UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS HUMANAS, LETRAS E ARTES
MESTRADO PROFISSIONAL EM GESTÃO DE PROCESSOS INSTITUCIONAIS

Instituição de um Núcleo para Tratamento e Resposta a Incidentes de Segurança da Informação em uma IFES

Bruno Augusto da Costa Ferreira

Natal – RN
2021

UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS HUMANAS, LETRAS E ARTES
MESTRADO PROFISSIONAL EM GESTÃO DE PROCESSOS INSTITUCIONAIS

Instituição de um Núcleo para Tratamento e Resposta a Incidentes de Segurança da Informação em uma IFES

Bruno Augusto da Costa Ferreira

Plano de Intervenção submetido à coordenação do Mestrado Profissional em Gestão de Processos Institucionais do Centro de Ciências Humanas, Letras e Artes da UFRN, como requisito à obtenção do título de Mestre em Gestão de Processos Institucionais.

Orientador: Prof. Dr. Josué Vitor de Medeiros Júnior
Coordenadora: Prof. Dra. Patrícia Borba Vilar Guimarães.

Natal – RN
2021

Universidade Federal do Rio Grande do Norte - UFRN
Sistema de Bibliotecas - SISBI
Catalogação de Publicação na Fonte. UFRN - Biblioteca Setorial do Centro de Ciências Humanas, Letras e Artes – CCHLA

Ferreira, Bruno Augusto da Costa.
Instituição de um Núcleo para Tratamento e Resposta a Incidentes de Segurança da Informação em uma IFES / Bruno Augusto da Costa Ferreira. - 2021.
70f.: il.

Dissertação (mestrado) - Centro de Ciências Humanas, Letras e Artes, Programa de Pós-Graduação em Gestão de Processos Institucionais, Universidade Federal do Rio Grande do Norte, Natal, RN, 2021.
Orientador: Prof. Dr. Josué Vitor de Medeiros Júnior.

1. Segurança da Informação - Dissertação. 2. Grupo de Resposta a Incidentes de Segurança (CSIRT) - Dissertação. 3. Núcleos de Tratamento e Resposta a Incidentes de Segurança da Informação - Dissertação. I. Medeiros Júnior, Josué Vitor de. II. Título.

RN/UF/BS-CCHLA CDU 004.056

Elaborado por Ana Luísa Lincka de Sousa - CRB-15/748

BRUNO AUGUSTO DA COSTA FERREIRA

INSTITUIÇÃO DE UM NÚCLEO PARA TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO EM UMA IFES

Plano de Intervenção submetido à coordenação do Mestrado Profissional em Gestão de Processos Institucionais do Centro de Ciências Humanas, Letras e Artes da UFRN, como requisito à obtenção do título de Mestre em Gestão de Processos Institucionais.

Orientador: Prof. Dr. Josué Vitor de Medeiros Júnior
Coordenadora: Prof. Dra. Patrícia Borba Vilar

Aprovado em: _____/_____/_____

BANCA EXAMINADORA

_____

Prof. Dr. Josué Vitor de Medeiros Júnior
Orientador
UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

_____

Prof. Dr. Manoel Veras Sousa Neto
Membro interno
UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

_____

Prof. Dr. Professor Bruno Campelo Medeiros
Membro externo
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

Dedico esse trabalho a Deus, Causa Primeira de todas as coisas, e aos meus pais, que ajudaram a forjar em mim Caráter e Hombridade.

AGRADECIMENTOS

Agradeço à minha esposa, por todo o apoio, tanto nos momentos bons quanto naqueles mais difíceis. Aos meus pais, pelo constante incentivo à educação durante toda a minha vida. Aos meus filhos, pela compreensão, carinho e todos os ensinamentos que tem me proporcionado. Ao meu orientador, o Professor Dr. Josué Vítor, por toda a sua dedicação na construção desse trabalho. À UFRN, pela oportunidade de crescimento como pesquisador e como profissional da área de Tecnologia da Informação.

Agradeço a Deus, pelos recursos fornecidos nos momentos em que estive sem forças para prosseguir.

The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: "Cybersecurity is much more than an IT topic.”

Stephane Nappo

RESUMO

A segurança da informação nos dias atuais ganha importância cada vez mais relevante. Em particular, as instituições públicas, movidas pelo desejo de alcançar a eficiência em seus processos têm dado maior atenção a esse ramo de estudos da ciência da computação. Dentro desse contexto, os CSIRTs (*Computer Security Incident Response Teams*) – Núcleos de Tratamento e Resposta a Incidentes em Segurança da Informação – tem se tornado comuns em diversas organizações em todo o mundo. Esse trabalho é uma pesquisa qualitativa associada a um projeto de intervenção aplicado à Universidade Federal do Rio Grande do Norte, que tem como objetivo a instituição formal de um CSIRT. Como estratégia metodológica para alcançar seus objetivos, foi adotada da abordagem visual LCC (*Life Cycle Canvas*) e o *framework* ágil Scrum para planejar o projeto e coordenar as entregas dos produtos decorrentes dele. Como resultado, foi criado o CeTRIS (Centro de Tratamento e Resposta a Incidentes de Segurança), um CSIRT que trabalha com uma equipe de técnicos própria e atua preventiva e reativamente buscando promover na instituição a melhoria da segurança em seu ambiente computacional. Além disso, foram produzidos documentos com diretrizes e orientações para o seu funcionamento e indicadores para medir sua eficiência e desempenho. Foi também criado um *site web*, para apresentação do grupo à comunidade universitária e para divulgação de alertas e notícias. O CeTRIS, estabelecido, iniciou suas atividades, apresentando efeitos positivos para a segurança da informação na UFRN, tais como a redução da ocorrência de incidentes.

Palavras-chave: Segurança da Informação. CSIRT, Núcleos de Tratamento e Resposta a Incidentes de Segurança da Informação, Instituição Federal de Ensino Superior.

ABSTRACT

Information security nowadays is becoming increasingly important. In particular, public institutions, driven by the needs to achieve efficiency in their processes, have given greater attention to this branch of computer science studies. Within this context, CSIRTs (Computer Security Incident Response Teams), have become commonplace in many organizations around the world. This work is a qualitative research associated with an intervention project applied to the Federal University of Rio Grande do Norte, which aims at the formal institution of a CSIRT. As a methodological strategy to achieve its objectives, the LCC (Life Cycle Canvas) visual approach and the Scrum agile framework were adopted to plan the project and coordinate the deliveries of its products. As a result, CeTRIS (Center for the Treatment and Response to Security Incidents) was created, a CSIRT that works with its own team of technicians and acts preventively and reactively seeking to promote in the institution the improvement of security in its computational environment. In addition, documents were produced with guidelines for its operation and indicators to measure its efficiency and performance. A website was also created to present the group to the university community and disseminate alerts and news. The group was created and started its activities with positive effects for information security at UFRN, such as reducing the occurrence of incidents.

Keywords: Information security. CSIRT. Computer Security Incident Response Team. Federal Institution of Higher Education.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1. Introdução

Os sistemas computacionais e as redes de computadores tornaram-se elementos fundamentais para o funcionamento da nossa sociedade, pois nos trouxeram expressivos avanços em termos de velocidade de processamento, comunicabilidade, conectividade e acessibilidade de informação. E as tecnologias que surgem com base nesses sistemas são capazes de moldar o mundo, como o desenvolvimento de pesquisas sobre *Smart Cities* e estudos sobre aquecimento global e emissão de poluentes (Dhar, 2013). Grandes empresas de comunicações, como Google, IBM e Microsoft tem usado a tecnologia da informação para movimentar seus negócios atingindo bilhões de pessoas mundialmente. E o setor público, ciente desses benefícios, tem levado seus serviços para as plataformas cibernéticas em rede, com vistas a trazer maior efetividade no atendimento ao público.

Entretanto, juntamente com os progressos alcançados, surgem novos desafios. Um deles refere-se à questão da ética relacionada a dados (Floridi, 2016) e privacidade das informações. Além disso, no atual sistema socioeconômico, tão dependente de sistemas informacionais, as ameaças cibernéticas são diversas (Kettani, 2019), exigindo que sejam combatidas. A migração massiva dos dados de todos os tipos para a Internet, o comércio eletrônico, a globalização do mercado e das comunicações, o aumento exponencial no uso dos smartphones e o surgimento do conceito da Internet das Coisas (IoT – Internet of Things) fazem com que a segurança da informação esteja em lugar de destaque entre as preocupações de organizações públicas ou privadas.

Um ciberataque bem sucedido pode impactar negativamente a imagem de uma empresa, e o acesso não autorizado a dados de um serviço público terá potencial para prejudicar milhares ou até milhões de pessoas. Em 2014, um relatório revelou que anualmente companhias multinacionais têm um prejuízo de cerca de 7 milhões de dólares (Watkins, 2014). No ano de 2015, um popular site de relacionamentos extraconjugais sofreu um ataque que causou o vazamento de dados sensíveis de 37 milhões de seus usuários (Digital Guardian, 2017), fazendo com a empresa pagasse cerca de 11 milhões de dólares para encerrar ações judiciais (Reuters, 2017). Em 2019, a empresa Facebook sofreu um vazamento de dados pessoais de mais de 250 milhões de seus usuários devido a uma falha na configuração de um banco de dados com acesso online (Infosecurity Magazine, 2019). Nesse mesmo ano, em fevereiro, uma lista com dados de 620 milhões de contas de usuários de diversos sites na

Internet foi posta à venda (The Register, 2019) por hackers na Dark Web[1]. E em outubro, uma falha nos sistemas do DETRAN/RN expôs informações de aproximadamente 70 milhões de brasileiros (Infomoney, 2019).

Apesar desses eventos citados serem relativamente recentes, os incidentes em segurança de TI já ocorrem há décadas, como em 1988, quando um verme[2] criado por Robert Tappan Morris se proliferou pelas redes de computadores Unix nos Estados Unidos, infectando cerca de 10% de toda a Internet na época e levando a prejuízos de dezenas de milhares de dólares (Furnell, 2019). Um estudo posterior revelou que os danos causados em todo a Internet norte-americana na época, poderiam ter sido drasticamente minimizados se houvesse uma rede de comunicações e coordenação eficientes para a resposta ao problema (Skierka et al, 2015).

Quando se trata da segurança da informação, as organizações públicas mostram-se particularmente sensíveis a ciberincidentes, já que armazenam repositórios de dados particulares de milhões de cidadãos. Mais especificamente, as IFES (Instituições Federais de Ensino Superior) detém dados pessoais e acadêmicos de enorme quantidade de discentes, docentes e técnicos administrativos, além de inúmeros trabalhos e pesquisas científicas que, em caso de vazamento, alteração maliciosa ou perda, resultaria em prejuízos difíceis de mensurar. Cenário similar ocorre com organizações públicas em todos os países.

Cientes do grande impacto desses incidentes, instituições públicas e privadas vem se movimentando ao longo dos anos, tentando estabelecer estratégias para se proteger das diversas ameaças cibernéticas. Nesse contexto, uma das estratégias estabelecidas com sucesso para a defesa contra ciberataques tem sido a criação dos chamados times de tratamento e resposta a incidentes de segurança[3] (Bradshaw, 2015), ou CSIRT's – Computer Security Incident Response Teams[4]. Os CSIRTs são entidades concretas[5], grupos multidisciplinares de profissionais que visam coordenar ações relacionadas à tratamento e resposta a incidentes de segurança. Dessa forma, os CSIRTS colocam-se como um pilar relevante para a segurança, já

1 A Dark Web é um conjunto de redes, intranets e serviços que são acessados anonimamente e de forma criptografada, através de navegadores específicos, muitas vezes para fins ilícitos. Constituem uma parte da Deep Web, que por sua vez é a parte da Internet não acessível através dos mecanismos de busca e indexação.

2 Um verme de computador é um tipo de malware que se replica em redes de computadores utilizando-se de vulnerabilidades nos sistemas que as compõem.

3 Os termos "incidente" e "incidente de segurança" no contexto desse trabalho relacionam-se especificamente à segurança da informação no âmbito computacional.

4 Os CSIRT's são conhecidos também na literatura internacional como Computer Emergency Response Team (CERT), e em documentos e normativas do Governo Federal Brasileiro são chamados de ETIR - Equipes de Tratamento a Incidentes em Redes.

5 O artigo "Defining Computer Security Incident Response Teams", do Software Engineering Institute (Carnegie Mellon University) define como entidade concreta aquela com um ou mais colaboradores.

que desempenham papel ativo nas atividades de combate a atividades cibernéticas maliciosas tanto no sentido reativo (resposta e tratamento) como no proativo (prevenção).

Em face disso, o governo brasileiro tem emitido normativas relacionadas à segurança da informação na administração pública. Já em 2008 era publicada a Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional da Presidência da República (Brasil/GSI/PR, 2008), que "Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências", e, em sua Norma Complementar 05, trata da "criação de equipes de tratamento e resposta a incidentes em redes computacionais – ETIR" nos órgãos e entidades da Administração Pública Federal, direta e indireta (Brasil/GSI/PR/DSIC, 2009). Soma-se a isso, o Decreto 9.367, de 26 de novembro de 2018, que prescreve a instituição de "equipe de prevenção, tratamento e resposta a incidentes cibernéticos" (Brasil/PR, 2018). Em suma, o que o Governo Federal Brasileiro determina é que os órgãos públicos no âmbito federal deverão desenvolver um processo de gestão para a segurança da informação e, além disso, manter equipes (CSIRTs) próprias voltadas para a prevenção, o tratamento e a resposta aos incidentes de segurança em suas redes computacionais.

A UFRN historicamente tem mostrado disposição em adotar tecnologias da informação para o desenvolvimento de suas atividades. Conforme exposto no PDTIC[6] da UFRN (PDTIC/UFRN, 2015), já em 1975, foi criado o Núcleo de Processamento de Dados (NPD), "com o objetivo de implantar tecnologias computacionais de apoio às atividades administrativas da UFRN". Desde então, a universidade tem se desenvolvido fortemente em sua malha de comunicação computacional, através de investimentos em redes e cabeamento óptico e metálico, ativos cibernéticos e desenvolvimento de sistemas. Em 1999, é instituída a Superintendência de Informática (SINFO), para ser a entidade gestora de todo esse ambiente de tecnologia da informação na UFRN. Atualmente grande parte das atividades administrativas e acadêmicas são realizadas de forma eletrônica, sendo seus dados e informações armazenados nos sistemas desenvolvidos e mantidos pela Superintendência de Informática – os chamados SIG (Sistemas Integrados de Gestão). Por esses motivos, a instituição vem demonstrando cuidado com sua segurança cibernética. Sob a perspectiva estratégica, o Plano de Gestão 2019-2020 da instituição, tem como uma de suas metas a redução da ocorrência de incidentes de segurança da informação (UFRN, 2020).

6 Plano Diretor de Tecnologia da Informação e Comunicações.

1.1 Objetivos Geral e Específicos

Esse trabalho é uma pesquisa qualitativa associada a um projeto de intervenção, aplicado à Universidade Federal do Rio Grande do Norte. Usa a técnica visual LCC e o framework Scrum para a gerência do projeto e controle das entregas, e busca encontrar respostas práticas para a redução de incidentes de segurança da informação em uma IFES. O estudo **tem como objetivo geral a implantação de um CSIRT em uma Instituição Federal do Ensino Superior**. Ao final do projeto, deseja-se que o CSIRT esteja devidamente oficializado pela alta gestão da universidade, que esteja em funcionamento, que tenha autonomia para tratar e responder a incidentes de segurança da informação no âmbito da instituição e seja capaz de desenvolver ações de prevenção a eles. Entre as atividades esperadas que o CSIRT tenha pode-se listar a conscientização dos usuários para o uso seguro da rede da UFRN (através de cursos, palestras e outros recursos), a gestão de incidentes de segurança (que envolve basicamente o tratamento, a resposta e a recuperação), serviços de perícia forense a ativos da UFRN, serviços de monitoramento de vulnerabilidades na rede de computadores (inicialmente restrito aos ativos de rede nos datacenters da UFRN), assessoria técnica à gestão para a tomada de decisões e elaboração de normas e políticas referentes à segurança de TI.

Assim, como objetivos específicos, pretende-se *estruturar uma equipe de servidores para atuar preventiva e reativamente no processo de tratamento e resposta a incidentes*. Tal equipe deverá trabalhar de forma dedicada à segurança da informação. Será produzido *um regimento interno, especificando responsabilidades, modo de atuação e autonomia, formalizado por colegiado na instituição, além de um documento guia com diretrizes de funcionamento e indicadores de desempenho*. *Pretende-se ainda criar um site para o CSIRT, que será hospedado na hierarquia de domínio UFRN.BR*, contendo a apresentação da equipe, sua carta de serviços, uma área com documentação, normas, apostilas e notícias referentes a cibersegurança para a comunidade universitária. O site terá como propósitos principais disseminar as boas práticas em segurança da informação, alertar para os constantes problemas nessa área, como ataques, vulnerabilidades em sistemas e como proceder para evitá-los. Servirá também como ponto de contato e referência na UFRN para assuntos relacionados a segurança da informação. *Serão desenvolvidos indicadores de acompanhamento* com a

finalidade de avaliar o desempenho do CSIRT. Por fim, além dos objetivos específicos assinalados, para comprovar a efetividade da atuação do grupo, serão apresentados os resultados iniciais da implantação do CSIRT na Instituição.

2. Referencial Teórico

A Segurança da Informação, ou cibersegurança, deve ser gerenciada de uma perspectiva integral. De fato, o termo “cibersegurança” define o conjunto de ferramentas, boas práticas, guias e tutoriais, políticas e normas, ações, treinamentos e tecnologias que visem proteger a disponibilidade, integridade e confidencialidade dos seus ativos (ITU, 2018). A falha em criar uma processo rigoroso de gestão de segurança da informação tem levado a ocorrência de ciberataques em diversas instituições (Ruefle *et al*, 2014). Por outro lado, no caso da ocorrência de uma ataque, os danos causados são reduzidos e os gastos para o seu tratamento e recuperação são menores quando ele é detectado com rapidez (Cichonski et al, 2012). Não basta tentar se proteger. É essencial que haja um processo efetivo para responder e tratar problemas de segurança, quando eles ocorram (ITU, 2018).

2.1 Ciber Segurança e os CSIRTs

Uma eficiente estratégia estabelecida para a defesa contra ciberataques em empresas públicas e privadas no mundo todo tem sido a instituição de CSIRTs (Bradshaw, 2015). São também conhecidos como CERT®[7] (Computer Emergency Response Team). Os termos foram cunhados pelo Instituto de Engenharia de Software da Universidade de Carnegie Mellon (CMU), ao final da década de 1980, quando, em resposta ao incidente do Verme de Morris em 1988 (Furnell, 2019), foi formado o grupo denominado CERT/CC (CERT Coordination Center) em Pittsburgh, Pennsylvania.

O objetivo de um CSIRT é minimizar os danos provenientes de um incidente de segurança, fornecendo os recursos para uma resposta eficiente e rápida recuperação dos danos causados (Ruefle, 2007). Agem, portanto, com um fim em comum: o desenvolvimento e manutenção de um ecossistema de tecnologia da informação seguro, privilegiando os serviços de rede e minimizando as falhas que possam permitir ataques e levar a indisponibilidades. Essencialmente, um CSIRT deverá atender e reagir a incidentes de segurança, mas além disso trabalhar preventivamente na busca de evitá-los. Quando um CSIRT existe dentro de uma

7 O termo CERT é registrado pela CMU no Escritório de Marcas e Patentes dos EUA.

organização, ele é o ponto focal na coordenação e nas ações da resposta aos incidentes de segurança (Cichonski et al, 2012).

Deve-se observar que a crescente dependência dos governos e nações no uso de serviços computacionais e em redes, levaram ao surgimento da categoria dos CSIRTs Nacionais (Haller et al, 2011), ou seja, aqueles voltados à coordenação da gestão de incidentes a nível nacional e internacional. Muitos países já mantêm seus próprios CSIRTs Nacionais, por exemplo o AusCERT (Austrália), JPCERT/CC (Japão), US-CERT (EUA) e CERT.BR (Brasil). Os CSIRTs Nacionais podem ser organizações não governamentais, mas também estar ligados direta ou indiretamente ao governo (Morgus et al, 2015). No caso do Brasil, o CERT.BR encontra-se ligado ao governo através do Comitê Gestor da Internet – CGI.BR, que é coordenado pelo Ministério da Ciência e Tecnologia (Brasil, Decreto 4.829, 2003). Os CSIRTs, seja a nível nacional, regional e organizacional, de fato, vem a formar uma rede de comunicação e coordenação para resposta rápida aos incidentes cibernéticos, contribuindo para a sua resolução e o rápido retorno à normalidade, com menor prejuízo. O setor público e os governos assim, obtém uma eficiente barreira de proteção contra ataques à sua infraestrutura.

No livro eletrônico "*Handbook for Computer Security Incident Response Teams (CSIRTs)*" (West-Brown et al, 2003), é dada uma definição detalhada do que é o CSIRT, explicando sua missão e responsabilidades, sendo apresentado um framework para seu funcionamento. Já o white paper "Create a CSIRT" (CMU, 2017) é mostrado um passo a passo mais direto e mais resumido que pode ser usado como referência rápida na criação de CSIRTs. Em ambos os documentos são tratadas questões essenciais, como: recomendações e requisitos necessários para a sua constituição (planejamento, criação e formação), sua localização dentro da hierarquia da instituição, serviços oferecidos, fluxo de informação, relacionamento com outras equipes, tipos de CSIRTs, tamanho da equipe, custos de implementação, monitoramento e avaliação, entre outros. Esses documentos foram usados como guia para a implantação do CSIRT nesse plano de intervenção.

