

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE MATEMÁTICA
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

BEATRIZ DE ANDRADE CAMPOS
GRAZIELLE ALESSA ALVES DOS SANTOS

GESTÃO DE VULNERABILIDADES E O IMPACTO NA RESPOSTA A INCIDENTES

RIO DE JANEIRO

2017

BEATRIZ DE ANDRADE CAMPOS
GRAZIELLE ALESSA ALVES DOS SANTOS

GESTÃO DE VULNERABILIDADES E O IMPACTO NA RESPOSTA A INCIDENTES

Trabalho de conclusão de curso de graduação apresentado ao Departamento de Ciência da Computação da Universidade Federal do Rio de Janeiro como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Vinícius Simas Pereira Fernandes
Co-orientador: Paulo Henrique de Aguiar Rodrigues

RIO DE JANEIRO
2017

C198g

Campos, Beatriz de Andrade

Gestão de vulnerabilidades e o impacto na resposta a incidentes /
Beatriz de Andrade Campos, Grazielle Alessa Alves dos Santos. –
Rio de Janeiro, 2017.

60 f.

Orientador: Vinícius Simas Pereira Fernandes.

Trabalho de Conclusão de Curso (graduação) - Universidade
Federal do Rio de Janeiro, Instituto de Matemática, Bacharel em
Ciência da Computação, 2017.

1. Segurança da informação. 2. Resposta a incidentes. 3. Gestão
de vulnerabilidades. I. Santos, Grazielle Alessa Alves dos. II.
Fernandes, Vinícius Simas Pereira (Orient.). III. Universidade
Federal do Rio de Janeiro, Instituto de Matemática. IV. Título.

Beatriz de Andrade Campos
Grazielle Alessa Alves dos Santos

Gestão de Vulnerabilidades e o Impacto na Resposta a Incidentes.

Trabalho de conclusão de curso de graduação apresentado ao Departamento de Ciência da Computação da Universidade Federal do Rio de Janeiro como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Aprovado por:

Prof. Vinícius Simas Pereira Fernandes, M.Sc.

Prof. Paulo Henrique de Aguiar Rodrigue, Ph.D.

Prof. Daniel Sadoc Menasche, Ph.D.

Prof. Claudio Miceli de Farias, D.Sc.

Prof^a. Vanessa Quadros Gondim Leite, M.Sc.

AGRADECIMENTOS

Agradecemos, em primeiro lugar, a Deus e as nossas famílias pelo apoio e as oportunidades dadas para que pudéssemos chegar até aqui.

Um agradecimento especial à Universidade Federal do Rio de Janeiro pela oportunidade de ter uma excelente base educativa no Ensino Superior e ao Grupo de Respostas a Incidentes de Segurança (GRIS/DCC) por despertar nosso interesse na área de Segurança da Informação.

Agradecemos também a à Diretoria de Segurança da Informação da Universidade Federal do Rio de Janeiro por fornecer todo apoio e estrutura disponível para construção deste trabalho e todos os professores que nos acompanharam durante a graduação, principalmente ao Prof. Dr. Paulo Henrique de Aguiar Rodrigues.

Agradecemos em particular, ao Vinícius Fernandes e Vanessa Quadros pela orientação, incentivos profissionais e amizade.

RESUMO

A Diretoria de Segurança da Superintendência de Tecnologia de Informação e Comunicação (SuperTIC) da Universidade Federal do Rio de Janeiro (UFRJ) tem como sua principal função a resposta e tratamento de incidentes. Desde que a Diretoria começou a monitorar a rede, houve um grande número de notificações de incidentes e vulnerabilidades. A situação revelou uma necessidade de boa gestão para garantir a qualidade de tratamento e um tempo de resposta adequado para atender a comunidade acadêmica. Este trabalho visa melhorar a metodologia atual de resposta a incidentes baseada na prevenção: investigar e mitigar vulnerabilidades para evitar os ataques. Com este objetivo, são expostos conceitos de segurança da informação para compreensão do trabalho, é realizada uma contextualização do cenário atual e suas dificuldades e, por fim, sugerido soluções para problemas encontrados no processo de prevenção de incidentes.

Palavras-Chave: Segurança da Informação. Resposta a incidentes. Gestão de vulnerabilidades.

ABSTRACT

The Security Division of the Superintendence of Information and Communication Technology (SuperTIC) of the Federal University of Rio de Janeiro (UFRJ) has as its main objective the response and treatment of incidents. Since SuperTIC started monitoring UFRJ infrastructure, there was a large number security incidents and vulnerabilities reported. This situation reveals the need for improving the management to ensure adequate quality of operation and suitable response time to request from the academic community. This work aims focus on prevention to improve the current methodology of incident response work: investigating and mitigating vulnerabilities to avoid cyber attacks. To this end, this paper presents the foundation and concepts of information security on initially investigated, following by contextualization of the obstacles and deficiencies of current UFRJ scenario, and, finally, solutions to mitigate the weakness of existing incident prevention processes or proposed and tested.

Keywords: Security Information. Incident Response. Vulnerability Management.

LISTA DE FIGURAS

Figura 1.1: Representação gráfica do processo de notificações	3
Figura 1.2: Estatísticas de Vulnerabilidades na UFRJ no ano de 2015	4
Figura 1.3: Estatísticas de Vulnerabilidades na UFRJ no ano de 2016	5
Figura 2.1: Pilares da Segurança da Informação	8
Figura 2.2: Relação entre os Conceitos de Segurança da Informação	8
Figura 2.3: Ciclo de Resposta a Incidentes [12]	12
Figura 2.4: Ciclo de Vida de Vulnerabilidades	15
Figura 2.5: Ciclo de Gestão de Vulnerabilidades	16
Figura 3.1: Tabelas presentes no banco de dados do sistema SGRC	21
Figura 3.2: Lista de vulnerabilidades e incidentes com seus respectivos números de identificação no sistema SGRC	22
Figura 3.3: Resultado da tabela de notificações do sistema SGRC	23
Figura 3.4: Campos de busca presentes no sistema SGIS	24
Figura 3.5: Rolagem de página do sistema SGIS	24
Figura 3.6: Percentual das Vulnerabilidades Gerais da UFRJ	26
Figura 3.7: Percentual das Vulnerabilidades UFRJ - 2016	27
Figura 3.8: Percentual das Vulnerabilidades UFRJ – 2017	27
Figura 3.9: Notificação de Incidentes Gerais da UFRJ	32

LISTA DE TABELAS

Tabela 2.1: Matriz de Risco utilizada no método Somerville	11
Tabela 4.1: Tabela de Probabilidade por Incidência de Vulnerabilidades	36
Tabela 4.2: Matriz de Risco para classificação das vulnerabilidades presentes nos protocolos / serviços	36
Tabela 4.3: Tabela de Incidentes x Pilares de Segurança afetados	37
Tabela 4.4: Tabela de Vulnerabilidade x Pilares de Segurança afetados	38

LISTA DE ABREVIATURAS E SIGLAS

CBPF	Centro brasileiro de Pesquisas Físicas
CMS	Content Management System
(D)DoS	(Distributed) Denial of Service
DNS	Domain Name System
DSI	Diretoria de Segurança da Informação
DSSC	Diretoria de Suporte a Sistemas Corporativos
HTTP	Hypertext Transfer Protocol
InfraTIC	Diretoria de Infraestrutura de Redes
IP	Internet Protocol
IPS	Intrusion Prevention System
LBCD	Laboratório Brasileiro de Controle de Dopagem
mDNS	Multicast DNS
POODLE	Padding Oracle On Downgraded Legacy Encryption
OSI	Open System Interconnection
RNP	Rede Nacional de Pesquisa
RPC	Remote Procedure Call
SGIS	Sistema de Gestão de Incidentes de Segurança
SGRC	Sistema de Gerenciamento
SNMP	Protocolo Simples de Gerenciamento de Redes
SSL	Secure Sockets Layer
SuperTIC	Superintendência de Tecnologia de Informação e Comunicação
TI	Tecnologia da Informação
TLS	Transport Layer Security
WLAN	Wireless Local Area Network
ZAP	Zed Attack Proxy
NGINX	Engine X
WHM	WebHost Manager
CVE	Common Vulnerabilities Exposures
OSSIM	Open Source Security Information Management
PoPS	Pontos de Presença
SGBD	Sistema de Gerenciamento de Banco de Dados
SQL	Structured Query Language

SUMÁRIO

1 INTRODUÇÃO	1
1.1 TEMA	1
1.2 OBJETIVO E MOTIVAÇÃO	2
1.3 JUSTIFICATIVA	2
1.4 METODOLOGIA	4
1.5 DESCRIÇÃO	6
2 REFERENCIAL TEÓRICO	7
2.1 SEGURANÇA DA INFORMAÇÃO	7
2.2 CONCEITOS NECESSÁRIOS	8
2.3 MATRIZ DE RISCO	10
2.4 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	11
2.5 RESPOSTA A INCIDENTES	12
2.6 GESTÃO DE VULNERABILIDADES	14
3 ANÁLISE DO CENÁRIO	19
3.1 CONTEXTO CIBERNÉTICO DA UFRJ	19
3.2 COLETA DE DADOS	20
3.3 VULNERABILIDADES IDENTIFICADAS	25
3.4 INCIDENTES IDENTIFICADOS	32
4 PROPOSTAS PARA MITIGAÇÃO DE PROBLEMAS DE SEGURANÇA NA UFRJ	35
4.1 CLASSIFICAÇÃO DE IMPACTOS E RISCOS	35
4.2 RELAÇÃO ENTRE VULNERABILIDADES E INCIDENTES	37
4.3 PROCEDIMENTOS PARA MITIGAÇÃO DAS VULNERABILIDADES	38
4.4 BOAS PRÁTICAS PARA GESTÃO DE VULNERABILIDADES	45
4.5 CASOS DE SUCESSO DE GESTÃO DE VULNERABILIDADE NA UFRJ	48
4.6 SUGESTÕES PARA MELHORIAS	51
5 CONSIDERAÇÕES FINAIS	53
5.1 Dificuldades encontradas	53
5.2 Prevenção de Incidentes versus Tratamento de Incidentes	54
5.3 Trabalhos Futuros	56
REFERÊNCIAS	57

Capítulo 1

Introdução

Neste capítulo é apresentado o tema principal deste trabalho, seguido pelo seu objetivo e motivação. Também é apresentada uma introdução ao cenário de vulnerabilidades da Universidade Federal do Rio de Janeiro (UFRJ) e o processo existente de notificações utilizado pela instituição.

1.1 Tema

Este trabalho é um estudo do cenário de vulnerabilidades de segurança da UFRJ, com ênfase na mitigação das ocorrências de maior risco e incidência, incorporando sugestões para a melhoria do processo de correção das falhas detectadas. Diversos fatores podem levar ao aparecimento de vulnerabilidades em sistemas computacionais, como versões desatualizadas de software, falta de monitoramento de serviços, má configuração de equipamentos de rede, etc. Para prevenir e mitigar falhas de segurança no ambiente computacional da UFRJ, uma análise do cenário operacional é feita e soluções são propostas.

1.2 Objetivo e Motivação

O objetivo deste trabalho é analisar e correlacionar as vulnerabilidades presentes na comunidade acadêmica da UFRJ aos incidentes reportados à sua diretoria de segurança da informação e apresentar soluções. A motivação para analisar e compreender a relação entre as vulnerabilidades e incidentes é propor um aperfeiçoamento do método atual de respostas a incidentes, a fim de melhorar o atendimento à comunidade acadêmica e aumentar o nível de segurança operacional de toda UFRJ.

1.3 Justificativa

A UFRJ possui uma Superintendência de Tecnologia de Informação e Comunicação (SuperTIC) que foi responsável, inicialmente, pelo suporte de tecnologia da informação (TI) do prédio da reitoria da universidade. Com o tempo, esse suporte se estendeu ao restante da instituição e foi necessária a criação de uma Diretoria de Segurança da Informação (DSI) para direcionar as boas práticas de segurança e proteger as informações da universidade. Ao receber a notificação de que uma determinada máquina, associada a um endereço IP, possui uma vulnerabilidade, a ação tomada pela DSI é notificar aos responsáveis e esperar que estes realizem as ações necessárias para solucionar o problema.

O recebimento das notificações de segurança é feito por diversos meios e sistemas. O Sistema de Gestão de Incidentes de Segurança (SGIS), pertencente a Rede Nacional de Ensino e Pesquisa (RNP) [27], notifica a DSI sobre incidentes e vulnerabilidades, que são encontrados por *scripts* que varrem toda a rede da UFRJ. A diretoria também recebe notificações, principalmente de incidentes, via e-mail institucional. Esses e-mails são reportados através do `abuse@ufrj.br` (endereço para denúncias de incidentes de segurança da instituição) e catalogados em formas de tickets atribuídos à DSI em um sistema interno da UFRJ (OSTicket) para posterior comunicação com o requerente e acompanhamento do problema. Também é possível que o usuário cadastre a requisição no OSTicket e abra o ticket manualmente, sem envio de e-mail. Este sistema funciona como um gestor de ordens de serviços

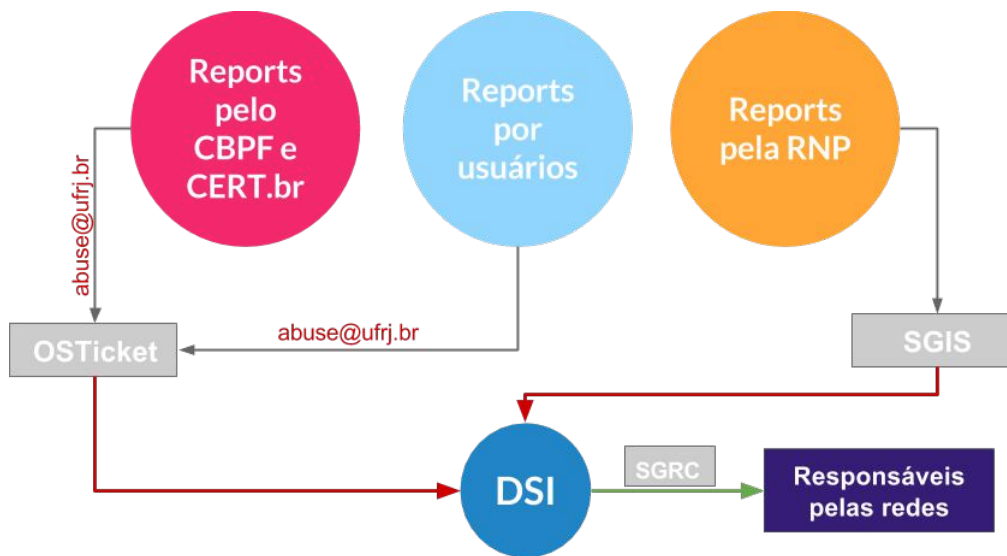


Figura 1.1: Representação gráfica do processo de notificações.

requisitados pelos usuários (discentes, docentes, funcionários da UFRJ ou público externo), onde as demandas da SuperTIC são registradas nesses tickets.

Destaca-se como usuário fixo de *reports* de incidente, funcionários do Centro Brasileiro de Pesquisas Físicas (CBPF). Todos os incidentes de rede são encaminhados aos Pontos de Presença (PoPs) dos 27 estados da federação [28], onde a RNP mantém equipes técnicas e administrativas para garantir acesso à rede de seu *backbone* aos usuários finais, sejam estes vinculados a organizações que conectam diretamente ao *backbone* ou as que conectam indiretamente através de redes metropolitanas ou acadêmicas. O CBPF auxilia a RNP a operar e distribuir as notificações de incidentes encaminhados ao Pop-RJ, ponto de presença responsável pelo estado do Rio de Janeiro, devido a falta de estrutura de pessoal. Outro local que contém dados que são utilizados para análise é o Sistema Gerenciador de Redes Corporativas (SGRC), que é utilizado pela equipe da DSI para notificar, por e-mails, o responsável técnico sobre o incidente ocorrido. A Figura 1.1 mostra graficamente como ocorre, até o momento da confecção deste trabalho, o processo de notificações dentro da UFRJ.

