exemplo, a gente tem cópias desse mesmo hardware. Então se esse servidor onde está sendo usado o sistema acadêmico hoje parar, a gente tem plena condição de migrar para esse outro hardware sem problema nenhum. O que especificamente seria uma falha de hardware. Se for uma ação mais catastrófica ainda, como por exemplo, houve um incêndio no datacenter, a gente possui um backup externo dos mesmos dados em outro local separado. Inclusive a gente está em uma fase de testes de migração de alguns desses locais externos para os campis do interior, então a gente vai ter o mesmo backup daqui a 200km daqui. Estamos vendo a situação de largura de banda, de tempo de recuperação desses dados via internet, também de segurança já que todos os dados estarão sendo trafegados por uma via pública, então a gente precisa ter garantia de segurança nesse sentido. Mas a gente tem backups externos fora do data center, para que num desastre pleno a gente possa fazer um recover sem problemas.*

Pergunta: A PoSIC da UFERSA indica a utilização de classificação para aspectos de confidencialidade, integridade, autenticidade e disponibilidade. Como funciona essa classificação e como ela é adotada nos procedimentos de segurança da instituição?

Resposta: *Na verdade, esse artigo não é baseado no achismo, vamos dizer assim, mas ele é baseado no normativo anterior que trata da classificação de informações que foi implementado pela política de informação ao cidadão que foi criada de 2012 para 2013, eu não vou te dar uma data certa. A partir da criação dessa política, todos os órgãos federais ou vinculados ao governo federal, do executivo legislativo judiciário e em posteriores momentos também a esfera estadual e municipal, tinha a obrigação de divulgar dados ao cidadão com o mínimo possível de interferência, com o mínimo possível de necessidade do cidadão se identificar e dar porquês e tudo mais, então tudo isso fazia parte dessa política de transparência. E para conseguir dar essa transparência, a primeira coisa que precisava ser feita era dizer "ah, que dados podem ou não podem ser publicados?" Ou seja, o quê que é secreto, o quê que não é secreto, "existem dados secretos em uma universidade, por exemplo?", "o quê que a gente pode ou não pode divulgar?", Então, "eu posso divulgar um e-mail de um aluno?", ou "eu posso divulgar uma nota de um aluno?", "há diferença entre e-mail e nota?", então nessa época, esses dados foram classificados. Então, por exemplo, já que eu citei dados de alunos... Dado de aluno nenhum é público. Exceto, por exemplo, a lista de aprovados. Eu tenho que ter lá o nome do cara, o número CPF do cara para dizer que ele foi aprovado e ele poder vir, então nesse caso pode. Mas uma vez ele ingressado na universidade, eu não posso divulgar nenhum outro dado acadêmico dele. Nenhum dado da vida acadêmica dele e nenhum dado da vida privada dele. Então essa classificação foi feita pela PoSIC, mas ela é seguida de acordo com os parâmetros que foram anteriormente descritos. Então aquilo que é dito confidencial, a PoSIC respeita e não altera esse conceito, que esse conceito foi muito bem feito quanto a implantação da política de informação ao cidadão. Inclusive nesse momento deve estar sendo refeito uma segunda versão dessa política de informação ao cidadão, um dos itens que precisa ser revisto, não no sentido de corrigir, mas no sentido de aprimorar é justamente a metodologia de classificação. A reitoria me informou que ontem iria emitir uma portaria com esse tema. Então, quer dizer, isso vai impactar na PoSIC? Vai. Porque se as informações forem reclassificadas, a gente vai ter que ver outros dados que a gente precisa proteger ou não proteger em virtude dessa classificação da informação ao cidadão, não da política explicitamente.*

Pergunta: Quais práticas a UFERSA adota para garantir o controle físico e lógico dos seus ativos?