A instituição de um CSIRT em instituições públicas federais, no Brasil passa pelo crivo da legislação do país. As instruções normativas e normas complementares do Departamento de Segurança da Informação (DSIC) do Gabinete de Segurança Institucional (GSI) demandam a criação das ETIR[8] dentro dos órgãos da Administração pública federal e definem requisitos

8 ETIR (Equipes de Tratamento a Incidentes de Redes) – nomenclatura utilizada para CSIRTs nas instruções normativas do Governo Federal.

para a sua constituição (BRASIL, 2003). Especificamente a Instrução Normativa 1, do Gabinete de Segurança Institucional da presidência da República, publicada em 27 de maio de 2020, (BRASIL/GSI, 2020) diz em seu capítulo 5, inciso 4, que compete aos órgãos e entidades da administração pública federal (APF):

> *Instituir e implementar Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, que constituirá a rede de equipes, integrada pelos órgãos e pelas entidades da administração pública federal, coordenada pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo do Gabinete de Segurança Institucional da Presidência da República.*

Ou seja, todas as entidades públicas federais precisam ter uma equipe de profissionais trabalhando no tratamento e resposta a incidentes de segurança da informação, na forma de um CSIRT ou, como prescreve a nomenclatura do Governo, uma ETIR. Além disso, tais equipes deve reportar-se ao CTIR GOV[9].

Em adição a essa instrução normativa, a uma Norma Complementar número 05 - NC-05, traça diversas diretrizes orientadoras para a correta instituição de um CSIRT nas entidades da APF, (Brasil/GSI/PR/DSIC, 2009). Nela são abordados temas como: o responsável pela coordenação do grupo; os objetivos, missão, visão e responsabilidades dos integrantes; o modelo de implementação e estrutura organizacional; o nível de autonomia do CSIRT e, por fim, em anexo, é dado um modelo para a criação de documento de constituição para a equipe.

Segundo a norma, o responsável pela equipe, chamado de *Agente Responsável*, deverá ser um servidor público efetivo, o que provavelmente visa garantir a estabilidade de uma pessoa nessa função, já que estagiários ou terceirizados tem maior rotatividade. As definições de *missão* e *visão* da equipe deverão servir de linhas de base para toda a atuação e objetivos da equipe, dando especial atenção à atividade de coordenação de ações de tratamento e resposta a incidentes.

Ponto importante da norma é a definição do *modelo de implementação* da equipe, que será definido segundo a organização hierárquica e tamanho da instituição. Poderá ser assumido um modelo centralizado, tendo todos os colaboradores reunidos numa equipe única; descentralizado, quando os componentes estarão dispersos em diversos setores da instituição;

9 CTIR GOV – Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores, entidade subordinada ao Departamento de Segurança Institucional da Presidência da República - (https://ctir.gov.br/)

ou misto, tendo uma equipe principal centralizada e diversas equipes menores ou componentes em outros setores.

A norma trata ainda da autonomia da equipe[10], que afeta a sua capacidade de atuação. São definidos três níveis de autonomia, a saber:

1. Autonomia completa: Total autonomia, dada pela alta gestão, para respostas a incidentes de segurança, ações preventivas e de conscientização;
2. Autonomia compartilhada: Ações do grupo serão tomadas em conjunto com algum setor de gestão da organização.
3. Sem autonomia: só poderá agir com a autorização de um membro da organização com autoridade específica. Esse membro deverá estar devidamente designado no documento de constituição do CSIRT

2.2 Planejamento e Gerência do Projeto - LCC

A gerência e execução de projetos exige planejamento adequado, disciplina, foco e método. Muitos modelos e boas práticas têm sido desenvolvidos, sendo um dos mais conhecidos o PMBOK - *Project Management Body of Knowledge*, um conjunto de padrões de boas práticas para a gerência de projetos. Segundo o Guia PMBOK, um "*Projeto é um esforço temporário empreendido para criar um produto, serviço ou resultado único*" (Guia PMBOK, 2017).

Ultimamente, modelos que se baseiam em quadros (canvas) para a gerência de projetos tem sido adotados amplamente nas organizações, pois apresentam-se visualmente mais amigáveis aos seres humanos, permitindo uma melhor visualização (Eaidgah et al, 2016). A técnica visual LCC – Life Cycle Canvas (Veras, 2016), concebida pelo Professor Manoel Veras[11], propõe a gestão visual de todo o ciclo de vida de um projeto. Ela integra conceitos do PMBOK em quadros (canvas), também chamados de telas, contendo diversos elementos que indicarão informações importantes no planejamento e execução de um projeto. Por ter essa

10 Liberdade que o CSIRT terá para a realização de suas atividades de tratamento, mitigação e resposta aos incidentes de segurança da informação.

11 Dr. Manoel Veras: Professor Titular da Universidade Federal do Rio Grande do Norte, Centro de Ciências Sociais Aplicadas.

abordagem visual, cria um documento intuitivo tanto para produzir quanto para interpretar. Recentemente, um estudo, utilizando-se de uma série de indicadores de desempenho, concluiu que o LCC é eficaz na gestão do ciclo de vida de um projeto (Medeiros, 2016). Em um outro estudo, é acompanhada a aplicação do LCC a um projeto do governo do Rio Grande do Norte, concluindo ser o mesmo adequado também ao contexto público (Medeiros et al, 2017). Na figura 1 podemos ver o exemplo de uma tela do LCC.

Figura 1 - Tela LCC e seus fatores

Coluna 1 Por que	**Coluna 2** O que	**Coluna 3** Quem	**Coluna 4** Como	**Coluna 5** Quando/como
Justificativas	**Produto**	**Partes Interessadas**	**Premissas**	**Riscos**
Objetivos	**Requisitos**	**Comunicações**	**Entregas**	**Custos**
Benefícios	**Restrições**	**Equipe**	**Aquisições**	**Tempo**

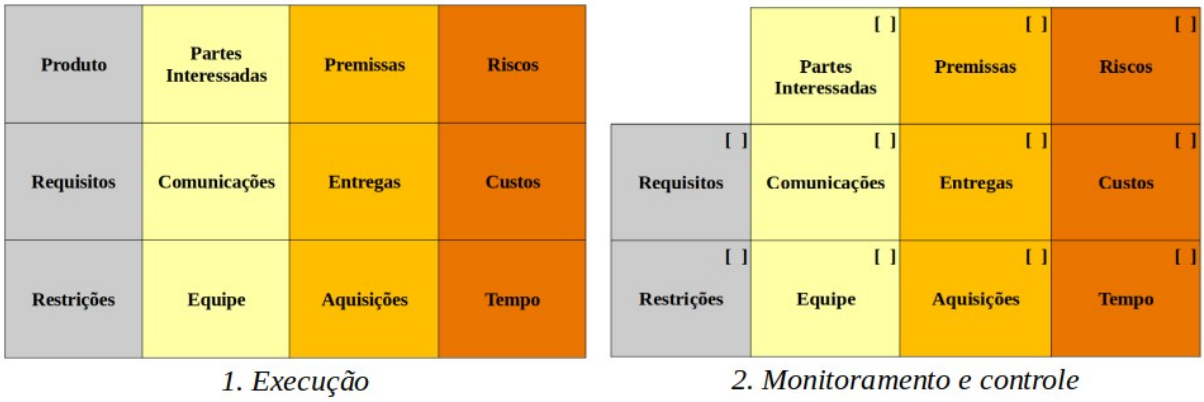
Fonte: Veras, 2016

O quadro (ou tela) LCC é dividido em linhas e colunas, formando caixas. Nessas caixas são dispostos fatores importantes para todo o ciclo de vida do projeto. Portanto, tais caixas são chamadas de fatores do LCC. Por exemplo, na figura, a primeira coluna (em verde), vê-se os fatores “Justificativas”, “Objetivos” e “Benefícios”, que dão ao gerente e à sua equipe o vislumbre geral de tudo aquilo que motiva a consecução do projeto. Os títulos dos fatores são auto explicativos, mostrando os argumentos para o empreendimento, suas finalidades e os benefícios que ele trará.

Já a segunda coluna (cinza), contendo os fatores “Produto”, “Requisitos” e “Restrições”, irá detalhar respectivamente os produtos que serão entregues, os requisitos esperados e as restrições do projeto. Por exemplo, em um projeto hipotético, o fator produto poderia ser descrito como “Uma ETIR instituída na empresa ‘XYZ’” e “Um site para a ETIR instituída”. Como requisitos poderíamos ter “Estar formalizado pela alta gestão” e/ou “Site deverá ter backups diários”. Por fim, nas restrições, define-se aquilo que restringirá o projeto, por exemplo: “Recursos limitados a R$10.000,00” ou “Equipe trabalhará em regime de 20 horas semanais”, ou ainda “Projeto deverá ser finalizado em X meses”.

As colunas restantes e seus fatores, também de maneira visual e intuitiva, tratarão de temas como interessados (*stakeholders*), ferramentas de comunicação, a equipe do projeto, aquisições do projeto, premissas e riscos, custos e tempo (cronograma). Dessa forma, o LCC guarda todos os elementos chave para o planejamento e desenvolvimento de um projeto. Tal quadro poderá ser impresso e posto em uma parede, visível para todos, ou poderá ser colocado em ferramenta online (por exemplo, uma aplicação WEB[12]) à qual todos tenham acesso e possam consultar periodicamente.

Figura 2 - Telas LCC de execução (1) e Monitoramento e Controle (2)



Fonte: Veras, 2016

O LCC segue um ciclo de vida que reflete as diferentes atividades em cada fase do projeto: Iniciação → Planejamento → Execução → Encerramento. Cada uma dessas fases apresenta um quadro com conjunto de fatores específicos para o gerente do projeto e equipe. Os quadros para as fases de iniciação e planejamento são os mesmos (Veras, 2016, p. 171), contendo 15 fatores, conforme exposto na figura 1. O quadro de Execução apresenta 12

12 Há um exemplo de LCC online e editável disponível em https://www.lifecyclecanvas.com.br/canvas/.

fatores (figura 2, tela 1). O de monitoramento e controle tem 11 fatores que contém, cada um deles, um campo indicador que representará o estado do andamento das tarefas (figura 2, tela 2). Por exemplo, um atraso poderá ser representado com uma indicação vermelha no fator “Tempo”. Uma elevação não esperada nos custos, representará um alerta no fator “Custos”. Por fim o quadro de encerramento refletirá todos os fatores do quadro de iniciação, mas em seu estado final – produto final, lições aprendidas, objetivos alcançados, custos e tempo reais, etc (figura 3).

Figura 3 - Tela de Encerramento

Fonte: Veras, 2016

Em paralelo à definição e atualização do projeto através dos preenchimentos das telas do LCC, há um conjunto de atividades que se desenvolvem no gerenciamento do ciclo de vida em um projeto. O quadro abaixo (Veras, 2016) relaciona algumas atividades e suas respectivas fases no ciclo de vida.

Quadro 1 – Ciclo de Vida do LCC

INICIAÇÃO	PLANEJAMENTO	EXECUÇÃO	ENCERRAMENTO
Definir interessados, gerente e patrocinador do projeto. Autorização para a realização do projeto.	Definição do escopo Definir e sequenciar atividades Estimar a duração das atividades.	Orientar e gerenciar o trabalho do projeto. Mobilizar a equipe do projeto.	Formalizar a aceitação dos produtos/serviços Encerrar o projeto formalmente

Definir recursos financeiros Criação da TAP e sua aprovação pelo patrocinador	Desenvolver cronograma. Planejar gerência e estimar custos. Planejar a gestão de recursos humanos. Planejar gestão de comunicações. Identificar riscos. Planejar resposta aos riscos. Planejar gestão de aquisições.	Realizar a garantia da qualidade. Gerenciar a equipe do projeto. Gerenciar comunicações Conduzir aquisições. Gerenciar o engajamento das partes interessadas.	Encerrar aquisições. Criação do TEP.

Fonte: Veras, 2016

Vê-se portanto que a gerência de um projetos, dentro da visão LCC não se restringe apenas ao preenchimento de fatores em quadros. Há uma série de ações independentes, logicamente concatenadas, que são essenciais ao bom andamento do projeto, baseadas nas boas práticas constantes em guias como o PMBOK. Tais atividades são recomendações, podendo ser aplicadas, ou não, dependendo das necessidades e do tamanho do projeto.

2.3 Gerenciando as Entregas do Projeto - SCRUM

Conforme exposto anteriormente, a gestão de um projeto exige cuidados, dedicação e disciplina. Há diversas formas de se gerir um projeto e vários métodos, ferramentas e conjuntos de boas práticas - PMBOK, Prince, Lean, Waterfall, Kanban, Agile etc. Dentre elas, com o passar dos anos, tem-se constatado o crescimento das metodologias ágeis, que buscam alcançar seus objetivos através do uso de equipes multidisciplinares e auto organizáveis, visando entregas rápidas, adaptabilidade, entregas rápidas e melhorias contínuas (Beck et al, 2013).

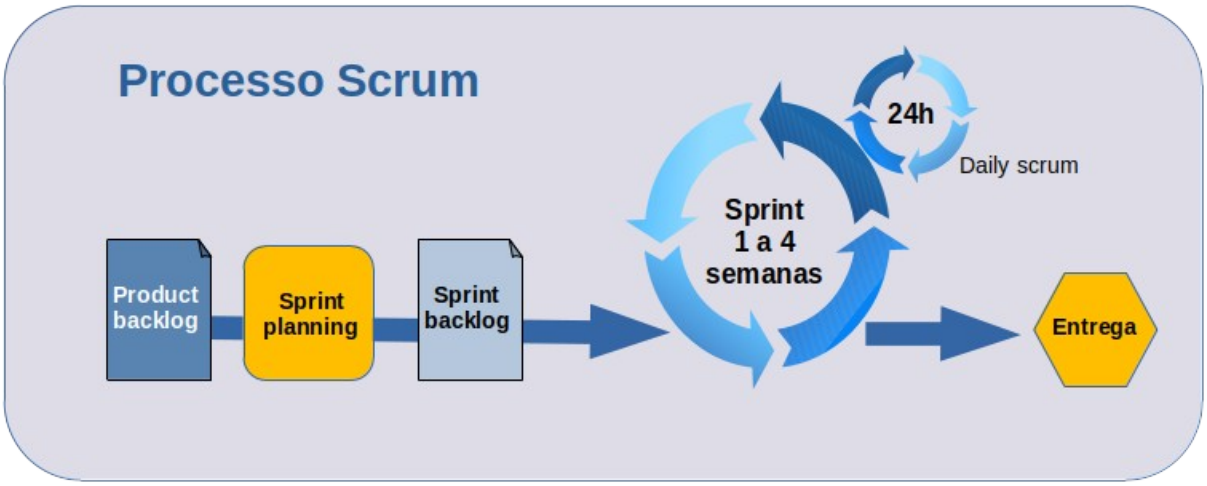
Dentre as abordagens ágeis, ganhou bastante relevância o Scrum (Sutherland, 2019), um framework[13] para o desenvolvimento e entrega de produtos complexos (Schwaber &

13 Abstração composta por códigos de programação, algoritmos ou procedimentos para prover funcionalidades genéricas em um projeto. Muito usado em desenvolvimento de software.

Sutherland, 2017). A ênfase do Scrum é o desenvolvimento de software, mas tem sido utilizado com sucesso em projetos de diversas outras áreas (Wykowski & Wykowska, 2019).

A abordagem usada no Scrum baseia-se na divisão de uma tarefa grande e complexa – por exemplo, a o desenvolvimento de um software – em diversas tarefas menores, passíveis de ser implementadas em curtos períodos de tempo, por equipes pequenas, de forma ágil. O conjunto total de tarefas, na nomenclatura scrum, chama-se *Product Backlog*. As tarefas escalonadas são adicionadas às *Sprint Backlog*. E as unidades de tempo (ou ciclos) chamam-se de *sprints* (figura 4).

Figura 4 - Processo Scrum



Fonte: Sutherland, 2019

Para a composição dos itens do backlog, pode ser utilizado o conceito de “histórias de usuário”, ou apenas histórias, que são frases simples e objetivas contendo o que o cliente espera do produto. Deve-se notar entretanto que o backlog não contém histórias. Ele contém itens. As histórias servem para compor tais itens (Deemer et al, 2012).

O Scrum foi idealizado para ser usado em equipes de pequeno porte (5 a 10 membros), trabalhando em ciclos de ação – *sprints*, que usualmente duram de duas semanas a um mês cada. Cada sprint divide-se em: 1) definição de seu backlog (o conjunto de entregas para aquela sprint), 2) o planejamento da sprint, e 3) execução. Os dois primeiros passos são realizados em uma reunião de inicialização da sprint. O passo 3 envolve todas as ações para a entrega do resultado. Ao final do ciclo, é realizada uma reunião de avaliação e nova sprint é iniciada. Dentro de cada sprint ocorrem reuniões diárias de curta duração, chamadas de *daily scrums*, onde a equipe informa suas realizações, dificuldades encontradas e planeja os

próximos passos. Essas reuniões auxiliarão no monitoramento das atividades. Cada sprint visa a entrega de um ou mais produtos. O scrum é um framework leve e de execução simples, mas que pode ser aplicado com sucesso a projetos de alta complexidade (Verheyen, 2013).

A responsabilidade pela execução de um projeto baseado em Scrum encontra-se em três papéis principais: o Product Owner, o Scrum Master e a Scrum Team (Schwaber. 2004). O *Product Owner (PO)* é o responsável pelo projeto. Ele guiará a equipe na criação dos backlogs em cada sprint, dividindo o processo geral em diversas atividades menores, que possam ser concluídas dentro do tempo previsto para cada ciclo. O PO deverá sempre manter o backlog dos produtos atualizado e visível para toda a equipe. Ele é o responsável pelo contato com o cliente e deverá conhecer todas as necessidades dele e do projeto. O PO é a interface entre o cliente e a equipe (Reis, 2010). Portanto, ele avaliará se as entregas estão de acordo com o que foi acordado. Caso perceba que a equipe não alcançará as metas propostas e o projeto não trará o retorno desejado, o PO poderá cancelar a sprint ou até mesmo suspender todo o projeto. Tal decisão e seus impactos deverão ser muito bem avaliados tecnicamente, para evitar danos ao cliente. Como líder, o PO deverá buscar motivar a equipe, mantendo sempre com ela um bom relacionamento (Varaschim, 2009).

O *Scrum Master* (SM) é a pessoa responsável pelo bom andamento das práticas Scrum (o rito scrum) durante todo o projeto. Ele deverá representar o PO em seus interesses e atuará como facilitador para a equipe, buscando remover quaisquer empecilhos que atrapalhem a consecução do projeto. (Carroll, O’Connor & Edison, 2018). Entre as responsabilidades do SM, estão esclarecer os envolvidos sobre as práticas scrum, auxiliar o PO na manutenção do backlog, auxiliar no processo de auto organização da equipe, auxiliar na remoção de impedimentos ao projeto e auxiliar a equipe na definição das entregas.

Por fim, a *Scrum Team* (ST) é a equipe de técnicos responsáveis pela avaliar a viabilidade e a realização das tarefas que levarão às entregas, ou produtos, incrementais de cada sprint. Sempre observando as prioridades definidas pelo PO e SM nos backlogs do produto e das sprints. As equipes deverão ser pequenas, variando de três a nove componentes, privilegiando a produção individual de cada indivíduo e tendo capacidade de se auto organizar (Morris, 2017).

O quadro seguinte associa os papéis do modelo Scrum e suas responsabilidades (Schwaber & Sutherland, 2017).

Quadro 2 – Papéis No Framework Scrum

PRODUCT OWNER	SCRUM MASTER	SCRUM TEAM
Faz o papel de cliente diante da equipe scrum e do scrum master. Representa as partes interessadas (interface entre a equipe scrum e os clientes) Conversa com os clientes Define os requisitos do produto Determina a data de entrega e conteúdo Prioriza as necessidades (histórias do usuário) de acordo com o valor de negócio Mantém o backlog do produto atualizado e priorizado Aceita ou rejeita as entregas ao final das sprints	Responsável pela aplicação dos valores da prática Scrum Remove impedimentos Atua como facilitador Auxilia o PO na manutenção do backlog. Assegura que a equipe está funcional e produtiva Blinda o time das interferências externas Assegura que a equipe esteja funcional e produtiva	Recomenda-se de 3 a 9 pessoas Estima as histórias Avalia se histórias poderão ser aceitas na sprint (se a equipe conseguirá desenvolver as histórias na sprint) Estima os tempos previstos para cada história Aceita (ou não) as histórias do backlog que entrarão nas sprints Compromete-se a entregar o incremento do produto Garante o funcionamento do incremento do produto Não há líder ou liderado dentro da equipe. São autônomos: Organizam-se na execução do trabalho na sprint (equipe auto organizada)

Fonte: Schwaber & Sutherland, 2017

O scrum assenta-se em três pilares: transparência, inspeção e adaptação (Schwaber & Sutherland, 2017).

Quadro 3: Pilares Do Scrum

TRANSPARÊNCIA	INSPEÇÃO	ADAPTAÇÃO
Todo o trabalho deve ser claramente definido e conhecido por todas as partes envolvidas no projeto. Envolvidos compartilham uma mesma visão do que está sendo realizado.	Todo trabalho deve ser inspecionado periodicamente para garantir a qualidade desejada. Devido ao pilar da transparência, tudo pode ser avaliado/inspecionado pelos envolvidos. Detecta desvios indesejáveis.	capacidade de adaptar o projeto à necessidades e mudanças repentinas. Capacidade de reajustar o projeto em resposta a desvios indesejados. Todos os envolvidos devem estar preparados para ajustes.

Fonte: Schwaber & Sutherland, 2017

Dos pilares acima relacionados, vê-se que o framework Scrum tem características que defendem grande visibilidade dos processos em um projeto para todos os envolvidos, alta possibilidade de inspeção e avaliação e capacidade de adaptar-se à mudanças sem a perda do controle do projeto. Tais pilares fornecem ao product owner, scrum master e a equipe scrum diretrizes ágeis para gerir, desenvolver e finalizar as entregas definidas no backlog.

Para prover o nível de transparência/inspeção/adaptação necessário ao Scrum, ferramentas podem ser utilizadas. Por exemplo, o quadro Kanban[14]. Trata-se de um quadro onde são dispostas em colunas o conjunto total de tarefas (product backlog), as tarefas a fazer (“to do”), aquelas que estão sendo feitas (“doing”) e as terminadas (“done”). O quadro deve ser disposto de forma facilmente visível por toda a equipe Scrum para que todos possam facilmente ter a percepção do trabalho que está sendo realizado por cada um dos membros durante cada sprint que está sendo realizada. Essa perspectiva baseada em fluxo do Kanban ajuda a complementar e melhorar o framework Scrum, contribuindo para que as equipes alcancem seus objetivos, dando transparência à execução das tarefas, promovendo assim a entrega de valor (Vacaniti & Scrum.org. 2019).