As Figuras 1.2 e 1.3 são gráficos gerados pelo sistema SGIS e apresentam a quantidade de vulnerabilidades notificadas à UFRJ durante os períodos de Junho/2015 até Junho/2016 e Julho/2016 até Julho/2017, respectivamente. Os gráficos mostram a quantidade de vulnerabilidades notificadas por mês à DSI.

Na Figura 1.2 é possível perceber que a quantidade de notificações aumentou a partir de Abril de 2016, uma explicação possível para este aumento de notificações é que a RNP normalmente insere novos *scripts* de varredura anualmente no sistema. Infelizmente, não é conhecido o critério utilizado pela RNP de prioridade para criação e inserção de *scripts* nas varreduras. Na Figura 1.3 é possível observar um nível elevado de notificações recebidas pela DSI. Como as notificações são repassadas aos administradores de rede para correção, era esperado que o volume de notificações caísse com o tempo, o que não veio ocorrendo na Figura 1.3, onde as notificações continuam num nível bem elevado, com pequenas oscilações eventuais.

Diante desses dados, é importante ressaltar que há repetição de endereços IPs nas notificações, muitas vezes pelas mesmas vulnerabilidades e, dessa forma, percebe-se que os responsáveis não possuem uma solução eficiente. Essa situação levantou a questão se a abordagem atual seria adequada para a solução do problema de vulnerabilidade e qual o papel que a DSI deveria assumir, seja proativo ou reativo.

Para tais questionamentos, a hipótese provável é a utilização de uma metodologia pouco eficiente de notificações e resolução dos problemas encontrados e que a mitigação das vulnerabilidades resultaria em parcial diminuição dos incidentes da UFRJ.

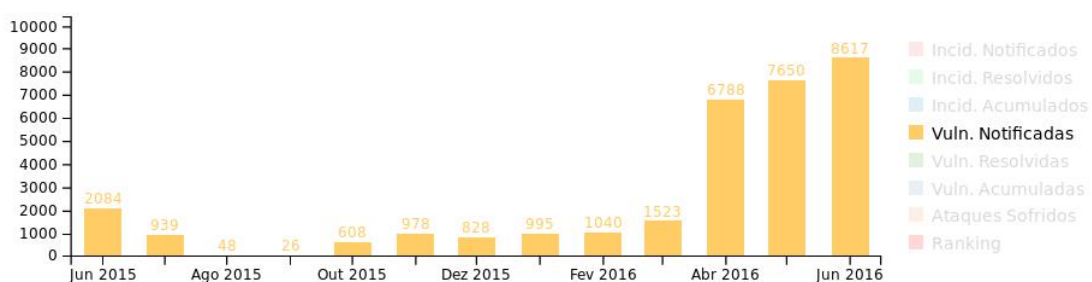


Figura 1.2: Estatísticas de Vulnerabilidades na UFRJ no ano de 2015

1.4 Metodologia

Neste trabalho, foi aplicado um estudo quantitativo e qualitativo das vulnerabilidades encontradas na UFRJ, com objetivo de auxiliar na prevenção de incidentes.

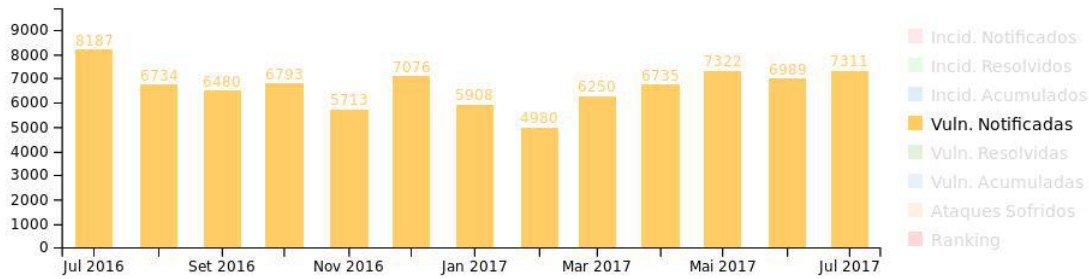


Figura 1.3: Estatísticas de Vulnerabilidades na UFRJ no ano de 2016

Foram utilizados como fonte de dados dois dos sistemas, dos quais a DSI se serve para receber e enviar notificações, respectivamente: SGIS, SGRC. Estas notificações podem ser tanto de incidentes quanto de vulnerabilidades. Porém estes sistemas não possuem uma forma eficiente para a extração desses dados, então inicialmente foi realizado um trabalho de coleta e catalogação de forma manual dos dados desses sistemas. Para o sistema SGRC foi realizada a mineração diretamente do banco de dados do sistema, enquanto o sistema SGIS foi realizada a mineração através da própria aplicação. O processo de extração de dados é explicado de forma mais completa no Capítulo 3.

Após a coleta e mineração dos dados foi realizada uma análise destes. Esta etapa incluiu a avaliação dos riscos e impactos associados a cada vulnerabilidade, conforme elucidado no Capítulo 2, e a elaboração de técnicas de mitigação para aquelas que possuem maior risco e incidência, como será abordado no Capítulo 3. Também foi elaborado um modelo de sugestões de melhorias para o processo atual de tratamento de vulnerabilidades baseado no processo de Gestão de Vulnerabilidades, explicado no Capítulo 2, com ênfase na redução de incidentes, que possui seu conceito abordado no Capítulo 2.

Por fim é avaliado o impacto que o processo de Gestão de Vulnerabilidades possui na Resposta a Incidentes, elucidada no Capítulo 2, e o ganho obtido ao utilizá-la como parte da Prevenção de Incidentes, também abordada no Capítulo 2 de uma instituição. São expostos, no Capítulo 4, os locais da UFRJ onde parte do processo de Gestão de Vulnerabilidades foi implantado e como a quantidade de incidentes destes locais foi afetada.

1.5 Descrição

O presente trabalho é descrito em 5 capítulos. No Capítulo 1 é apresentado o tema e uma abordagem geral do cenário de vulnerabilidades da UFRJ, as justificativas para a confecção deste trabalho, seu objetivo e motivação.

No capítulo 2 é realizada uma revisão dos conceitos necessários para a compreensão do estudo. Os conceitos abordados são sobre segurança da informação, gestão de risco, tratamento de incidentes e gestão de vulnerabilidades.

No capítulo 3 é realizado uma avaliação do cenário atual da UFRJ. São especificadas as vulnerabilidades encontradas, os meios de notificação de incidentes e demonstrada a relação entre vulnerabilidades encontradas e incidentes identificados.

No capítulo 4 são expostas as sugestões de melhora para segmentos do processo de resposta a incidentes da UFRJ. Esta etapa abrange a avaliação dos riscos associados às vulnerabilidades encontradas, procedimentos técnicos para mitigação destas e soluções para melhoria do processo atual. Também são apresentados casos de sucesso ao se aplicar a gestão de vulnerabilidades em duas unidades da UFRJ.

O capítulo 5 possui as considerações finais sobre o estudo realizado. Explica-se o impacto que a gestão de vulnerabilidades possui sobre a ocorrência de incidentes em uma instituição acadêmica e recomenda-se procedimentos e atos complementares para melhorar a segurança em trabalhos futuros.

Capítulo 2

Referencial Teórico

Neste capítulo são apresentados conceitos sobre segurança da informação que são necessários para a compreensão do trabalho. São expostos inicialmente os pilares da segurança da informação, conceitos sobre risco e impacto. Também é explicado o conceito de gestão de vulnerabilidades e resposta a incidentes.

2.1 Segurança da Informação

A Segurança da Informação baseia-se na proteção de dados que tem valor para algum indivíduo ou organização, sendo estes dados privados ou expostos publicamente. Ela possui três requisitos básicos chamados de Pilares Fundamentais da Segurança da Informação [29] que estão ilustrados na Figura 2.1.

- **Confidencialidade** - É o princípio que garante que apenas pessoas autorizadas terão acesso e conhecimento daquela informação.
- **Integridade** - É o princípio que garante que a informação não foi alterada ou violada indevidamente.
- **Disponibilidade** - É o princípio que garante que a informação deve estar disponível para acesso sempre que desejado.

Sendo assim, a quebra de apenas um dos pilares é o suficiente pra afirmar que a



Figura 2.1: Pilares da Segurança da Informação

segurança daquela informação não foi garantida [29].

2.2 Conceitos Necessários

Para entender melhor a motivação e a metodologia do nosso estudo, precisamos introduzir os conceitos de Vulnerabilidade, Incidente, Ameaça, Risco e Impacto, para utilizar métricas para a classificação das vulnerabilidades e de seus riscos associados.

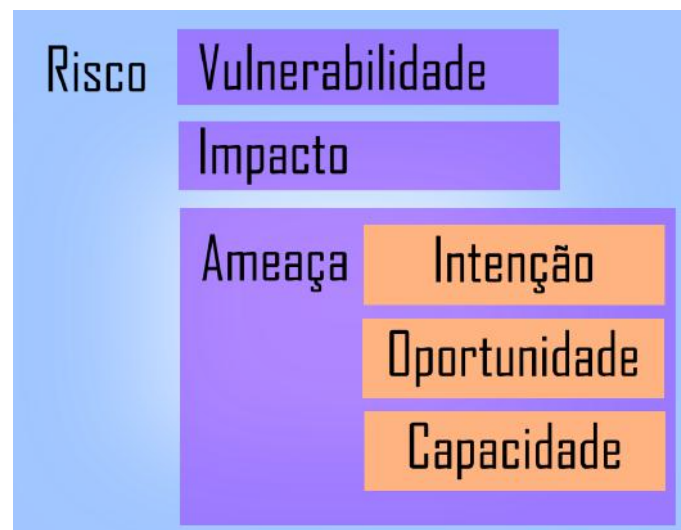


Figura 2.2: Relação entre os Conceitos de Segurança da Informação

As **vulnerabilidades** são fraquezas ou brechas presentes nos sistemas que podem sofrer com a exploração de ameaças permitindo assim a ocorrência de um Incidente

de Segurança. Elas, por serem elementos passivos, não causam o incidente, pois necessitam obrigatoriamente de um agente causador [7].

Ameaças são a possibilidade de um agente, interno ou externo, explorar acidentalmente ou propositalmente uma vulnerabilidade específica [3]. Os sub-conceitos de ameaça importantes a serem analisados são:

- **Intenção:** é a vontade de um agente de atacar um alvo específico. Não pode ser influenciado por ações de segurança, já que trata-se apenas do que motiva o atacante.
- **Oportunidade:** ter conhecimento sobre alvo e do caminho a percorrer para explorar a vulnerabilidade.
- **Capacidade:** é a habilidade do atacante de explorar determinada brecha do sistema e aproveitar uma oportunidade.

O **Incidente de Segurança** é um evento inesperado ou indesejado que ocorreu em um sistema de informação. Ele pode ser considerado como a concretização da ameaça que implicou na quebra de, pelo menos, um dos pilares fundamentais da segurança da informação.

Tipos de incidente comuns são: “Negação de Serviço” (DDoS), que visa impedir ou dificultar o acesso legítimo a sistemas, redes ou aplicações exaurindo seus recursos de *hardware*; “Código Malicioso” (*malware*), que é um programa ou pedaço de código que infecta uma máquina a fim de causar algum prejuízo a mesma; “Uso Inapropriado”, que ocorre quando há violação do uso aceitável de algum recurso da instituição, que deve ser definida na política de segurança [12]. O conceito de política de segurança é abordado na seção 2.4.

A relação entre vulnerabilidade e incidente sucede do fato que a vulnerabilidade é a brecha que leva a ameaça a produzir um incidente. Podemos dizer que o **impacto** de um incidente são as potenciais consequências que este incidente possa causar à instituição [3]. O **risco** associado a um incidente é a relação entre a probabilidade de ocorrência e o respectivo impacto, onde **probabilidade** é a chance da falha

de segurança acontecer baseada nas vulnerabilidades encontradas, como mostra a equação 2.1. A Figura 2.2 ilustra a relação entre esses conceitos. Essa é a base para a identificação dos pontos que demandam por investimentos em segurança da informação [3].

$$risco = probabilidade \times impacto \quad (2.1)$$

2.3 Matriz de Risco

O risco da exploração de uma vulnerabilidade, por parte de uma ou mais ameaças, pode ser calculado atendendo a dois fatores: o grau de impacto da vulnerabilidade existente e a probabilidade de ocorrência desta. A **Matriz de Risco** serve para avaliar os riscos envolvidos nos projetos. É formada por dois eixos principais: o de probabilidade de ocorrência de uma situação (eixo vertical) e o de impacto desta situação no projeto (eixo horizontal) [16]. Para os fins deste trabalho utilizaremos a **Matriz Simples de Somerville**, representada na Tabela 2.1, que classifica os riscos em “Alto”, “Médio” e “Baixo” [4]. Outros métodos para o cálculo do risco associado as vulnerabilidades possuem mais níveis de classificação, todavia, tendo em vista a característica heterogênea dos dados coletados, em questão de quantidade, utilizamos esta escala.

O **eixo da probabilidade** contém três classificações, que são interpretadas como: “Alta”, onde a chance do evento ocorrer é grande e / ou frequentemente ele ocorre de fato; “Média”, onde há probabilidade ocasional de acontecimento do evento; “Baixa”, onde há pouca chance de acontecer algum problema advindo desse evento [4]. A Tabela 4.1 mostra como foi realizada a classificação entre “Alta”, “Média” e “Baixa” para o conjunto de dados da UFRJ e possui na seção 4.1 maiores explicações sobre sua construção. É importante perceber que só é possível identificar se a frequência de uma vulnerabilidade é “Alta” ou “Baixa” após analisar os dados coletados. Essa classificação é diferente para conjuntos de dados distintos.

O **eixo do impacto** contém três classificações, que são interpretadas como:

“Alto”, quando o evento ocorrido quebra mais de um dos pilares da segurança; “Médio”, quando o evento ocorrido quebra um dos pilares da segurança ; “Baixo”, quando o evento causa a quebra parcial ou momentânea dos pilares da segurança. A relação entre estas duas variáveis permite, de forma simplificada, obter o valor associado ao risco de cada vulnerabilidade, como demonstrado na Tabela 2.1. O valor 3 (três) simboliza o mais alto risco e o que possui maior prioridade de intervenção; o valor 2 (dois) o risco médio; o valor 1 (um) o risco mais brando e o que possui menor prioridade de intervenção [4].

Embora exista a escala de *Common Vulnerability Scoring System* (CVSS) [20], que avalia o impacto de vulnerabilidades, não foi interessante utilizá-la. Pois em sua última versão são utilizados quatro níveis de impacto, o que não está adequada com o tipo de matriz de risco que é utilizada para a avaliação das vulnerabilidades. A matriz de risco foi escolhida de forma que distribuisse da melhor forma possível as probabilidades de ocorrência das vulnerabilidades, dado os dados obtidos.

R = P x I	Probabilidade		
	Baixo	Médio	Alto
Impacto			
Baixa	1	1	2
Média	1	2	3
Alta	2	3	3

Tabela 2.1: Matriz de Risco utilizada no método Somerville

2.4 Política de Segurança da Informação

O documento da Política de Segurança é essencial para as instituições poderem estabelecer orientação sobre um padrão desejável para proteção de suas informações, sendo que, de forma complementar, podem ser publicadas normas e procedimentos a serem seguidos [11].

A política de Segurança é constituída de diretrizes, que têm papel estratégico e definem a importância da segurança da informação para a instituição. As normas possuem caráter tático e descrevem situações, processos específicos e fornecem

orientação para o uso adequado das informações. Os procedimentos são descrições operacionais de ações que devem ser seguidas em cada situação que venha ocorrer. Podemos observar que as normas são desdobramentos das diretrizes da política e os procedimentos são desdobramentos das normas [8] [3].