Resposta: *Na verdade, são dois mundos bem diferentes o físico e o lógico. Se a gente tiver falando de físico, a gente começa a falar lá desde a menina da limpeza trancar a sala quando o último aluno sair, a você ter câmeras de segurança em todo o perímetro da universidade, você ter uma empresa de segurança que é ativa e que passa mensagem, que vistoria, então fisicamente a gente tem isso. Além das coisas mais diretamente ligadas a TI, que é você ter equipamentos com cabo de aço que amarra tudo, é você ter um equipamento que você não consiga configurar fora da instituição ou fora da rede da instituição, então são alguns elementos que fisicamente conseguem agir de alguma forma. Consegue garantir? Não, não consegue garantir, é impossível. Mas a gente busca mecanismos para tentar, dentro do possível, minimizar essa situação. É tanto que faz uns bons anos que a gente não tem notícias, por exemplo, de um roubo de um computador, coisas desse tipo. Já houve? Já houve. Mas coisa drástica assim de termos perdido dados por causa de um computador foi roubado, isso nunca nem aconteceu pra dizer a verdade. Do ponto de vista lógico, aí é um outro cenário, um outro mundo completamente diferente. Porque a gente tem hoje muitos sistemas institucionais, a maior parte desses sistemas estão sobre a nossa tutela hoje, alguns outros dados não estão sobre a nossa tutela, mas estão em serviços contratados, por exemplo o serviço de e-mail hoje da instituição utiliza a infraestrutura do google, gmail. Então são dados que não estão conosco, mas existe uma política de segurança também do google, existe uma relação contratual entre nós que é onde se dá essa garantia. Mas internamente, além do backup que você já tinha perguntado, a gente tem política de senhas fortes para os usuários, a gente tem política de separação de dados que usuários podem acessar e dados que não deveriam ser acessados por ninguém, mesmo em sistemas que são coletivos, como o acadêmico onde docentes e discentes tem acesso ao mesmo núcleo de dados com senhas diferentes e perfis diferentes que permitem coisas diferentes. Então, do ponto de vista lógico, existe uma série de outras infraestruturas que permitem claramente essa separação e tentam, dentro do possível, garantir que esses dados não vão ser fragilizados de alguma forma. Mas é como eu falei, tentam garantir. Até porque sempre vão surgir novas vulnerabilidades, as vezes é uma coisa até que a gente não espera, como uma versão nova de um software que saiu e a gente atualiza para corrigir um*

problema e acaba aparecendo outro, então é um mundo bem complexo de você ter essa palavra "garantia", mas dentro do possível é isto.

Pergunta: A PoSIC da UFERSA indica o uso de auditorias. Desde sua implementação, já ocorreu necessidade de alguma auditoria? Se sim, o que motivou o processo e quais foram os resultados?

Resposta: *Eu não posso dizer o que motivou, porque muitas dessas auditorias são sigilosas, certo? Mas sim, já houveram diversas. Na verdade, assim, hoje qualquer cidadão, mesmo quem não faz parte da comunidade, pode abrir um processo na instituição para localização de algum dado. Você imagine, por exemplo, que um candidato a uma vaga na UFERSA entendeu que o processo seletivo dele não foi coerente, foi lá no SISU, não tem nada a ver com a universidade, mas o caminho de contato dele é com a universidade, então ele vem ao caminho. Alguns desses pedidos realmente necessitam de serem validados internamente, porque, afinal de contas, a gente tem o dado e tem a responsabilidade, principalmente com a política de informação ao cidadão. Nenhum órgão federal, estadual ou municipal pode simplesmente dizer "ah não, isso não tem nada a ver comigo. Vá embora!", então em qualquer situação a gente tem a responsabilidade de dar uma resposta coerente, de dizer os porquês e tal. Então já existiram "n" auditorias nesse sentido, mas a maioria que realmente teve que ser levada a fundo e que gerou algum resultado por isso assim, foram questionamentos por exemplo de aluno questionando notas ou alguém que teve a senha do e-mail roubada, um e-mail Hotmail, que não tinha nada a ver com a instituição, o cara teve uma senha roubada e ele está com medo que a conta dele no sistema institucional tenha sido usada indevidamente, então a gente vai rastrear se houve algum uso indevido daquele sistema ou não. Então assim, tem alguns motivos autênticos pelo qual já foram feitos e existem auditorias que não tem uma motivação direta, por exemplo, ah eu quero verificar se houve alguma tentativa de acesso a conta de um docente, alguém tentou roubar a senha de um docente, então a gente faz uma auditoria, não em cima de um docente específico, mas por exemplo, se houve algum usuário onde houve tentativas de entrada de senhas múltiplas, que é uma indicação de que alguém está tentando quebrar a senha do camarada. Então não foi gerada por um motivo, mas é uma investigação que a gente faz com uma certa periodicidade para tentar entender se o sistema está tentando ser invadido, se alguém*