Uma das tarefas da equipe scrum (ST), é avaliar a viabilidade das tarefas. Para tentar minimizar as incertezas nessa avaliação, muitos times scrum utilizam a técnica de Planning Poker (Grenning. 2002). A técnica consiste em obter a opinião dos participantes de uma equipe sobre a dificuldade em se realizar uma determinada demanda. A fim de alcançar um consenso na equipe, é utilizado um conjunto de cartas, numeradas de forma crescente (por exemplo, pode-se utilizar a sequência de Fibonacci1[15]), representando níveis de dificuldade. Assim, de forma lúdica, cada membro apresenta sua estimativa, explicando brevemente seus motivos, e busca-se chegar a um consenso geral. Ao analisar cada um dos pontos de vista de seus companheiros, é comum que algumas pessoas mudem de ideia, pois não haviam levado em consideração certos fatores que outros citaram (Cohn, 2013).

14 Não confundir aqui com o Sistema Kanban, um modelo ágil e visual para controle de produção e gerência de tarefas (Ohno, 1988). O quadro é apenas uma de suas ferramentas.

15 Sequência crescente de inteiros, onde cada número é a soma dos dois anteriores.

3. Metodologia

O presente trabalho é uma pesquisa qualitativa associada a um plano de intervenção que teve como objetivo geral a instituição de um grupo de tratamento e resposta a incidentes de segurança em uma IFES. Para alcançar esse propósito, foi definido, através dos objetivos específicos, que o grupo deverá ser devidamente criado através de instrumento formal da instituição (portaria ou resolução), funcionando com uma equipe de servidores própria e dedicada às tarefas de segurança da informação, tendo suas características, visão, missão modo de atuação claramente descritas em um regimento interno, baseado boas práticas e em consonância com a legislação vigente. Foi proposta a entrega de um site web para o grupo, hospedado na hierarquia de nomes da UFRN, que servirá como canal de comunicação com a comunidade universitária. O site atuará também como fonte de notícias e documentação referentes boas práticas, conscientização e incidentes em segurança da informação. Consta ainda nos objetivos específicos a produção de um documento contendo diretrizes de funcionamento e indicadores de acompanhamento para orientar e permitir a avaliação das ações do CSIRT.

Esses produtos encontram-se alinhados aos objetivos gerais e específicos citados na introdução deste trabalho. Para atendê-los, foi proposta a adoção da abordagem visual LCC (*Life Cycle Canvas*), enquanto estratégia metodológica para esse projeto de intervenção, e do framework *Scrum*, para a gerência de suas entregas.

A abordagem Life Cycle Canvas tem como objetivo acompanhar o ciclo de vida completo de um projeto, de forma prática, objetiva e visual, desde a fase da iniciação, passando por planejamento, execução (com processos de monitoramento e controle) e a fase de encerramento. A escolha dessa abordagem buscou proporcionar uma visão ampla de todo o projeto, dando ao pesquisador e participantes informações essenciais como: Justificativas, objetivos, produtos, entregas, restrições, custos, cronograma, entre outros. Outra motivação para a sua escolha é o fato de o LCC ser uma técnica visual já conhecida e utilizada pelo pesquisador, por dar subsídios a projetos de intervenção (Medeiros et al, 2017) e por ter seus benefícios validados em estudo recente (Medeiros, 2016).

No Referencial Teórico, foi apresentada a abordagem LCC, que divide o ciclo de vida de um projeto em quatro fases. Nas seções abaixo, detalha-se processo metodológico utilizado nesse trabalho e as ações do plano de intervenção, em cada uma das fases.

3.1 Primeira Fase: Iniciação

A primeira fase do projeto teve sua abertura no dia 04 de novembro de 2019. Nessa fase foi realizada o preenchimento dos fatores chave de iniciação do projeto no quadro LCC, através de reuniões realizadas entre os componentes da equipe de segurança da informação da SINFO. Foram realizados três encontros onde inicialmente foi explicado à equipe participante os objetivos gerais do projeto – a instituição do CSIRT e seus benefícios para a UFRN – e a partir disso foram debatidos os objetivos específicos, chegando a sugestões que seriam posteriormente adicionadas aos fatores do LCC.

Em sequência, foi apresentada a estratégia metodológica para o projeto – uso do LCC associado ao Scrum. Foi escolhido o patrocinador, responsável por contribuir através do apoio institucional e/ou através de outros recursos. Esse importante ator deve apresentar grande interesse pelo projeto e ter influência e poder de decisão na organização para defender a execução do mesmo. Por esses motivos, a própria equipe sugeriu o Superintendente Adjunto de Informática da UFRN. Na última reunião dessa fase, o projeto foi apresentado a ele, que acolheu a proposta, assumindo o papel como patrocinador.

Todas essas definições foram postas no quadro LCC de iniciação que, aprovado pelo patrocinador, gerou o Termo de Abertura do Projeto (TAP)[16], saída principal da fase de iniciação e entrada para a fase de planejamento. O LCC de iniciação pode ser visualizado no Apêndice I.

3.2 Segunda Fase: Planejamento

Um projeto é um esforço temporal (tem começo, meio e fim bem definidos) para a entrega de um produto, serviço ou resultado (PMBOK Guide, 2017). O planejamento do projeto visa mantê-lo sob controle, evitando atrasos, retrabalho e extrapolação de custos.

O planejamento deste plano de intervenção foi iniciado no dia 02 de dezembro de 2019 quando deu-se o preenchimento do quadro LCC dessa fase. Para o encaminhamento, outro ator importante foi definido: o gerente do projeto, que o guiou durante todo o ciclo de vida,

16 O documento TAP pode ser encontrado no endereço https://cetris.ufrn.br/documentos/ , na seção “CeTRIS – Projeto”.

movendo a equipe em suas atividades e, através de reuniões de *brainstorm* com os envolvidos, definiu o escopo, que contém as atividades necessárias para que o projeto alcance as finalidades a que se propõe de acordo com as características especificadas. Foram revisados/atualizados os fatores definidos na fase de iniciação e estabelecida a periodicidade dessas revisões.

Para o controle de atividades e entregas, o projeto utilizou o framework Scrum. Foi feito o levantamento dos interessados e envolvidos no projeto, em especial os papéis para o framework scrum: *Product Owner* (assumido pelo Gerente do Projeto)[17], *Scrum Master* e a Equipe Scrum. Os fatores disponíveis no quadro LCC foram a base para o desenvolvimento das tarefas do modelo Scrum. O período definido para as sprints foi de quatro semanas com duas reuniões semanais para a gerência das entregas. Após a iniciação, a equipe estava definida da seguinte forma.

Nessa fase de planejamento, em uma das reuniões, o patrocinador do projeto solicitou que a equipe produzisse um documento para a Gestão de Incidentes de Segurança. Essa demanda foi aceita pelo gerente e adicionada como nova entrega e novo objetivo específico do projeto.

Com o escopo delineado, foi realizada a estimativa de atividades e o tempo necessário a elas – o que deu forma a ao cronograma. Foram acordados entre pela equipe e o gerente a forma de comunicação e tecnologias envolvidas. Em seguida foi feito o levantamento de aquisições. Verificou-se a necessidade de duas aquisições: equipe de desenvolvimento Web, necessária para a entrega do site, e a equipe de comunicações da SINFO, para a divulgação dos produtos entregues à comunidade universitária. Nesse momento foi importante o acionamento do patrocinador, que deu encaminhamento tanto ao pedido de desenvolvimento do site à Diretoria de Sistemas da SINFO, quanto à alocação da equipe de comunicações, no que foi prontamente atendido em ambas as demandas.

Os dados produzidos foram utilizados para a composição do quadro LCC da fase de planejamento (Apêndice II), atualizando a versão do artefato, que foi aprovada pelo gerente do projeto de forma a dar encaminhamento para a fase seguinte. Nesse artefato, vê-se que foram definidos como produtos o CSIRT funcionando e os seus objetivos específicos, consoante a natureza prática desse projeto de intervenção. Nos fatores “Restrições” e em “Premissas” foi indicado o problema da equipe de trabalho ser reduzida, bem como seu

17 Nesse projeto, ao invés de criar um Product Owner específico para o framework Scrum, o papel foi assumido pelo Gerente do Projeto definido na fase de planejamento da técnica visual LCC.

envolvimento em outras atividades da SINFO. Isso levou à criação de item no fator “Riscos”, alertando para a possibilidade do atraso em algumas entregas. Outro importante ponto observado foi a premissa relacionada à necessidade de envolvimento e aprovação da gestão da UFRN, sem a qual o CSIRT não teria a autoridade e autonomia necessárias para a realização de suas ações. No fator “Entregas” foram relacionados objetivos específicos. Em Aquisições foi adicionada a equipe de desenvolvimento. A premissa “Custos” não foi preenchida, já que a equipe de desenvolvedores já trabalhava na UFRN e o desenvolvimento de páginas para o interesse da UFRN já estava previsto em suas atividades cotidianas, não incorrendo assim em custos extra.

Para encaminhar a entrega do Site para o grupo, foram realizadas duas reuniões com a equipe de desenvolvimento *Web* da SINFO (que fora adicionada no fator LCC - Aquisições), chegando a uma definição de estrutura base e um cronograma específico. Todas as reuniões foram realizadas com o gerente do projeto, um dos membdos da equip scrum e a líder da equipe de desenvolvimento Web da SINFO. Foi usada a técnica de *brainstorming*, onde os participantes levantaram diversas idéias sobre a construção, formato e funcionalidades do site, gerando um protótipo em papel (Vianna et al, 2012), representando sua interface gráfica, contendo a descrição visual dos menus, suas funcionalidades e formato geral do site. Foram passados também, oralmente, requisitos relacionados à segurança e robustez da aplicação. O protótipo e requisitos foram encaminhados à equipe de desenvolvimento WEB, que passaria a trabalhar inicialmente em um modelo *mock-up*[18], para posterior apresentação e, sendo aprovado, daria início à programação efetiva do site. Tanto o mock-up, quanto a versão final foram produzidos na fase posterior, de execução do projeto, na execução das sprints.

Nesta fase, foi iniciado o levantamento de documentos do governo, como Leis, Decretos, Instruções Normativas e Normas Complementares, de forma a embasar a realização desse plano de intervenção. Além desses documentos, foram levantados guias de boas práticas para a gestão da segurança da informação, normas técnicas com recomendações sobre o assunto e diversas publicações. Tais fontes, listadas nas referências desse trabalho, serviram de base para a posterior formação do CSIRT na fase posterior, a de execução, e a produção de documentos como Regimento, Guia de Diretrizes e Indicadores, Guia do Processo de Gestão de Incidentes de Segurança e outros que estão no momento em planejamento para o futuro, mas fora do escopo desse trabalho.

18 Um modelo Mock-up é um protótipo de alta fidelidade do produto a entregar (Vianna et al, 2012). No caso, foi produzido um modelo semi-funcional do site do CeTRIS.

Foi realizado também o planejamento do processo Scrum, dividido em sprints de quatro semanas. O TAP do processo scrum utilizou o mesmo gerado pelo LCC. As *sprints* ficaram divididas conforme exposto no quadro abaixo, sendo que os prazos das entregas ocorrem sempre no fim de cada mês.

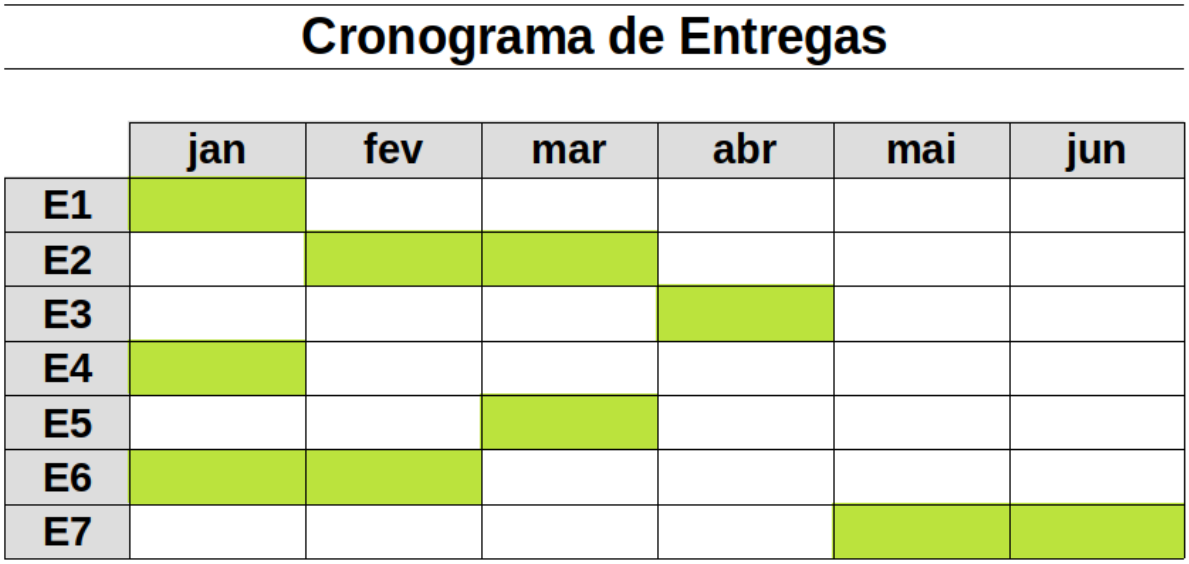
Quadro 4 – Divisão do Projeto em Sprints

Sprint	Descrição
1. Jan/2021	Entrega 1 – Diretrizes de Funcionamento Entrega 4 – Definição e estruturação da equipe Entrega 6 – Site do grupo (protótipo eletrônico – modelo mockup)
2. Fev/2021	Entrega 2 – Regimento Interno (parte 1) Entrega 6 – Site do grupo (versão final)
3. Mar/2021	Entrega 2 – Regimento Interno (parte 2) Entrega 5 – Indicadores de Acompanhamento
4. Abr/2021	Entrega 3 – Formalizar Regimento (Resolução CONSAD ou Portaria)
5. Mar/2021	Entrega 7 – Guia do Processo de Gestão de Incidentes (parte 1)
6. Jun/2021	Entrega 7 – Guia do Processo de Gestão de Incidentes (parte 2)

Fonte: Elaborado pelo autor.

E o cronograma planejado para o primeiro semestre de 2020 é mostrado na figura 5.

Figura 5 - Cronograma proposto na fase de planejamento (ano 2021)



Fonte: Elaborado pelo autor.

3.3 Terceira Fase: Execução, Monitoramento e Controle

A fase de execução realizou a integração de pessoas e recursos de forma a desenvolver as atividades dispostas na fase de planejamento. Processos como gerenciar o trabalho, gerenciar e mobilizar a equipe, gerenciar as comunicações, gerir aquisições, administrar o engajamento das partes interessadas fizeram parte desse momento (Veras, 2016). Nessa fase ocorreu paralelamente o monitoramento e controle do projeto, envolvendo processos como monitorar e controlar o trabalho, gerenciar controle de mudanças, validar e controlar escopo, controlar o cronograma e custos, controlar qualidade, riscos e aquisições.

Seguindo o ciclo de vida do LCC[19], os quadros de Execução e de Monitoramento e Controle foram iniciados e preenchidos. Ambos os quadros geraram cinco versões durante a execução do projeto (Apêndices III e IV). Mudanças que ocorreram foram devidamente registradas em seus fatores, sendo realizado também o acompanhamento da execução, através de seus indicadores-chave, onde se buscou evitar exceder custos, tempo e outros recursos.

Para a execução e entrega das tarefas, foi posto em ação o *framework scrum*, conforme planejado, dando uma abordagem ágil às tarefas, e colaborando com o engajamento da equipe do projeto. O ritual *scrum* definido na fase de planejamento foi posto em execução, com início, meio e fim de *sprints*, monitoramento constante através de reuniões diárias rápidas e avaliação ao final de cada uma delas. Para a estimativa do tempo e esforço das tarefas e o acompanhamento das mesmas, ferramentas como o quadro *Kanban* e técnicas de *planning poker* foram aplicadas.

Foi criada uma EAP (estrutura analítica de projeto) simplificada, baseada nas entregas dispostas no LCC, chamadas de macro entregas, que por sua vez foram divididas em sub entregas, que pudessem ser encaixadas mais facilmente nas *sprints*. Essa estrutura pode ser visualizada no apêndice VII.

Cada uma das entregas e sub entregas foram dispostas em quadro Kanban, em colunas nomeadas da seguinte forma:

1. **Entregas**: Essas são as entregas macro, conforme descritas no LCC;
2. S**ub Entregas**: Subdivisões das macro entregas em tarefas menores, conforme EAP simplificada;

19 Ver Referencial Teórico.

3. **Em execução**: Sub entregas que estão sendo realizadas no momento;
4. **Em Impedimento**: Sub entregas que estão paradas devido a algum impedimento;
5. **Feito**: Sub entregas finalizadas.

Para cada uma das sub entregas foi definido um responsável pela sua execução. Inicialmente, a ideia seria utilizar um quadro *kanban* físico para o projeto, mas a ocorrência da pandemia do COVID-19 e consequentes medidas de isolamento e trabalho remoto exigiram o uso de uma ferramenta de projetos *online*[20]. A figura 6 mostra captura de tela da ferramenta em um momento da execução do projeto (figura contém trechos borrados por questões de privacidade de dados).

Figura 6 - Representação de quadro Kanban em ferramenta Web online

Fonte: Página do Projeto CSIRT UFRN, no Trello (https://trello.com).

Durante todo o processo de execução, estiveram em funcionamento os mecanismos de observação e coleta de dados relacionados a incidentes de segurança na UFRN definidos na fase de planejamento, agregando dados que vieram a validar a efetividade das ações promovidas pelo grupo. No processo de coleta de dados foram utilizadas concomitantemente as técnicas de observação e de coleta documental (Marconi & Lakatos, 2003). Na observação, foram levados em consideração os chamados abertos no sistema da Superintendência de Informática relacionados segurança, os incidentes registrados no sistema SGIS e os incidentes de segurança não registrados, mas percebidos pelo pesquisador e a equipe dentro do campo de observação delimitado. Já a análise de conteúdo recolheu subsídios nas instruções e normas

20 Foi utilizada a versão gratuita da ferramenta Trello – https://trello.com

do governo federal, na legislação vigente e nas recomendações técnicas padronizadas, para a definição das diretrizes, responsabilidades, modo de operação, autonomia e ações a serem desenvolvidas pela equipe. Essas informações coletadas serviram como base para o desenvolvimento do regimento interno do grupo e para a definição de indicadores de acompanhamento para suas ações.

Ao final da fase de execução, o CeTRIS solicitou os serviços da equipe de comunicações da SINFO (ver fator “Aquisições” do LCC), para a apresentação do grupo perante a comunidade universitária e divulgação de seus serviços e do Site.

3.4 Quarta Fase: Avaliação/Encerramento

A última fase tratou do encerramento do projeto e a validação dos indicadores de resultado concebidos na iniciação e planejamento. Foi produzido o quadro de encerramento do projeto, contendo todos os fatores atualizados de acordo com as mudanças ocorridas no transcurso do projeto. Uma importante adição nessa fase foi o registro de lições aprendidas que, devidamente documentadas, poderão ser usadas como referência no futuro por outras equipes desse tipo que desejem ser formadas em outras instituições[21]. Foi documentado também o tempo e custos reais, riscos que ocorreram, as entregas aceitas, restrições e premissas validadas, comunicações efetivamente utilizadas e produto final.

Foi realizada a avaliação dos resultados das ações empreendidas, através de indicadores coletados durante o período das fases anteriores. Através da análise dos dados coletados, verificou-se que houve melhorias no processo relativo à segurança da informação no ambiente observado após a instituição do CSIRT e início de suas atividades[22]. Os indicadores avaliados basearam-se em informações e gráficos dos sistemas de monitoramento escolhidos no momento do planejamento. Foram avaliadas as quantidades de incidentes ocorridos em todo o ano anterior (2019) e comparada com a quantidade de incidentes no ano de 2020. A redução da ocorrência de incidentes de segurança indica a efetividade das ações preventivas do CeTRIS. Os frutos de tais ações estão descritos no capítulo seguinte – Resultados.

21 O documento de lições aprendidas foi anexado ao TEP – Termo de Encerramento do Projeto.
22 Ver capítulo Resultados.

O projeto gerou seu documento final – o Termo de Encerramento (TEP), além da conclusão dos resultados da pesquisa, descritos nesse texto. O TEP foi encaminhado ao patrocinador, quando então foi realizado aceite e encerramento formal[23].

23 TEP e Lições aprendidas podem ser encontrados no endereço https://wiki.cetris.ufrn.br/doku.php?id=administrativo:projeto_cetris:documentos

4. Resultados

Este capítulo descreve os resultados alcançados no plano de intervenção, segundo a metodologia proposta, que levaram à instituição do CeTRIS – Centro de Tratamento e Resposta a Incidentes de Segurança da informação na Universidade Federal do Rio Grande do Norte.

As seções seguintes relatam as ações realizadas e os resultados alcançados durante o ciclo de vida desse projeto.

4.1 Resultados das Fases de Iniciação e de Planejamento

As fases de Iniciação e Planejamento já trouxeram alguns resultados tangíveis, relevantes para a concretização dos objetivos propostos nos produtos e entregas desse projeto. Em reuniões com os envolvidos no projeto, foram detectados alguns problemas que precisaram de atendimento imediato. Um deles refere-se ao descontentamento e frustração que alguns colaboradores apresentaram por dividirem suas tarefas em diversas frentes, não podendo assim dedicar-se completamente às tarefas relacionadas ao projeto. Isso ocorria pois a quantidade de funcionários na diretoria de redes da Superintendência de Informática, sendo reduzida[24], mantinha-os trabalhando em diversas frentes. Alguns atendiam também demandas da equipe de infraestrutura e conectividade de redes e outros a demandas da equipe de serviços de rede. Esse cenário entrava em conflito direto com um dos requisitos listados nos fatores do LCC: *“Ter uma equipe dedicada”*. Foi também listado no fator Riscos: *“Membros com tarefas em outras áreas”*.