O documento da Política de Segurança deve ser seguido pelos funcionários da instituição e, para isso, sua divulgação deve ser ampla, com texto claro e reuniões frequentes para reavaliar novas necessidades e a eficiência das normas que podem precisar de adequações.

2.5 Resposta a Incidentes

O conceito de Respostas a Incidentes é baseado em um conjunto de ações que podem ser tomadas para recuperar o sistema (*software* ou processo) do evento ocorrido. O processo de Resposta a Incidentes pode ser dividido em quatro fases, como mostra a Figura 2.3 [12]. Essas fases são explicadas a seguir.



Figura 2.3: Ciclo de Resposta a Incidentes [12].

Preparação é a etapa na qual a estrutura para a detecção e prevenção de incidentes é implantada e aprimorada. Sem ela, não é possível realizar qualquer tipo de resposta satisfatória aos incidentes que podem vir a ocorrer na instituição, pois não há definição de escopo do que deve ser monitorado e procurado na rede, nem métodos de monitoramento.

Uma das fases da preparação é a prevenção de incidentes. O objetivo da prevenção é manter os índices de incidentes o mais baixo possível a fim de melhorar o desempenho da instituição. Quando um incidente ocorre, alguns serviços são danificados ou tornam-se indisponíveis, causando transtornos para o negócio. A prevenção

consiste em realizar revisões periódicas nos sistemas e aplicações utilizadas pela empresa, além de monitorar atividades na rede a fim de identificar ações maliciosas [12].

Algumas ações que podem ser consideradas como prevenção de incidentes são: gerenciamento de *patch* (atualizações de *software*), configurações voltadas para a segurança (*hardening*) de máquinas, utilização de softwares de IPS (*Intrusion Prevention System*, em português Sistema de Prevenção de Intrusão) e treinamentos regulares sobre as normas de segurança da informação da instituição.

O processo de gestão de vulnerabilidades também é considerado uma prática de prevenção. O ato de resolver e mitigar vulnerabilidades existentes nos sistemas dificulta a ação maliciosa de usuários, visto que há diminuição de brechas a serem exploradas.

Detecção e análise é a etapa na qual os incidentes reportados ou identificados são analisados, estudados e categorizados. Esta é uma etapa importante pois direciona os tipos de ações utilizadas na próxima etapa. Para realizar a detecção de alguma anomalia na rede ou nos sistemas podem ser utilizadas ferramentas de monitoramento, que auxiliam na visualização do problema e na posterior análise [12].

Ressaltamos que para identificar uma atividade como incidente é importante conhecer o comportamento esperado da utilização dos sistemas e da rede, para então comparar com a atividade suspeita. Após identificada alguma irregularidade na utilização dos recursos, é realizada a categorização do incidente como “Negação de Serviço”, “Código Malicioso”, “Acesso não autorizado”, “Uso Inapropriado” ou outra categoria. Também é possível que um incidente possua mais de uma categoria, por exemplo: uma máquina infectada por um *malware* pode causar uma negação de serviço em uma outra máquina da mesma rede.

Na etapa de **Contenção, Eliminação e Recuperação** ocorrem três ações importantes: a contenção do sistema infectado, para prevenir que mais danos sejam causados à instituição, a eliminação da causa raiz do incidente, para que o problema

não aconteça novamente no mesmo sistema e a recuperação do sistema, a fim de voltar a normalidade das atividades. Uma das fases desta etapa é o tratamento de incidentes que ocorre durante as três ações. O objetivo do tratamento é efetivamente resolver o problema causado pelo incidente, realizando a contenção e eliminação do problema. É importante ressaltar que diferentes tipos de incidente podem necessitar de tratamentos distintos [12].

Alguns métodos de tratamento para determinados tipos de incidente são [31]: “Negação de Serviço” - Configurar os servidores para proteção contra excesso de requisições HTTP e SYN, bloquear IPs identificados como originários dessas requisições; “Código Malicioso (*malware*)” - isolar a(s) máquina(s) infectadas o mais breve possível, a fim de evitar novas infecções, realizar uma varredura na rede para verificar se existem outras máquinas comprometidas; “Acesso não autorizado” - detectar, monitorar e investigar as tentativas de acesso, principalmente dos usuários que possuem acesso a informações sensíveis e/ou críticas e dos usuários que possuem privilégios no sistema, bloquear tentativas de acesso identificadas como ilegítimas. O **Aprimoramento** é a etapa na qual verifica-se quais são os pontos fracos da instituição que permitiram a ocorrência do incidente e analisam-se os dados coletados nas fases anteriores com o intuito de melhorar o processo de resposta [12].

2.6 Gestão de Vulnerabilidades

O conceito de Gestão de Vulnerabilidade, como definido em [23], pode ser compreendido como o processo no qual as vulnerabilidades de um sistema (*software* ou processo) são identificadas e o risco associado a cada uma delas é avaliado para corrigir-las, remover ou mitigar seus riscos associados ou obter uma aceitação formal do mesmo.

É importante ressaltar que vulnerabilidades sempre irão existir em sistemas e instituições, pois é impossível identificar e corrigir todos os pontos de falha em todos os softwares utilizados. O objetivo da gestão de vulnerabilidades é fornecer informações para tomada de decisão e priorização de resoluções e mitigação dos

pontos fracos.

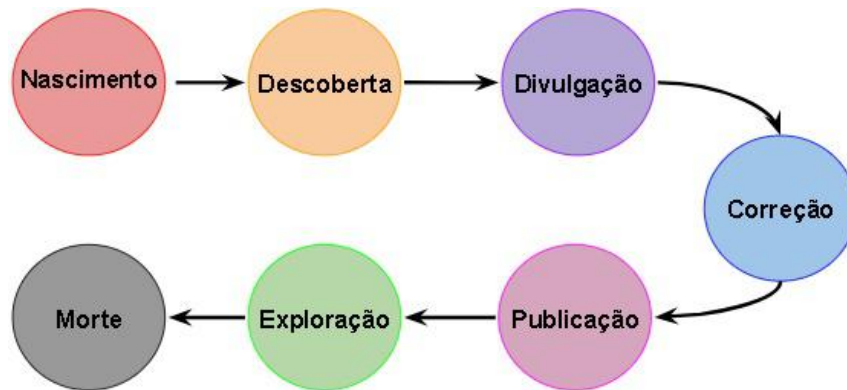


Figura 2.4: Ciclo de Vida de Vulnerabilidades

Um conceito importante é o de **Ciclo de Vida de Vulnerabilidades**. O termo “Ciclo de Vida” descreve uma mudança de estado, onde cada estado representa uma etapa. É definido um ciclo, pois o primeiro estado é o nascimento e o último é a morte do processo. As etapas do Ciclo de Vida de Vulnerabilidade são: nascimento, descoberta, divulgação, correção, publicação e exploração, como está mostrado na figura 2.4 [35].

Na etapa de **Nascimento**, considera-se a criação da falha que normalmente ocorre involuntariamente. As vulnerabilidades surgem, principalmente de três fontes: erros de programação, má configuração de serviço e falha humana. Se o nascimento da falha é intencional, as etapas *nascimento* e *descoberta* se unem. Por consenso considera-se que a vulnerabilidade só existe no ambiente em produção (desconsidera-se testes). Na **Descoberta** temos a situação onde alguém encontrou a vulnerabilidade, seja usuário comum ou um agente mal-intencionado. Esta etapa pode nunca vir a ser conhecida se o responsável por descobrir não revelar publicamente.

A **Divulgação** acontece quando a vulnerabilidade descoberta é revelada publicamente. Isso pode ser feito através de listas de vulnerabilidade, ou em fóruns de segurança. Uma vulnerabilidade é corrigida quando é disponibilizado um *patch* de correção para os usuários ou uma mudança de configuração é aplicada a fim de retirar a falha. Isso ocorre na etapa de **Correção**. Na **Publicação** a divulgação da

vulnerabilidade sai do controle, fazendo com que esta seja em grande escala. Isso pode acontecer de várias maneiras: Notícia detalhando a falha, um CSIRT emitindo um relatório, entre outros.

No processo de **Exploração** os agentes maliciosos que conseguiram tirar proveito da brecha, lançam *scripts* ou tutoriais para que qualquer um consiga fazer a exploração. A última etapa, **Morte** de uma vulnerabilidade, acontece quando há um número insignificante de alvos com a brecha. Isso acontece quando os administradores lançam atualizações ou o sistema é substituído, ou outra situação que tire os interesses dos atacantes e da mídia sobre a vulnerabilidade.

Na etapa de descoberta do ciclo de vida, há o surgimento de *exploits* Zeroday - uma vulnerabilidade não explorada e não documentada, onde não há correção disponível. A brecha é considerada zeroday apenas quando foi descoberta por terceiros, pois significa que a empresa e os desenvolvedores não tiveram tempo de proteger sua aplicação [10].

O processo de **Gestão de Vulnerabilidades** possui cinco fases, como demonstra a Figura 2.5.



Figura 2.5: Ciclo de Gestão de Vulnerabilidades

A **Preparação** é a fase na qual é decidido o escopo da gestão de vulnerabilidades, quais sistemas serão incluídos e quais os tipos de varredura serão realizadas. Para isso, é realizado um inventário das máquinas que serão monitoradas e escaneadas de tempos em tempos. Também são definidas quais e quantas vulnerabilidades serão procuradas por vez. Inicialmente é comum que essa quantidade seja pequena e cresça aos poucos para facilitar a implantação das medidas necessárias para a mitigação das vulnerabilidades encontradas [23].

Varredura de Vulnerabilidades é a fase na qual são realizadas varreduras nos sistemas para verificar quais vulnerabilidades selecionadas para busca existentes neles. Esta etapa pode demorar entre horas e dias, dependendo da quantidade de sistemas e vulnerabilidades a serem escaneadas. As varreduras podem causar lentidão nos serviços oferecidos pela instituição. Neste caso deve se estudar uma forma de reduzir o impacto delas nas atividades [23].

No que se refere a varreduras, é escolhido se serão utilizadas varreduras internas, externas ou ambas. Varreduras externas são capazes de identificar vulnerabilidades que podem ser detectadas por atacantes que estejam fora da rede da organização. O resultado obtido por este tipo de varredura fornece, além das vulnerabilidades encontradas, uma visão das configurações presentes na rede para evitar ataques. Varreduras internas são realizadas na rede interna da organização e fornecem uma ideia de quais configurações a máquina possui para evitar ataques [23].

Na **Definição de Ações** são decididas as ações a serem tomadas para cada tipo de vulnerabilidade encontrada e são identificados os riscos e o impactos correspondente a elas. A solução para a vulnerabilidade pode está na alteração de alguma configuração de um *software*, na atualização de um *software* ou na remoção completa de um serviço desnecessário. Porém, em alguns casos não é possível resolver completamente o problema encontrado, então o risco associado à vulnerabilidade é aceito e são elaboradas formas de proteger o sistema vulnerável [23]. Um caso típico desse tipo ocorre quando um software que possui uma determinada vulnerabilidade, conhecida pelos administradores, necessita ser utilizado pela organização. Neste caso assume-se o risco presente e são sugeridas práticas para dificultar a exploração da vulnerabilidade. Na seção 4.5 é abordado um caso onde ocorreu esse tipo de situação na UFRJ.

A **Implementação de Ações** é a fase na qual são implantadas as ações decididas na fase anterior. Os resultados da implantação das soluções deve ser avaliado e registrado para verificar se houve ou não impacto negativo nos sistemas. Caso haja impacto negativo, a solução elaborada na fase anterior deve ser alterada de forma a manter a normalidade dos sistemas [23]. Pode ser necessário realizar uma

nova varredura a fim de verificar a eficiência das ações postas em prática na fase anterior, e realizada de forma semelhante à varredura inicial e buscando as mesmas vulnerabilidades.

É importante perceber que sem um processo de gestão de vulnerabilidades a instituição não terá como saber os riscos cibernéticos aos quais ela está exposta, nem os impactos que podem ser causados na exploração de alguma brecha. Sem esse gerenciamento de riscos, não há como prever quais incidentes terão maior chance de ocorrer. Isto torna o cenário de tratamento de incidentes mais lento já que eles podem não seguir um padrão de tipo ou local de ocorrência.

Capítulo 3

Análise do Cenário

Este capítulo descreve o quadro cibernético da UFRJ. É explicado como foi realizada a coleta de dados dos sistemas de notificações e as dificuldades encontradas neste processo. São expostas as vulnerabilidades e os incidentes identificados pela instituição, bem como suas respectivas incidências e descrições.

3.1 Contexto cibernético da UFRJ

A estrutura da rede da UFRJ é controlada pela SuperTIC, que administra o *backbone* da universidade. Ele é formado por comutadores de camada 3 (camada de rede no modelo OSI), roteadores, pontos de acesso e controladores de redes sem fio. Uma característica dessa estrutura é o controle descentralizado das sub-redes, ou seja, há responsáveis técnicos pelas redes locais que tomam suas próprias decisões e colocam equipamentos, servidores e estações de trabalho locais que não podem ser vistos ou controlados pela superintendência. Essa situação pode ser um problema se não houver normas e padrões na montagem de servidores e não houver o cumprimento de uma mesma política de segurança. Sem uma padronização de normas, não há como definir qual ação deve ser seguida por cada administrador de servidor ou rede, permitindo que serviços sejam instalados sem configuração de segurança e, por este motivo, gerando brechas de segurança na instituição.

A universidade possui uma sub-rede /16, três sub-redes /23 e três sub-redes /24, resultando num total de 67.826 endereços IP reais disponíveis. Até a data da coleta de dados, foram identificados 472 equipamentos ativos de rede. Ressalta-se também que a instituição figura entre as maiores universidades do país, com 52.848 alunos da graduação [26] (ativos e com matrícula trancada), 15.055 funcionários (docentes e técnicos) [25] divididos em aproximadamente 75 unidades com atuação em 3 cidades [9]. Com a análise destes dados, levando em conta a complexidade de se manter uma instituição geograficamente dispersa e com tantos usuários, é possível mensurar a rede da UFRJ como de grande porte.

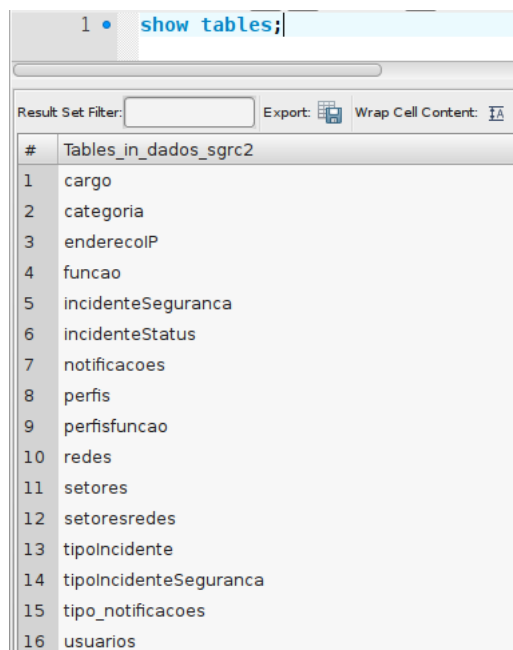
A UFRJ possui uma Política de Segurança [34] que contém 8 itens, de caráter gerais. Os tópicos abordam o objetivo do documento, a estrutura normativa da segurança da informação na UFRJ, define as atribuições de responsabilidades por parte da SuperTIC, diretores de unidades e comunidade acadêmica. Não existem no documento ações a serem executadas em caso de incidentes ou em ocorrência de vulnerabilidade, e não houve qualquer atualização do documento desde sua criação em 2012.