está tentando corromper algum dado ou algo do tipo. Do ponto de vista de resultados, alguns desses procedimentos são meramente de controle interno. Então a gente realiza, por exemplo, um teste desses de usuário e verifica se está tudo ok e não precisa fazer nada ou se vai precisar ter algum processo que faça parte de um processo administrativo. Então, um usuário por exemplo que teve a senha roubada, ele entende que o sistema foi usado de uma forma que não deveria e não foi ele ou algo desse tipo. Então ele vai abrir um processo administrativo, esse relatório de auditoria vai constar neste processo administrativo, dizendo que "sim, foi mal uso" ou dizendo que "não, não houve mal uso" e ai as decisões são tomadas da forma como a norma da instituição e como as leis do país dizem que devam ser tomadas.

Pergunta: A UFERSA dispõe de um plano de contingência no caso de ocorrer algum incidente? Se sim, poderia me explicar, de modo geral, o que esse plano determina?

Resposta: *Essa de existir um plano de contingência é similar àquela que eu te falei da política de segurança. A política é a formalização, ter um plano de contingência existe um nível de formalização, que hoje realmente a gente não tem, e existe o nível prático que é quando as coisas acontecem e como é feito. A gente tem uma meta para esse ano de 2019 de formalizar um plano de contingência, mas isso não quer dizer que nós não temos as boas práticas. Então, quando há qualquer tipo de sinistro e já houve alguns, por exemplo, falta de energia por 48 horas ou 72 horas, já houve na instituição. Ou queima de condicionador de ar do datacenter, também já houve. Então já houveram alguns sinistros onde a gente teve que acionar essas boas práticas. O principal elemento dessas boas práticas é a gente ter pessoas que dentro de suas atribuições já entendem e já sabem o que fazer nesses momentos de sinistro. Então a gente tem pessoas que lidam com a parte de banco de dados, de sistemas, de hardware, de rede, que quando qualquer sinistro ou qualquer vislumbre de que um sinistro vai acontecer, elas já começam a colocar em prática essas ações que são necessárias. O segundo ponto primário desse nosso plano de contingência é contar com aqueles elementos de backup que eu também já citei, o backup de dados, o backup de hardware, o backup de rede. Então, já aconteceu por exemplo de passar um caminhão, derrubar um poste e romper uma fibra e a gente ter uma fibra secundária para gente levar e não deixar um prédio fora do ar durante muito tempo. Então, a gente tem elementos de backup dos mais diversos âmbitos, desde software,*

hardware e infraestrutura. E esses profissionais acionam esses elementos de backup quando necessário. Então as pessoas e os elementos de backup são os dois principais fundamentos dessa nossa forma de responder a qualquer incidente de grande porte. Isso está formalizado hoje? Ainda não. Mas é uma meta para 2019. Está no plano de desenvolvimento de tecnologia de informação da instituição desenvolver esse planejamento para esse ano.

Pergunta: Uma das medidas de segurança determinada na PoSIC da UFERSA é ter cópias de dados mantidas em local diferente de onde se encontra o ativo da informação. A UFERSA conseguiu implementar essa medida? Como?