Buscando solução a esse problema, foram feitas reuniões com a gestão da SINFO e o patrocinador do projeto e, com isso, os colaboradores conseguiram a aprovação para trabalhar de forma dedicada às atividades de segurança da informação. Isso colaborou também para atender, em parte, o fator Produto: ter uma *“Equipe Dedicada a Segurança da Informação”*. Outro problema detectado foi a falta de um ambiente adequado à realização algumas tarefas. Não há uma sala reservada, nem equipamentos adequados, para a realização de tarefas como

24 Tais problemas resultaram em itens adicionados nos fatores “Restrições” e “Riscos” do LCC de Iniciação e Planejamento.

perícias técnicas em dispositivos de informática[25]. Essas deficiências foram parcialmente resolvidas. A gestão da SINFO adquiriu equipamento para possibilitar a realização das perícias, mas uma sala reservada ainda não foi conseguida.

As melhorias alcançadas nesse momento do projeto foram essenciais para garantir o andamento das fases posteriores. Sem elas, haveria grandes dificuldades, tanto para a equipe, quanto para o gerente do projeto, em adequar as demandas do projeto com demandas externas a ele.

4.2 Resultados das Fases de Execução e de Encerramento

Essa fase concretizou a instituição do CSIRT, formalizando-o perante a UFRN, através de portaria, bem como marcando o início das suas atividades.

A equipe responsável pelo projeto trabalhou na materialização dos objetivos definidos nas fases anteriores. Na primeira *sprint*, que envolve a definição do corpo técnico do CSIRT, criação de diretrizes de funcionamento e protótipo do site (entregas 1, 4 e 6 do LCC, respectivamente), foram feitos estudos das normas do governo e literatura relacionada à segurança da informação e equipes de tratamento e resposta a incidentes de segurança. Foram levadas em consideração principalmente as Instruções Normativas e Normas Complementares do DSIC[26], que se referem à segurança da informação e instituição de equipes de tratamento e resposta a incidentes nas instituições federais, bem como normas da ABNT. O quadro no Apêndice VI relaciona as leis, decretos, instruções normativas e normas técnicas principais.

Esses documentos (ver Apêndice VI - Documentos para Instituição do CSIRT), forneceram as bases para o encaminhamento inicial dos objetivos específicos do projeto. Em especial foram usados o *white paper* “Create a CSIRT” (CMU, 2017), o livro “Handbook for Computer Security Incident Response Teams (CSIRTs)” (West-Brown et al, 2003) e a Norma Complementar nº 05/IN01/DSIC/GSIPR. Esses documentos serviram como base para a criação de marcos para a implantação do CSIRT na UFRN, que segue descrito no quadro 5, abaixo.

25 Eventualmente a equipe de segurança é requisitada pela UFRN a realizar perícias técnicas em equipamentos que foram alvo de incidentes de segurança da informação.

26 Departamento de Segurança da Informação e Comunicações, subordinado ao Gabinete de Segurança da Informação da Presidência da República.

Quadro 5 – Marcos para a instituição do CSIRT

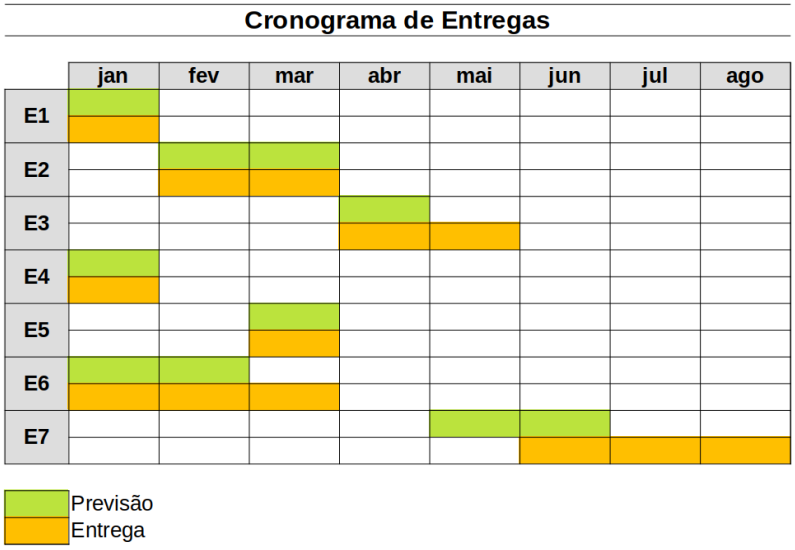
Marco	Descrição	Relaciona-se a
Obter apoio da gestão	Apoio da gestão é essencial para a formalização do grupo e para a sua existência e autoridade para executar suas tarefas.	Fase: Iniciação do LCC.
Planejar a instituição do CSIRT	Essencial para garantir as entregas e alcançar resultados.	Fase: Planejamento do LCC e Scrum.
Obter informações sobre incidentes na instituição	Procura obter uma visão dos incidentes mais importantes e dará subsídios para definir o modo de operação e responsabilidades do CSIRT. Dará subsídios à criação do regimento.	Fase: Execução do LCC. Entregas: 1 – Diretrizes de Funcionamento 2 – Regimento Interno 5 – Indicadores de Acompanhamento 7 – Guia do Processo de Gestão de Incidentes
Definir Diretrizes de funcionamento e indicadores de efetividade.	Documento guia para a atuação e avaliação do CSIRT. Dará subsídios à criação do regimento e ao processo de avaliação dos resultados das ações do gupo.	Fase: Execução do LCC. Entregas: 1 – Diretrizes de Funcionamento 2 – Regimento Interno 5 – Indicadores de Acompanhamento
Definir a Visão e Missão do grupo	Formará a identidade para o CSIRT e seu funcionamento. Dará subsídios à criação do regimento.	Fase: Execução do LCC. Entrega 2 – Regimento Interno
Constituir a equipe	Corpo técnico do grupo, seus papeis e responsabilidades.	Fase: Execução do LCC. Entrega 4 – Definição e estruturação da equipe
Definir modo de operação, autonomia e responsabilidades	Como o CSIRT atuará e que autonomia terá na execução de suas tarefas. Dará subsídios à criação do regimento.	Fase: Execução do LCC. Entrega 2 – Regimento Interno
Criar regimento e Formalizar o CSIRT	O regimento conterá toda a identidade, responsabilidades, modo de atuação, coordenação do CSIRT, oficializados perante a gestão da instituição.	Fase: Execução do LCC. Entrega 2 – Regimento Interno Entrega 3 – Formalizar Regimento
Divulgar o CSIRT	Publicizar o início das atividades para a comunidade atendida. No caso desse plano de intervenção, consiste na entrega do site, que atuará para divulgar a grupo, divulgar ações de conscientização e alertas em segurança da informação e como canal de comunicação entre comunidade e CSIRT.	Fase: Execução do LCC. Entrega 6 – Site do grupo
Avaliar a efetividade do CSIRT	Visa verificar se as ações empreendidas tem alcançados resultados adequados.	Fase: Encerramento do LCC

Fonte: Elaborado pelo autor.

Esses marcos são pontos relevantes, boas práticas destacadas na documentação estudada, para o encaminhamento da implantação de um CSIRT em uma instituição. Pode servir de base para a execução desse tipo de projeto em outras instituições públicas, podendo também ser adaptado segundo as suas necessidades.

Inicialmente foram realizadas reuniões presenciais, duas vezes por semana, na sala de reuniões da Superintendência de Informática (SINFO). Entretanto, em meados de março de 2020, ocorreu a suspensão das atividades presenciais na UFRN devido à pandemia do COVID-19, o que forçou as reuniões ocorrerem em formato remoto, através de videoconferências. Toda a equipe teve de se adaptar ao novo formato, tendo ainda de conciliar atividades extras que surgiram decorrentes do processo de trabalho remoto[27].

Figura 7 - Cronograma Real de Entregas, em 2020.



Fonte: Elaborado pelo autor.

É importante observar que, com relação ao cronograma original do LCC (fator “Tempo”) houve atrasos em algumas entregas (figura 7). A possibilidade de atrasos foi prevista no fator riscos do LCC de Iniciação e no de Planejamento. A equipe de trabalho do projeto estava envolvida em outras atividades relacionadas à rede da UFRN, nas quais constantemente necessitavam de sua intervenção. O período de abril a junho de 2020 foi especialmente atribulado devido à exigência da adoção do trabalho remoto (*home office*) na

27 Tais atividades se constituíram principalmente na configuração e manutenção de equipamentos servidores para acesso remoto (VPN – Virtual Private Network) e a criação de contas para técnicos, professores e alunos da UFRN.

UFRN, em atendimento a medidas de prevenção impostas pela pandemia do COVID-19. Tal imperativo resultou na necessidade de criação, configuração e suporte de acessos remotos para uma alta quantidade de usuários da comunidade universitária, o que elevou muito o trabalho da equipe nesses momentos.

Além disso, a equipe de desenvolvimento WEB, listada no fator Aquisições, apresentava também sobrecarga de trabalho, pois atendia a diversos outros projetos de sites para a UFRN. A figura 7 mostra os tempos de entregas planejados em verde e os atrasos ocorridos em laranja. Já o quadro 6, em seguida, mostra a distribuição de entregas por *sprints*, com os atrasos destacados também na cor laranja.

Esses atrasos causaram um efeito limitador temporário: em um determinado momento, o grupo já dispunha de corpo técnico e diretrizes definidos, bem como um regimento proposto, mas não da devida oficialização da gestão para atuar. Por esse motivo, o grupo iniciou seus trabalhos, atuando com escopo e autonomia limitados e sob supervisão da Superintendência de Informática. Já os atrasos relacionados à entrega do site limitaram temporariamente as ações do grupo, que não tinham ainda um canal de comunicação eficiente com a comunidade universitária. Somente após a publicação da portaria e entrega do site, o grupo passou a funcionar plenamente, conforme planejado no projeto.

Quadro 6 – Distribuição das Sprints e atrasos ocorridos

Sprint	Descrição
1. Jan	Entrega 1 – Diretrizes de Funcionamento Entrega 4 – Definição e estruturação da equipe Entrega 6 – Site do grupo (protótipo)
2. Fev	Entrega 2 – Regimento Interno (rascunho) Entrega 6 – Site do grupo (versão final)
3. Mar	Entrega 2 – Regimento Interno (versão final) Entrega 5 – Indicadores de Acompanhamento Entrega 6 – Site do grupo (versão final)
4. Abr	Entrega 3 – Formalizar Regimento.
5. Mai	Entrega 3 – Formalizar Regimento. Entrega 7 – Guia do Processo de Gestão de Incidentes (rascunho)
6. Jun	Entrega 7 – Guia do Processo de Gestão de Incidentes (rascunho)
7. Jul	Entrega 7 – Guia do Processo de Gestão de Incidentes (final)
8. Ago	Entrega 7 – Guia do Processo de Gestão de Incidentes (versão final).

Fonte: Elaborado pelo autor.

Apesar de certos atrasos, as entregas foram sendo realizadas. As primeiras relacionaram-se à documentação do CSIRT. Foi inicialmente realizado um levantamento dos tipos mais comuns de incidentes de segurança da informação na UFRN. Para isso, serviram como fontes de dados o sistema de chamados da Superintendência de Informática, o sistema de detecção de intrusão[28] que lá opera e a própria experiência de sua equipe de segurança. Conhecendo os ataques, alertas e incidentes mais comuns, a equipe passou à etapa seguinte. Foi produzido o guia listando diretrizes[29], contendo diversos requisitos a serem seguidos pelo grupo para a sua atuação na UFRN. Posteriormente, em nova versão, esse documento foi unificado ao documento com indicadores de acompanhamento (entrega 5 desse projeto). O documento pode ser encontrado no site do CeTRIS[30], na seção “Documentos” → “Políticas e Normas da UFRN” → “Diretrizes e Indicadores – CeTRIS”. As diretrizes levam em consideração a autonomia, responsabilidades e atuação do grupo, como por exemplo, manter um regimento interno formalizado perante a gestão da UFRN, manter sistemas de detecção de incidentes de segurança da informação, realizar ações permanentes de resposta a tais incidentes, realizar ações de conscientização e alertas voltados à comunidade universitária como forma de prevenção, acompanhar os sistemas de registro de incidentes, revisar bienalmente os indicadores de eficiência do grupo, entre outras.

Ainda na primeira *sprint* foi realizada a estruturação do corpo técnico do CSIRT – definição de componentes, papeis, responsabilidades e atividades individuais – deu-se nas reuniões semanais, parte presenciais quando anteriormente à pandemia, parte por videoconferência, em reuniões após ela. Nas reuniões, foram levantadas as habilidades dos participantes do projeto, que por já participarem da equipe de segurança da SINFO, foram os candidatos naturais para compor a equipe do CSIRT. Os próprios componentes, baseando-se na documentação levantada, sugeriram os papéis e responsabilidades.

Dessa forma foi definido e estruturado o corpo técnico do CSIRT. Seguindo os requisitos definidos, todos os componentes tinham experiência na área de segurança da informação. Os postos de cada componente, preenchidos conforme suas habilidades, formaram: um coordenador geral; um técnico em perícia forense; um técnico em detecção de vulnerabilidades e testes de penetração; dois técnicos voltados para atuar na área de

28 Um IDS (do inglês *Intrusion Detection System*) é um sistema automatizado que “escuta” a rede de computadores em busca de sinais de invasões e ataques cibernéticos.

29 O guia de diretrizes, em sua versão final, foi unificado ao documento de indicadores de acompanhamento (entrega 5), fundindo-se em um único documento - “Diretrizes de Funcionamento e Indicadores de Acompanhamento”.

30 https://cetris.ufrn.br/documentos

comunicação, visando a conscientização em segurança da informação. Todos atuariam de forma geral nos processos relacionados a tratamento e resposta a incidentes. O quadro 7 relaciona papéis e suas descrições.

Quadro 7 – Estrutura e Responsabilidades da Equipe do CeTRIS

Papel	Descrição	Responsável[31]
Coordenação	Coordenação geral do CeTRIS. Coordenação geral do processo de gestão de incidentes de segurança.	Membro 1
Perícia Forense	Realização de perícias forense em computadores e redes.	Membro 1 Membro 2
Detecção de Vulnerabilidades e Testes de Penetração	Detectar falhas de segurança em computadores e redes; buscar vulnerabilidades, auxiliando em sua correção; Realizar testes de penetração.	Membro 3
Comunicação, prevenção e conscientização em Segurança da Informação	Coordenar processos de conscientização em segurança da informação na UFRN. Criar documentação sobre boas práticas no uso da rede computacional. Produzir alertas, documentos e avisos voltados à comunidade universitária com o objetivo de prevenir incidentes de segurança.	Membro 4 Membro 5

Fonte: Elaborado pelo autor.

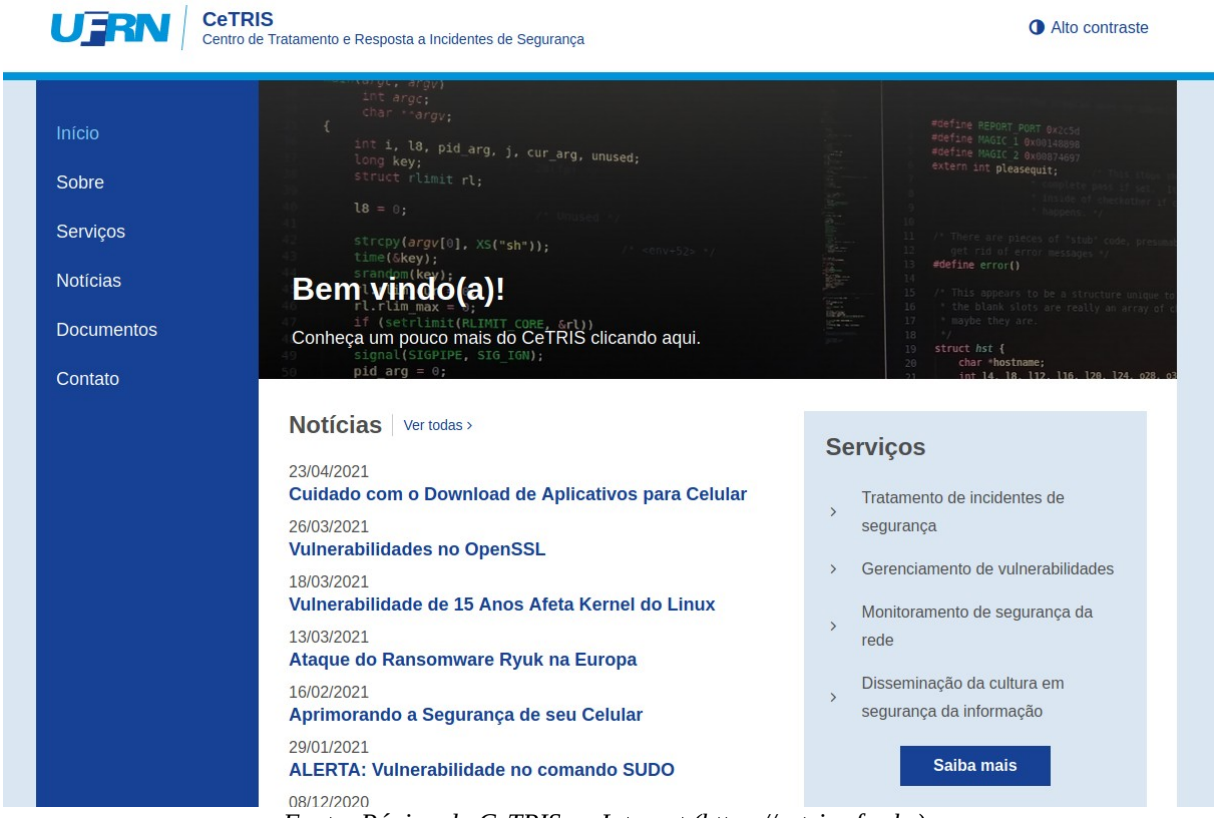
O desenvolvimento do site foi acompanhado através de comunicações por conferência de voz, através da ferramenta *Skype* e e-mails, envolvendo o *product owner* e componentes da equipe de desenvolvimento *Web*. Como estabelecido no planejamento, a equipe de desenvolvimento criou modelos *mock-up* de alta fidelidade para o site, de forma a demonstrar suas funcionalidades. Esses modelos eram versões online contendo recursos de navegação, que atenderam bem ao seu propósito: demonstrar o que seria e como ficaria o produto final. cada melhoria do modelo era apresentado ao *product owner*, que posteriormente às discutia por videoconferência com a equipe do projeto, coletando observações e sugestões, para retorná-las para o pessoal de desenvolvimento do site. Uma captura de tela de um dos modelos *mock-up* pode ser visualizada no Anexo 1[32].

Um dos requisitos principais solicitados pela equipe foi a segurança do site, quando se pediu o uso de tecnologia resistente a tentativas de invasões. Também foi solicitado que a página fosse intuitiva e de fácil navegação. Foi pedida a implementação de páginas para conter informações específicas sobre o grupo, carta de serviços, informações de contato, uma

31 Nomes dos membros não especificados devido a questões de privacidade.
32 O modelo encontra-se disponível temporariamente no endereço: https://xd.adobe.com/view/4ebba370-c1dc-45eb-5f47-d5df113cb8dc-388a/

página para a divulgação de notícias, uma para publicizar documentos, uma página para publicações da equipe e uma de contato. A equipe de desenvolvimento Web recomendou o uso de framework Vue.js[33] que já vinha sendo usado amplamente na SINFO, com sucesso. Nas semanas subsequentes, foram desenvolvidas e avaliadas versões de protótipos que receberam sugestões de melhoria e ajustes em reuniões de avaliação nas *sprints*. Entretanto, devido a excesso de demandas sobre a equipe de desenvolvimento, ocorreram atrasos na entrega da versão final, que foi postergada para a *sprint* 3. Em abril de 2020, o site foi posto em produção e vem funcionando desde então no endereço https://cetris.ufrn.br. Esse é um dos produtos entregues nesse projeto de intervenção. Sua página principal pode ser visualizada na figura 8.

Figura 8 - Página principal do site do CeTRIS



Fonte: Página do CeTRIS na Internet (https://cetris.ufrn.br).

Para atender a medidas de segurança solicitadas, o site foi construído usando um sistema de zonas de segurança. A primeira zona, de acesso restrito à equipe de desenvolvimento da SINFO, consiste de um servidor em uma ambiente de rede onde são

33 Vue.js é um framework para desenvolvimento Web em linguagem de programação Javascript.

desenvolvidos os códigos. Nesse servidor, os códigos produzidos são compilados em páginas HTML estáticas e enviados ao servidor de produção, que fica acessível ao público. Um segundo ambiente roda uma aplicação protegida por credenciais de acesso (login e senha), chamada Gestore[34], responsável pela gerência de arquivos e notícias que irão para o site. Por fim, um terceiro ambiente roda o servidor de produção, que recebe as páginas HTML estáticas e compiladas com os dados e as notícias provenientes dos dois primeiros ambientes. Se houver um ataque e comprometimento desse servidor que atua em ambiente público, tanto os códigos das páginas quanto as notícias permanecerão protegidos, pois estão armazenados nos ambientes restritos.

Dando encaminhamento à consecução dos objetivos do projeto, foram definidos a identidade do CSIRT e a formalização do seu corpo técnico, definido anteriormente. Como identidade, refere-se ao nome, visão e missão da equipe. Para esse fim, era necessário a produção e formalização de um regimento interno. Para a produção desse documento, foram levados em consideração os dados colhidos das pesquisas e coleta documental realizadas sobre a legislação vigente, instruções normativas do DSIC e suas normas complementares, bem como o documento de diretrizes, criado no início do projeto. Foram primeiramente trabalhados os textos da visão e a missão do grupo, que serviriam como base para a produção do regimento interno e definição do nome do mesmo. Após algumas discussões, a equipe chegou aos seguintes resultados:

Visão:

> *Promover a segurança da informação na UFRN, sendo sua referência para o tratamento e resposta a incidentes de segurança em redes computacionais.*

E sua missão:

> *Atuar na detecção, análise e resposta a incidentes de segurança na rede computacional da UFRN, atendendo à sua comunidade universitária e promovendo entre os seus usuários as melhores práticas relativas à segurança da informação.*

34 O Gestore é uma aplicação desenvolvida pela equipe da Superintendência de Informática da UFRN voltada à gestão de sites hospedados em sua infraestrutura.