3.2 Coleta de dados

Nesta seção é explicado como foi realizada a coleta e mineração de dados para a análise do cenário atual de incidentes e vulnerabilidades da UFRJ. Como mencionado na seção 1.3, a UFRJ possui três sistemas que contém dados sobre varreduras de vulnerabilidades e incidentes: SGIS, SGRC e OSTicket. O sistema OSTicket não possui um modo de filtragem eficiente que permite a extração dos dados por tipo de incidente, vulnerabilidade ou outro modo de agrupamento de informações de um mesmo tipo, para obter as informações acerca do cenário atual de incidentes e vulnerabilidades foram recolhidos dados dos sistemas SGIS e SGRC.

No caso do SGRC, sistema utilizado apenas pela DSI para notificar incidentes e vulnerabilidades aos administradores de rede, os dados foram extraídos diretamente do *dump* do banco de dados do sistema, que foi realizado no dia 07 de Março de

2017 e que contém os dados de 2014, quando entrou em produção, até 2017. Pela urgente necessidade da DSI em obter um sistema que realizasse notificações de forma automática, o SGRC entrou em produção ainda sem possuir todas as funcionalidades planejadas, sem previsão de implementação de funcionalidades pendentes e não foi possível obter a documentação do sistema. Isto impactou diretamente as informações que eram gravadas no banco de dados, desenvolvido com o Sistema de Gerenciamento de Banco de Dados (SGBD) *MySQL* e com os scripts em *SQL*, bem como as relações internas entre tabelas.



```
1 • show tables;|
```

#	Tables_in_dados_sgrc2
1	cargo
2	categoria
3	enderecolP
4	funcao
5	incidenteSeguranca
6	incidenteStatus
7	notificacoes
8	perfis
9	perfisfuncao
10	redes
11	setores
12	setoresredes
13	tipoincidente
14	tipoincidenteSeguranca
15	tipo_notificacoes
16	usuarios

Figura 3.1: Tabelas presentes no banco de dados do sistema SGRC.

O arquivo de *dump* do banco de dados contém a estrutura de todas as tabelas planejadas inicialmente para o sistema, porém apenas as tabelas com informações sobre os incidentes foram relevantes para este estudo. A Figura 3.1 mostra todas as tabelas presentes no banco do SGRC. Destas, duas tabelas destacam-se: “tipoincidente”, que relaciona um número de identificação para cada tipo de vulnerabilidade ou incidente, como mostra a Figura 3.2; “notificacoes”, que contém os dados das notificações enviadas aos administradores de rede, como mostra a Figura 3.3. Porém, observando as duas Figuras, apenas com as tabelas “tipoincidente” e “notificacoes” não é possível realizar uma contagem dos números de incidentes e vulnerabilidades. O atributo “tipoincidente” presente na tabela “notificacoes” que, aparentemente,

deveria relacionar as notificações ao seu tipo de vulnerabilidade / incidente nem sempre possui um valor atribuído ou possui o mesmo valor de tipo de incidente para situações, descritas no campo “descricao”, diferentes.

The screenshot shows a SQL query window with the following content:

```
1 • SELECT * FROM tipoIncidente
```

The result set is displayed in a table with two columns: 'idtipoincidente' and 'descricao'.

idtipoincidente	descricao
1	Host infectado com Bot - Botnet
2	DNS Recursivo Aberto
3	Invasão de Página Web
4	Phishing
5	Spam
7	Violação de Direitos Autorais
10	Ataque de Força Bruta SSH
11	Vulnerabilidade no OpenSSL
12	Negação de Serviço
13	SSDP aberto
14	NetBios aberto
15	IPMI aberto
16	Servidores NTP vulneráveis
17	Servidores SNMP vulneráveis
18	Host(s) aparentemente com o serviço de QOTD
19	Host executando protocolo NAT-PMP
20	Servidores Memcached vulneráveis
21	Servidores MS-SQL vulneráveis
22	Servidor Jboss comprometido
23	Open DNS Resolver
24	Servidores Redis vulneráveis
25	Servidores SSL vulneráveis
26	Vulnerabilidade
27	Vulnerabilidade no serviço PortMapper
28	Vulnerabilidade no Protocolo mDNS
29	Tentativas de acesso não autorizado
30	Servidor Comprometido por Vulnerabilidade
31	Host executando atividades possivelmente mali

Figura 3.2: Lista de vulnerabilidades e incidentes com seus respectivos números de identificação no sistema SGRC.

Para solucionar esse problema, foi elaborado um *script SQL* para realizar uma série de comandos do tipo *update* no banco de dados, a fim de incluir no atributo “tipoincidente” da tabela “notificacoes” o número correspondente ao tipo de problema do qual a notificação se trata, como mostrado na Figura 3.2, que ilustra a tabela de “tipoIncidente”. Para isso foram analisadas palavras chaves contidas no campo “descricao”, presente na tabela “notificacoes” das tuplas que possuíam campo “tipoincidente” nulo. Este processo foi realizado até que não houvesse mais tuplas com o campo “tipoincidente” nulo. Por exemplo, para notificações de incidentes do tipo “violação de direitos autorais”, expressões como “autorais”, “bittorrent” e “copyright”

estavam presentes no campo “descricao” da tabela “notificacoes”. Essas expressões foram utilizadas para filtrar as tuplas de notificações e atualizar seu campo “tipoincidente”. Após todo esse processo, foi realizada uma nova consulta ao banco de dados, dessa vez para realizar a contagem de quantos incidentes de cada tipo foram encontrados para cada incidente. Ressalta-se que esse processo foi demorado, dado a quantidade de tuplas existentes no banco de dados, pois o SGRC não é utilizado exclusivamente para notificar incidentes, vulnerabilidades também.

Os dados coletados do SGRC referem-se apenas a incidentes notificados, visto que o SGIS guarda todas as informações sobre vulnerabilidades. O número total de incidentes notificados utilizando o sistema SGRC, desde seu início em Agosto de 2013 até 07 de março de 2017 é 8.755. A partir da quantidade absoluta obtida de cada incidente foi realizado um cálculo de frequência relativa que gerou o gráfico 3.9 e a interpretação dele será abordada na seção 3.4.

idnotificaca	endereco_ip	descricao	data	idtipoNotific	idusuario	idincidenteSeguran	tipoincidente
645	146.164.2.18	Arquivo malicioso	2013-09-09 11:05:54	1	3	457	1
646	146.164.61.3	Host infectado	2013-09-09 11:12:58	1	3	458	1
647	200.20.112.147	Host infectado	2013-09-09 11:16:05	1	3	459	1
648	146.164.80.7	Host infectado	2013-09-09 11:16:08	1	3	460	1
649	146.164.26.19	Host infectado	2013-09-09 11:16:09	1	3	461	1
650	146.164.111.2	Host infectado	2013-09-09 11:16:11	1	3	462	1
651	146.164.22.197	Host infectado	2013-09-09 11:17:14	1	3	463	1
652	146.164.80.48	Host infectado	2013-09-09 11:18:43	1	3	464	1
653	146.164.2.18	Host infectado	2013-09-09 11:22:09	1	3	465	1
654	146.164.2.18	Alerta de Phishir	2013-09-09 14:40:30	1	4	NULL	4
655	146.164.92.133	Hacking Activity	2013-09-09 14:51:15	1	4	NULL	NULL
656	146.164.29.51	Host Infectado c	2013-09-09 17:02:54	1	2	466	1

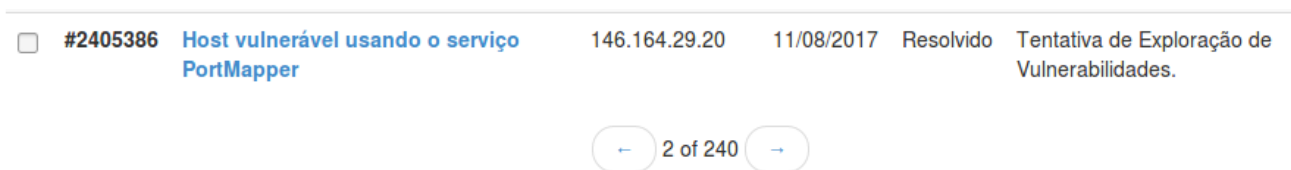
Figura 3.3: Resultado da tabela de notificações do sistema SGRC.

No caso do SGIS, sistema da RNP, a coleta foi realizada utilizando a própria interface do sistema, visto que este não pertence a UFRJ e não é possível obter acesso ao seu banco de dados. O SGIS também não possui um sistema de filtragem de dados satisfatório, visto que a versão em produção está em constante aprimoramento. Para realizar filtragem de vulnerabilidades, foi acessada a plataforma e utilizado o campo “Procurar”, no qual foi inserido o nome da vulnerabilidade que se desejava encontrar os dados, como ilustra a Figura 3.4. Porém, esta triagem retorna apenas

o número total de vulnerabilidades do tipo desejado que foram notificadas a UFRJ, sem um campo para selecionar a data das notificações. Para resolver este problema, foi necessário utilizar a navegação de listagem, encontrada ao final da página de consulta, como ilustra a Figura 3.5 e explicada abaixo. O retorno desta busca divide os resultados em páginas com 100 notificações cada, não podendo personalizar este número.



Figura 3.4: Campos de busca presentes no sistema SGIS.



<input type="checkbox"/>	#2405386	Host vulnerável usando o serviço PortMapper	146.164.29.20	11/08/2017	Resolvido	Tentativa de Exploração de Vulnerabilidades.
--------------------------	----------	---	---------------	------------	-----------	--

← 2 of 240 →

Figura 3.5: Rolagem de página do sistema SGIS.

Para realizar a contagem anual de um tipo de vulnerabilidade, foi buscado na interface o tipo desejado da vulnerabilidade; ordenou-se as notificações por data; contou-se quantas páginas inteiras de notificações de um determinado tipo de vulnerabilidade existem e multiplicou-se esse valor por 100 (número fixo de notificações por página); após isso, foi somado o valor que fosse remanescente em outra página. Este processo foi feito para todas as 17 vulnerabilidades presentes no SGIS. O número total de vulnerabilidades reportadas pelo SGIS, desde quando iniciou sua varredura na UFRJ em janeiro de 2015 até 10 de agosto de 2017 foi de 125.840. A partir da quantidade absoluta obtida de cada vulnerabilidade, de forma geral e na filtragem dos anos de 2016 e 2017, foi realizado um cálculo de frequência relativa que gerou respectivamente os gráficos 3.6, 3.7 e 3.8 e a interpretação deles será abordada na seção 3.3.

3.3 Vulnerabilidades identificadas

Atualmente a DSI da UFRJ utiliza, para coleta de dados sobre as vulnerabilidades existentes, o sistema SGIS, que realiza varreduras diárias na rede. Esse sistema verifica e notifica dezessete tipos distintos de vulnerabilidades, das quais dezesseis são provenientes da má configuração das aplicações instaladas.

Analisando as notificações recebidas, é possível observar que algumas aplicações ou protocolos recebem muito mais notificações de vulnerabilidades do que outras, como mostra a Figura 3.6, que contém a proporção das vulnerabilidades da UFRJ desde janeiro 2015 até fevereiro de 2017. Os serviços relacionados aos cinco protocolos presentes no gráfico 3.6 são responsáveis por 85,69% das notificações recebidas pela DSI nesse intervalo de tempo, sendo que apenas dois dos protocolos possuem percentual acima de 10%, demonstrando assim a concentração das notificações de determinado tipo. As 12 vulnerabilidades restantes possuem um percentual menor que 5% cada uma. Elas estão presentes nos seguintes serviços / protocolos: LDAP; DB2; IPMI; MongoDB; SSDP; NetBios; ElasticSearch; Xdmcp; TFTP; Redis; Microsoft SQL; NTP; Memcached. Analisando os anos de 2016 e 2017, percebe-se que as vulnerabilidades que se destacam ao longo do tempo se mantêm entre as mais frequentes, como mostram as Figuras 3.7 e 3.8, respectivamente.

O SGIS adiciona anualmente novos *scripts* para varredura de vulnerabilidades e realiza alterações nos algoritmos para reduzir o número de falsos positivos encontrados. O critério utilizado pela RNP para criar e alterar os *scripts* não é divulgado. As vulnerabilidades sobre DNS recursivo, SSL e SNMP são notificadas a UFRJ desde 2015 e PortMapper e mDNS são notificadas desde 2016.

Para este estudo, as cinco vulnerabilidades com maior índice de notificações recebidas desde 2015 conforme a 3.6 serão estudadas. Cabe aqui ressaltar que, nos anos de 2016 e 2017, é possível identificar, com base na rotina de notificações atual, onde é comum obter diariamente entre 100 e 300 notificações, foi constatado que o grande volume de notificações recebidas pela DSI acerca das cinco vulnerabilidades mencionadas na Figura 3.6 dificultam a observação e a resolução das outras

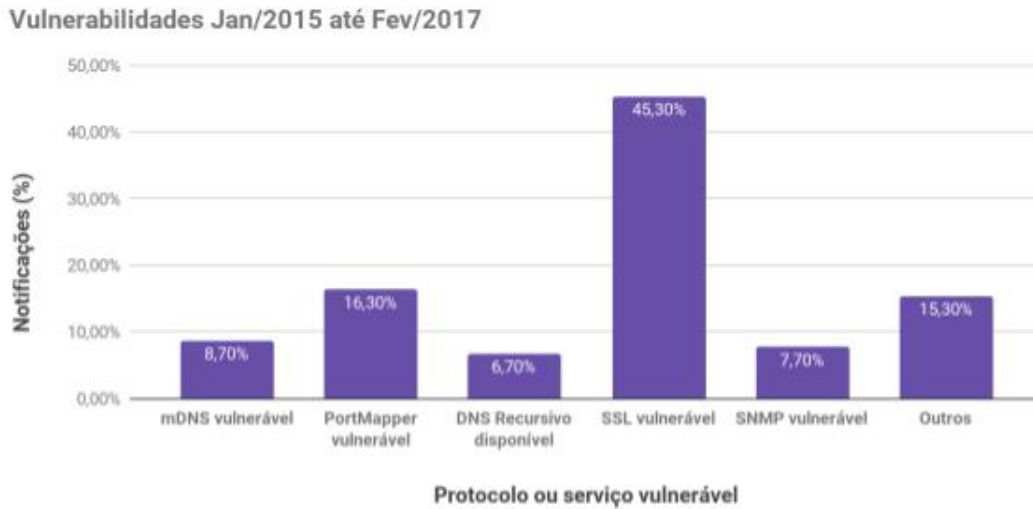


Figura 3.6: Percentual das Vulnerabilidades Gerais da UFRJ

Observação: O número total de vulnerabilidades notificadas é 125.840. As vulnerabilidades catalogadas como “Outros” possuem, cada uma, menos de 5% de incidência.

vulnerabilidades notificadas, pois as vulnerabilidades são expostas no sistema SGIS em grupos de cem e ordenadas por data. Sabe-se também que ao receber diversas notificações acerca de um determinado tipo de vulnerabilidade, estas podem não receber a devida atenção dos administradores de rede e sistemas e acabar por não ser solucionadas de maneira efetiva. Nos anos de 2016 e 2017 é possível identificar um outro serviço vulnerável presente nas Figuras 3.7 e 3.8, o TFTP (*Trivial File Transfer Protocol*). A vulnerabilidade neste serviço passou a ser identificada pela RNP no ano de 2016 e desde então Figura entre os cinco mais notificados. O TFTP possui uma vulnerabilidade que, se explorada, afeta apenas a máquina que o executa. Em contrapartida a vulnerabilidade que afeta o DNS pode afetar diversas máquinas. Por este motivo e por não haver redução significativa de notificações desde 2015 até 2017 sobre a vulnerabilidade no DNS, neste trabalho foi escolhido tratar desta vulnerabilidade e não da presente no TFTP.

