INSTITUTO FEDERAL GOIANO - CAMPUS MORRINHOS

CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS PARA INTERNET

LÍVIA ESTER FELIPUSSO TIMÓTEO

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO ALINHADAS A ISO 27001 COM BASE NA OWASP *TOP* 10 APLICADAS À GERÊNCIA DE PROJETOS PARA APLICAÇÕES *WEB*.

MORRINHOS - GO
2023

LÍVIA ESTER FELIPUSSO TIMÓTEO

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO ALINHADAS A ISO 27001 COM BASE NA OWASP *TOP* 10 APLICADAS À GERÊNCIA DE PROJETOS PARA APLICAÇÕES *WEB*.

Monografia apresentada ao Curso Superior de Tecnologia em Sistemas para Internet do Instituto Federal Goiano – Campus Morrinhos - GO, como requisito parcial para obtenção de título de Tecnólogo em Sistemas para Internet.
Orientadora: Profª MSc. Ana Maria Martins Carvalho.

MORRINHOS - GO
2023

FICHA CATALOGRÁFICA

Sistema desenvolvido pelo ICMC/USP
Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas - Instituto Federal Goiano

Timóteo, Lívia Ester Felipusso
TT585p POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO ALINHADAS A ISO 27001 COM BASE NA OWASP TOP 10 APLICADAS À GERÊNCIA DE PROJETOS PARA APLICAÇÕES WEB. / Lívia Ester Felipusso Timóteo; orientadora Ana Maria Martins Carvalho. -- Morrinhos, 2023.
82 p.

Monografia (Pós-graduação Lato Sensu em em Curso Superior de Tecnologia em Sistemas para Internet) -- Instituto Federal Goiano, Campus Morrinhos, 2023.

1. Política de Segurança da Informação. 2. Desenvolvimento seguro web. 3. ISO 27001. 4. OWASP. I. Carvalho, Ana Maria Martins, orient. II. Título.

Responsável: Johnathan Pereira Alves Diniz - Bibliotecário-Documentalista CRB-1 n°2376

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO

PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO

Com base no disposto na Lei Federal nº 9.610, de 19 de fevereiro de 1998, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano a disponibilizar gratuitamente o documento em formato digital no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

IDENTIFICAÇÃO DA PRODUÇÃO TÉCNICO-CIENTÍFICA

- ☐ Tese (doutorado)
- ☐ Dissertação (mestrado)
- ☐ Monografia (especialização)
- ☒ TCC (graduação)
- ☐ Artigo científico
- ☐ Capítulo de livro
- ☐ Livro
- ☐ Trabalho apresentado em evento
- ☐ Produto técnico e educacional - Tipo:

Nome completo do autor: Lívia Ester Felipusso Timóteo

Matrícula: 2017104211710072

Título do trabalho: POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO ALINHADAS A ISO 27001 COM BASE NA OWASP TOP 10 APLICADAS À GERÊNCIA DE PROJETOS PARA APLICAÇÕES WEB.

RESTRIÇÕES DE ACESSO AO DOCUMENTO

Documento confidencial: ☒ Não ☐ Sim, justifique:

Informe a data que poderá ser disponibilizado no RIIF Goiano: 11 / 08 / 2023

O documento está sujeito a registro de patente? ☐ Sim ☒ Não

O documento pode vir a ser publicado como livro? ☐ Sim ☒ Não

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O(a) referido(a) autor(a) declara:

• Que o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;

• Que obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autoria, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;

• Que cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

Morrinhos - GO (Local) — 11 / 08 / 2023 (Data)

DocuSigned by:
Lívia Ester Felipusso Timóteo
D50CB132438C406...
Assinatura do autor e/ou detentor dos direitos autorais

Ciente e de acordo:

Assinatura do(a) orientador(a)

gov.br
Documento assinado digitalmente
ANA MARIA MARTINS CARVALHO
Data: 13/08/2023 12:08:36-0300
Verifique em https://validar.iti.gov.br