Em seguida, foi definido o nome do grupo e a abrangência de suas atividades. Como requisitos primários para o nome, ele deveria ser claro, informativo e fácil de memorizar. O nome deveria ser esteticamente aceitável, evitando cacofonias. Deveria ser curto, a ponto de ser posto com facilidade em uma URL[35] e dentro do sistema de nomes do domínio UFRN.BR. Essas exigências foram levantadas para facilitar a sua aceitação e assimilação pelo público alvo – a comunidade universitária. O nome deveria também representar a missão e visão do grupo criado. Dessa forma, para atender a todos esses requisitos, a equipe produziu o nome "Centro de Tratamento e Resposta a Incidentes de Segurança" abreviado através da sigla CeTRIS. Como URL, ficou definido https://cetris.ufrn.br. A atuação do grupo ficou restrita à rede, ativos de rede e serviços de rede da Universidade Federal do Rio Grande do Norte.

Dois aspectos bastante importantes foram o modelo organizacional e a autonomia do CSIRT. O primeiro, o modelo organizacional, foi baseado no disposto na Norma complementar 05/IN01/DSIC/GSIPR de 14 de agosto de 2009, em seu artigo 7. Esse modelo indica uma equipe que não trabalha com exclusividade nas tarefas de tratamento e resposta a incidentes, mas divide-se entre segurança e outras tarefas relacionadas a tecnologia da informação. Esse modelo foi escolhido devido à reduzida quantidade de servidores na Diretoria de Redes da SINFO.

Já a autonomia do grupo foi discutida com bastante cuidado. A autonomia indica a liberdade que um grupo tem de implementar ações de segurança, tratamento, resposta e mitigação a incidentes, sem depender da aprovação de instâncias superiores. De acordo com a mesma norma complementar citada acima, no artigo 9, uma equipe poderá ter autonomia completa, compartilhada ou nenhuma autonomia. Para que o grupo tivesse respostas rápidas às necessidades de segurança da instituição, decidiu-se optar pela autonomia total. Era uma decisão arriscada, pois dessa forma o regimento poderia não ser aprovado pela gestão da UFRN. Mas consideramos necessário para que as ações do grupo não ficassem "engessadas" aguardando a ratificação dos gestores[36].

Em reuniões posteriores foram discutidos e definidos o agente responsável[37] pela equipe, sua estrutura organizacional e posicionamento na UFRN, e suas responsabilidades.

35 URL – Uniform Resource Location é uma referência para um recurso na Internet, que pode ser um computador ou um serviço. Coloquialmente falando, um endereço web.

36 O regimento posteriormente foi submetido à gestão da UFRN e aprovado, dando a autonomia desejada ao grupo.

37 Servidor efetivo da instituição, responsável pela coordenação do grupo.

Com todos esses passos finalizados, foi produzida a versão final do texto do regimento do grupo[38]. Conforme pode ser observado no artigo 5.6, as atividades e responsabilidades da equipe do CeTRIS envolvem o processo de gestão de incidentes (tratamento, mitigação, recuperação e resposta), o contato com outras ETIR's no Brasil, a documentação de incidentes e formas de resolução em base de conhecimento, manter e preservar adequadamente evidências e artefatos encontrados em incidentes, sugerir melhorias para a segurança da rede computacional da UFRN, intervindo quando necessário.

Já o artigo 5.4 lista as responsabilidades do agente responsável: coordenar as atividades do CeTRIS e representá-lo perante a UFRN e outras instituições, atuar como contato com o CTIR Gov[39], atuar como contato com autoridades policiais e judiciais nos casos de incidentes que tipifiquem crimes e elaborar relatórios sobre os incidentes ocorridos na UFRN.

Toda a estrutura do regimento foi baseada em informações obtidas na fase de coleta de dados documental, especialmente na norma complementar 05 da Instrução Normativa 01 DSIC/GSI/PR.

Na *sprint* 3 foi produzida mais uma entrega: o documento contendo indicadores de acompanhamento para o CSIRT. Foram definidos indicadores que pudessem levar a avaliar a efetividade das ações tomadas pelo CSIRT, com relação à diminuição dos incidentes de segurança na UFRN. Os dados para os indicadores são provenientes de equipamentos que monitoram os incidentes em rede na UFRN, do seu sistema de chamados, do sistema SGIS/RNP[40] e da observação direta de ocorrência de incidentes. O quadro 8, abaixo, relaciona as fontes de dados e sua descrição.

Quadro 8 – Fontes de Dados para Avaliação de Resultados

Fonte de Dados	Descrição
Monitoramento de Incidentes	Sistema de detecção de incidentes instalado na rede da UFRN.
Sistema de Chamados da SINFO	Incidentes relatados pela comunidade universitária (Servidores da UFRN).
SGIS/RNP (sgis.fnp.br)	Incidentes relatados pela Rede Nacional de Pesquisa.
Observação	Incidentes detectados diretamente pela equipe do projeto.

Fonte: Elaborado pelo autor.

38 O regimento pode ser encontrado na seção de documentos do site do CeTRIS: https://cetris.ufrn.br/documentos.

39 CTIR Gov (ctir.gov.br) – CSIRT que atua no Departamento de Segurança de Informação (DSI), do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

40 SGIS é o Sistema de Gestão de Incidentes de Segurança, mantido pela RNP (https://sgis.rnp.br) e oferecido às IFES para o registro e gerência dos incidentes de segurança computacional.

Ao final da *sprint*, a equipe resolveu unificar o documento de Diretrizes de Funcionamento, produzido anteriormente, ao documento de Indicadores, gerando um único documento chamado de “Diretrizes de Funcionamento e Indicadores de Acompanhamento para o CeTRIS”. O documento foi posto publicamente na seção “Documentos” do site do CeTRIS[41].

Com esse documento e a proposta de regimento, a equipe encaminhou à gestão da SINFO, que o submeteu à gestão da UFRN. O regimento interno foi aprovado por portaria em maio de 2020 (UFRN. 2020), sendo assim vencida mais uma etapa para atingir o objetivo geral do trabalho. A oficialização deveria ter ocorrido na *sprint* 4, mas devido a fatores externos, que não puderam ser resolvidos a tempo pelo patrocinador do projeto, ocorreu apenas na *sprint* 5.

Por fim, a equipe passou a trabalhar na última entrega: o documento para gestão de incidentes de segurança, que fora solicitado pela gestão da Superintendência de Informática durante a fase de planejamento. A equipe debruçou-se sobre a norma da ABNT (ABNT NBR ISO/IEC 27002, 2013), gerando a versão inicial do Guia do Processo de Gestão de Segurança da Informação da UFRN, sendo posto no site do CeTRIS (seção “Documentos”) e ficando disponível para as equipes de TI da UFRN e de outras instituições.

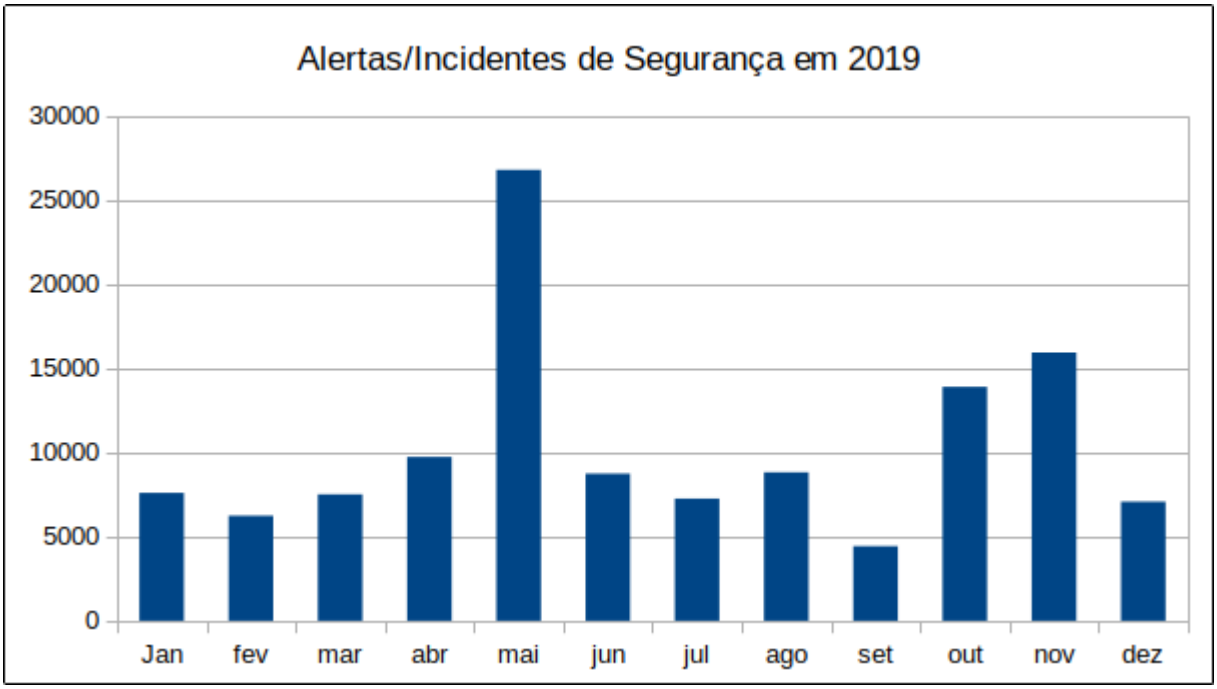
4.3 Avaliação dos Resultados Alcançados

Com o CSIRT formado e oficializado, as primeiras ações do grupo relacionaram-se com campanhas de conscientização voltadas aos administradores de sistemas das equipes de TI das diversas unidades da UFRN. Foram iniciadas também ações proativas e reativas a incidentes que vinham ocorrendo com frequência. Essas ações estão alinhadas ao produto 1 definido no LCC – ter um *“CSIRT oficializado e atuando na UFRN”*, e ao Fator Requisito 6: “*Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN”*. Em 2018, a equipe de segurança da SINFO havia instalado um IDS[42], sistema que monitora o tráfego da rede e busca por padrões de ataque. Em meados de 2019 começou a ser

41 https://cetris.ufrn.br/documentos
42 IDS – Intrusion Detection System (sistema de detecção de intrusão).

detectada uma alta incidência de ataques de login por força bruta[43] contra servidores SSH[44] que se encontravam na rede interna da UFRN. Esse serviço é muito visado por atacantes por potencialmente permitir o acesso ao sistema operacional de um servidor, como se fosse um acesso local. Ataques com sucesso permitem a execução arbitrária de comandos, escravizar a máquina para realizar outros ataques, realizar processamento do interesse do atacante (por exemplo, a mineração de criptomoedas) etc.

Figura 9 - Alertas/Incidentes de segurança ocorridos na UFRN em 2019



Fonte: Elaborado pelo autor.

No final de 2019 e início de 2020, com a equipe já iniciando seu planejamento para a formação do CeTRIS, analisando dados do IDS, percebeu a necessidade de realizar uma campanha de segurança, voltada aos administradores de rede da UFRN, visando implementar medidas de segurança que contribuíssem para minimizar a ocorrência dos ataques de força bruta[45]. O grupo passou a divulgar notas recomendando o uso de dispositivos de firewall local

43 Um ataque de login por força bruta é aquele no qual o atacante, utilizando-se de método automatizado, tenta exaustivamente acessar um sistema alvo, usando milhares de pares login/senha.

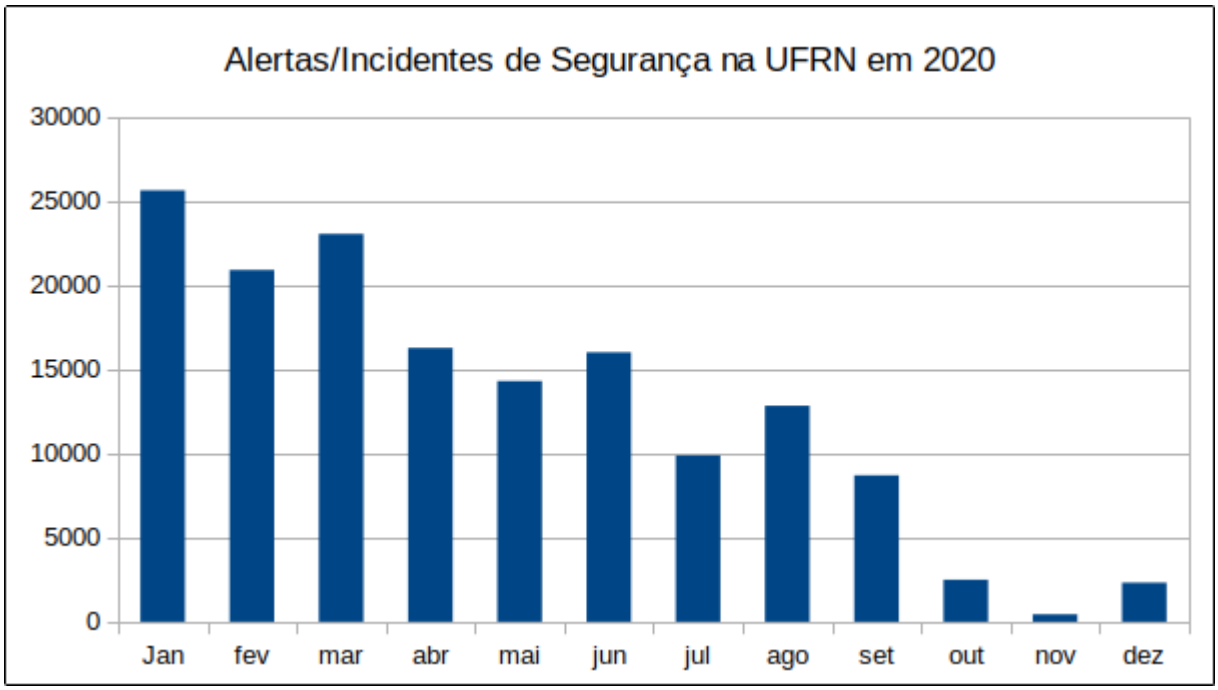
44 SSH (Secure Shell) é um serviço que permite o acesso (login) remoto ao computador que o executa. Muito usado para a realização de tarefas administrativas à distância.

45 Essa ação vem em atendimento ao objetivo específico: “estruturar uma equipe de servidores para atuar no processo de tratamento e resposta a incidentes”, já que as atividades dos CSIRTS envolvem atividades preventivas.

nos servidores, uso de senhas fortes e configuração de portas[46] alternativas para o SSH[47]. Infelizmente, nesse momento, houve pouca adesão ao solicitado na campanha. Um gráfico de ocorrência de incidentes (alertas de segurança) em 2019 pode ser visto na figura 9.

Nota-se que a média geral permanece praticamente a mesma, apresentando ligeiras flutuações, durante quase todo o ano de 2019, havendo alguns picos anômalos nos meses de maio, outubro e novembro[48].

Figura 10 - Alertas/Incidentes de segurança ocorridos na UFRN em 2020



Fonte: Elaborado pelo autor.

Já no ano de 2020, o IDS começou a detectar um considerável aumento nas ocorrências desse tipo de tentativa de ataque. O CeTRIS, já operando e trabalhando em parceria com a Superintendência de Informática, intensificou as campanhas e passou a notificar os administradores sobre a elevação dos riscos e da importância da segurança em seus servidores. Com a oficialização grupo por portaria, dando a ele maior autonomia e autoridade,

46 Uma porta é um identificador para um serviço de rede. Cada serviço de rede na Internet (HTTP, E-mail, Serviço de transferência de arquivos FTP, acesso remoto SSH) tem uma porta específica padrão. A porta do SSH é a 22.

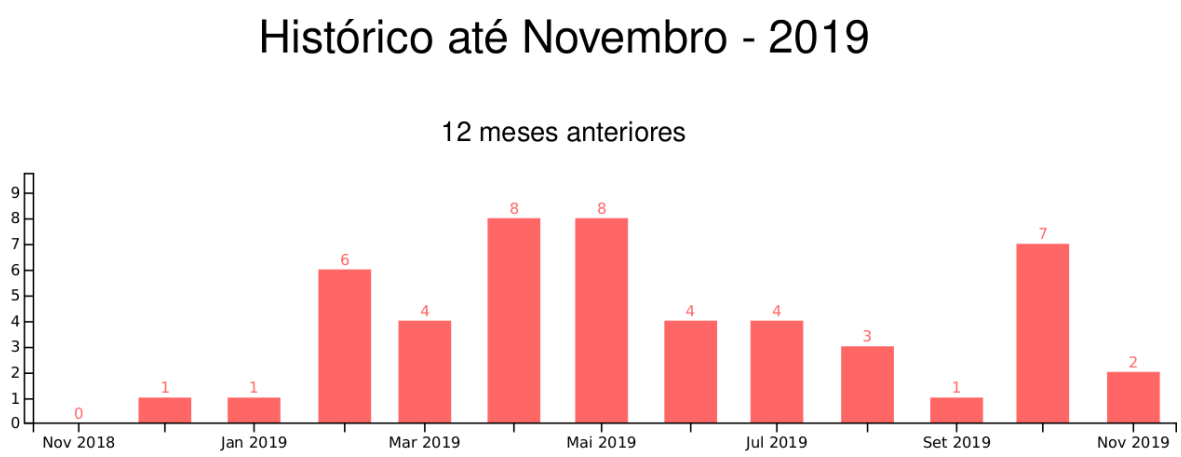
47 A lógica da mudança de portas relaciona-se ao fato de que os ataques de força bruta contra serviços SSH, em sua imensa maioria, são automatizados, visando a porta padrão 22. Se mudarmos para uma outra porta não utilizada por outros serviços, a possibilidade de ataque cai drasticamente.

48 Os incidentes contabilizados nos gráficos são os aqueles simples, que correspondem a alertas de segurança ou tentativas de invasão que não obtiveram sucesso. Incidentes médios e graves não foram contabilizados nesse trabalho por ser informação considerada sensível.

iniciou-se uma campanha mais incisiva, alertando para a possibilidade de bloqueios de servidores que são alvo constante e tem alto risco de invasão, com o objetivo de preservar a segurança de rede computacional e imagem da UFRN[49]. A partir de abril de 2020, os incidentes começaram a diminuir. A figura 10 mostra o gráfico de incidentes ocorrido nesse ano[50].

Percebe-se que, a partir do mês de abril começou a haver uma resposta muito positiva às ações de conscientização e bloqueio de portas promovidos pelo CeTRIS. O número de alertas registrados começou a decair mensalmente, chegando nos últimos três meses a valores menores que a média de 2019 e a níveis quase irrelevantes no mês de novembro. Esses indicadores ajudam a demonstrar que mesmo ações simples podem ter efeitos expressivos para a segurança computacional de uma instituição.

Figura 11 - Incidentes registrados no SGIS em 2019



Fonte: Elaborado pelo autor.

Outra importante fonte de indicadores de efetividade das ações do CeTRIS foi o sistema SGIS/RNP, que permite gerir os incidentes ocorridos em todas as entidades que utilizam o acesso Internet provido pela Rede Nacional de Pesquisas no Brasil. No ano de 2019, foram registrados cerca de 48 incidentes de segurança na UFRN. A figura 11 mostra gráfico gerado

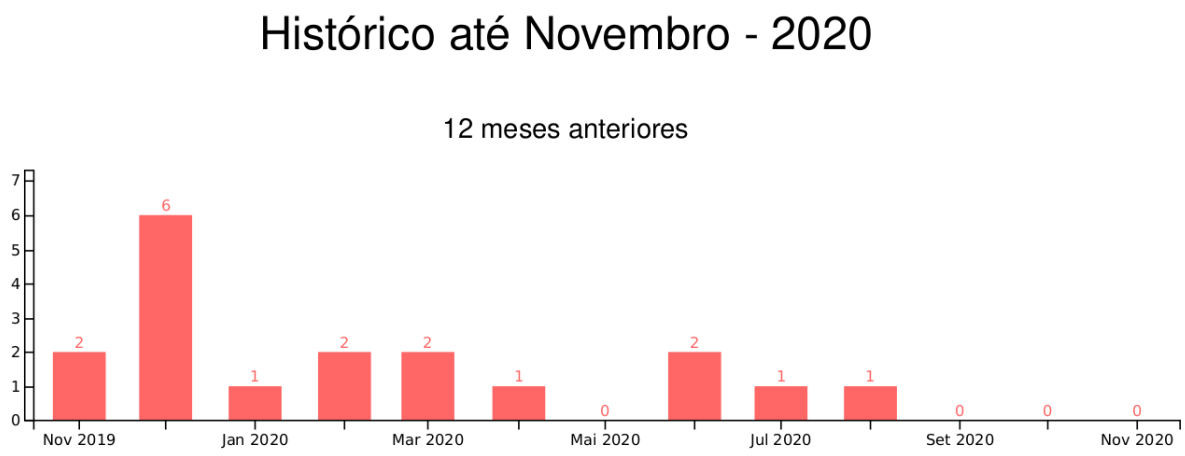
49 Servidores invadidos comumente são utilizados como vetor de outros tipos de ataque. Uma instituição com alta ocorrência de servidores invadidos, termina tendo seus endereços IP cadastrados em listas negras na Internet e pode ter seu acesso bloqueado em alguns sites.

50 Esses gráficos vem demonstrar resultados da atuação do grupo, atendendo ao objetivo específico de ter “uma equipe de servidores para atuar no processo de tratamento e resposta a incidentes”.

pelo módulo de relatórios[51] desse sistema. Esses incidentes incluem tentativas de ataques, desfigurações de páginas, problemas relacionados a transmissão e cópia de material protegido por direitos autorais (pirataria), tentativas de *phishing scam*[52], ataques de *Denial of Service (DoS)*[53], entre outros.

Em 2020, o CeTRIS passou a trabalhar com as equipes de serviços de rede da Superintendência de Informática e equipes de TI na UFRN, buscando ações preventivas para certas fontes de problemas, tais como: contas de e-mail ou outros serviços de rede com senhas muito frágeis, servidores/serviços desatualizados, servidores abandonados[54] etc. Além de ações preventivas, manteve observação a comportamentos atípicos na rede computacional que pudessem indicar ataques em andamento. Essas ações, também demonstraram efetividade, fazendo com que a quantidade de incidentes registrados no ano de 2020, fosse menor, conforme gráfico na figura 12, que indica 10 registros de janeiro a novembro de 2020.