Resposta: *Hoje nós temos, além do nosso datacenter que tem vários discos, backups dentro do próprio datacenter. Então, eu tenho um banco de dados de produção e tem mais de uma cópia desse banco. Além disso a gente tem cópias externas desse banco em datacenters isolados hoje aqui no campus, mas a meta para 2019 é a gente levar para pelo menos um dos campis do interior essa mesma informação. Então hoje a gente tem e já implementa esses backups externos.*

Pergunta: Para que uma política de segurança da informação seja eficaz é importante que todos os usuários a conheçam e adotem. A UFERSA promove treinamentos quanto sua política de segurança? Como ela é divulgada?

Resposta: *Treinamentos formais como "ah, vamos montar um curso sobre a política de segurança da informação" não, a gente não faz isso. Pelo menos não fez até agora, a gente não entendeu que houve essa necessidade ainda. A nossa política é nova e ela ainda está sendo regulamentada, então existem normativos que ainda estão em tramitação, principalmente os normativos que impactam mais diretamente o usuário, eles ainda estão em tramitação no Conselho Gestor de Governança de TI. Então, por exemplo, norma específica de como usar o e-mail institucional, é uma coisa que vai afetar mais diretamente o usuário, está implícito dentro da política de segurança, mas como é uma norma que vai afetar o dia a dia, ela não pode estar descrita no corpo da política, ela tem que ser regida por uma norma que detalha esse dia a dia. Então, a medida em que essa política que vai mudar o dia a dia do usuário, que vai restringir*

ou que vai dizer como ele vai fazer o seu dia a dia acontecer, a medida em que essas normas estejam todas aprovadas pelo CONSUNI e tudo mais, muito possivelmente vá ter essa necessidade de fazer um treinamento de fato com os técnicos, professores e alunos também. Então muito possivelmente a gente vai ter que adotar uma política, algum padrão de treinamento mais explícito. O que a gente faz hoje é conversar com os setores, sempre que a gente visita os setores, não só eu como gestor de segurança, mas sim a comunidade inteira da universidade, faz toda questão de levar essa informação corretamente para os setores administrativos e tudo mais. Mas a medida em que essas normas operacionais do dia a dia surgirem, é possível que a gente tenha que implementar outras técnicas para fazer essa informação chegar mais diretamente.

Pergunta: A UFERSA já sofreu algum tipo de ataque malicioso contra seus ativos? Caso sim, poderia relatar alguns deles?

Resposta: *A gente sofre milhares de tentativas de ataques por dia. As universidades como um todo, não só a UFERSA, sofrem um volume muito alto de tentativas de invasão que geralmente acontecem por um motivo principal: as universidades todas hoje no Brasil, mesmo as mais distantes, elas hoje contam com links tecnicamente muito bons, estáveis e com grande largura de banda. Então, se você pegar o link da UFERSA por exemplo, é 1GB hoje em Mossoró. Então você imagine o quão é bom para um hacker, por exemplo, ter domínio sobre algumas máquinas de dentro da instituição para utilizar esse 1GB de banda para fazer o que ele quiser... É muito diferente dele invadir o da minha casa, que eu só tenho 5MB. Então os elementos maliciosos têm muito interesse em invadir as universidades para ter domínio sobre esses links de grande porte, para ser uma bandeira de sucesso dentro da comunidade deles e poder dizer "olha, eu invadi a universidade tal", então a gente hoje é muito visado. Inclusive não só por elementos externos, a gente sempre fala assim "ah, o malicioso está fora", mas não é. As vezes a gente também tem elementos internos, as vezes é aquele carinha que está em casa assistindo a um vídeo no YouTube "como invadir não sei o que" e pensa "ah, deixa eu tentar aqui na universidade" aí ele vai lá e tenta. Então a gente tem milhares de casos por dia. O que acontece é que boa parte desses milhares ficam retidos logo na nossa primeira barreira, que é o firewall, porque o firewall tem uma série de elementos, inclusive elementos de inteligência artificial,*