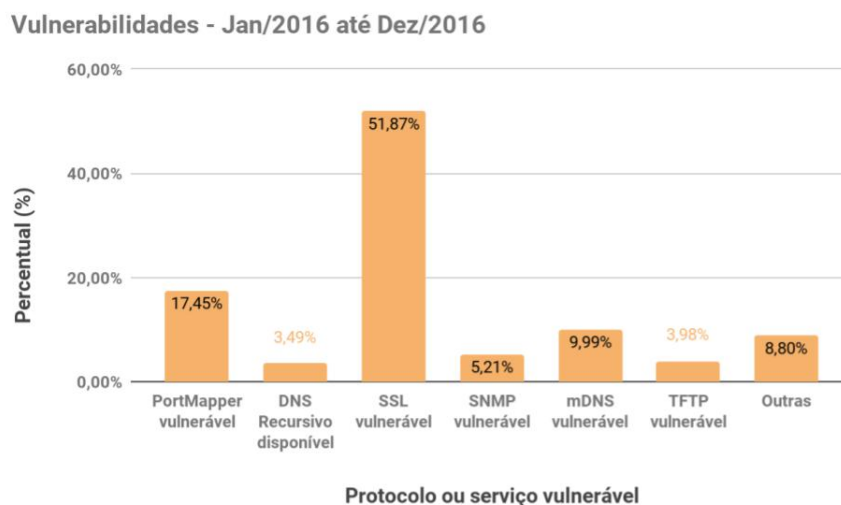


Figura 3.7: Percentual das Vulnerabilidades UFRJ - 2016

Observação: O número total de vulnerabilidades notificadas é 61.269. As vulnerabilidades catalogadas como “Outros” possuem, cada uma, 3,0% de incidência ou menos.

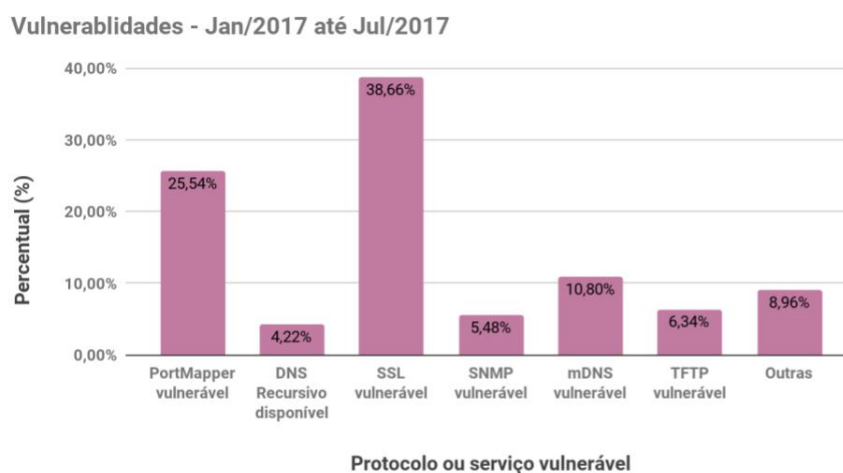


Figura 3.8: Percentual das Vulnerabilidades UFRJ - 2017

Observação: O número total de vulnerabilidades notificadas é 41.493. As vulnerabilidades catalogadas como “Outros” possuem, cada uma, menos de 4,0% de incidência.

Para poder resolver de forma bem-sucedida os problemas notificados, é necessário primeiramente identificar e conhecer os serviços que serão alvos das resoluções e o tipo de vulnerabilidade presente neles. Abaixo estão explicados os serviços e seus

respectivos problemas.

O protocolo **SSL**, é utilizado para fazer a troca criptografada de mensagens entre servidores e clientes. Embora o SSL atualmente seja um protocolo ultrapassado, muitos servidores o mantêm habilitado por questões de compatibilidade com a máquina cliente, que pode não trabalhar com o TLS, protocolo sucessor do SSL. A vulnerabilidade presente na versão 3.0 do SSL que é escaneada pela RNP, e que corresponde a 45,3% das notificações gerais, é proveniente do tipo de criptografia utilizada pelo protocolo que possui seu método de decifração conhecido. Essa falha pode ser explorada pelo ataque **PODDLE** (*Padding Oracle On Downgraded Legacy Encryption*) [19], brevemente explicado abaixo.

No processo de conexão cliente-servidor é realizado *handshake*, onde o cliente oferece inicialmente a versão mais recente dos protocolos que possua (SSL ou TLS). A versão mais recente para criptografia de dados é o TLS 1.2. Porém, se o servidor não for compatível com o protocolo oferecido, a resposta enviada é a oferta do protocolo inferior ao qual o servidor tem acesso. Esse processo continua até que ambas as partes consigam se comunicar, usando as mesmas versões de protocolo. O problema surge quando usuários maliciosos conseguem colocar-se entre o cliente e o servidor, fingindo ser o cliente na comunicação com o servidor e vice-versa. Essa técnica de ataque é conhecida como *man-in-the-middle*. Desse modo, o atacante pode forçar a utilização do SSL 3.0 para realizar a quebra da criptografia das mensagens e ter acesso a elas [19]. Também é possível que usuários legítimos em contato com o servidor, que utilizem o como versão mais recente o SSL 3.0, tenham seus pacotes interceptados por usuários maliciosos que podem estar na mesma rede. Essa brecha é um problema é inerente ao SSL 3.0 e, se explorada, torna-se um incidente que compromete a confidencialidade dos sistemas internos.

O **PortMapper** é um serviço que mapeia dinamicamente portas TCP/UDP para serviços do tipo RPC e vice-versa. O RPC é um protocolo que regula a comunicação utilizada entre processos de diferentes máquinas na mesma rede [17]. A ideia do PortMapper é que outros serviços sejam controlados por ele e que apenas as portas TCP/UDP que necessitam ser utilizadas em determinado momento estejam abertas.

Dessa forma, caso uma máquina cliente deseje realizar uma chamada a um serviço na máquina servidora, o primeiro contato seria através do PortMap, o que leva a este serviço poder controlar uma grande gama de portas a fim de delegá-las a outros serviços.

A vulnerabilidade nesse serviço reside em má configuração, que permite que máquinas externas à rede possam encontrar o IP onde se encontra o serviço e utilizá-lo para obter informações sobre serviços disponíveis na rede e suas respectivas versões. Outro problema encontrado é a utilização do PortMapper para amplificação de ataques (D)DoS, também conhecido como DoS refletido, pois passa por uma máquina intermediária antes do alvo final. Essa técnica consiste no atacante enviar inúmeras requisições para o servidor que possui o PortMapper (ou outro serviço utilizado para reflexão) informando um IP falso, ao qual o servidor responderá. Dessa forma, o servidor realizará o ataque de negação de serviço no lugar da máquina atacante. Esse ataque é considerado uma amplificação pois os pacotes enviados pelo servidor ao alvo final podem ser maiores em tamanho e quantidade. O valor de amplificação do PortMapper está entre 7 e 28 vezes a mais do que uma máquina realizando o ataque de forma tradicional [33]. Essas brechas, se exploradas, tornam-se incidentes que comprometem a confidencialidade e a disponibilidade dos sistemas internos, respectivamente.

O protocolo **mDNS**, ou Multicast DNS, é um modo de resolver nomes em IPs e descobrir outros serviços e dispositivos em redes. Embora o protocolo utilize consultas multicast (comunicação na qual um quadro é enviado para um grupo específico de dispositivos ou clientes), alguns servidores podem responder a consultas do tipo unicast (comunicação na qual um quadro é enviado de uma máquina e endereçado a um destino específico). Em alguns casos onde há má configuração, o servidor que dispõe do serviço mDNS está disponível para consulta fora da rede interna, ou seja, na internet. O problema desse tipo de ocorrência é que um usuário mal intencionado pode utilizar esse protocolo para obter informações do estado da rede ao qual ele não deveria ter acesso, e que serão respondidas apenas a ele, dificultando que outras máquinas da rede descubram a anomalia. Além disso, a máquina pode ser utilizada para amplificar ataques de negação de serviço em sistemas internos e externos. O

valor de amplificação do mDNS está entre 2 e 10 vezes a mais do que uma máquina realizando o ataque de forma tradicional [33]. Caso estas situações ocorram, tornam-se incidentes que comprometem a confidencialidade e a disponibilidade dos sistemas internos, respectivamente.

O **SNMP** é o protocolo padrão para gerenciamento de redes, permitindo que ele possa ter acesso a diversos dados de sistemas monitorados como informações de *hardware*, pacotes instalados na máquina e processos em execução. Ele é utilizado em diversos tipos de agentes de monitoramento e atualmente está em sua terceira versão. As máquinas que gerenciam a rede (servidores, roteadores, comutadores) podem utilizar esse protocolo para comunicarem-se com os dispositivos a serem monitorados (estações de trabalho, impressoras, etc.).

As duas primeiras versões do protocolo não possuem criptografia dos dados, o que possibilita um usuário malicioso descobrir senhas de acesso ao dispositivo de gerenciamento. Outro problema encontrado nas versões anteriores do SNMP permite a extração de informação e até a alteração de dados nas máquinas monitoradas fazendo o uso de Strings Comunitárias (SNMP *Community String*). Elas são palavras compartilhadas entre as máquinas monitoradas e o servidor SNMP e funcionam como uma identificação entre eles. As *strings* são enviadas quando é realizada uma requisição entre *host* e servidor [14]. O problema ocorre quando a palavra de identificação padrão não é alterada, facilitando a requisição de usuários maliciosos. Além disso, a máquina pode ser utilizada para amplificar ataques de negação de serviço em sistemas internos e externos. O valor de amplificação do SNMP é aproximadamente 6,3 vezes mais do que uma máquina realizando o ataque de forma tradicional [33]. Essas situações, se ocorrerem, tornam-se incidentes que comprometem todos os pilares da segurança dos sistemas internos.

O **DNS Recursivo Disponível** é um problema de má configuração do DNS, que é um sistema hierárquico e distribuído de gerenciamento de nomes que converte nomes em IPs e vice-versa. Quando configurado no modo “recursivo”, o serviço de DNS é responsável por receber as consultas dos clientes locais e consultar os servidores externos, de modo a obter respostas às consultas efetuadas. O problema

surge quando clientes externos (qualquer IP na internet) conseguem realizar consultas recursivas no servidor, de forma que o servidor responda a qualquer consulta a qualquer IP [5]. Em uma situação normal, o servidor de DNS deve responder recursivamente apenas a IPs aos quais possui autoridade, mas isso depende da configuração do DNS.

Nessa má configuração, agentes maliciosos podem envenenar o cache do DNS. Neste ataque, o usuário malicioso envia ao DNS uma requisição solicitando a resolução de um determinado endereço e, em seguida, envia diversas requisições para o mesmo DNS informando ser o proprietário do IP desejado [24]. O servidor também pode ser utilizado para amplificar ataques de (D)DoS, o valor de amplificação de DoS do DNS varia entre 28 e 54 vezes mais do que uma máquina realizando o ataque de forma tradicional[27]. Caso estes casos ocorram tornam-se incidentes que comprometem todos os pilares da segurança.

As três principais fontes de relatório de vulnerabilidades são o SGIS, que reporta apenas vulnerabilidades e incidentes das quais possui *scripts* para identificar, denúncias de usuários e as denúncias do CBPF. Porém, como já mencionado anteriormente, são notificadas apenas 17 tipos distintos de vulnerabilidade pelo SGIS, e até agosto de 2017 estão catalogados mais de 89.000 tipos diferentes pela MITRE Corporation [6]. Além disso, em atendimentos a unidades específicas, são feitas varreduras pontuais que não são registradas nos sistemas como vulnerabilidades e/ou incidentes identificados na rede. Dessa forma, podem existir diversas outras vulnerabilidade que não são identificadas e que podem ser exploradas por atacantes. Outro fator preocupante é o número de páginas web hospedadas na rede da UFRJ. Esses sites podem possuir, cada um, diversos tipos de vulnerabilidade exclusivas de aplicações web e que podem comprometer a segurança do servidor que hospeda a aplicação e da rede.

Não existe atualmente na UFRJ um sistema implantado pela DSI de varredura para a notificação automática das vulnerabilidades apontadas. Este trabalho já foi realizado e testado pela DSI, porém devido ao grande volume de notificações geradas, como comentado na seção 1.3, as mesmas tornam-se obsoletas para os

administradores de sistemas. Como foi dito em 3.3, ao receber diversas notificações acerca de um determinado tipo de vulnerabilidade, estas podem não receber a devida atenção dos administradores de rede e sistemas e acabar por não ser solucionadas de maneira efetiva.

3.4 Incidentes identificados

É utilizado pela DSI para coleta de dados sobre incidentes, o sistema SGIS e notificações via e-mails, que são catalogados em sistemas internos da UFRJ. Para realizar notificações aos administradores responsáveis, a DSI utiliza o sistema SGRC, do qual foi coletado os dados da Figura 3.9.

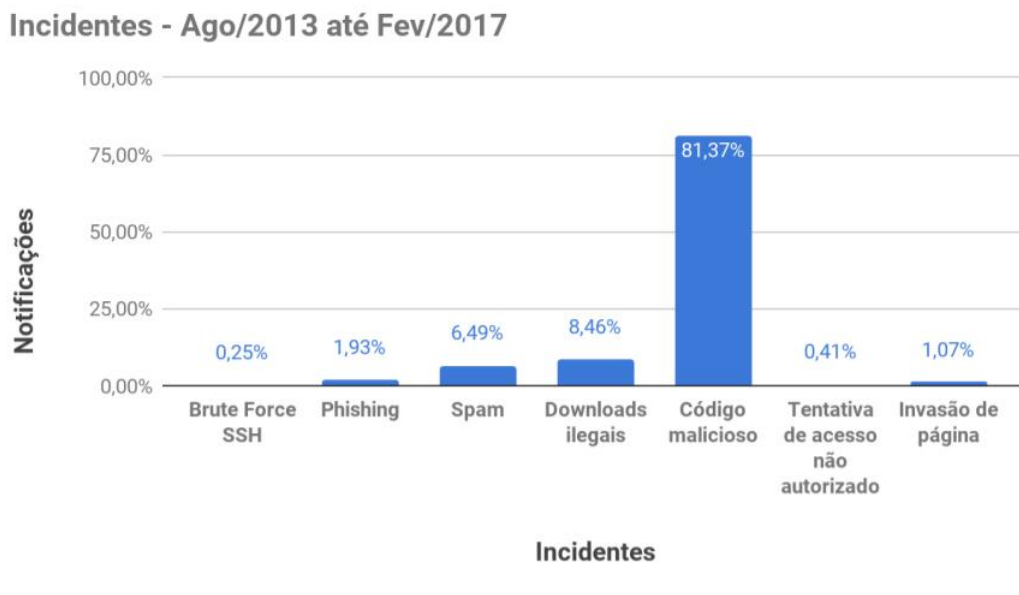


Figura 3.9: Notificação de Incidentes Gerais da UFRJ

É importante ressaltar que os dados presentes na Figura 3.9 referem-se tanto a incidentes originados na UFRJ quanto destinados a ela. Os casos de “invasão de página” referem-se a ataques que afetaram a instituição, ou seja, atingiram alguma página oficial da UFRJ. Nos casos de “*brute force* SSH” e “tentativa de acesso não autorizado” não foi possível identificar através da consulta ao banco de dados do sistemas se o ataque partiu da instituição ou foi destinado a ela, pois as descrições do problema não são padronizadas e pelo volume de entradas no banco de dados

não foi possível verificar tupla a tupla. Os casos de “Phishing” e “SPAM” referem-se a incidentes originados na instituição, ou seja, que servidores de e-mail da UFRJ foram infectados e enviaram mensagens maliciosas ou indesejadas. “Downloads Ilegais” refere-se aos casos de *download* de conteúdo protegido por direitos autorais (como filmes, livros, etc.) que foram realizados na UFRJ. Não há na instituição um sistema que catalogue os incidentes entre “origem” e “destino” de forma satisfatória. O sistema SGIS possui essa proposta, porém não possui todas as informações das ocorrências na instituição e ainda necessita de melhora na categorização das notificações de incidentes.