Figura 12 - Incidentes registrados no SGIS em 2020



Fonte: Elaborado pelo autor.

Além das ações concretas e seus desdobramentos práticos com relação à segurança da informação na UFRN, o CeTRIS vem promovendo a conscientização no uso de recursos

51 Na figura é mostrado o período de novembro do ano anterior a novembro do ano corrente, pois um bug no sistema impediu a correta formatação do gráfico quando solicita-se o período janeiro-dezembro.

52 Phishing Scam é um golpe que busca obter informações sensíveis, como logins, senhas, números de cartão de crédito etc. O atacante sempre tenta se passar por uma entidade confiável. Muito comum vir através de mensagens por e-mail, SMS ou aplicativos de mensagens instantâneas.

53 DoS - Ataque cibernético que visa derrubar (tornar indisponível) o acesso a computadores ou redes, ao esgotar seus recursos e impedir que respondam a requisições.

54 Servidores que foram postos em funcionamento por algum programa, departamento ou unidade da UFRN, mas que foram deixados sem qualquer manutenção, e sem atualizações e cuidados, terminam sendo alvo de invasores.

computacionais na instituição através de seu web site, relacionado como produto e uma das entregas do projeto. Na sua seção Notícias[55], a equipe vem se empenhando em publicar ao menos duas notícias mensais que levem a comunidade universitária a melhor entender os incidentes de segurança, o que pode ocasioná-los e como se proteger. Em paralelo ao uso do site como fonte de disseminação da cultura da segurança da informação, a equipe vem usando o sistema de e-mails da UFRN para ampliar o alcance do processo. Temas como vírus, golpes de *phishing*, atualização de sistemas, uso de senhas, cuidados no uso de celulares, proteção a informações pessoais, vulnerabilidades, certificados digitais e diversos outros assuntos já foram abordados durante o ano de 2020 e 2021.

O documento para a gestão de incidentes de segurança, outra entrega do projeto, encontra-se disponível, publicado no site, para que as equipes de TI da UFRN possam utilizá-lo como guia para o tratamento de seus incidentes. E o CeTRIS, conforme suas diretrizes e regimento, vem dando o apoio necessário à comunidade universitária em assuntos relacionados à segurança da informação.

Através dos dados e gráficos mostrados, percebe-se que a atuação de um CSIRT em uma instituição acadêmica é capaz de trazer melhorias para a segurança do ambiente de redes, mitigando os incidentes, principalmente através da criação de uma postura defensiva, fortalecida por ações preventivas e de divulgação de boas práticas no uso dos recursos computacionais.

55 https://cetris.ufrn.br/noticias

5. Conclusão

Este plano de intervenção, aplicado à Universidade Federal do Rio Grande do Norte, teve como objetivo principal a instituição de um centro de atendimento e resposta a incidentes de segurança da informação, equipe conhecida como CSIRT. Sendo esse seu objetivo geral, teve como objetivos específicos o desenvolvimento e instituição de um regimento interno (especificando responsabilidades, parâmetros de funcionamento, autonomia e modo de atuação) devidamente formalizado por colegiado na instituição, a estruturação de uma equipe de servidores dedicada para atuar na gestão dos incidentes, o desenvolvimento de um site web para o grupo, contendo informações úteis visando melhorar a cultura de segurança cibernética na instituição, a produção de documento com diretrizes de funcionamento e definição de indicadores de acompanhamento com a finalidade de avaliar o funcionamento da equipe criada e, por fim, a entrega de um documento guia para a gestão de incidentes de segurança da informação.

Todos os objetivos, tanto gerais como específicos foram alcançados, conforme exposto nos capítulos Metodologia e Resultados. A UFRN hoje dispõe de uma equipe dedicada de funcionários, trabalhando na gestão de incidentes cibernéticos – o CeTRIS. Essa equipe, além de atuar reativamente nos incidentes que ocorrem, tem postura preventiva ao realizar mensalmente a divulgação de notícias relacionadas a segurança de TI em seu site web (https://cetris.ufrn.br) e diversas ações mais técnicas em dispositivos de controle, como Firewalls, sistemas IDS e IPS (*Intrusion Detection Systems* / *Intrusion Prevention Systems*). O grupo trabalha de acordo com seu regimento interno, formalizado pela alta gestão da universidade, seguindo as diretrizes e autonomia nele definidas.

Através de indicadores elaborados na pesquisa, bem como dados colhidos e gráficos produzidos, vê-se que a instituição do CSIRT teve resultados positivos, diminuindo os incidentes e alertas de segurança, mês a mês, durante o período observado, tanto através dos sistemas internos (IDS na rede) como no sistema externo (SGIS/RNP)[56]. Essa diminuição coincidiu com o início das ações promovidas pelo CeTRIS – processos de conscientização usuários da rede de computadores, ações de bloqueios de vetores de ataque, melhorias nas configurações de segurança de servidores no Datacenter da UFRN e melhorias nas

56 Ver capítulo Resultados.

configurações dos sistemas de firewall. Desta forma, verifica-se que a existência e atuação de um CSIRT traz resultados positivos para a segurança de uma instituição acadêmica.

Em adição a essas ações e resultados, o CeTRIS vem atuando de forma a apoiar a gestão, tanto da Superintendência de Informática quanto a da UFRN, nas questões relacionadas a segurança computacional, elaboração de normas e políticas, respostas a órgãos de controle (como TCU, CGU), produção de textos de comunicação (na área de segurança) para a comunidade universitária, apoio às equipes de TI dos diversos departamentos, unidades e setores da universidade.

A instituição do CeTRIS e a consecução dos objetivos almejados nesse projeto, dotou a UFRN de ferramentas para melhor gerir, responder, tratar e prevenir os incidentes cibernéticos de forma mais ágil, sólida e eficiente, possibilitando um ambiente de rede computacional mais seguro e estável à comunidade universitária. A conclusão do projeto abre portas para futuros estudos e encaminhamento de ações, especialmente nas áreas de *análise de malwares*, *análise de vulnerabilidades*, procedimentos de *testes de invasão*, técnicas de defesa, projetos de conscientização em segurança da informação, entre outros. Tais processos são comuns em CSIRTs maduros e bem desenvolvidos. Nesse aspecto, o CeTRIS, em parceria com docentes e alunos da UFRN, pode vir a servir como base para profícuas pesquisas na área de segurança da informação.

A UFRN é uma organização grande, com milhares de servidores e alunos. Sugere-se, como desdobramento desse trabalho, que a instituição encoraje equipes de TI em suas diversas unidades a formar grupos locais dedicados à segurança da informação, coordenados pelo CeTRIS, com o objetivo de disseminar melhor a cultura da segurança na comunidade universitária e colaborar de forma mais pontual e eficiente na mitigação dos incidentes.

Referências

1. DHAR, V. D**ata Science and Prediction**. Communications of the ACM, december 2013, vol. 56, no. 12.
2. FLORIDI, L; TADDEO, M. **What is Data Ethics?** 2016. Royal Society. Phil. Trans. R. Soc. A 374: 20160360.
3. KETANNI, H.; WAINWRIGHT, P. **On the Top Threats to Cyber Systems**. 2019. IEEE 2nd International Conference on Information and Computer Technologies
4. WATKINS, B. **The Impact of Cyber-Attacks on the Private Sector.** 2014. Disponível em: http://www.amo.cz/wp-content/uploads/2015/11/amocz-BP-2014-3.pdf, Acessado em 05 abr. 2020.
5. DIGITAL GUARDIAN. **A Timeline of the Ashley Madison Hack**. 2017. Disponível em https://digitalguardian.com/blog/timeline-ashley-madison-hack. Acessado em 21 abr. 2020.
6. REUTERS. **Ashley Madison parent in $11.2 million settlement over data breach**. 2017. Disponível em https://www.reuters.com/article/us-ashleymadison-settlement-idUSKBN19Z2F0. Acessado em 21 abr. 2020.
7. THE REGISTER. **620 million accounts stolen from 16 hacked websites now for sale on dark web**. 2019. Disponível em https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/. Acessado em 20 abr. 2020.
8. INFOSECURITY MAGAZINE; **Data Leak Exposes 267 Million Facebook Users**. 2019. Disponível em https://www.infosecurity-magazine.com/news/data-leak-exposes-267-million/ Acessado em 20 fev. 2020.
9. INFOMONEY, **Falha no sistema do Detran-RN causa vazamento de dados de 70 milhões de brasileiros**. 2019. Disponível em: https://www.infomoney.com.br/minhas-financas/falha-no-sistema-do-detran-rn-causa-vazamento-de-dados-de-70-milhoes-de-brasileiros/. Acessado em: 07 nov. 2019.
10. FURNELL, S.; SPAFFORD, E. **The Morris Worm at 30**. 2019. ITNOW, Volume 61, Issue 1, Spring 2019, Pages 32–33.
11. RUEFLE, R.; **Defining Computer Security Incident Response Teams**. 2007. Carnegie Mellon University. Disponível em https://resources.sei.cmu.edu/asset_files/WhitePaper/2007_019_001_294579.pdf. Acessado em 01 abr. 2020.
12. International Telecommunication Union (ITU), The World Bank, Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). **Guide to Developing a National Cybersecurity Strategy – Strategic engagement in cybersecurity**. 2018. Disponível em https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf. Acessado em 05 abr. 2020.
13. BRADSHAW, S. **Combating Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity**. 2015. SSRN Electronic Journal. 10.2139/ssrn.2700899.
14. RUEFLE, R.; DOROFEE, A.; MUNDIE, D.; HOUSEHOLDER, A. D.; MURRAY, M.; PERL, S. J. **Computer Security Incident Response Team Development and Evolution**. 2014. IEEE Security & Privacy, vol. 12, no. 5, pp. 16-26, Sept.-Oct. 2014.
15. CICHONSKI, P.; MILLAR, T.; GRANCE, T.; SCARFONE, K. **Computer security incident handling guide**. 2012. NIST Spec. Publ.
16. SKIERKA, I.; MORGUS, R.; HOHMANN, M.; MAURER, T. **CSIRT Basics for Policy-Makers**. 2015. Transatlantic Dialogues on Security and Freedom in the Digital Age.

17. HALLER, J.; MERRELL, S.A.; BUTKOVIC, M. J.; **Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0.** Disponível em: https://kilthub.cmu.edu/articles/Best_Practices_for_National_Cyber_Security_Building_a_National_Computer_Security_Incident_Management_Capability_Version_2_0/6572093/1. Acessado em: 25 abr. 2020.
18. MORGUS, R.; SKIERKA, I.; HOHMANN, M.; MAURER, T. **National CSIRTs and Their Role in Computer Security Incident Response**. 2015. Transatlantic Dialogues on Security and Freedom in the Digital Age.
19. BRASIL. **Decreto Nº 4.829, de 3 de setembro de 2003. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências**. 2003. Disponível em http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm. Acessado em 25 abr. 2020.
20. BRASIL/GSI/PR. **Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências**. 2008. Disponível em https://www.gov.br/governodigital/pt-br/legislacao/14_IN_01_gsidsic.pdf. Acessado em 19 mai. 2021.
21. BRASIL/GSI/PR. **Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 - Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.** 2020. Disponível em https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215. Acessado em 19 mai. 2021.
22. BRASIL/GSI/PR/DSIC. **Norma Complementar nº 05/IN01/DSIC/GSIPR, Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR**. 2009, Disponível em: http://dsic.planalto.gov.br/legislacao/copy_of_nc_05_etir.pdf. Acessado em: 21 abr. 2020.
23. BRASIL/PR. **Decreto 9.367, de 26 de novembro de 2018 - Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997**. 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acessado em 19 abr 2020.
24. UFRN. **Plano Diretor de Tecnologia da Informação 2016-2017**. 2015, Disponível em https://ufrn.br/resources/documentos/planodiretordeti/PDTI%202016-2017.pdf. Acessado em 29 mar. 2020.
25. UFRN. **Plano de Gestão 2019 - 2023**. 2020, Disponível em https://ufrn.br/resources/documentos/planodiretordeti/PDTI%202016-2017.pdf. Acessado em 29 nov. 2020.
26. WEST-BROWN, M.; STIKVOORT, D.; KOSSAKOWSKI, K.; KILLCRECE, G.; RUEFLE, R.; ZAJICEK, M. **Handbook for Computer Security Incident Response Teams (CSIRTs)**. 2003. CMU. Disponível em https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf. Acessado em 08 jul 2020.
27. CMU. **Create a CSIRT**. 2017. Disponível em https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485693. Acessado em 08 jul 2020.
28. PROJECT MANAGEMENT INSTITUTE. **Um Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK)**. 2017. 6a Edição. Project Management Institute.
29. EAIDGAH, Y., MAKI, A. A., KURCZEWSKI, K., & ABDEKHODAEE, A. Visual management, performance management and continuous improvement: a lean manufacturing approach.2016. International Journal of Lean Six Sigma, 7(2), 187-210.
30. VERAS, M. **Gestão Dinâmica de Projetos: LifeCycleCanvas**. 2016. Ed. Brasport. ISBN: 9788574527925.

31. MEDEIROS, B., ARAÚJO, V., & OLIVEIRA, M. **Life Cycle Canvas (LCC): Um Modelo Visual para a Gestão do Ciclo de Vida do Projeto**. 2018. Revista de Gestão e Projetos, 9(1), 87-101. doi:https://doi.org/10.5585/gep.v9i1.628.
32. MEDEIROS, B, VERAS, M., NOBRE, A., NOGUEIRA, G. **Planejando projetos com o Life Cycle Canvas (LCC): um estudo sobre um projeto de infraestrutura pública estadual**. 2017. Exacta – EP, São Paulo, v. 15, n. 1, p. 155-170. ISSN: 1678-5428.
33. Beck, K.M., Beedle, M., Bennekum, A.V., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R., Kern, J., Marick, B., Martin, R.C., Mellor, S.J., Schwaber, K., Sutherland, J., & Thomas, D. **Manifesto for Agile Software Development**. 2013. S2CID 109006295. Disponível em http://athena.ecs.csus.edu/~buckley/CSc191/Manifesto%20for%20Agile%20Software%20Development.pdf. Acessado em 13 jul 2020.
34. SUTHERLAND, J. **SCRUM: a arte de fazer o dobro do trabalho na metade do tempo**. 2019. Editora Sextante. ISBN-10: 8543107164.
35. SCHWABER, K.; SUTHERLAND, J. **The Scrum Guide: The Definitive Guide to Scrum: The Rules of the Game**. 2017. Disponível em https://www.scrumguides.org/docs/scrumguide/v2017/2017-Scrum-Guide-US.pdf. Acessado em: 15 jul 2020.
36. WYKOWSKI, T.; WYKOWSKA, J. **Lessons learned: Using Scrum in non-technical teams**. 2018. XP 2018 Conference. Disponível em: https://www.agilealliance.org/resources/experience-reports/lessons-learned-using-scrum-in-non-technical-teams/. Acessado em 15 jul 2020.
37. DEEMER, P.; BENEFIELD, G.; LARMAN. C.; VODDE, B.; **The Scrum Primer: A Lightweight Guide to the Theory and Practice of Scrum (Version 2.0)**. 2012. Disponível e: https://www.infoq.com/minibooks/Scrum_Primer/ . Acessado em: 11 dez 2020.
38. VERHEYEN, G. 2013. **Scrum: Framework, not methodology**. Disponível em https://guntherverheyen.com/2013/03/21/scrum-framework-not-methodology/ . Acessado em 17 out 2020.
39. SCHWABER, K. **Agile Project Management with Scrum**. 2004. Ed. Microsoft Press.
40. REIS, H. M. **Scrum: Método Ágil para Gestão de Projetos de Software**. 2010. Disponível em http://helenamcd.ueuo.com/images/artigos/gestaodeprojetos/scrum.pdf, Acessado em 20 out 2020.
41. VARASCHIM, J. D. **Implantando o SCRUM em um Ambiente de Desenvolvimento de Produtos para Internet**. 2009. Monografia em Ciência da Computação do Departamento de Informática da Pontifícia Universidade Católica do Rio de Janeiro.
42. CARROLL, N, O'CONNOR, M. EDISON, H. **The Identification and Classification of Impediments to Software Flow**, 2018. The Americas Conference on Information Systems (AMCIS 2018), August 16–18, New Orleans, Louisiana, USA.
43. MORRIS, D. **Scrum in Easy Steps: An Ideal Framework for Agile Projects**. 2017. Ed. In Easy Steps Limited. ISBN 9781840787313.
44. OHNO, T. **Toyota Production System - beyond large-scale production**. 1988. Productivity Press. p. 29. ISBN 0-915299-14-3.
45. VACANITI, D. & SCRUM.ORG. **The Kanban Guide for Scrum Teams**, 2019. Disponível em https://scrumorg-website-prod.s3.amazonaws.com/drupal/2019-11/2019-09-Kanban-Guide-for-Scrum-Teams-English.pdf. Acessado em 18 out 2020.
46. GRENNING. J. **Planning Poker or How to avoid analysis paralysis while release planning**, 2002. Hawthorn Woods: Renaissance Software Consulting, Vol. 3.
47. COHN, M. **Agile Estimating and Planning**. 2013. 1ª Edição. Ed. Pearson.
48. VIANNA, M.; VIANNA, Y.; ADLER, I.; LUCENA, B.; RUSSO, B. **Design Thinking – Inovação em Negócios**, 2012. MJV Press.
49. MARCONI, M.; LAKATOS, E.; **Fundamentos de Metodologia Científica**. 2003. Ed. Atlas. 5ª Edição.

Apêndices

Apêndice I – LCC de Iniciação

LifeCycle CANVAS	**Projeto** Título: CSIRT UFRN Pitch:	**Status da Execução**	**Ciclo de Vida:** [**IN**] [PL] [EX] [EN] **Artefato:** [**TAP**] [PGP] [REP] [TEP]	**Versão:** **Local:** UFRN/SINFO **Data:** 04/nov/2019
Justificativas	**Produtos**	**Partes Interessadas**	**Premissas**	**Riscos**
1. Segurança em TI na UFRN necessita de melhorias contínuas. 2. UFRN ainda não atende orientação dada pela Norma Complementar Nº 05 da Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República 3. UFRN ainda não atende a disposição dada no art. 23 da POSIC/UFRN. 4. A UFRN não dispõe das melhores práticas para resposta a incidentes de segurança em TI.	1. CSIRT oficializado e atuando na UFRN 2. Equipe Dedicada à Segurança. 3. Documentação Guia para o CSIRT (diretrizes, indicadores, procedimentos) 4. Site para o grupo	1. Superintendência de Informática 2. Reitoria 3. Equipes de TI da UFRN 4. Comunidade universitária	1. Apoio da gestão da SINFO. 2. Apoio da gestão da UFRN.	1. Equipe pequena pode atrasar o andamento do projeto. 2. Membros com tarefas em outras áreas (serviços de rede, conectividade) pode impactar no atendimento aos requisitos (equipe dedicada). 3. Sobrecarga da equipe de desenvolvimento WEB pode atrasar entrega do site.
Objetivos	**Requisitos**	**Comunicações**	**Entregas**	**Custos**
1. Implantar um CSIRT (Computer Security Incident Response Team) na UFRN.	1. Ser aprovado pela alta gestão da UFRN. 2. Estar em acordo com a Instrução Normativa 01 do DSIC e suas normas complementares. 3. Contar com uma equipe dedicada ao tratamento de incidentes de segurança. 5. Fornecer apoio na resolução de incidentes de segurança às equipes de TI da UFRN. 6. Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN.	1. Sistema de E-mail da UFRN 2. Trello 3. Reuniões presenciais 4. Skype 5. Whatsapp	1. Diretrizes de funcionamento do grupo. 2. Produção do Regimento interno (com responsabilidades, modo de operação, atuação, diretrizes). 3. Regimento e grupo formalizados na UFRN (via portaria ou resolução) 4. Corpo técnico definido e estruturado 5. Documento de indicadores para acompanhamento permanente 6. Site grupo	
Benefícios	**Restrições**	**Equipe**	**Aquisições**	**Tempo**
1. Aprimorar a segurança de TI na UFRN 2. Permitir respostas mais rápidas e precisas aos incidentes de segurança em TI. 3. Divulgar boas e melhores práticas no uso de recursos de TI na UFRN. 4. Comunicação mais estreita com outros CSIRTS externos.	1. O site deverá estar hospedado no datacenter da UFRN;	1. Bruno Ferreira 2. Luciano Medeiros 3. Manoel Bezerra 4. Anderson Luiz	1. Equipe de desenvolvimento WEB para a página do CSIRT	**T1** –30 dias **T2** – 60 dias **T3** – 30 dias **T4** – 15 dias **T5** – 15 dias **T6** – 60 dias
		Gerente do Projeto: Bruno Ferreira	Patrocinador: Marcos Madruga	Cliente: UFRN