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

Ata nº 5/2023 - CCSTSI-MO/CEG-MO/DE-MO/CMPMHOS/IFGOIANO

ATA DE DEFESA DE TRABALHO DE CURSO

Aos 4 dias do mês de agosto de 2023, às 19 horas e 30 minutos, reuniu-se a banca examinadora composta pelos docentes: Ma. Ana Maria Martins Carvalho (orientadora), Dr. Antônio Neco de Oliveira (membro), Esp. José Pereira Alves (membro), para examinar o Trabalho de Curso intitulado “POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO ALINHADAS A ISO 27001 COM BASE NA OWASP TOP 10 APLICADAS À GERÊNCIA DE PROJETOS PARA APLICAÇÕES WEB” da estudante LÍVIA ESTER FELIPUSSO TIMÓTEO, Matrícula nº 2017104211710072, do Curso Superior de Tecnologia em Sistemas para Internet, do Instituto Federal Goiano – Campus Morrinhos. A palavra foi concedida à estudante para a apresentação oral do Trabalho de Curso, houve arguição da candidata pelos membros da banca examinadora. Após tal etapa, a banca examinadora decidiu pela APROVAÇÃO da estudante. Ao final da sessão pública de defesa foi lavrada a presente ata que segue assinada pelos membros da Banca Examinadora.

(Assinado Eletronicamente)

Ma. Ana Maria Martins Carvalho

Orientador(a)

Dr. Antônio Neco de Oliveira

Membro

Esp. José Pereira Alves

Membro

Documento assinado eletronicamente por:

- **Livia Ester Felipusso Timoteo, 2017104211710072 - Discente**, em 06/08/2023 14:27:24.
- **Jose Pereira Alves, PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 06/08/2023 12:30:02.
- **Antonio Neco de Oliveira, COORDENADOR(A) DE CURSO - FUC1 - CCSTSI-MO**, em 06/08/2023 09:30:18.
- **Ana Maria Martins Carvalho, PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 05/08/2023 11:39:33.

Este documento foi emitido pelo SUAP em 04/08/2023. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 517959
Código de Autenticação: b598e8254a

INSTITUTO FEDERAL GOIANO
Campus Morrinhos
Rodovia BR-153, Km 633, Zona Rural, SN, Zona Rural, MORRINHOS / GO, CEP 75650-000
(64) 3413-7900

LÍVIA ESTER FELIPUSSO TIMÓTEO

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO ALINHADAS A ISO 27001 COM BASE NA OWASP *TOP* 10 APLICADAS À GERÊNCIA DE PROJETOS PARA APLICAÇÕES *WEB*.

Data da defesa: 04 de agosto de 2023.

Resultado: APROVADA.

BANCA EXAMINADORA — ASSINATURAS ELETRÔNICAS

Profª MSc. Ana Maria Martins Carvalho
IF Goiano Campus Morrinhos – GO

gov.br
Documento assinado digitalmente
ANA MARIA MARTINS CARVALHO
Data: 09/08/2023 11:47:45-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Antônio Neco de Oliveira
IF Goiano Campus Morrinhos – GO

Assinado de forma digital por ANTONIO NECO DE OLIVEIRA:33548315100
Dados: 2023.08.09 12:09:59 -03'00'

Prof. Esp. José Pereira Alves
IF Goiano Campus Morrinhos – GO

gov.br
Documento assinado digitalmente
JOSE PEREIRA ALVES
Data: 09/08/2023 15:40:30-0300
Verifique em https://validar.iti.gov.br

MORRINHOS - GO
2023

DEDICATÓRIA

Dedico este trabalho aos meus pais Anderson e Daniella e a minha irmã Rebecca, que estão comigo em todos os momentos.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por sua graça em minha vida.

Aos meus pais e minha irmã por todo apoio e compreensão.

À minha orientadora MSc. Ana Maria, por sua orientação e dedicação para que eu pudesse realizar este trabalho.

E ao Instituto Federal Goiano – Campus Morrinhos juntamente com todos os professores que passaram pelo meu caminho e pelo ensino de qualidade.