O incidente de **(D)DoS** não está presente na Figura 3.9. Este fato não ocorre pela ausência do incidente, mas sim pela dificuldade de encontrar os registros deles, pois este incidente não possui entradas no sistema SGRC. Comumente a notificação de (D)DoS é realizada via telefone ou presencialmente, já que o impacto dele é imediato. Ressalta-se que ataques do tipo *brute force* e tentativa de acesso não autorizado podem resultar em ataques de (D)DoS, se tiverem como alvo um IP pertencente a UFRJ, já que podem comprometer a disponibilidade dos serviços afetados.

A DSI categoriza os incidentes em 7 tipos distintos, destacando-se com maior incidência o incidente causado por “Código Malicioso”. Esse incidente é identificado pelo tráfego gerado entre um IP e uma URL maliciosa previamente identificada pela RNP e então é notificado a DSI. Destacamos com importância não saber quais dados são efetivamente trafegados entre as máquinas infectadas e as URLs maliciosas. Essas máquinas podem estar enviando informações sensíveis que coletam de dentro da rede da UFRJ para auxiliar ataques posteriores. Essas informações coletadas podem ser obtidas explorando vulnerabilidades como as expostas anteriormente.

As vulnerabilidades apontadas anteriormente como sendo de maior incidência na rede, inicialmente podem não apresentar problemas considerados gravíssimos em aspectos de quebra de confidencialidade. Porém é importante ressaltar que essas vulnerabilidades podem ser utilizadas por usuários maliciosos para adquirir conhecimentos sobre a estrutura da rede e, de posse deste conhecimento, explorar

uma outra vulnerabilidade que possa ser encontrada através da exploração dessas apresentadas. Esta situação ocorre em ataques combinados, para que o atacante crie a sua oportunidade sobre o alvo desejado. Dificilmente é identificado pela DSI um incidente relacionado a quebra de confidencialidade se não houver impactos explícitos na organização, pois um atacante pode obter dados da rede e não divulgá-los ou causar danos que não estejam explicitamente ligados a esses dados. Por esse motivo é importante reduzir ao máximo as vulnerabilidades contidas no ambiente.

Capítulo 4

Propostas para Mitigação de Problemas de Segurança na UFRJ

Neste capítulo foram realizadas as etapas de classificação de impactos e riscos das vulnerabilidades e definidos procedimentos técnicos que podem ser implantados para mitigar ou solucionar as vulnerabilidades listadas. São expostas sugestões que podem ser implantadas na rede para melhorar o processo de Resposta a Incidentes, em termos de monitoramento, coleta e armazenamento de informações sobre incidentes e vulnerabilidades. Por fim, são apresentadas duas unidades da UFRJ onde foi realizado o processo de gestão de vulnerabilidade.

4.1 Classificação de Impactos e Riscos

Para realizar a classificação do impacto causados pelas vulnerabilidades anteriormente apresentadas, foi analisado o comprometimento que a exploração delas pode causar aos pilares de segurança. A vulnerabilidade mDNS possui impacto alto pois compromete a confidencialidade e a disponibilidade dos sistemas; a vulnerabilidade no protocolo SNMP possui impacto alto pois compromete a confidencialidade e a integridade dos sistemas; a vulnerabilidade no PortMap possui impacto alto pois compromete a confidencialidade e a disponibilidade dos sistemas; a vulnerabilidade no DNS Recursivo Disponível possui impacto alto pois compromete a integridade e

a disponibilidade dos sistemas; a vulnerabilidade no SSL possui impacto médio pois compromete a confidencialidade do sistema.

	Probabilidade	Incidência
Baixa	raras vezes	abaixo de 1%
Média	algumas vezes	entre 1% e 5%
Alta	quase sempre	acima de 5%

Tabela 4.1: Tabela de Probabilidade por Incidência de Vulnerabilidades

$R = P \times I$		Probabilidade		
Impacto		Baixo	Médio	Alto
Baixa				
Média				SSL
Alta				mDNS, SNMP, PortMapper, DNS Recursivo Disponível.

Tabela 4.2: Matriz de Risco para classificação das vulnerabilidades presentes nos protocolos / serviços.

De forma semelhante, porém respeitando a distribuição da porcentagem dos dados, realizamos a classificação das probabilidades conforme a tabela 4.1, baseada na distribuição de vulnerabilidades geral como demonstra a Figura 3.6. Apenas cinco das vulnerabilidades reportadas a DSI possuem probabilidade de ocorrência maior que 5%, outras cinco possuem probabilidade entre 5% e 1%. O restante das vulnerabilidades identificadas possuem menos de 1% de ocorrência.

Dessa forma concluiu-se que todas as vulnerabilidades destacadas possuem probabilidade alta, visto que todas elas possuem mais do que 5% de chance de ocorrência. O resultado da junção do impacto com a probabilidade de ocorrência da vulnerabilidade pode ser observado na Tabela 4.2.

Ressalta-se que, após a avaliação das vulnerabilidades e de seus respectivos impactos, é possível observar que a escolha motivada por volume de notificação ou por grau de risco, neste caso, leva as mesmas cinco vulnerabilidades. Isto porque elas

possuem impacto alto e médio associados e alta probabilidade de ocorrência. A probabilidade, como mostrado na equação de risco, contribui para gravidade do risco e também para volume de notificação. Desta forma, as vulnerabilidades que serão selecionadas para mitigação serão as 5 mais frequentes e de alto risco associadas, como mostra a tabela 4.2.

4.2 Relação entre Vulnerabilidades e Incidentes

No capítulo 3 foram apresentadas estatísticas sobre vulnerabilidades e incidentes que são notificados à UFRJ. Para tornar clara a relação entre incidente e vulnerabilidade serão utilizadas duas tabelas: na Tabela 4.3 encontram-se os tipos de incidentes catalogados na UFRJ e os pilares da segurança que são quebrados na ocorrência desses e na Tabela 4.4 encontram-se as cinco vulnerabilidades mais notificadas na UFRJ e os pilares de segurança que elas podem quebrar, como já mencionado na seção 3.3.

Incidente	Pilar da segurança afetado
Brute Force SSH	Confidencialidade
SPAM	Disponibilidade
Phishing	Confidencialidade e integridade
Downloads ilegais	Confidencialidade
Código malicioso	Confidencialidade e integridade
Tentativa de acesso não autorizado	Confidencialidade
(D)DoS	Disponibilidade
Invasão de página web	Todos

Tabela 4.3: Tabela de Incidentes x Pilares de Segurança afetados

É possível perceber que os pilares afetados pelas vulnerabilidades de maior incidência se repetem nos incidentes que ocorrem dentro da instituição. As vulnerabilidades que permitem a quebra da disponibilidade podem estar diretamente ligadas aos incidentes identificados que quebram este pilar. As vulnerabilidades que afetam a confidencialidade podem permitir o conhecimento indevido sobre serviços internos, que desta forma tornam-se alvos fáceis para ataques que comprometem todos

os pilares. E brechas que afetam a integridade estão relacionadas ao comprometimento total ou parcial de sistemas, como na ocorrência de phishing, SPAM, código malicioso e invasão de página web.

Vulnerabilidade	Pilar de Segurança afetados
DNS Recursivo disponível	Disponibilidade e integridade
SSL/TLS	Confidencialidade
SNMP	Confidencialidade e integridade
PortMap	Disponibilidade e confidencialidade
mDNS disponível	Disponibilidade e confidencialidade

Tabela 4.4: Tabela de Vulnerabilidade x Pilares de Segurança afetados

Neste cenário, destaca-se o incidente de “Downloads ilegais ‘ ‘, que é oriundo da instituição e afeta outra instituição, logo a confidencialidade quebrada refere-se, neste caso, ao conteúdo de outra empresa ou organização. Também se realça o incidente de ‘ “Código malicioso“ que, como exposto anteriormente, pode trafegar qualquer tipo de informação sobre os sistemas da instituição.

O fato da porcentagem das cinco vulnerabilidades listadas ser bastante grande, é um forte indicador de que estas vulnerabilidades estão ligadas aos incidentes identificados. Conhecendo a relação entre os incidentes que afetam a UFRJ e as vulnerabilidades presentes na rede da instituição é possível afirmar que o tratamento das vulnerabilidades analisadas deve reduzir consideravelmente o número de incidentes identificados, pois ao eliminar uma brecha que permite o acontecimento de um determinado incidente, elimina-se um novo ponto de ocorrência. Esse comportamento é esperado já que a Gestão de Vulnerabilidades é uma parte da Prevenção de Incidentes.

4.3 Procedimentos para mitigação das vulnerabilidades

Nesta seção serão descritos os procedimentos sugeridos à equipe de administração de servidores da TIC para a mitigação das vulnerabilidades mencionadas anteriormente. As soluções descritas são válidas para ambiente Linux, que é o ambiente

padrão dos sistemas corporativos da UFRJ.

Os testes para verificar a eficácia das mitigações foi realizado em ambiente de teste com máquinas com sistema Debian 8, na rede utilizada pela UFRJ para a manutenção de *honeypots* - máquinas conhecidamente vulneráveis com o intuito de atrair usuários maliciosos e identificar seus perfis de ataque, para realizar mitigações preventiva na rede. O processo de teste seguiu os seguintes passos: instalação do sistema operacional; instalação da aplicação que contém a vulnerabilidade; varredura para verificar a presença dela; realização da mitigação da mesma; uma nova varredura para verificar a eficiência da mitigação. Seguem abaixo as recomendações específicas para mitigação das vulnerabilidades.

1. **Protocolo mDNS:** Para esta vulnerabilidade, podem ser seguidas duas alternativas que estão descritas abaixo.

Bloqueio ao acesso externo. O mDNS trabalha na porta 5353 UDP. Para controlar o tráfego nessa porta, utilizando o IPTables, execute os seguintes comandos no terminal como super usuário [13]:

```
# iptables -A INPUT -p udp -s! 192.168.0.0/24 --dport 5353 -j DROP
# iptables -A INPUT -p udp -s 192.168.0.0/24 --dport 5353 -j ACCEPT
```

Observação: Substitua o IP do exemplo (192.168.0.0) para o desejado.

Desabilitar serviço mDNS. Caso a máquina em questão não necessite executar o serviço mDNS, uma boa prática é desabilitá-lo, assim como qualquer outro serviço que não seja relevante para a mesma. Em distribuições Debian, o *daemon* utilizado como mDNS é o Avahi. Para desabilitá-lo o procedimento adequado é:

- 1 - Abra o arquivo `etc/cinit/avahi-daemon.conf` e altere:

```
"start on (filesystem and started dbus)"
```

para

```
"start on (never and filesystem and started dbus)".
```

2 - Abra o arquivo `etc/default/avahi-daemon` e altere:

```
“AVAHI\_DAEMON\_DETECT\_LOCAL=1”
```

para

```
“AVAHI\_DAEMON\_DETECT\_LOCAL=0”.
```

2. **PortMapper:** Para esta vulnerabilidade, podem ser seguidas duas alternativas que estão descritas abaixo.

Proteção do PortMap. Caso seja necessário manter o PortMap ativo, existem meios de mitigar o uso indevido da máquina. O PortMap trabalha nas portas 111 TCP/UDP, para controlar o tráfego nelas utilizando o IPTables, no terminal como super usuário, execute os comandos [13]:

```
# iptables -A INPUT -p tcp -s! 192.168.0.0\24 --dport 111 -j DROP
# iptables -A INPUT -p tcp -s 127.0.0.1 --dport 111 -j ACCEPT
# iptables -A INPUT -p udp -s! 192.168.0.0\24 --dport 111 -j DROP
```

Observação: Substitua o IP do exemplo (192.168.0.0) para o desejado.

Desabilitando o PortMap. Por ser uma ferramenta que facilita comunicação entre processos em máquinas distintas, é recomendado que o PortMap seja desabilitado das máquinas que não necessitem fazer uso dele. Abaixo, alguns exemplos de como desabilitar esse serviço.

Para distribuições Debian-Like:

```
# update-rc.d -f rpcbind remove
```

Observação: O comando acima deve ser executado a cada nova atualização do PortMap.

3. **DNS Recursivo Disponível:** A solução sugerida é para servidores que utilizam o sistema BIND para configuração de DNS, como é o caso da UFRJ. Essa solução é utilizada em casos que o servidor de DNS em questão funciona como

autoritativo (para responder requisições externas) e recursivo (para responder requisições internas) ao mesmo tempo. Esse modelo tem por objetivo separar os IPs no próprio arquivo de configuração a fim de que cada tipo tenha um determinado tratamento destinado pela aplicação [5].

No arquivo `named.conf` realize as seguintes alterações:

```
// lista de redes ou maquinas que podem fazer consultas recursivas
acl clientes {
localhost;
192.0.2.64/26;
192.0.2.192/28;
};

// definicao da view interna -- deve vir antes da view externa
// esta view permite recursao para as redes da acl clientes
view "interna" {
match-clients { clientes; };
recursion yes;

// dentro desta view sao colocadas as zonas padrao:
// ".", localhost, etc, e qualquer outra zona que
// seja somente interna para a rede em questao
};

// definicao da view externa -- deve ser a ultima view definida
// esta view permite consultas de qualquer rede, mas nao permite
// consultas recursivas
view "externa" {
match-clients { any; };
recursion no;
additional-from-auth no;
additional-from-cache no;
```

```
// aqui sao colocadas as zonas master
// zone "exemplo.com.br" {
// type master;
// file "master/exemplo.com.br";
// };

// aqui sao colocadas as zonas slave
// zone "exemplo.net.br" {
// type slave;
// file "slave/exemplo.net.br";
// masters { 192.0.2.1; [...] };
// };
};
```

4. **SSL:** A vulnerabilidade encontrada é a POODLE que só funciona se o navegador do cliente e a conexão do servidor suportarem SSL 3.0, portanto a recomendação é desabilitar essa versão do SSL em qualquer aplicativo usado. A desvantagem é que se o servidor estiver configurado para apenas trabalhar com a versão 3.0, será preciso a habilitação dos protocolos anteriores. Como os serviços de aplicação web mais utilizados na UFRJ são o Apache e o NGINX, segue os métodos utilizados para desabilitar [32]:

Apache: É preciso editar a configuração do Apache, no Debian e no Ubuntu o arquivo pode ser encontrado pelo caminho `/ETC/APACHE2/MODS-AVAILABLE/SSL.CONF`. Para desabilitar, basta adicionar a linha na configuração do Apache:

```
SSLProtocol All -SSLv2 -SSLv3
```

Isso permitirá todos os protocolos, exceto SSL 2.0 e 3.0. É preciso reiniciar o serviço.

Apache no cPanel/WHM: O cPanel é um painel utilizado para gerenciamento de hospedagens de sites e WHM é a ferramenta de gerenciamento de

contas. O cPanel não permite a edição de arquivos de configuração do Apache, neste caso há a opção de configurar a cifra SSL com o painel de controle.

- (a) No WHM, digite Apache no campo de busca e aparecerá as configurações do Apache na lista de menus. Depois de clicar em Configuração do Apache, navegue até Configuração Global.
- (b) A primeira opção é *SSL Cipher Suite*, e você precisará modificar o valor atual para incluir -SSLv3. Um exemplo disso é mostrado abaixo.

```
ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-SSLv3:-EXP:!kEDH
```

- (c) Depois de salvar a página, você será solicitado a reiniciar o Apache, após isso as alterações estarão salvas.