que identificam padrões e já barram essas tentativas. Como elementos que passam pelo firewall por parecerem ser coisas autênticas e a gente só acaba descobrindo em outros momentos, por exemplo, como o caso de um aplicativo de quebra de senha no SIGAA que o cara vai lá e tenta logar normalmente, então o firewall não entende que aquilo é nocivo, ele só pensa que tem uma pessoa tentando logar no sistema. Mas o SIGAA entende isso, então o SIGAA lá uma hora mostra um captcha, outra hora bloqueia a conta do usuário, então a gente vai tendo várias camadas de segurança para fazer isso acontecer. Inclusive já teve situações onde a gente chegou a ter máquina invadida sim e isso foi uma das preocupações que motivou a nossa política de segurança, porque com o desenvolvimento de um monte de tecnologia cada vez é mais comum, por exemplo, o professor lá da química dizer "ah, tem um aplicativo legal que tem que rodar em um servidor. Eu vou montar aqui na minha máquina para os meus alunos usarem e tem que estar disponível na internet", então quer dizer, o professor está querendo usar aquela ferramenta ali para uma atividade acadêmica que vai trazer um benefício bacana para os seus alunos e pode trazer até um benefício para a comunidade externa, massa! A gente dá todo o suporte. Só que ele quer fazer isso na máquina dele, lá na sala dele, sem a nossa supervisão, sem a gente verificar se realmente aquele sistema operacional está com os testes de segurança em dia, se a máquina tem um firewall instalado e ele quer ter domínio sobre isso. Então o desenvolvimento da tecnologia permite que isso hoje seja feito muito facilmente, você baixa lá uma distribuiçãozinha mínima que seja com tudo instalado, coloca lá e pronto, montou um servidor. Acontece que ao fazer isso, essa máquina não está sobre o domínio da SUTIC, está externo, sobre os cuidados de um terceiro e se eventualmente ocorrer alguma invasão aquela máquina, muitas vezes a gente não consegue se quer saber que houve aquela invasão. Então já houve situações sim desse tipo, exatamente nesse contexto que eu estou lhe dizendo, de ter alguém que queira montar um serviço lá no seu local de trabalho e em virtude desta máquina ter alguma fragilidade de algum tipo, ela ser invadida. E aí a gente descobriu a invasão. Algumas vezes eles fazem por conta própria, já outras eles até comunicam a gente porque as vezes ele pede "preciso de um IP externo para uma atividade minha aqui" e a gente informa, "olha, tem os riscos associados, você entende isso?" e ele responde "ah, não, entendo. Estou tratando de tudo aqui." Quando na verdade ele não está tratando de tudo, tinha alguma fragilidade lá que ele não entendeu. É muito complexa a decisão de você dizer um não para o usuário, pois ele pode até interpretar isso como um