RESUMO

A segurança na *web* é fundamental para utilizarmos tranquilamente os serviços e sistemas disponibilizados em rede, por isso o desenvolvimento *web* seguro deve ser aplicado desde o início de um projeto. A utilização de Políticas de Segurança da Informação é uma boa maneira de controlar e padronizar métodos de desenvolvimento seguro para equipes. O propósito desta pesquisa foi mostrar políticas de segurança da informação criadas com base nas vulnerabilidades A04: *Desing* Inseguro e A07: Falhas de identificação e autenticação, do projeto OWASP *Top Ten* 2021 e também são embasadas na LGPD, ISO 27001 e ISO 27002. Com o objetivo de ilustrar este cenário, utilizou-se o *software* de gerenciamento de projetos *GanttProject* juntamente com o uso do *GanttProject Cloud* para o compartilhamento do projeto em equipes, sendo exibido de forma intuitiva e de fácil compreensão. Dessa forma, pretende-se auxiliar alunos de graduação e profissionais de desenvolvimento como um todo, na criação de sistemas seguros, minimizando riscos.

Palavras-chave: Política de Segurança da Informação. Desenvolvimento seguro *web*. ISO 27001. ISO 27002. OWASP.

ABSTRACT

Web security is fundamental for us to use the services and systems available on the network safely, so a secure web development should be applied from the beginning of a project. The use of Information Security Policies is a good way to control and standardize safe development methods for teams. The purpose of this research was to show information security policies created which are based on vulnerabilities A04: Insecure Design and A07: Identification and authentication failures, from the OWASP Top Ten 2021 project and are also based on the LGPD, ISO 27001 and ISO 27002. In order to illustrate this scenario, we used the project management software GanttProject along with GanttProject Cloud for sharing the project in teams, being displayed in an intuitive and easy to undestand way. In this way, it is intended to assist undergraduate students and development professionals as a whole, in the development of secure systems, minimizing risks.

Keywords: Information Security Policy. Secure web development. ISO 27001. ISO 27002. OWASP.

LISTA DE FIGURAS

Figura 1 - Criação de um novo projeto no GanttProject. 43
Figura 2 - Criação de um nome para o projeto. 43
Figura 3 - Selecionando o domínio do projeto. 44
Figura 4 - Configurando finais de semana e feriados. 45
Figura 5 - Criação e personalização dos colaboradores. 46
Figura 6 - Lista de colaboradores criados. 47
Figura 7 - Criação de novas funções. 48
Figura 8 - Nova função: Arquiteto da Informação, disponível para uso. 49
Figura 9 - Criação de nova tarefa. 50
Figura 10 - Definição das propriedades da tarefa. 51
Figura 11 - Adicionando colaborador responsável pela tarefa. 51
Figura 12 - Definindo uma tarefa predecessora. 52
Figura 13 - Gráfico gantt de acordo com tarefas criadas até o momento. 52
Figura 14 - Gráfico gantt de todo o projeto. 53
Figura 15 - Diagrama de recursos de todo o projeto. 54
Figura 16 - Exibir gráfico PERT 54
Figura 17 - Gráfico PERT 55
Figura 18 - Formas de exportação do projeto. 55
Figura 19 - Criando uma conta no GanttProject Cloud. 56
Figura 20 - Conectando o software GanttProject no GanttProject Cloud 57
Figura 21 - Definindo a validade do token de autenticação. 58
Figura 22 - Validade do token definida. 58
Figura 23 - Nuvem: conectado. 59
Figura 24 - Novo time no GanttProject Cloud 60
Figura 25 - Salvando o projeto do Software na Nuvem GanttProject. 61
Figura 26 - Projeto de desenvolvimento de software.gan. 61
Figura 27 - Convidar pessoas para o projeto. 62
Figura 28 - Enviar convite 62
Figura 29 - Convite recebido no e-mail. 63
Figura 30 - Acesso ao projeto no GanttProject Cloud através de outra máquina. 63
Figura 31 - Pasta do projeto criado em outra máquina. 64