Apêndice II – LCC's de Planejamento

LCC de Planejamento, Versão 1

LifeCycle CANVAS	**Projeto** Título: CSIRT UFRN Pitch:	**Status da Execução**	**Ciclo de Vida:** [IN] [PL] [EX] [EN] **Artefato:** [TAP] [PGP] [REP] [TEP]	**Versão:** 1 **Local:** UFRN/SINFO **Data:** 02/dez/2019
Justificativas	**Produtos**	**Partes Interessadas**	**Premissas**	**Riscos**
1. Segurança em TI na UFRN necessita de melhorias contínuas. 2. UFRN ainda não atende orientação dada pela Norma Complementar Nº 05 da Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República 3. UFRN ainda não atende a disposição dada no art. 23 da POSIC/UFRN. 4. A UFRN não dispõe das melhores práticas para resposta a incidentes de segurança em TI.	1. CSIRT oficializado e atuando na UFRN 2. Equipe Dedicada à Segurança. 3. Documentação Guia para o CSIRT (diretrizes, indicadores, procedimentos) 4. Site para o grupo	1. Superintendência de Informática 2. Reitoria 3. Equipes de TI da UFRN 4. Comunidade universitária	1. Apoio da gestão da SINFO. 2. Apoio da gestão da UFRN. 3. Equipe de técnicos deverá ter experiência em assuntos relacionados a segurança de TI.	1. Equipe pequena pode atrasar o andamento do projeto. 2. Membros com tarefas em outras áreas (serviços de rede, conectividade) pode impactar no atendimento aos requisitos (equipe dedicada). 3. Sobrecarga da equipe de desenvolvimento WEB pode atrasar entrega do site.
Objetivos	**Requisitos**	**Comunicações**	**Entregas**	**Custos**
1. Implantar um CSIRT (Computer Security Incident Response Team) na UFRN.	1. Ser aprovado pela alta gestão da UFRN. 2. Estar em acordo com a Instrução Normativa 01 do DSIC e suas normas complementares. 3. Contar com uma equipe dedicada ao tratamento de incidentes de segurança. 5. Fornecer apoio na resolução de incidentes de segurança às equipes de TI da UFRN. 6. Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN. 7. Site deverá usar tecnologias que reforcem sua segurança.	1. Sistema de E-mail da UFRN 2. Trello 3. Reuniões presenciais e remotas (via Google Meet) 4. Skype 5. Whatsapp	1. Diretrizes de funcionamento do grupo. 2. Produção do Regimento interno. 3. Regimento e grupo formalizados na UFRN (via portaria ou resolução) 4. Corpo técnico definido e estruturado 5. Documento de indicadores para acompanhamento permanente 6. Site grupo 7. Documento guia para gestão de incidentes de segurança	O projeto não apresentou custos financeiros, pois utilizará recursos pessoais e materiais já existentes na instituição.
Benefícios	**Restrições**	**Equipe**	**Aquisições**	**Tempo**
1. Aprimorar a segurança de TI na UFRN 2. Permitir respostas mais rápidas e precisas aos incidentes de segurança em TI. 3. Divulgar boas e melhores práticas no uso de recursos de TI na UFRN. 4. Comunicação mais estreita com outros CSIRTS externos.	1. O site deverá estar hospedado no datacenter da UFRN; 2. Site deverá ser construído com tecnologias abertas;	1. Bruno Ferreira 2. Luciano Medeiros 3. Manoel Bezerra 4. Anderson Luiz 5. Fernando Batista	1. Equipe de desenvolvimento WEB para a página do CSIRT 2. Equipe de Comunicações da SINFO.	**T1** –31/jan **T2** – 31/mar **T3** – 30/abr **T4** – 31/jan **T5** – 31/mar **T6** – 28/fev **T7** – 30/jun
		GERENTE: Bruno Ferreira	**PATROCINADOR**: Marcos Madruga	**CLIENTE**: UFRN

LCC de Planejamento, Versão 2 (final)

LifeCycle CANVAS	**Projeto** Título: CSIRT UFRN Pitch:	**Status da Execução**	**Ciclo de Vida:** [IN] [PL] [EX] [EN] **Artefato:** [TAP] [PGP] [REP] [TEP]	**Versão:** 2 **Local:** UFRN/SINFO **Data:** 02/mar/2019
Justificativas	**Produtos**	**Partes Interessadas**	**Premissas**	**Riscos**
1. Segurança em TI na UFRN necessita de melhorias contínuas. 2. UFRN ainda não atende orientação dada pela Norma Complementar Nº 05 da Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República 3. UFRN ainda não atende a disposição dada no art. 23 da POSIC/UFRN. 4. A UFRN não dispõe das melhores práticas para resposta a incidentes de segurança em TI.	1. CSIRT oficializado e atuando na UFRN 2. Equipe Dedicada à Segurança. 3. Documentação Guia para o CSIRT (diretrizes, indicadores, procedimentos) 4. Site para o grupo	1. Superintendência de Informática 2. Reitoria 3. Equipes de TI da UFRN 4. Comunidade universitária	1. Apoio da gestão da SINFO. 2. Apoio da gestão da UFRN. 3. Equipe de técnicos deverá ter experiência em assuntos relacionados a segurança de TI.	1. Equipe pequena pode atrasar o andamento do projeto. 2. Membros com tarefas em outras áreas (serviços de rede, conectividade) pode impactar no atendimento aos requisitos (equipe dedicada). 3. Sobrecarga da equipe de desenvolvimento WEB pode atrasar entrega do site. 4. Pandemia COVID-19 pode afetar expediente na UFRN e causar atrasos nas entregas.
Objetivos	**Requisitos**	**Comunicações**	**Entregas**	**Custos**
1. Implantar um CSIRT (Computer Security Incident Response Team) na UFRN.	1. Ser aprovado pela alta gestão da UFRN. 2. Estar em acordo com a Instrução Normativa 01 do DSIC e suas normas complementares. 3. Contar com uma equipe dedicada ao tratamento de incidentes de segurança. 5. Fornecer apoio na resolução de incidentes de segurança às equipes de TI da UFRN. 6. Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN. 7. Site deverá usar tecnologias que reforcem sua segurança.	1. Sistema de E-mail da UFRN 2. Trello 3. Reuniões presenciais e remotas (via Google Meet) 4. Skype 5. Whatsapp	1. Diretrizes de funcionamento do grupo. 2. Produção do Regimento interno. 3. Regimento e grupo formalizados na UFRN (via portaria ou resolução) 4. Corpo técnico definido e estruturado 5. Documento de indicadores para acompanhamento permanente 6. Site grupo 7. Documento guia para gestão de incidentes de segurança	O projeto não apresentou custos financeiros, pois utilizará recursos pessoais e materiais já existentes na instituição.
Benefícios	**Restrições**	**Equipe**	**Aquisições**	**Tempo**
1. Aprimorar a segurança de TI na UFRN 2. Permitir respostas mais rápidas e precisas aos incidentes de segurança em TI. 3. Divulgar boas e melhores práticas no uso de recursos de TI na UFRN. 4. Comunicação mais estreita com outros CSIRTS externos.	1. O site deverá estar hospedado no datacenter da UFRN; 2. Site deverá ser construído com tecnologias abertas;	1. Bruno Ferreira 2. Luciano Medeiros 3. Manoel Bezerra 4. Anderson Luiz 5. Fernando Batista	1. Equipe de desenvolvimento WEB para a página do CSIRT 2. Equipe de Comunicações da SINFO.	**T1** –31/jan **T2** – 31/mar **T3** – 30/abr **T4** – 31/jan **T5** – 31/mar **T6** – 28/fev **T7** – 30/jun
		GERENTE: Bruno Ferreira	**PATROCINADOR**: Marcos Madruga	**CLIENTE**: UFRN

Apêndice III – LCC's de Execução

LCC Execução, Versão 1

Projeto Título: CSIRT UFRN	**Status da Execução**	**Ciclo de Vida:** [IN] [PL] [EX] [EN] **Artefato:** [TAP] [PGP] [REP] [TEP]	**Versão:** 1 **Local:** UFRN/SINFO **Data:** 07/jan/2020
Produtos	**Partes Interessadas**	**Premissas**	**Riscos**
1. CSIRT oficializado e atuando na UFRN 2. Equipe Dedicada à Segurança. 3. Documentação Guia para o CSIRT (diretrizes, indicadores, procedimentos) 4. Site para o grupo	1. Superintendência de Informática 2. Reitoria 3. Equipes de TI da UFRN 4. Comunidade universitária	1. Apoio da gestão da SINFO. 2. Apoio da gestão da UFRN. 3. Equipe de técnicos deverá ter experiência em assuntos relacionados a segurança de TI.	1. Equipe pequena pode atrasar o andamento do projeto. 2. Membros com tarefas em outras áreas (serviços de rede, conectividade) pode impactar no atendimento aos requisitos (equipe dedicada). 3. Sobrecarga da equipe de desenvolvimento WEB pode atrasar entrega do site.
Requisitos	**Comunicações**	**Entregas**	**Custos**
1. Ser aprovado pela alta gestão da UFRN (CONSAD) ou por Portaria. 2. Estar em acordo com a Instrução Normativa 01 do DSIC e suas normas complementares. 3. Contar com uma equipe dedicada ao tratamento de incidentes de segurança. 5. Fornecer apoio na resolução de incidentes de segurança às equipes de TI da UFRN. 6. Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN. 7. Site deverá usar tecnologias que reforcem sua segurança.	1. Sistema de E-mail da UFRN 2. Trello 3. Reuniões presenciais e remotas (via Google Meet) 4. Skype 5. Whatsapp	1. Diretrizes de funcionamento do grupo. 2. Produção do Regimento interno. 3. Regimento e grupo formalizados na UFRN (via portaria ou resolução) 4. Corpo técnico definido e estruturado 5. Documento de indicadores para acompanhamento permanente 6. Site grupo 7. Documento guia para gestão de incidentes de segurança	O projeto não apresentou custos financeiros, pois utilizará recursos pessoais e materiais já existentes na instituição.
Restrições	**Equipe**	**Aquisições**	**Tempo**
1. O site deverá estar hospedado na UFRN 2. Site deve ser construído com tecnologias abertas;	1. Bruno Ferreira 2. Luciano Medeiros 3. Manoel Bezerra 4. Anderson Luiz 5. Fernando Batista	1. Equipe de desenvolvimento WEB para a página do CSIRT 2. Equipe de Comunicações da SINFO.	**T1** – 31/jan **T2** – 31/mar **T3** – 30/abr **T4** – 31/jan **T5** – 31/mar **T6** – 28/fev **T7** – 30/jun
	GERENTE: Bruno Ferreira	**PATROCINADOR**: Marcos Madruga	**CLIENTE**: UFRN

LCC Execução, Versão 2

Projeto Título: CSIRT UFRN	**Status da Execução**	**Ciclo de Vida:** [IN] [PL] [EX] [EN] **Artefato:** [TAP] [PGP] [REP] [TEP]	**Versão:** 2 **Local:** UFRN/SINFO **Data:** 02/mar/2020
Produtos	**Partes Interessadas**	**Premissas**	**Riscos**
1. CSIRT oficializado e atuando na UFRN 2. Equipe Dedicada à Segurança. 3. Documentação Guia para o CSIRT (diretrizes, indicadores, procedimentos) 4. Site para o grupo	1. Superintendência de Informática 2. Reitoria 3. Equipes de TI da UFRN 4. Comunidade universitária	1. Apoio da gestão da SINFO. 2. Apoio da gestão da UFRN. 3. Equipe de técnicos deverá ter experiência em assuntos relacionados a segurança de TI.	1. Equipe pequena pode atrasar o andamento do projeto. 2. Membros com tarefas em outras áreas (serviços de rede, conectividade) pode impactar no atendimento aos requisitos (equipe dedicada). 3. Sobrecarga da equipe de desenvolvimento WEB pode atrasar entrega do site. 4. Pandemia COVID-19 pode afetar expediente na UFRN e causar atrasos nas entregas.
Requisitos	**Comunicações**	**Entregas**	**Custos**
1. Ser aprovado pela alta gestão da UFRN (CONSAD) ou por Portaria. 2. Estar em acordo com a Instrução Normativa 01 do DSIC e suas normas complementares. 3. Contar com uma equipe dedicada ao tratamento de incidentes de segurança. 5. Fornecer apoio na resolução de incidentes de segurança às equipes de TI da UFRN. 6. Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN. 7. Site deverá usar tecnologias que reforcem sua segurança.	1. Sistema de E-mail da UFRN 2. ~~Trello~~ 3. Reuniões presenciais e remotas (via Google Meet) 4. Skype 5. Whatsapp	1. Diretrizes de funcionamento do grupo. 2. Produção do Regimento interno. 3. Regimento e grupo formalizados na UFRN (via portaria ou resolução) 4. Corpo técnico definido e estruturado 5. Documento de indicadores para acompanhamento permanente 6. Site grupo 7. Documento guia para gestão de incidentes de segurança	O projeto não apresentou custos financeiros, pois utilizará recursos pessoais e materiais já existentes na instituição.
Restrições	**Equipe**	**Aquisições**	**Tempo**
1. O site deverá estar hospedado na UFRN 2. Site deve ser construído com tecnologias abertas;	1. Bruno Ferreira 2. Luciano Medeiros 3. Manoel Bezerra 4. Anderson Luiz 5. Fernando Batista	1. Equipe de desenvolvimento WEB para a página do CSIRT 2. Equipe de Comunicações da SINFO.	**T1** –31/jan T2 – 31/mar **T3** – 30/abr **T4** – 31/jan **T5** – 31/mar **T6** – 28/fev → 27/03 (atraso) **T7** – 30/jun
	GERENTE: Bruno Ferreira	**PATROCINADOR**: Marcos Madruga	**CLIENTE**: UFRN

LCC Execução, Versão 3

Projeto Título: CSIRT UFRN	**Status da Execução**	**Ciclo de Vida:** [IN] [PL] [EX] [EN] **Artefato:** [TAP] [PGP] [REP] [TEP]	**Versão:** 3 **Local:** UFRN/SINFO **Data:** 04/mai/2020
Produtos	**Partes Interessadas**	**Premissas**	**Riscos**
1. CSIRT oficializado e atuando na UFRN 2. Equipe Dedicada à Segurança. 3. Documentação Guia para o CSIRT (diretrizes, indicadores, procedimentos) 4. Site para o grupo	1. Superintendência de Informática 2. Reitoria 3. Equipes de TI da UFRN 4. Comunidade universitária	1. Apoio da gestão da SINFO. 2. Apoio da gestão da UFRN. 3. Equipe de técnicos deverá ter experiência em assuntos relacionados a segurança de TI.	1. Equipe pequena pode atrasar o andamento do projeto. 2. Membros com tarefas em outras áreas (serviços de rede, conectividade) pode impactar no atendimento aos requisitos (equipe dedicada). 3. Sobrecarga da equipe de desenvolvimento WEB pode atrasar entrega do site. 4. Pandemia COVID-19 pode afetar expediente na UFRN e causar atrasos nas entregas.
Requisitos	**Comunicações**	**Entregas**	**Custos**
1. Ser aprovado pela alta gestão da UFRN (CONSAD) ou por Portaria. 2. Estar em acordo com a Instrução Normativa 01 do DSIC e suas normas complementares. 3. Contar com uma equipe dedicada ao tratamento de incidentes de segurança. 5. Fornecer apoio na resolução de incidentes de segurança às equipes de TI da UFRN. 6. Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN. 7. Site deverá usar tecnologias que reforcem sua segurança.	1. Sistema de E-mail da UFRN 2. Reuniões presenciais e remotas (via Google Meet) 3. Skype 4. Whatsapp	1. Diretrizes de funcionamento do grupo. 2. Produção do Regimento interno. 3. Regimento e grupo formalizados na UFRN (via portaria ou resolução) 4. Corpo técnico definido e estruturado 5. Documento de indicadores para acompanhamento permanente 6. Site grupo 7. Documento guia para gestão de incidentes de segurança	O projeto não apresentou custos financeiros, pois utilizará recursos pessoais e materiais já existentes na instituição.
Restrições	**Equipe**	**Aquisições**	**Tempo**
1. O site deverá estar hospedado na UFRN 2. Site deve ser construído com tecnologias abertas;	1. Bruno Ferreira 2. Luciano Medeiros 3. Manoel Bezerra 4. Anderson Luiz 5. Fernando Batista	1. Equipe de desenvolvimento WEB para a página do CSIRT 2. Equipe de Comunicações da SINFO.	**T1** –31/jan T2 – 31/mar **T3** – 30/abr → 29/05 (atraso) **T4** – 31/jan **T5** – 31/mar **T6** – 28/fev → 27/03 (atraso) **T7** – 30/jun
	GERENTE: Bruno Ferreira	**PATROCINADOR**: Marcos Madruga	**CLIENTE**: UFRN

LCC Execução, Versão 4

Projeto Título: CSIRT UFRN	**Status da Execução**	**Ciclo de Vida:** [IN] [PL] [EX] [EN] **Artefato:** [TAP] [PGP] [REP] [TEP]	**Versão:** 4 **Local:** UFRN/SINFO **Data:** 06/jul/2020
Produtos	**Partes Interessadas**	**Premissas**	**Riscos**
1. CSIRT oficializado e atuando na UFRN 2. Equipe Dedicada à Segurança. 3. Documentação Guia para o CSIRT (diretrizes, indicadores, procedimentos) 4. Site para o grupo	1. Superintendência de Informática 2. Reitoria 3. Equipes de TI da UFRN 4. Comunidade universitária	1. Apoio da gestão da SINFO. 2. Apoio da gestão da UFRN. 3. Equipe de técnicos deverá ter experiência em assuntos relacionados a segurança de TI.	1. Equipe pequena pode atrasar o andamento do projeto. 2. Membros com tarefas em outras áreas (serviços de rede, conectividade) pode impactar no atendimento aos requisitos (equipe dedicada). 3. Sobrecarga da equipe de desenvolvimento WEB pode atrasar entrega do site. 4. Pandemia COVID-19 pode afetar expediente na UFRN e causar atrasos nas entregas.
Requisitos	**Comunicações**	**Entregas**	**Custos**
1. Ser aprovado pela alta gestão da UFRN (CONSAD) ou por Portaria. 2. Estar em acordo com a Instrução Normativa 01 do DSIC e suas normas complementares. 3. Contar com uma equipe dedicada ao tratamento de incidentes de segurança. 5. Fornecer apoio na resolução de incidentes de segurança às equipes de TI da UFRN. 6. Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN. 7. Site deverá usar tecnologias que reforcem sua segurança.	1. Sistema de E-mail da UFRN 2. Reuniões presenciais e remotas (via Google Meet) 3. Skype 4. Whatsapp	1. Diretrizes de funcionamento do grupo. 2. Produção do Regimento interno. 3. Regimento e grupo formalizados na UFRN (via portaria ou resolução) 4. Corpo técnico definido e estruturado 5. Documento de indicadores para acompanhamento permanente 6. Site grupo 7. Documento guia para gestão de incidentes de segurança	O projeto não apresentou custos financeiros, pois utilizará recursos pessoais e materiais já existentes na instituição.
Restrições	**Equipe**	**Aquisições**	**Tempo**
1. O site deverá estar hospedado na UFRN 2. Site deve ser construído com tecnologias abertas;	1. Bruno Ferreira 2. Luciano Medeiros 3. Manoel Bezerra 4. Anderson Luiz 5. Fernando Batista	1. Equipe de desenvolvimento WEB para a página do CSIRT 2. Equipe de Comunicações da SINFO.	**T1** –31/jan T2 – 31/mar **T3** – 30/abr → 29/05 (atraso) **T4** – 31/jan **T5** – 31/mar **T6** – 28/fev → 27/03 (atraso) **T7** – 30/jun → 31/07 (atraso)
	GERENTE: Bruno Ferreira	**PATROCINADOR**: Marcos Madruga	**CLIENTE**: UFRN

LCC Execução, Versão 5 (final)

Projeto Título: CSIRT UFRN	**Status da Execução**	**Ciclo de Vida:** [IN] [PL] [EX] [EN] **Artefato:** [TAP] [PGP] [REP] [TEP]	**Versão:** 5 **Local:** UFRN/SINFO **Data:** 03/ago/2020
Produtos	**Partes Interessadas**	**Premissas**	**Riscos**
1. CSIRT oficializado e atuando na UFRN 2. Equipe Dedicada à Segurança. 3. Documentação Guia para o CSIRT (diretrizes, indicadores, procedimentos) 4. Site para o grupo	1. Superintendência de Informática 2. Reitoria 3. Equipes de TI da UFRN 4. Comunidade universitária	1. Apoio da gestão da SINFO. 2. Apoio da gestão da UFRN. 3. Equipe de técnicos deverá ter experiência em assuntos relacionados a segurança de TI.	1. Equipe pequena pode atrasar o andamento do projeto. 2. Membros com tarefas em outras áreas (serviços de rede, conectividade) pode impactar no atendimento aos requisitos (equipe dedicada). 3. Sobrecarga da equipe de desenvolvimento WEB pode atrasar entrega do site. 4. Pandemia COVID-19 pode afetar expediente na UFRN e causar atrasos nas entregas.
Requisitos	**Comunicações**	**Entregas**	**Custos**
1. Ser aprovado pela alta gestão da UFRN (CONSAD) ou por Portaria. 2. Estar em acordo com a Instrução Normativa 01 do DSIC e suas normas complementares. 3. Contar com uma equipe dedicada ao tratamento de incidentes de segurança. 5. Fornecer apoio na resolução de incidentes de segurança às equipes de TI da UFRN. 6. Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN. 7. Site deverá usar tecnologias que reforcem sua segurança.	1. Sistema de E-mail da UFRN 2. Reuniões presenciais e remotas (via Google Meet) 3. Skype 4. Whatsapp	1. Diretrizes de funcionamento do grupo. 2. Produção do Regimento interno. 3. Regimento e grupo formalizados na UFRN (via portaria ou resolução) 4. Corpo técnico definido e estruturado 5. Documento de indicadores para acompanhamento permanente 6. Site grupo 7. Documento guia para gestão de incidentes de segurança	O projeto não apresentou custos financeiros, pois utilizará recursos pessoais e materiais já existentes na instituição.
Restrições	**Equipe**	**Aquisições**	**Tempo**
1. O site deverá estar hospedado na UFRN 2. Site deve ser construído com tecnologias abertas;	1. Bruno Ferreira 2. Luciano Medeiros 3. Manoel Bezerra 4. Anderson Luiz 5. Fernando Batista	1. Equipe de desenvolvimento WEB para a página do CSIRT 2. Equipe de Comunicações da SINFO.	**T1** –31/jan T2 – 31/mar **T3** – 30/abr → 29/05 (atraso) **T4** – 31/jan **T5** – 31/mar **T6** – 28/fev → 27/03 (atraso) **T7** – 30/jun → 31/07 → 28/08 (atraso)
	GERENTE: Bruno Ferreira	**PATROCINADOR**: Marcos Madruga	**CLIENTE**: UFRN