NGINX: É preciso alterar o arquivo de configuração (nginx.conf) adicionando a seguinte linha:

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;}
```

Isso irá desativar o uso do SSL 3.0 no NGINX. Após isso é preciso reiniciar o serviço.

5. **SNMP:** Para esta vulnerabilidade podem ser seguidas três alternativas:

Proteção do SNMP: caso as versões 1 e 2 do protocolo necessitem se manter ativas, é imprescindível que no servidor a porta de operação do protocolo rejeite pacotes da internet. Como ele trabalha na porta 161 UDP, é possível controlar o tráfego nela utilizando o IPTables. No terminal, como super usuário, execute os comandos [13]:

```
# iptables -A INPUT -p udp -s! 192.168.0.0/24 --dport 161 -j DROP
# iptables -A INPUT -p udp -s 127.0.0.1 --dport 161 -j ACCEPT
# iptables -A INPUT -p udp -s! 192.168.0.0/24 --dport 161 -j DROP
```

Observação: Substitua o IP do exemplo (192.168.0.0) para o desejado.

Desabilitar totalmente o serviço: é viável para máquinas que não necessitam fazer comunicações através desse protocolo.

Para distribuições Debian-Like

```
# update-rc.d -f snmpd remove
```

Desabilitar as versões 1 e 2 do protocolo: caso haja necessidade de manter o SNMP ativo na máquina, é recomendado que ele utilize apenas a última versão. Para isso, no arquivo `/etc/snmp/snmp.conf` comente as seguintes linhas [1]:

```
# desabilita o acesso para grupos publicos / comunitarios
#com2sec notConfigUser default public
#access notConfigGroup "" any noauth exact systemview none none