Figura 32 - Abrindo o projeto no software através de outra máquina por outro usuário. 64
Figura 33 - Projeto aberto por outro usuário em outra máquina através do software. 65
Figura 34 - Criação de novo usuário na máquina 2.....65
Figura 35 - Notificação de atualização do projeto na máquina 1.....66
Figura 36 - Projeto atualizado na máquina 1.....66
Figura 37 - Bloquear alterações no projeto. 67
Figura 38 - Tempo para o bloqueio de alterações no projeto.....68
Figura 39 - Projeto bloqueado para outros usuários modificarem. 68
Figura 40 - Bloqueio do projeto no software.....69
Figura 41 - Mensagem de projeto bloqueado.....69
Figura 42 - Janela de bloqueio do projeto. 70
Figura 43 - Histórico do projeto no software.....70
Figura 44 - Acesso ao histórico da versão do projeto no GanttProject Cloud 71
Figura 45 - Histórico completo da versão do projeto no GanttProject Cloud.....71
Figura 46 - Reverter o projeto para determinada versão.....72
Figura 47 - Preços do GanttProject Cloud.....72
Figura 48 - Custo do GanttProject Cloud nesse projeto. 73
Figura 49 - Configurações do GanttProject Cloud.....73
Figura 50 - Exemplo de ciclo de vida do modelo espiral. 74
Figura 51 - Exemplo de ciclo de vida do modelo incremental 75
Figura 52 - Exemplo de ciclo de vida do modelo evolutivo.....75
Figura 53 - Exemplo de ciclo de vida do modelo evolutivo continuação. 76
Figura 54 - Exemplo de ciclo de vida do modelo cascata.....76

LISTA DE ABREVIAÇÕES

ABNT - Associação Brasileira de Normas Técnicas

CGSI - Comitê Gestor de Segurança da Informação

COBEI - Comitê Brasileiro de eletricidade, eletrônica, iluminação e telecomunicações

HTML - Linguagem de marcação de hipertexto

ID – Identidade

IEC - Comissão Eletrotécnica Internacional

ISO - Organização Internacional de Normalização

LGPD - Lei Geral de Proteção de Dados

NBR - Norma Brasileira

OWASP - Projeto Aberto de Segurança em Aplicações Web

PERT - Técnica de revisão de avaliação de programas

PSI - Política de Segurança da Informação

REGEX - Expressão Regular

SDLC - Ciclo de Vida de Desenvolvimento de *Software*

TI - Tecnologia da Informação

URL - Localizador Uniforme de Recursos

SUMÁRIO

1 INTRODUÇÃO 13
2 OBJETIVOS 15
2.1 OBJETIVO GERAL 15
2.2 OBJETIVOS ESPECÍFICOS 15
3 TRABALHOS CORRELATOS 16
4 REFERENCIAL TEÓRICO 20
4.1 SEGURANÇA DA INFORMAÇÃO 20
4.2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 20
4.3 OWASP 20
4.4 OWASP *TOP* 10 21
4.5 LGPD 21
4.6 IEC 21
4.7 ISO/IEC 27001:2013 22
4.8 ISO/IEC 27002:2013 22
4.9 SDLC 22
4.10 AMEAÇA 22
4.11 CONTROLE 23
4.12 INCIDENTE DE SEGURANÇA DA INFORMAÇÃO 23
4.13 VULNERABILIDADE 23
5 METODOLOGIA 24
6 DESENVOLVIMENTO 26
6.1 POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO PARA APLICAÇÕES *WEB* 26
6.2 POLÍTICA DE IMPLEMENTAÇÃO DO SDLC (Ciclo de Vida de Desenvolvimento de *Software*) 33
6.3 POLÍTICA PARA IDENTIFICAÇÃO E AUTENTICAÇÃO SEGURA 38
6.4 UTILIZAÇÃO DO *GANTTPROJECT* SIMULANDO UM PROJETO DE DESENVOLVIMENTO DE *SOFTWARE* 42