Apêndice IV – LCC's de Monitoramento e Controle

LCC Monitoramento e Controle, Versão 1

Projeto Título: CSIRT UFRN Pitch:	**Status da Execução**	**Ciclo de Vida:** [IN] [PL] [EX] [EN] **Artefato:** [TAP] [PGP] [REP] [TEP]	**Versão:** 1 **Local:** UFRN/SINFO **Data:** 07/jan/2020
	Partes Interessadas [🟩]	**Premissas [🟩]**	**Riscos [🟩]**
	1. Superintendência de Informática 2. Reitoria 3. Equipes de TI da UFRN 4. Comunidade universitária	1. Apoio da gestão da SINFO. 2. Apoio da gestão da UFRN. 3. Equipe de técnicos deverá ter experiência em assuntos relacionados a segurança de TI.	1. Equipe pequena pode atrasar o andamento do projeto. 2. Membros com tarefas em outras áreas (serviços de rede, conectividade) pode impactar no atendimento aos requisitos (equipe dedicada). 3. Sobrecarga da equipe de desenvolvimento WEB pode atrasar entrega do site.
Requisitos [🟩]	**Comunicações [🟩]**	**Entregas [🟩]**	**Custos [🟩]**
1. Ser aprovado pela alta gestão da UFRN. 2. Estar em acordo com a Instrução Normativa 01 do DSIC e suas normas complementares. 3. Contar com uma equipe dedicada ao tratamento de incidentes de segurança. 5. Fornecer apoio na resolução de incidentes de segurança às equipes de TI da UFRN. 6. Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN. 7. Site deverá usar tecnologias que reforcem sua segurança.	1. Sistema de E-mail da UFRN 2. Trello 3. Reuniões presenciais e remotas (via Google Meet) 4. Skype 5. Whatsapp	1. Diretrizes de funcionamento do grupo. 2. Produção do Regimento interno. 3. Regimento e grupo formalizados na UFRN (via portaria ou resolução) 4. Corpo técnico definido e estruturado 5. Documento de indicadores para acompanhamento permanente 6. Site grupo 7. Documento guia para gestão de incidentes de segurança	O projeto não apresentou custos financeiros, pois utilizará recursos pessoais e materiais já existentes na instituição.
Restrições [🟩]	**Equipe [🟩]**	**Aquisições [🟩]**	**Tempo [🟩]**
1. O site deverá estar hospedado na UFRN 2. Site deve ser construído com tecnologias abertas;	1. Bruno Ferreira 2. Luciano Medeiros 3. Manoel Bezerra 4. Anderson Luiz 5. Fernando Batista	1. Equipe de desenvolvimento WEB para a página do CSIRT 2. Equipe de Comunicações da SINFO.	**T1** – 31/jan [🟩] **T2** – 31/mar [🟩] **T3** – 30/abr [🟩] **T4** – 31/jan [🟩] **T5** – 31/mar [🟩] **T6** – 28/fev [🟩] **T7** – 30/jun [🟩]
	GERENTE: Bruno Ferreira	**PATROCINADOR**: Marcos Madruga	**CLIENTE**: UFRN

LCC Monitoramento e Controle, Versão 2

Projeto Título: CSIRT UFRN Pitch:	**Status da Execução**	**Ciclo de Vida:** [IN] [PL] [EX] [EN] **Artefato:** [TAP] [PGP] [REP] [TEP]	**Versão:** 2 **Local:** UFRN/SINFO **Data:** 02/mar/2020
	Partes Interessadas [🟩]	**Premissas [🟩]**	**Riscos [🟧]**
	1. Superintendência de Informática 2. Reitoria 3. Equipes de TI da UFRN 4. Comunidade universitária	1. Apoio da gestão da SINFO. 2. Apoio da gestão da UFRN. 3. Equipe de técnicos deverá ter experiência em assuntos relacionados a segurança de TI.	1. Equipe pequena pode atrasar o andamento do projeto. 2. Membros com tarefas em outras áreas (serviços de rede, conectividade) pode impactar no atendimento aos requisitos (equipe dedicada). 3. Sobrecarga da equipe de desenvolvimento WEB pode atrasar entrega do site. 4. Pandemia COVID-19 pode afetar expediente na UFRN e causar atrasos nas entregas.
Requisitos [🟩]	**Comunicações [🟩]**	**Entregas [🟩]**	**Custos [🟩]**
1. Ser aprovado pela alta gestão da UFRN. 2. Estar em acordo com a Instrução Normativa 01 do DSIC e suas normas complementares. 3. Contar com uma equipe dedicada ao tratamento de incidentes de segurança. 5. Fornecer apoio na resolução de incidentes de segurança às equipes de TI da UFRN. 6. Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN. 7. Site deverá usar tecnologias que reforcem sua segurança.	1. Sistema de E-mail da UFRN 2. ~~Trello~~ 3. Reuniões presenciais e remotas (via Google Meet) 4. Skype 5. Whatsapp	1. Diretrizes de funcionamento do grupo. 2. Produção do Regimento interno. 3. Regimento e grupo formalizados na UFRN (via portaria ou resolução) 4. Corpo técnico definido e estruturado 5. Documento de indicadores para acompanhamento permanente 6. Site grupo 7. Documento guia para gestão de incidentes de segurança	O projeto não apresentou custos financeiros, pois utilizará recursos pessoais e materiais já existentes na instituição.
Restrições [🟩]	**Equipe [🟩]**	**Aquisições [🟩]**	**Tempo [🟧]**
1. O site deverá estar hospedado na UFRN 2. Site deve ser construído com tecnologias abertas;	1. Bruno Ferreira 2. Luciano Medeiros 3. Manoel Bezerra 4. Anderson Luiz 5. Fernando Batista	1. Equipe de desenvolvimento WEB para a página do CSIRT 2. Equipe de Comunicações da SINFO.	**T1** – 31/jan [🟩] **T2** – 27/mar [🟩] **T3** – 29/mai [🟩] **T4** – 31/jan [🟩] **T5** – 27/mar [🟩] **T6** – 28/fev → 27/mar [🟧] **T7** – 26/jun [🟩]
	GERENTE: Bruno Ferreira	**PATROCINADOR**: Marcos Madruga	**CLIENTE**: UFRN

LCC Monitoramento e Controle, Versão 3

Projeto Título: CSIRT UFRN Pitch:	**Status da Execução**	**Ciclo de Vida:** [IN] [PL] [EX] [EN] **Artefato:** [TAP] [PGP] [REP] [TEP]	**Versão:** 3 **Local:** UFRN/SINFO **Data:** 04/mai/2020
	Partes Interessadas [🟩]	**Premissas [🟩]**	**Riscos [🟧]**
	1. Superintendência de Informática 2. Reitoria 3. Equipes de TI da UFRN 4. Comunidade universitária	1. Apoio da gestão da SINFO. 2. Apoio da gestão da UFRN. 3. Equipe de técnicos deverá ter experiência em assuntos relacionados a segurança de TI.	1. Equipe pequena pode atrasar o andamento do projeto. 2. Membros com tarefas em outras áreas (serviços de rede, conectividade) pode impactar no atendimento aos requisitos (equipe dedicada). 3. Sobrecarga da equipe de desenvolvimento WEB pode atrasar entrega do site. 4. Pandemia COVID-19 pode afetar expediente na UFRN e causar atrasos nas entregas.
Requisitos [🟩]	**Comunicações [🟩]**	**Entregas [🟩]**	**Custos [🟩]**
1. Ser aprovado pela alta gestão da UFRN. 2. Estar em acordo com a Instrução Normativa 01 do DSIC e suas normas complementares. 3. Contar com uma equipe dedicada ao tratamento de incidentes de segurança. 5. Fornecer apoio na resolução de incidentes de segurança às equipes de TI da UFRN. 6. Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN. 7. Site deverá usar tecnologias que reforcem sua segurança.	1. Sistema de E-mail da UFRN 2. Reuniões presenciais e remotas (via Google Meet) 3. Skype 4. Whatsapp	1. Diretrizes de funcionamento do grupo. 2. Produção do Regimento interno. 3. Regimento e grupo formalizados na UFRN (via portaria ou resolução) 4. Corpo técnico definido e estruturado 5. Documento de indicadores para acompanhamento permanente 6. Site grupo 7. Documento guia para gestão de incidentes de segurança	O projeto não apresentou custos financeiros, pois utilizará recursos pessoais e materiais já existentes na instituição.
Restrições [🟩]	**Equipe [🟩]**	**Aquisições [🟩]**	**Tempo [🟧]**
1. O site deverá estar hospedado na UFRN 2. Site deve ser construído com tecnologias abertas;	1. Bruno Ferreira 2. Luciano Medeiros 3. Manoel Bezerra 4. Anderson Luiz 5. Fernando Batista	1. Equipe de desenvolvimento WEB para a página do CSIRT 2. Equipe de Comunicações da SINFO.	**T1** – 31/jan [🟩] **T2** – 27/mar [🟩] **T3** – 30/abr → 29/mai [🟧] **T4** – 31/jan [🟩] **T5** – 27/mar [🟩] **T6** – 28/fev → 27/mar [🟧] **T7** – 26/jun [🟩]
	GERENTE: Bruno Ferreira	**PATROCINADOR**: Marcos Madruga	**CLIENTE**: UFRN

LCC Monitoramento e Controle, Versão 4

Projeto Título: CSIRT UFRN Pitch:	**Status da Execução**	**Ciclo de Vida:** [IN] [PL] [EX] [EN] **Artefato:** [TAP] [PGP] [REP] [TEP]	**Versão:** 4 **Local:** UFRN/SINFO **Data:** 06/jul/2020
	Partes Interessadas [🟩]	**Premissas [🟩]**	**Riscos [🟧]**
	1. Superintendência de Informática 2. Reitoria 3. Equipes de TI da UFRN 4. Comunidade universitária	1. Apoio da gestão da SINFO. 2. Apoio da gestão da UFRN. 3. Equipe de técnicos deverá ter experiência em assuntos relacionados a segurança de TI.	1. Equipe pequena pode atrasar o andamento do projeto. 2. Membros com tarefas em outras áreas (serviços de rede, conectividade) pode impactar no atendimento aos requisitos (equipe dedicada). 3. Sobrecarga da equipe de desenvolvimento WEB pode atrasar entrega do site. 4. Pandemia COVID-19 pode afetar expediente na UFRN e causar atrasos nas entregas.
Requisitos [🟩]	**Comunicações [🟩]**	**Entregas [🟩]**	**Custos [🟩]**
1. Ser aprovado pela alta gestão da UFRN. 2. Estar em acordo com a Instrução Normativa 01 do DSIC e suas normas complementares. 3. Contar com uma equipe dedicada ao tratamento de incidentes de segurança. 5. Fornecer apoio na resolução de incidentes de segurança às equipes de TI da UFRN. 6. Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN. 7. Site deverá usar tecnologias que reforcem sua segurança.	1. Sistema de E-mail da UFRN 2. Reuniões presenciais e remotas (via Google Meet) 3. Skype 4. Whatsapp	1. Diretrizes de funcionamento do grupo. 2. Produção do Regimento interno. 3. Regimento e grupo formalizados na UFRN (via portaria ou resolução) 4. Corpo técnico definido e estruturado 5. Documento de indicadores para acompanhamento permanente 6. Site grupo 7. Documento guia para gestão de incidentes de segurança	O projeto não apresentou custos financeiros, pois utilizará recursos pessoais e materiais já existentes na instituição.
Restrições [🟩]	**Equipe [🟩]**	**Aquisições [🟩]**	**Tempo [🟧]**
1. O site deverá estar hospedado na UFRN 2. Site deve ser construído com tecnologias abertas;	1. Bruno Ferreira 2. Luciano Medeiros 3. Manoel Bezerra 4. Anderson Luiz 5. Fernando Batista	1. Equipe de desenvolvimento WEB para a página do CSIRT 2. Equipe de Comunicações da SINFO.	**T1** – 31/jan [🟩] **T2** – 27/mar [🟩] **T3** – 30/abr → 29/mai [🟧] **T4** – 31/jan [🟩] **T5** – 27/mar [🟩] **T6** – 28/fev → 27/mar [🟧] **T7** – 30/jun → 31/jul [🟧]
	GERENTE: Bruno Ferreira	**PATROCINADOR**: Marcos Madruga	**CLIENTE**: UFRN

LCC Monitoramento e Controle, Versão 5

Projeto Título: CSIRT UFRN Pitch:	**Status da Execução**	**Ciclo de Vida:** [IN] [PL] [EX] [EN] **Artefato:** [TAP] [PGP] [REP] [TEP]	**Versão:** 5 **Local:** UFRN/SINFO **Data:** 03/ago/2020
	Partes Interessadas [ ]	**Premissas [ ]**	**Riscos [ ]**
	1. Superintendência de Informática 2. Reitoria 3. Equipes de TI da UFRN 4. Comunidade universitária	1. Apoio da gestão da SINFO. 2. Apoio da gestão da UFRN. 3. Equipe de técnicos deverá ter experiência em assuntos relacionados a segurança de TI.	1. Equipe pequena pode atrasar o andamento do projeto. 2. Membros com tarefas em outras áreas (serviços de rede, conectividade) pode impactar no atendimento aos requisitos (equipe dedicada). 3. Sobrecarga da equipe de desenvolvimento WEB pode atrasar entrega do site. 4. Pandemia COVID-19 pode afetar expediente na UFRN e causar atrasos nas entregas.
Requisitos [ ]	**Comunicações [ ]**	**Entregas [ ]**	**Custos [ ]**
1. Ser aprovado pela alta gestão da UFRN. 2. Estar em acordo com a Instrução Normativa 01 do DSIC e suas normas complementares. 3. Contar com uma equipe dedicada ao tratamento de incidentes de segurança. 5. Fornecer apoio na resolução de incidentes de segurança às equipes de TI da UFRN. 6. Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN. 7. Site deverá usar tecnologias que reforcem sua segurança.	1. Sistema de E-mail da UFRN 2. Reuniões presenciais e remotas (via Google Meet) 3. Skype 4. Whatsapp	1. Diretrizes de funcionamento do grupo. 2. Produção do Regimento interno. 3. Regimento e grupo formalizados na UFRN (via portaria ou resolução) 4. Corpo técnico definido e estruturado 5. Documento de indicadores para acompanhamento permanente 6. Site grupo 7. Documento guia para gestão de incidentes de segurança	O projeto não apresentou custos financeiros, pois utilizará recursos pessoais e materiais já existentes na instituição.
Restrições [ ]	**Equipe [ ]**	**Aquisições [ ]**	**Tempo [ ]**
1. O site deverá estar hospedado na UFRN 2. Site deve ser construído com tecnologias abertas;	1. Bruno Ferreira 2. Luciano Medeiros 3. Manoel Bezerra 4. Anderson Luiz 5. Fernando Batista	1. Equipe de desenvolvimento WEB para a página do CSIRT 2. Equipe de Comunicações da SINFO.	**T1** – 31/jan [ ] **T2** – 27/mar [ ] **T3** – 30/abr → 29/mai [ ] **T4** – 31/jan [ ] **T5** – 27/mar [ ] **T6** – 28/fev → 27/mar [ ] **T7** – 30/jun → 28/ago [ ]
	GERENTE: Bruno Ferreira	**PATROCINADOR**: Marcos Madruga	**CLIENTE**: UFRN

Apêndice V – LCC de Encerramento

LifeCycle CANVAS	**Projeto** Título: CSIRT UFRN Pitch:	**Status da Execução**	**Ciclo de Vida:** [IN] [PL] [EX] [EN] **Artefato:** [TAP] [PGP] [REP] [TEP]	**Versão:** 1 **Local:** UFRN/SINFO **Data:** 31/ago/2020
Justificativas	**Produtos**	**Partes Interessadas**	**Premissas**	**Riscos**
1. Segurança em TI na UFRN necessita de melhorias contínuas. 2. UFRN ainda não atende orientação dada pela Norma Complementar Nº 05 da Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República 3. UFRN ainda não atende a disposição dada no art. 23 da POSIC/UFRN. 4. A UFRN não dispõe das melhores práticas para resposta a incidentes de segurança em TI.	1. CSIRT oficializado e atuando na UFRN 2. Equipe Dedicada à Segurança. 3. Documentação Guia para o CSIRT (diretrizes, indicadores, procedimentos) 4. Site para o grupo	1. Superintendência de Informática 2. Reitoria 3. Equipes de TI da UFRN 4. Comunidade universitária	1. Apoio da gestão da SINFO. 2. Apoio da gestão da UFRN. 3. Equipe de técnicos deverá estar capacitada e ter experiência em assuntos relacionados a segurança de TI.	1. Equipe pequena causou atrasos no andamento do projeto. 2. Membros com tarefas em outras áreas não afetou o atendimento aos requisitos (equipe dedicada). 3. Sobrecarga da equipe de desenvolvimento WEB causou atraso na entrega do site. 4. Pandemia COVID-19 impôs tarefas extras e sobrecarregou a equipe, atrasando entregas.
Objetivos	**Requisitos**	**Comunicações**	**Entregas**	**Custos**
1. Implantar um CSIRT (Computer Security Incident Response Team) na UFRN.	1. Ser aprovado pela alta gestão da UFRN. 2. Estar em acordo com a Instrução Normativa 01 do DSIC e suas normas complementares. 3. Contar com uma equipe dedicada ao tratamento de incidentes de segurança. 5. Fornecer apoio na resolução de incidentes de segurança às equipes de TI da UFRN. 6. Manter ações para disseminar as melhores práticas de segurança à comunidade universitária da UFRN. 7. Site deverá usar tecnologias que reforcem sua segurança.	1. Sistema de E-mail da UFRN 2. Reuniões presenciais e remotas (via Google Meet) 3. Skype 4. Whatsapp	1. Diretrizes de funcionamento do grupo. 2. Regimento interno. 3. Regimento e grupo formalizados na UFRN (via portaria ou resolução) 4. Corpo técnico definido e estruturado 5. Documento de indicadores para acompanhamento permanente 6. Site grupo 7. Documento guia para gestão de incidentes de segurança	O projeto não apresentou custos financeiros, pois utilizará recursos pessoais e materiais já existentes na instituição.
Benefícios	**Restrições**	**Equipe**	**Aquisições**	**Tempo**
1. Aprimorar a segurança de TI na UFRN 2. Permitir respostas mais rápidas e precisas aos incidentes de segurança em TI. 3. Divulgar boas e melhores práticas no uso de recursos de TI na UFRN. 4. Comunicação mais estreita com outros CSIRTS externos.	1. O site deverá estar hospedado no datacenter da UFRN; 2. Site deverá ser construído com tecnologias abertas;	1. Bruno Ferreira 2. Luciano Medeiros 3. Manoel Bezerra 4. Anderson Luiz 5. Fernando Batista	1. Equipe de desenvolvimento WEB para a página do CSIRT 2. Equipe de Comunicações da SINFO.	**T1:** 31/jan [ ] **T2:** 27/mar [ ] **T3:** 30/abr → 29/05 [ ] **T4:** 31/jan [ ] **T5:** 27/mar [ ] **T6:** 28/fev → 27/03 [ ] **T7:** 30/jun → 28/08 [ ]
		GERENTE: Bruno Ferreira	**PATROCINADOR**: Marcos Madruga	**CLIENTE**: UFRN

Apêndice VI – Documentos-base para Instituição do CSIRT

Documentos para Instituição do CSIRT	
Documento	**Descrição**
Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008	Instrução normativa do Governo Federal que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020	Instrução normativa do Governo Federal que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.
Norma Complementar nº 05/IN01/ DSIC/GSIPR	Norma complementar do Governo Federal que dispõe sobre a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR – na administração pública federal.
Decreto nº 9.637, de 26 de dezembro de 2018	Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997.
CREATE A CSIRT (CMU)	*White paper* publicado pela Carnegie Mellon University (CMU) com melhores práticas para o desenvolvimento de um CSIRT.
Handbook for Computer Security Incident Response Teams (CSIRTs)	Livro eletrônico publicado pela Carnegie Mellon University (CMU), contendo boas práticas para a instituição e manutenção de equipes de tratamento e resposta a incidentes em segurança da informação.
Defining Computer Security Incident Response Teams (Ruefle, 2007)	Artigo que descreve os papéis e responsabilidades de um CSIRT na prevenção, detecção, análise e resposta a incidentes de segurança.
Computer security incident handling guide (NIST)	Guia publicado pelo NIST (National Istitute of standards and Technology) com boas práticas para mitigar riscos e responder a incidentes em segurança da informação.
Best Practices for National Cyber Security (CMU)	Livro eletrônico publicado pela CMU, descrevendo as melhores práticas para criação de estratégias de ciber-segurança.
National CSIRTs and Their Role in Computer Security Incident Response	Livro eletrônico com recomendações e boas práticas para o tratamento e resposta a incidentes em segurança da informação.
Estabelecimento de CSIRTs e Processo de Tratamento de Incidentes de Segurança em Instituições Acadêmicas Brasileiras: estudo de caso da parceria CAIS/RNP e UFBA	Artigo apresentado na Sétima Conferência de Diretores de Tecnologia da Informação, TICAL 2017 Gestão de TIC para Pesquisa e Colaboração, San José, 3 a 5 de julho de 2017
ABNT NBR ISO/IEC 27002	Técnicas de segurança - Código de prática para controles de segurança da informação
ABNT NBR ISO/IEC 27005	Técnicas de segurança - Gestão de riscos de segurança da informação.

Apêndice VII – EAP Simplificada (entregas e sub entregas)

1. **Macro Entrega – Diretrizes de Funcionamento**
    1. Estudo da Legislação
    2. Estudo das melhores práticas
    3. Apresentação à equipe
    4. Coordenar Produção do texto
2. **Macro Entrega – Regimento Interno**
    1. Revisão da Legislação
    2. Revisão das melhores práticas
    3. Esboço do texto
    4. Produção do texto
    5. Revisão final
3. **Macro Entrega – Regimento e grupo formalizados na UFRN**
    1. Apresentar regimento à gestão da SINFO
    2. Encaminhar regimento à aprovação da UFRN.
    3. Aprovação da UFRN
4. **Estruturação da Equipe e Definição de papéis**
    1. Identidade do CSIRT (nome, visão, missão)
    2. Definir Catálogo de Serviços
    3. Definir coordenador, papeis e responsáveis.
    4. Levantar infraestrutura (página, sala, servidores, hardware e software)
    5. Definir Público Alvo
5. **Macro Entrega – Indicadores**
    1. Criar indicadores para acompanhamento
6. **Site**
    1. Reuniões com a equipe WEB
    2. Informações para a equipe WEB
    3. Aprovação do protótipo do site. Liberação p/ desenv.
    4. Realizar testes com site
    5. Configurar servidor para o site
    6. Pôr site em produção
    7. Popular site (notícias, documentos)
7. **Guia para gestão de incidentes de segurança**
    1. Estudo de normas técnicas
    2. Coordenação da produção do texto (rascunho)

Anexos

Anexo I – Modelo Mockup de Alta Fidelidade do Site

Protótipo produzido pela equipe de desenvolvimento Web da SINFO, usando a ferramenta AdobeXD.