cerceamento ali na forma de ele trabalhar ou algo desse tipo. E ao dizer sim ao usuário, a gente acaba assinando de que ele está pondo a universidade em risco, que em suma é isso que está acontecendo. Então é algo bem complexo. Antes da política de segurança, era uma decisão quase que pessoal, o que não é bom porque um setor público não pode ser pessoal, então é algo que não era bacana. Depois da política a gente teve como tratar isso de uma forma mais técnica dizendo "não, isso não pode" ou "isso pode". A gente passou a ter uma fundamentação maior para chegar e dizer "não, isso aqui é tecnicamente muito arriscado e esse é o motivo pelo qual você não pode fazer. Vamos fazer de uma outra forma, tratar de outro jeito, ao invés de colocar um servidor lá na sua sala vamos instalar em um servidor nosso aqui no datacenter, que aí sim eu vou ter firewall, eu tenho certeza que a versão do Linux que eu vou usar não tem falha de segurança ou se tem alguma falha, que seja uma que a gente já conhece e está sabendo proteger". Então assim, a gente tem migrado esses serviços para a área interna e tal, mas já aconteceu de ter algum serviço externo e ele ser invadido, foi por uma coisa boba, era um sisteminha que mandava notificações por e-mail para o usuário, a fragilidade estava exatamente no serviço de e-mail. Então o camarada invadiu o serviço de e-mail e começou a usar esse serviço de e-mail para mandar spam. Então assim, não houve nenhum comprometimento de dados institucionais, até porque era um computador que não tinha dados institucionais, mas ele causou algum problema porque quando esse spam parte de um IP nosso, os servidores internacionais de e-mail começam a verificar de quem é esse IP e aí quando eles viam que o IP era da UFERSA o que acontecia era "ah, vamos começar a bloquear as coisas do domínio da UFERSA", e a partir disso se deixa de mandar e-mail para um Hotmail ou deixa de mandar e-mail para um gmail e isso começa a afetar a comunidade, é nocivo de toda forma. Não houve o comprometimento de dados institucionais, mas houve a indisposição dos serviços institucionais e obviamente isso não é bom. Mas, por exemplo, ano passado não houve nada desse porte a computadores institucionais. E eu diria até que em 2017 também não. Acho que a última ocorrência foi em 2015 pra 2016, que é anterior a PoSIC da UFERSA.

Pergunta: Na ocorrência de ataques maliciosos, quais foram as medidas de correção adotadas? Houve algum prejuízo para a instituição?

Resposta: *Prejuízo de dano a dados ou de dano de hardware e coisas desse tipo, não. Algum prejuízo a imagem da instituição? Sim. Porque como por exemplo, essas notificações por spam ocorrem automaticamente, independe das pessoas e da instituição. O servidor lá do Hotmail percebe que tem um outro servidor mandando mil mensagens por minuto para ele, ele sabe "ah, isso aqui é spam, não recebo mais". Então é algo técnico que de alguma forma nos afeta e é ruim e óbvio que a gente precisa tratar. Mas dano, comprometimento de dados de alunos que é a nossa principal preocupação, dados de pesquisa, dados de alunos da pós-graduação ou de pesquisa da pós-graduação, ou de TCC da graduação que não deveria estar divulgado, isso nunca aconteceu. A gente tem uma equipe de resposta que está sendo formalizada agora no primeiro semestre desse ano, uma equipe de resposta a incidentes de segurança. Porque a gente tem as boas práticas, mas não tem a equipe formalizada. Então essa formalização também é uma meta para esse ano. Na verdade, para o ano de 2019 a gente tem como meta a formalização de uma série de coisas que nós só temos nas boas práticas e não só na área de segurança, mas na área de desenvolvimento de sistemas também e tal. A gente adota as boas práticas, a gente faz a coisa do jeito certo, mas a gente não tem isso documentado. E isso é ruim inclusive para a gente, porque nem sempre a gente tem como divulgar certas ações que a gente faz por não estarem formalizadas.*

Pergunta: Na UFERSA ocorre problemas de incidentes não maliciosos, em que o incidente acontece, por exemplo, devido a descuido ou falta de conhecimento do usuário?

Resposta: *Na verdade, assim, a gente trata qualquer incidente como incidente. No momento da ocorrência do incidente a gente não explicita juízo de valor. Se foi proposital ou não foi proposital, naquele momento não importa. O que importa é a gente tratar o incidente, minimizar qualquer dano que venha em virtude a ocorrer, não permitir que o incidente aconteça novamente e depois é que a gente vai parar para entender "ah, foi por isso" ou "não foi por isso". Então assim, se foi doloso ou não doloso é outra história. Mas acontece, na verdade em todo e qualquer sistema que lide com pessoas, em algum momento alguém vai clicar em um canto que a gente não esperava. Dentro dessa categoria aí eu vou te indicar um problema que é extremamente comum e que inclusive a PoSIC cobre e coíbe, mas que as pessoas*