6.5 UTILIZAÇÃO DO *GANTTPROJECT CLOUD* SIMULANDO UM PROJETO DE DESENVOLVIMENTO DE *SOFTWARE* 56

6.6 UTILIZAÇÃO DO *GANTTPROJECT CLOUD* A PARTIR DE OUTRA MÁQUINA PARA OUTROS USUÁRIOS TEREM ACESSO AO PROJETO 63

6.7 EXEMPLOS DE UTILIZAÇÃO DE CICLO DE VIDA DE DESENVOLVIMENTO DE *SOFTWARE* (SDLC) NO *GANTTPROJECT* 74

7 CONCLUSÃO 77

REFERÊNCIAS 78

APÊNDICE A - TERMO DE USO DE COMPROMISSO E RESPONSABILIDADE PARA COLABORADORES 81

1 INTRODUÇÃO

Com o crescente avanço das tecnologias da informação, surgem cada vez mais vulnerabilidades e riscos nesse meio, o que, consequentemente, leva à necessidade de maior cuidado e atenção com a segurança da informação.

A *Internet* é hoje essencial na vida da grande maioria das pessoas, principalmente no mundo pós pandemia Covid-19, onde houve um grande aumento no número de domicílios com acesso à *Internet* quando comparados aos anos de 2019 e 2020, devido a vários ramos de trabalhos onde foi adotado o *home office* e que em vários desses segue implantado até hoje, devido a atividades educacionais *online* entre outros usos da rede (NITAHARA, 2021). Porém, com o aumento do uso da *Internet* aumentou-se também o uso indevido e malicioso desta ferramenta, levando a um grande crescimento de golpes virtuais, prejudicando a segurança na rede e em aplicações *web* (OLHAR DIGITAL, 2022).

Na rede mundial de computadores temos diversos recursos tecnológicos que necessitam cada vez mais de segurança da informação, devido a enorme quantidade de dados sensíveis que nela trafegam em milionésimos de segundos, por isso é de extrema importância se atentar a cada metodologia, política, norma, leis e recursos disponíveis relacionados à segurança desde o início do projeto. A negligência de não se ater a segurança durante o desenvolvimento do projeto pode levar a falhas que se exploradas por pessoas com más intenções pode causar grandes transtornos aos usuários e até mesmo prejuízos financeiros, além de prejudicar a reputação da empresa (MONTANHEIRO, 2018).

Ao se utilizar boas políticas de segurança da informação em conformidade com os requisitos do projeto logo no início deste, pode-se elevar o nível de segurança do projeto final, evitando vulnerabilidades que possam vir a causar grandes prejuízos no futuro. As políticas de segurança são criadas e desenvolvidas a partir de várias leis, normas, estratégias e metodologias que visam a segurança e assim determinam regras e padrões que os desenvolvedores devem seguir, concomitantes a ferramentas e *softwares* seguros para se utilizar durante o desenvolvimento. E assim a segurança da informação é alcançada através da implementação dessas políticas, juntamente

com *softwares*, *hardwares* e demais procedimentos, que precisam ser monitorados, implementados, revisados e melhorados constantemente (HINTZBERGEN, 2018).

O objetivo desta pesquisa foi criar e apresentar para empresas, desenvolvedores e estudantes, Políticas de Segurança da Informação, baseadas no Projeto OWASP *TOP* 10 2021, com foco nas vulnerabilidades A04: *Design* Inseguro e A07: Falhas de Identificação e Autenticação (OWASP, 2021). As Políticas de Segurança da Informação podem ser utilizadas a fim de se prevenir por meio das normas, regras, padrões pré-estabelecidos, ferramentas e *softwares* indicados nessas políticas, visando a segurança de acordo com o foco de cada política de segurança. E podem ser, principalmente utilizadas como apoio para os que queiram utilizar as Políticas de Segurança da Informação presentes neste trabalho, a fim de auxiliá-los no processo de desenvolvimento seguro de *softwares* para aplicações *web*.

2 OBJETIVOS

2.1 OBJETIVO GERAL

Criação de Políticas de Segurança da Informação (PSI) aplicadas à gerência de projetos como auxílio no desenvolvimento de aplicações *web* seguras.