# desabilita a versao 1
#group notConfigGroup v1 notConfigUser

# desabilita a versao 2
#group notConfigGroup v2c notConfigUser
```

É importante ressaltar que após a implantação das técnicas descritas para mitigação das vulnerabilidades, os serviços/protocolos não estarão protegidos indefinidamente. Podem existir outras vulnerabilidades presentes neles que não são identificadas pelo sistema de detecção utilizado pela UFRJ. Porém, ao resolver problemas conhecidos é possível elaborar uma busca por novos problemas a serem resolvidos, como por exemplo, as vulnerabilidades com menor incidência no momento. Dessa forma, a mitigação de vulnerabilidades deve se tornar um requisito de manutenção da rede.

4.4 Boas práticas para Gestão de Vulnerabilidades

Nos passos abaixo foram separados três pontos que necessitam ser melhorados no processo de Gestão de Vulnerabilidades na UFRJ, estes pontos englobam as 5 etapas citadas na seção 2.6. São eles: Saber (preparação e varredura de vulnerabilidades), Avaliar (definição de ações) e Tratar (implementação de ações e nova varredura de vulnerabilidades).

1. **Saber:** O primeiro passo refere-se a tomar conhecimento das vulnerabilidades presentes nos sistemas utilizados. As vulnerabilidades normalmente não são reportadas pelos usuários, pois a descoberta delas nem sempre se torna conhecida, como citado no Capítulo 2. Para encontrar a falha sem contar com o acaso é preciso investigar os sistemas e aplicações.

Parte dessa investigação é feita na UFRJ através dos *scripts* da RNP como já citado na seção 1.3. Apenas isso é insuficiente para identificar todas as possíveis vulnerabilidades existentes na instituição. Há o agravante de que nem toda vulnerabilidade tem uma possibilidade razoável de acontecer em uma instituição de ensino pública - onde os programas e sistemas operacionais incentivados são *softwares* livres, como consta no documento “Padrões de Interoperabilidade de Governo Eletrônico - ePING“ [18]. Neste caso, é preciso levar em conta a porcentagem de usuários que usam sistemas operacionais e *softwares* proprietários, quais seriam eles e verificar se vale o empenho para mitigar uma minoria. No nosso caso de estudo, a universidade tem a maioria de uso de Windows e distribuições Linux, o que já foge um pouco da recomendação das leis.

O cenário ideal é onde a própria UFRJ, através da DSI, com possível parceria de docentes e alunos em iniciação científica, implementasse seus próprios *scripts* de varredura baseado no perfil da instituição: sistemas operacionais utilizados, necessidade de serviços ativos, Sistema de Gerenciamento de Conteúdo (CMS) padrão nos sites, entre outros pontos que devem ser analisados. Desta forma a varredura de vulnerabilidades focaria nos serviços mais utilizados, poupando a equipe de tratamento de desviar seus recursos para avaliar e

4.4. BOAS PRÁTICAS PARA GESTÃO DE VULNERABILIDADES 16

verificar vulnerabilidades com menor grau de risco. Para também se manter atualizado quanto as novas vulnerabilidades, seria uma boa estratégia a assinatura de listas de CVE's, dicionário de vulnerabilidades descobertas para conhecimento público, e a criação dos *scripts* deveria acompanhar o surgimento dessas novas brechas para garantir que o conhecimento das falhas da rede nunca estivesse defasado.

2. **Avaliar:** A etapa de avaliação é focada em analisar os riscos, selecionar os alvos de tratamento e escolher a melhor forma de resposta. Uma das maiores dificuldades da DSI refere-se aos sistemas utilizados para registro das ocorrências. Como já mencionado em 1, os sistemas utilizados no processo de tratamento, são o OSTicket, SGIS e SGRC. Esses sistemas são limitados de muitas maneiras - é impossível unificar os registros, os filtros não funcionam adequadamente, como já citado na seção 3.2, e o modo de cadastro do responsável não é atualizado frequentemente.

Para fazer uma boa avaliação das vulnerabilidades encontradas é preciso que todos os registros possam ser incluídos e consultados de maneira fácil e em um único sistema, para garantir que todas as ocorrências estejam presentes. As consultas das ocorrências por IP e categoria de incidentes/vulnerabilidade são essenciais para verificar e analisar reincidências - situação que aumenta a probabilidade de ocorrência daquela vulnerabilidade, o que pode impactar no grau do risco, tornando-a mais grave. É preciso que os responsáveis pelos IPs e servidores estejam cadastrados no sistema com os dados de contato e estes estejam sempre atualizados. A solução recomendada consiste na inserção de dados no sistema por todos os administradores de sistemas da universidade. O sistema deveria ter um esquema de relatórios e *ranking*, as categorias de vulnerabilidade mais frequentes e as vulnerabilidades maior impacto. Além disso, é necessário que haja uma estrutura de envio de e-mails para que todo o contato seja feito pelo sistema e possa ser consultado pelos demais integrantes da equipe.

No cenário ideal, a UFRJ deveria desenvolver um sistema que englobasse todas as características já citadas e descontinuar o uso dos sistemas atuais, pois

4.4. BOAS PRÁTICAS PARA GESTÃO DE VULNERABILIDADES 17

eles não são específicos para resposta de incidentes e a falta de um *software* deste tipo influencia diretamente no desempenho das atividades relacionadas ao tratamento e a resposta dos incidentes e vulnerabilidades.

3. **Tratar:** Para a etapa do tratamento são aplicadas medidas de defesa dos sistemas e processos de resposta as ocorrências (incidentes ou vulnerabilidades): Atualmente, o tratamento se resume a notificação ao responsável ou o bloqueio preventivo de um *host* que está sofrendo o incidente. Caso seja identificado uma vulnerabilidade, notificam ao responsável e aguardam *feedback*. Caso o *feedback* não seja feito em um tempo razoável, sendo este critério não formalizado, a notificação é feita novamente ou é pedido o bloqueio preventivo - o que retira o *host* ou serviço da rede temporariamente (até o pedido de desbloqueio ser solicitado pelo responsável). Desta forma, retira-se a possibilidade do incidente ocorrer ou continuar ocorrendo (caso a vulnerabilidade esteja sendo explorada). Neste cenário, algumas vulnerabilidades ficaram abertas durante anos e tiveram muita reincidência.

O método de notificações aos administradores responsáveis deve ser alterado para realizar poucos informes (agrupando logs de incidentes ou vulnerabilidades recentes de mesmo IP) e que estes contenham objetivamente as sugestões de mitigação da vulnerabilidade a fim de auxiliar ao administrador e evitar que o mesmo enxergue as notificações como importunas. O ideal seria, além da mudança do método de notificação, medidas mais duras para incentivar retorno mais rápido dos responsáveis: determinação de prazos aceitáveis para aguardo de *feedback* e caso a *deadline* não seja cumprida, bloqueio imediato; atendimento presencial, onde a equipe irá pessoalmente ao local para utilizar a solução que julgar mais adequada; aceitar os riscos da vulnerabilidade, caso haja necessidade do serviço; retirada do *host* da rede ou aplicação de *patches* de correção (atualização, recomendação ou desuso do serviço).

Além disso, é importante investir em monitoramento para estudar e avaliar formas de ataques que a instituição sofre para antecipar incidentes e fechar as brechas. Isto pode ser feito através de uso de *honeypots*, que são *hosts* atrativos

e propositalmente vulneráveis para instigar atacantes. Para monitorá-los pode ser utilizada a ferramenta OSSIM, um software *open source*, que monitora as atividades do *host* em tempo real, avalia vulnerabilidades e ainda funciona como um IDS [30]. O uso de *firewalls* e IPS são necessários para criar uma barreira primária de proteção na rede contra invasores externos. Eles já são usados pela UFRJ, porém não em todas as sub-redes e instituições acadêmicas, pois, como citado em 3.1, o controle é descentralizado e há pontos cegos na rede da universidade que são controladas pelos próprios docentes ou empresas externas.

4.5 Casos de sucesso de Gestão de Vulnerabilidade na UFRJ

Nesta seção serão apresentados casos de duas unidades da UFRJ que receberam o processo de gestão de vulnerabilidades de forma total ou parcial. As unidades são: o laboratório de informática do curso de Direito, que era alvo de inúmeras notificações de incidentes do tipo “código malicioso” não só pelos sistemas, como pelos próprios usuários do laboratório e o LBCD, Laboratório Brasileiro de Controle de Dopagem, que foi utilizado pelo Brasil para exames de dopagem dos atletas nas Olimpíadas de 2016 sediadas no Rio de Janeiro. Os casos possuíam dinâmicas diferentes em diversos aspectos: No caso do laboratório do curso de Direito, a gestão de vulnerabilidades foi realizada sem interrupção das atividades, enquanto que no caso do LBCD, a gestão de vulnerabilidades foi realizada antes de sua inauguração e utilização durante as Olimpíadas.

O laboratório de informática do curso de Direito da UFRJ é utilizado pelos alunos para fazer atendimento jurídico gratuito. Para reduzir o número de incidentes identificados e reclamações dos usuários foi utilizada parte do processo de gestão de vulnerabilidades. Inicialmente, na etapa de “preparação”, foi definido o que seria mitigado e o que seria afetado. Neste caso a gestão seria realizada em todos os computadores do laboratório do curso. O sistema operacional utilizado no laboratório era o Windows, sem políticas de atualização regular e sem utilização de antivírus local, por este motivo não foi realizado no laboratório uma etapa de “var-

redução de vulnerabilidades”, o conhecimento do estado dos sistemas do laboratório foi suficiente para as próximas fases. Na etapa de “definição de práticas” foi decidido que ação seria tomada a fim de sanar os problemas correntes e foi determinada a substituição do sistema de Windows para Linux no laboratório, a fim de reduzir os casos de *malware* nos computadores. O impacto no trabalho dos alunos não foi alto pois eles não necessitam de softwares específicos para trabalhar, apenas editores de texto e acesso à internet. Para ajudar na adaptação dos alunos, a DSI disponibilizou inicialmente um computador com o sistema Linux instalado e um funcionário durante um mês para que os alunos pudessem se ambientar com o novo sistema e sanar suas possíveis dúvidas, além de conscientizar e informar os alunos sobre a mudança. Após o prazo houve a “implantação da prática” decidida na fase anterior em todo o laboratório, o que ocorreu sem problemas dado o treinamento oferecido. Não houve, após a alteração do sistema, incidentes de código malicioso provenientes do laboratório de informática do curso de Direito. Essa experiência demonstra que é possível realizar o processo de gestão de vulnerabilidades para reduzir o número de incidentes, mesmo que a alteração em questão possa ser significativa e, se bem planejada, com impacto mínimo ao andamento das atividades necessárias.

O **LBCD** foi o laboratório utilizado pelo Brasil para realizar exames de dopagem dos atletas das Olimpíadas Rio 2016. O laboratório necessita utilizar mais de um sistema operacional, fazendo uso de Windows e Linux (em diversas versões). Alguns equipamentos de análise necessitam utilizar versões específicas do Windows, por motivos de compatibilidade. Para evitar a ocorrência de incidentes de segurança cibernética em um laboratório de grande importância e visibilidade, foi utilizado o processo de gestão de vulnerabilidades antes de sua utilização para as Olimpíadas. Na etapa da “preparação” foram definidos quais sistemas seriam verificados no processo, no caso todas as máquinas presentes no laboratório foram inseridas na análise. Na etapa de “varredura de vulnerabilidades”, foram escolhidas as ferramentas OWASP ZAP [21], que procura vulnerabilidades em aplicações web (utilizadas internamente como interface de acesso a sistemas), e Open Vas [22], que procura vulnerabilidades em sistemas operacionais, para realizar a varredura em todas as máquinas do laboratório. O resultado obtido norteou as “definições de práticas”

que concentraram-se em atualizar os sistemas operacionais, instalação de antivírus e criação de políticas de varredura de antivírus localmente e as definições foram todas implementadas. Em alguns casos porém, por motivos de compatibilidade com equipamentos utilizados pelo laboratório, não foi possível realizar tais procedimentos. Nestes casos, a rede em que se encontravam tais máquinas com seus respectivos sensores ou equipamentos foi segmentada e teve seu acesso a internet totalmente interrompido. Como tais máquinas não necessitavam de acesso à internet para realizar suas tarefas principais, o impacto gerado da decisão não foi significativo. Após o processo de gestão de vulnerabilidades no LBCD, durante as Olimpíadas, não foram identificados incidentes provenientes do laboratório, sejam por sistemas internos da UFRJ ou pelo sistema de notificações da RNP. Essa experiência demonstra como o processo de gestão de vulnerabilidades pode cessar a ocorrência de incidentes.

Em ambos os locais, o ideal é que existam varreduras periódicas ou avaliação do cenário de trabalho para melhoria ou reparo em sistemas que podem apresentar falhas. O intuito principal é expandir os casos acima para toda a rede da UFRJ. Um modo de iniciar esse processo é varrer poucas vulnerabilidades, reduzindo o escopo delas, tendo em vista o número de máquinas que devem ser avaliadas, e realizar a mitigação das mesmas. Com o passar do tempo, ampliar o número de vulnerabilidades a serem varridas e assim mitigar cada vez mais vulnerabilidades.

Os exemplos aqui apresentados utilizam os sistemas que a DSI dispõe atualmente e não necessita imediatamente de outros equipamentos. Porém, é imprescindível que as unidades da UFRJ possuam administradores de redes, que sigam a Política de Segurança definida pela DSI, aptos para receber as notificações e executar as ações previamente definidas pela diretoria, além da gestão da rede. Infelizmente existem unidades na instituição que não possuem qualquer profissional da área de informática. Para este problema apenas uma solução é possível: a contratação de novos profissionais, pois pelo tamanho físico da UFRJ é necessário que cada unidade possua ao menos um administrador de redes.

4.6 Sugestões para Melhorias

Como mencionado no Capítulo 1, duas perguntas chaves motivaram este estudo: “Apenas notificar aos administradores de sistemas é a melhor abordagem para resolver as vulnerabilidades?” e “Qual o papel da Diretoria de Segurança em relação a solução dos incidentes e vulnerabilidades notificados a ela?”. De acordo com os gráficos gerados sobre a proporção de vulnerabilidades durante o estudo e ao perceber que a proporção e o volume de vulnerabilidades notificadas não diminuiu a resposta para a primeira pergunta é “não, apenas a notificação não é o suficiente para sanar o problema”, o que leva à resposta da pergunta seguinte. A UFRJ possui uma estrutura descentralizada de administração de sistemas, algumas unidades possuem administradores próprios, outras estão sob administração da SuperTIC e outras não possuem funcionários para tratar da administração da rede e sistemas que possuem. Nesta questão, a resposta mais adequada é o papel da DSI deve ser distinto em cada um destes cenários“.

Para unidades que possuem administradores próprios, a DSI deve auxiliá-los da maneira mais prática possível na resolução dos problemas encontrados, sejam estes incidentes ou vulnerabilidades. As notificações devem ser enviadas aos administradores juntamente com procedimentos técnicos sugeridos para a resolução do problema, como aqueles expostos na seção 4.3. A notificação enviada deve ser seguida também de uma oferta para auxílio na resolução do problema.

A SuperTIC é responsável pela rede que hospeda os sistemas corporativos da UFRJ e alguns outros portais vinculados a universidade. Para unidades que possuem administração direta da SuperTIC o procedimento de notificações deve ser o mesmo, para registro estatístico de ambas as partes. Porém, a cada período de tempo a DSI deve avaliar quais vulnerabilidades estão presentes nestas sub-redes e enviar um memorando para a diretoria responsável para a aplicação dos procedimentos sugeridos. Nesta situação a diretoria notificada via memorando institucional deve aplicar os procedimentos ou responder tecnicamente o motivo da não implantação.

Para unidades que não possuem funcionários técnicos para administrar a rede

local e os sistemas, a DSI deve notificar ao funcionário responsável pela unidade (decano, diretor da unidade, etc.) para fins estatísticos, auxiliar na resolução do problema encontrado e sugerir a migração dos serviços para a diretoria correspondente da SuperTIC. Esse método foi realizado com um site que sofreu invasão de página web (portal do curso de Defesa e Gestão Estratégia Internacional) e o portal está sendo restaurado pela equipe responsável.

Destaca-se também o papel da DSI para a conscientização do público acadêmico através das redes sociais e palestras sobre segurança. A diretoria visa prestar suporte não apenas as outras diretorias, mas também criar uma cultura de segurança [2] para a instituição. A importância dessa vertente para o trabalho geral se dá pelo fato que alunos e funcionários cientes dos riscos cibernéticos existentes são menos propensos a serem vítimas. De acordo com os aspectos citados, é possível compreender a importância do papel da DSI para a UFRJ.

Capítulo 5

Considerações Finais

Este Trabalho de Conclusão de Curso introduziu o problema atual de Segurança da Informação da UFRJ (Capítulo 1), revisou alguns conceitos necessários para o entendimento do estudo (Capítulo 2), abordou o cenário de vulnerabilidades e incidentes da UFRJ e a forma de extração dos dados nos sistemas (Capítulo 3), a utilização dos dados para avaliação do grau de risco das vulnerabilidades para saber quais deveriam ser mitigadas primeiro e sugestões para melhoria do processo de Gestão de Vulnerabilidades (Capítulo 4).

5.1 Dificuldades encontradas

A tomada de decisão para eventos futuros é suportada pela avaliação de dados de situações passadas ou cenário atual. No caso dos dados relacionados as vulnerabilidades e aos incidentes da UFRJ essa tarefa é extremamente trabalhosa. Como pode ser observado na seção 3.2, embora existam sistemas que guardem as informações de incidentes e vulnerabilidades, eles não possuem um bom modo de extração de dados. Para a tomada de decisões futuras é imprescindível que seja implantado um sistema que junte as informações de incidentes e vulnerabilidades em um único local e que possa realizar automaticamente a filtragem dos dados. Sem dúvidas este é um obstáculo que interfere diretamente na visualização dos problemas ocorridos. Não há separação de incidentes e vulnerabilidades por ano, por impacto, por frequência

ou por reincidência de origem. Estes dados são de suma importância para a DSI e ela não os possui. Anteriormente a análise feita para este trabalho, o problema de extração de dados não havia sido abordado desta forma, nem notado seu impacto para o direcionamento das práticas, embora fosse um problema conhecido.

Outra questão importante é a falta de *scripts* próprios da DSI para a varredura de vulnerabilidades na rede da UFRJ. Como mencionado anteriormente, um trabalho com este intuito já foi realizado, mas sem a análise de quais sistemas mais utilizados na rede da UFRJ e quais vulnerabilidades necessitam realmente ser notificadas. Desta forma, os administradores de sistemas das unidades ao receber dezenas de notificações semanalmente, acabaram por não resolvê-las e ignorar os alertas gerados pela DSI. Uma maneira de retomar a esta ideia seria a criação de *scripts* que buscam vulnerabilidades em CMS que possuam impacto classificado como "alto". A rede da UFRJ possui diversas páginas web: para cursos de graduação, pós-graduação, grupos de extensão, etc. e estas páginas podem conter diversas vulnerabilidades proveniente dos CMS que elas utilizam. A busca inicial apenas por vulnerabilidades que possuam impacto "alto" é importante para reduzir ou eliminar o risco associado a elas. Destaca-se a importância de que as notificações exponham a gravidade do problema encontrado, sem gerar grande volume de e-mails.

5.2 Prevenção de Incidentes *versus* Tratamento de Incidentes

O tratamento de incidentes, como mencionado anteriormente, visa resolver os incidentes que ocorreram ou estejam ocorrendo em uma determinada instituição. Porém, é importante destacar que quando um incidente ocorre ele causa um impacto a instituição, não necessariamente relacionado a informação em si. Perdas financeiras, diminuição da produtividade e danos a imagem da empresa são danos que estão diretamente relacionados ao acontecimento de incidentes [15] e tratando-se de uma universidade é possível apontar também a espionagem acadêmica.

A diminuição da produtividade por inutilização de máquinas devido a presença de *malwares* foi um problema enfrentado pela DSI no laboratório de informática do

curso de Direito e que ainda persiste em outros locais da universidade. Ataques de (D)DoS também causam perda de produtividade, tanto dos funcionários quanto de alunos. A reputação da instituição é de extremo valor, visto que a UFRJ figura entre as maiores universidades do país. Ataques de alteração de página web, hospedagem de sites maliciosos em máquinas pertencentes a instituição causam impacto direto a imagem, depreciando-a. Embora seja uma universidade pública, a UFRJ possui convênios com diversas empresas privadas, que realizam investimentos em segmentos específicos. O dano a reputação e problemas na produtividade podem impactar na diminuição de investimentos externos e assim culminar em perdas financeiras para a universidade.

Destaca-se que todo incidente ocorrido necessita de um determinado tempo para ser solucionado. Este tempo de resposta, que varia de um incidente para outro, afeta a atividade que sofreu o dano. Por exemplo, uma página que sofreu alteração maliciosa: a página legítima sai do ar, prejudicando os usuários; recupera-se o *backup* da página; verifica-se qual vulnerabilidade foi explorada pelo atacante; é realizada a mitigação dessa vulnerabilidade; a página volta ao ar. Este exemplo assume que o atacante apenas substitui a página afetada e não deleta as informações contidas nela. É importante levar em conta o tamanho físico da UFRJ, o funcionário que possui o *backup* da página pode atuar em outro campus da universidade, o que adiciona tempo para a resolução do problema. Com base nisto, esta restauração pode demorar, no mínimo, três dias para ser solucionado: entre o problema ser descoberto, as informações legítimas serem recuperadas, a vulnerabilidade mitigada e o serviço estar disponível para acesso novamente.

Como mencionado na seção 2.5, o objetivo da prevenção de incidentes é reduzir a quantidade de incidentes das instituições. A gestão de vulnerabilidades, que é parte da prevenção de incidentes, auxilia no mapeamento dos riscos aos quais a instituição esta exposta e na resolução deles. Ao reduzir ou monitorar as vulnerabilidades existentes no ambiente, também é reduzido o número de incidentes. Com a redução do número de incidentes também há menos perdas financeiras, danos a reputação e diminuição da produtividade. É importante ressaltar que a UFRJ possui ferramentas, as quais foram utilizadas para a realização deste trabalho, para iniciar a

implantação deste processo. Os sistemas utilizados necessitam de melhorias, porém é possível utilizá-los como ponto de partida. Como mostrado na seção 4.5, o processo de gestão de vulnerabilidades ao ser aplicado em duas unidades da UFRJ, em caráter excepcional, reduziu a zero os incidentes provenientes das vulnerabilidades corrigidas. Esta é uma prova de que este processo não só funciona como deve ser adotado em larga escala para toda a universidade.

5.3 Trabalhos Futuros

Levando em conta o estudo realizado do cenário de vulnerabilidades da UFRJ e a quantidade de aparelhos móveis (*notebooks, smartphones, etc.*) que utilizam a rede sem fio da universidade existe a necessidade de configuração de ferramentas com a finalidade de gerenciar o tráfego proveniente destas máquinas, pois infecção por código malicioso também pode partir dos mesmos para redes públicas abertas. Também é interessante a inclusão de normas, no documento de política de segurança atual da UFRJ, para utilização da rede sem fio, voltadas ao usuário final.

O mapeamento de perfis de utilização da rede é importante para a configuração de *firewalls*, pois podemos personalizar e configurar regras para diferentes fins. Como, por exemplo, permitir um serviço específico para um laboratório de pesquisa que assim necessite e bloquear para os demais. Desta maneira, há um controle do que deve estar trafegando em cada sub-rede, o que facilita identificação de anomalias e permite varreduras focadas nas vulnerabilidades dos serviços em uso.

Referências

- [1] *snmp.conf(5) - Linux man page*. <https://linux.die.net/man/5/snmp.conf>. Acesso em: 24 Ago. 2017.
- [2] ALNATHEER, M. A. *Understanding and measuring information security culture in developing countries: case of Saudi Arabia*. PhD thesis, Queensland University of Technology, 2012.
- [3] CAMPOS, A. *Segurança da Informação - Conceitos*. <https://pt.scribd.com/document/36676311/Seguranca-da-Informacao-Conceitos>, 2016. Acesso em: 12 Jul. 2017.
- [4] CARVALHO, F. Estudo comparativo entre diferentes métodos de avaliação de risco, em situação real de trabalho. *Universidade Técnica de Lisboa, Faculdade de Motricidade Humana, Lisboa* (2007).
- [5] CERT.BR. *Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos*. <https://www.cert.br/docs/whitepapers/dns-recursivo-aberto/>, 2016. Acesso em: 20 Ago. 2017.
- [6] CORPORATION MITRE. *Common Vulnerabilities and Exposures*. <https://cve.mitre.org/>. Acesso em: 18 Jul. 2017.
- [7] DE ARAÚJO, V. *SeguranÇa Da Informação*. 2015.
- [8] DE OLIVEIRA MONTEIRO, I. L. C. *Proposta de um Guia para Elaboração de Políticas de Segurança da Informação e Comunicações em Órgãos da Administração Pública Federal*. Universidade de Brasília, Departamento de Ciência da Computação, 2009.

- [9] DO RIO DE JANEIRO, U. F. *Unidades Acadêmicas - UFRJ*. <https://ufrj.br/unidades-academicas>, 2016. Acesso em: 12 Jul. 2017.
- [10] ESET. *Zero-day*. <http://www.virusradar.com/en/glossary/zero-day>, 2007. Acesso em: 14 Ago.2017.
- [11] FRASER, B. Rfc 2196. site security handbook. 1997. URL: <https://www.ietf.org/rfc/rfc2196.txt> (2017).
- [12] GRANCE, T., E KELLY. Computer security incident handling guide (nist special publication 800-61). gaithersburg, md: Computer security division. *Information Technology Laboratory, National Institute of Standards and Technology* (2008).
- [13] GUIA FOCA GNU / LINUX. *Capítulo 10 - Firewall iptables*. <http://www.guiafoca.org/cgs/guia/avancado/ch-fw-iptables.html>. Acesso em: 24 Ago. 2017.
- [14] HELPSYSTEMS. *About SNMP Community Strings*. <https://community.helpsystems.com/knowledge-base/intermapper/snmp/snmp-community-strings/>, 2017. Acesso em: 20 Ago. 2017.
- [15] KASPERSKY LABS. *Measuring Financial Impact Of IT Security On Business*, 2016. IT Security Risks Report.
- [16] LUZ. *Como fazer o gerenciamento de riscos em projetos com uma matriz de riscos*. <http://blog.luz.vc/como-fazer/como-fazer-gerenciamento-de-riscos-em-projetos-com-matriz-de-riscos/>, 2016. Acesso em: 02 Mar. 2017.
- [17] MARGARET ROUSE, BREE MATTURRO, P. B., E HAZAN, F. *Remote Procedure Call (RPC)*. TechTarget, <http://searchmicroservices.techtarget.com/definition/Remote-Procedure-Call-RPC>. Acesso em: 15 Ago. 2017.
- [18] MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO. DEPARTAMENTO DE GOVERNO DIGITAL.

- Padrões de Interoperabilidade de Governo Eletrônico*, 2017. Padrões de Interoperabilidade de Governo Eletrônico. Documento de Referência.
- [19] MÖLLER, B., DUONG, T., E KOTOWICZ, K. This poodle bites: exploiting the ssl 3.0 fallback. *PDF online* (2014), 1–4.
- [20] NATIONAL VULNERABILITY DATABASE. *NVD CVSS Support*. <https://nvd.nist.gov/vuln-metrics/cvss>. Acesso em: 23 Maio 2017.
- [21] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). *Zed Attack Proxy (ZAP) Project*. https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project. Acesso em: 04 Set. 2017.
- [22] OPENVAS. *Open Source Vulnerability Scanner*. <http://www.openvas.org/>. Acesso em: 04 Set. 2017.
- [23] PALMAERS, T. Implementing a vulnerability management process. *SANS Institute Reading Room* (2013).
- [24] PETR, E. An analysis of the dns cache poisoning attack, 2009.
- [25] PORTAL DA TRANSPARÊNCIA - GOVERNO FEDERAL DO BRASIL. *Funcionários da UFRJ*. <http://www.portaldatransparencia.gov.br/servidores/>. Acesso em: 12 Jul. 2017.
- [26] PRÓ-REITORIA DE GRADUAÇÃO - UFRJ. *Graduação em Números*. https://xn-graduao-2wa9a.ufrj.br/images/Apresentao_site_pr1.pdf, 2016. Acesso em: 12 Jul. 2017.
- [27] RNP. *Rede Nacional de Ensino e Pesquisa*. <https://www.rnp.br/>. Acesso em: 10 Ago. 2017.
- [28] RNP - REDE NACIONAL DE ENSINO E PESQUISA. *Pontos de Presença*. <https://memoria.rnp.br/pops/>, 2003. Acesso em: 04 Set. 2017.
- [29] SÊMOLA, M. *Gestão Da Segurança Da Informação*. ELSEVIER EDITORA, 2003.

-
- [30] SOFTWARE ENGINEERING INSTITUTE - ALIENVAULT. *Open Source Security Information Management*. <https://www.alienvault.com/products/ossim>. Acesso em: 04 Set. 2017.
- [31] SOFTWARE ENGINEERING INSTITUTE - ALIENVAULT. *Insider's Guide to Incident Response*, 2016.
- [32] SPAGNUOLO, M. *How to disable SSLv3*. <http://disablenessl3.com/>. Acesso em: 24 Ago. 2017.
- [33] UNITED STATES COMPUTER EMERGENCY READINESS TEAM. *UDP-Based Amplification Attacks*. <https://www.us-cert.gov/ncas/alerts/TA14-017A>, 2014. Acesso em: 15 Ago.2017.
- [34] UNIVERSIDADE FEDERAL DO RIO DE JANEIRO. *Política de Segurança da Informação da UFRJ*, Jun 2012.
- [35] WILLIAM A. ARBAUGH, WILLIAM L.FITHEEN, J. M. Windows of vulnerability: A case study analysis.