ainda fazem na melhor das intenções, que é o professor quer montar um grupo de estudos lá na sala dele com os seus alunos, por algum motivo ele acha que o sinal do Wi-Fi lá na sala dele é fraco, aí ele vai lá no centro, compra um roteador e pluga na tomada. Então, o que acontece é que hoje apesar da gente ter mecanismos que restringem e dizem "nessa tomada só pode ser ligado tal equipamento", a gente entende que essa não é a melhor solução para a instituição, porque de repente, o professor, o servidor ou o aluno, que seja, poderia trazer o seu notebook de casa por algum motivo para trabalhar. Por querer trabalhar com o AutoCAD ou com alguma outra ferramenta pesadíssima e por ele achar que o computador da instituição não vai render, ele vai e traz o dele. E ele vai lá e pluga na tomada. Se eu disser que não é possível plugar essa outra máquina naquela tomada, eu vou gerar de alguma forma um prejuízo. Então a gente não entende que essa seja a melhor política. Mas ao não fazer bloqueio, que a gente poderia fazer mas optamos por não fazer, o cara vai lá e liga o roteador dele e ao ligar o roteador dele, ele de repente espalha IP na rede e aí já aconteceu caso assim de a gente ter um prédio inteiro parado porque alguém plugou um roteador na rede. Então é algo que gera transtorno? Gera. É algo que a gente tem tentado proibir? Tem. Mas é como eu falei, a gente trata como incidente. Se o cara fez aquilo de má intenção ou não, naquele momento de tratativa do incidente, não importa. Mas nesse caso do roteador, por exemplo, quase sempre é sem intenção. Ele faz sem nem entender quais são os impactos daquilo. Inclusive nessas situações, muito embora a gente tenha amparo técnico e legal pra isso, a gente nem indica punição e nem nada porque afinal de contas a gente realmente entende que o cara não teve a intenção de fazer aquilo ali. Então a gente teria o suporte legal para fazer isso, mas normalmente a gente não faz por entender que não houve uma má fé ali que levasse aquela situação.

Pergunta: A UFERSA dispõe de estatísticas relativas à segurança da informação? Se sim, o que elas indicam e quais medidas serão tomadas a partir delas?

Resposta: *Estatísticas formais, assim, vamos constituir um relatório específico para isso, até que não. Mas a gente tem uma série de indicadores do dia a dia, por exemplo, se você quiser saber agora quantas tentativas de invasão a gente já teve hoje, eu tenho como dizer nesse momento. Gráficos dos últimos 6 meses, gráficos de tráfegos, estatísticas de tráfegos, estatísticas de uso dos sistemas, tudo isso a gente tem. São dados que a gente usa operacionalmente, que a gente usa no dia a dia, então eu*

consigo ver, por exemplo, que por algum motivo o número de acessos ao SIGAA está muito alto sem nem ser época de matrícula e nem nada, logo, o que é que está havendo? Então existem vários indicadores que a gente usa durante o dia para ver as alterações, e isso no ponto de vista tanto de hardware e de software, como de segurança, que seja. A gente não tem um relatório formal constituído a respeito disso, mas a gente faz uso desses indicadores direto. No dia a dia a gente observa isso o tempo inteiro. Por exemplo, volume de tráfego da rede, então a gente tem gráficos que mostram em tempo real o que é que está passando na nossa rede. Então a gente fica o tempo inteiro observando esses gráficos para ver se há alguma anomalia de subida ou de descida fora de um certo padrão. Qualquer subida ou descida fora de um certo padrão é um indicativo de que pode ter ocorrido ali algum tipo de incidente, a partir disso, a gente já abre uma retificação para identificar aquele fato ali em específico. Então formalmente a gente não tem, mas no dia a dia a gente tem "n" indicadores que nos dão isso.

Pergunta: O que o senhor acha que deveria ser melhorado na política de segurança de informação da UFERSA?