2.2 OBJETIVOS ESPECÍFICOS

- Expor o conceito inicial a respeito da necessidade do desenvolvimento de aplicações *web* seguras aplicadas desde o início do projeto.
- Apresentar as Políticas de Segurança da Informação criadas nesta pesquisa.
- Mostrar os Ciclos de Vida de Desenvolvimento de *Software*.
- Configurar *software* específico para gerenciamento do projeto.
- Como resultado, apresentar as Políticas de Segurança da Informação criadas nesta pesquisa, juntamente com o Ciclo de Vida de Desenvolvimento de *Software* escolhido, simulados no *software* de gerenciamento de projeto proposto.

3 TRABALHOS CORRELATOS

Neste capítulo é apresentado um levantamento da bibliografia correlata, utilizado para o desenvolvimento deste trabalho, analisando as contribuições, metodologias, resultados e as limitações de cada trabalho. As informações presentes contribuíram e auxiliaram na direção deste trabalho e em sua contribuição ao meio acadêmico.

Em Montanheiro (2018) é apresentado, para desenvolvedores de aplicações *web*, a importância de agregar segurança nessas aplicações. O trabalho tem foco em principiantes no desenvolvimento *web*, incluindo alunos dos cursos de informática, e apresenta os riscos de aplicações *web* que são desenvolvidas sem o mínimo de segurança. É necessário pensar e implementar a segurança em cada parte do ciclo de desenvolvimento de um projeto, sendo assim, o autor criou um guia para o desenvolvimento de aplicações *web* seguras. Em seu trabalho o autor traz um exemplo de cenário de ataque real, em que uma falha no gerenciamento de sessão afetou um *site* de busca de empregos, que poderia ter levado ao fim de uma empresa, caso algum atacante tivesse explorado essa falha. Ele mostra que são necessários testes de segurança nas aplicações, tais como o desenvolvimento orientado a testes, revisão do código fonte, utilização de *scanners* automatizados e o conhecimento sobre as principais ferramentas automatizadas de invasão de sistemas para se prevenir. O autor apresenta formas de desenvolver sistemas seguros durante o ciclo de vida do projeto desde a sua criação até a sua entrega e posterior manutenção. O trabalho limita-se a não mostrar uma aplicação real deste guia e seus resultados, ficando esse legado para possíveis trabalhos futuros.

No trabalho de Alteff (2020) é apresentado um manual para a aplicação de técnicas de *ethical hacking*, com o intuito de identificar e reparar vulnerabilidades em sistemas *web*, antes que *hackers* mal intencionados explorem essas brechas. Seu objetivo foi mostrar com exemplos práticos e acessíveis como realizar testes de penetração em sistemas *web*, a fim de se prevenir de possíveis ataques. O manual foi elaborado de maneira intuitiva e de fácil entendimento, utilizando ferramentas gratuitas e de código aberto. Nele é apresentado inicialmente uma introdução teórica sobre a importância

da segurança da informação em aplicações *web*, o que é o *ethical hacking*, *pentesting* e a fundação OWASP. A aplicação *web* usada como alvo dos ataques foi a *Metasploitable* que é disponibilizada especificamente para estudos e os *softwares Nmap* e o *Metasploit* que foram rodados no Sistema Operacional *Kali Linux*. Em seguida é explicado as etapas para a realização do *pentest*, desde a instalação de uma máquina virtual, configuração do ambiente e execução dos testes de penetração em si. Foi usado para nortear os testes de penetração a metodologia da OWASP, a qual apresenta ferramentas e técnicas para detecção e tratamento de falhas de segurança em aplicações *web* e também um guia de testes. Os *scanners* executados no decorrer do trabalho tiveram êxito em seus resultados. Mediante a leitura deste material e posterior prática do roteiro contido neste, alunos de graduação e profissionais de informática podem adquirir conhecimento sobre *pentest* e segurança da informação. Sua limitação foi apresentar apenas duas ferramentas para os testes, porém ele indica como trabalhos futuros a utilização de outras que são bastante usadas no mundo do *pentest*.