Resposta: *Bem criticamente falando, quando a nossa política foi criada e eu até entendo o porquê que ela foi aprovada dessa forma, na nossa instituição o órgão máximo, a entidade máxima capaz de determinar normas é o CONSUNI, portanto tudo deve ou não passar pelo CONSUNI, o CONSUNI é quem diz quem deve ou não passar por ele. Em alguns momentos o CONSUNI determina "tal órgão vai decidir, não precisa passar por mim". Então, por exemplo, a PROGRAD ela tem toda liberdade de dizer em qual sala de aula vai funcionar tal disciplina. Isso não precisa passar pelo CONSUNI, a PROGRAD tem autonomia para tomar essa decisão. Quando a política foi aprovada, o nosso CONSUNI entendeu que todas as normas associadas a política também deveriam passar pelo CONSUNI e algumas normas, são normas operacionais, normas do dia a dia. São documentos que deveriam ser estudados e publicados com muita agilidade e incluir esse documento na pauta do Conselho Universitário faz com que a gente perca essa agilidade. Então, por exemplo, as vezes é criada uma norma para tratar de tal incidente que aconteceu hoje, isso vai ter que passar ainda pelo CONSUNI, vai ter que entrar na agenda do CONSUNI, passar nas discussões do CONSUNI. Então, uma norma que a gente cria hoje, ela só vai ser*

aprovada pelo CONSUNI daqui a 1 ano e meio, 2 anos... É muito tempo. Então esse tempo de execução, muito embora correto, muito embora seja um procedimento legal dentro da instituição ou que o CONSUNI entendeu que o melhor processo era esse, faz com que a gente perca o time do problema. O problema acontece, a gente termina resolvendo o problema, tratando esse problema e ele vai passar 2 anos na informalidade até que finalmente eu consiga aprovar uma norma que trate aquele problema. Então isso não é prático. O mais coerente é que o CONSUNI entendesse que poderia conceder a um outro setor ou a uma outra entidade, por exemplo, o Comitê de Governança Digital (CGD), que é um comitê que se reúne com mais frequência, que tem uma pauta menos lotada, que tem decisões tão importantes a tomar como o CONSUNI, mas que tem uma pauta menos lotada, que tem uma maior disponibilidade dos seus membros. Acabaria sendo muito mais ágil. Então eu acho que o principal elemento que hoje prejudica de alguma forma a atualização da política, é esse procedimento de aprovação das normas, que terminam fazendo com que a coisa demore muito mais tempo do que o que era necessário. Do ponto de vista técnico, legal e de fundamentação, eu acho que hoje a política ela não é melhor e nem pior que as outras instituições, mas ela está bem de acordo com as normas, ela está bem de acordo com o que o mundo da segurança da informação trata. Mas a gente vai ter dificuldade em manter essa política atualizada. Da forma como ela foi criada, ela foi criada com alguma vanguarda, mas daqui a mais de 2 anos já não vai ser mais vanguarda. Então, quer dizer, talvez a gente não consiga realmente acompanhar essa rotina das coisas. Só para te dar um exemplo, a gente já está tendo aí um monte de demandas de equipamentos que se comunicam pela internet a todo momento, que é a chamada "internet das coisas". Não existe um item explícito na política sobre a internet das coisas, a gente vai ter que criar uma norma específica. Só que já tem muitos professores, alunos, projetos de TCC e projetos de pós-graduação que precisam utilizar esse tipo de tecnologia, aí a gente vai lá, cria uma norma e explicita tudo direitinho, mas esse nosso professor, o aluno que está desenvolvendo TCC, o aluno da pós-graduação que está fazendo o seu doutorado ou o seu mestrado, vai poder esperar 2 anos para colocar em prática isso? Talvez eles não estejam mais nem aqui na instituição. Então a gente vai ter que terminar permitindo o uso, tratando a coisa com boas práticas, mas tratando de uma maneira não documental. Sem o suporte, sem o amparo da política de segurança. Então assim, eu acho que seria uma

boa decisão institucional se fosse feita essa mudança. Acho que talvez essa fosse a mudança mais significativa hoje a ser feita na PoSIC da instituição.