No trabalho de Novais (2020) os autores apresentam uma proposta de uma taxonomia para a implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) em organizações, baseada na norma ABNT NBR ISO 27001 utilizando seus processos como guia. O objetivo é que esse artigo seja fonte de pesquisa e auxílio para empresas a fim de que seus profissionais estejam coniventes com a lei. É feito um estudo de classificação, comparação e categorização dos dados presentes na norma e na lei, além de uma pesquisa aplicada e voltada para os profissionais de tecnologia da informação para verificar se estão em conformidade com a atual estrutura das organizações. Pode ser usado para orientar as organizações e profissionais a estarem em conformidade com a lei. Contudo, a utilização somente desse trabalho não é o bastante para a aplicação total da lei nas organizações, ainda é necessário apoio jurídico e técnico de uma equipe de tecnologia da informação.

Em Diniz (2021) é apresentado de que maneira a ABNT NBR ISO/IEC 27701:2019 e a família da norma ISO 27000 relaciona-se com a Segurança da Informação e a Lei Geral de Proteção de Dados (LGPD). A metodologia usada foi de caráter exploratório

e para o seu desenvolvimento foi exibido um referencial teórico trazendo informações sobre os dados e o fator humano na segurança dos dados, além de trazer informações sobre a LGPD, a Segurança da Informação, a série ISO 27000, a relação entre a família ISO 27000, LGPD e Segurança da Informação e ainda uma Política de Segurança da Informação (PSI). Com o estudo realizado desenvolveu-se uma PSI para uma empresa do setor de eventos e lazer. A PSI deste trabalho científico foca nas diretrizes e respostas a acidentes de segurança da informação, nos quais o documento detalha o que deve ser seguido pelos colaboradores para manter a Segurança da Informação na empresa, e o que deve ser feito caso ocorra uma quebra na Segurança da Informação.

Em Neves (2021) o objetivo dos autores foi fazer uma ligação entre a segurança da informação, a Lei Geral de Proteção de Dados (LGPD) e Políticas de Segurança da Informação (PSI), visando que as empresas fiquem em conformidade com a LGPD, o que ocorre se elas tiverem uma boa segurança da informação aplicada na empresa. A metodologia usada é de caráter exploratório e expõem sobre a quantidade de dados que são gerados todos os dias e sobre a relevância dos dados sensíveis das pessoas, falam também sobre a importância da lei LGPD para ajudar a proteger informações sigilosas e a responsabilidade das empresas ao lidar com os dados pessoais, os cuidados que devem tomar de acordo com a lei e as práticas que devem seguir. O trabalho indica a identificação do modelo de negócio da organização e a criação do plano de ação, que pode se ajustar à política de segurança da empresa, sua implementação e posterior revisão e testes periódicos. O artigo visa mostrar para as organizações que caso elas já tenham uma PSI aplicada na empresa, é possível que o tratamento de dados da LGPD já esteja bem adiantado em questão de conformidade e que a segurança da informação é o principal desafio das empresas a se adequarem à LGPD, pois se ainda não tiverem uma base, terão que iniciar do zero, dificultando o processo. Este trabalho não aprofundou em exemplos de PSI adequadas à LGPD.

Em Ortega (2021) é apresentado um estudo teórico com foco na segurança de aplicações *web* com a análise das vulnerabilidades descritas no OWASP *Top Ten* 2021 e através disso mostra a importância de uma estratégia de desenvolvimento

seguro, seguindo metodologias, políticas e estudos existentes. A metodologia abordada foi a análise de cada uma das 10 vulnerabilidades, começando por seu contexto histórico e posterior formas de exploração e mitigação, não só de acordo com a própria OWASP, mas também com as contribuições de vários outros autores. Com a análise das vulnerabilidades percebe-se que os cenários são interligados entre si e quanto mais brechas houver na aplicação maiores serão os impactos e mais difícil sua mitigação. Sua contribuição é ajudar profissionais de TI a se prevenir alertando sobre as 10 principais vulnerabilidades dos últimos anos. Todavia o trabalho limitou-se a não explorar nenhuma outra vulnerabilidade além das apresentadas no OWASP *Top Ten* 2021 e não exibir um exemplo prático das formas de ataque citadas em cada vulnerabilidade a fim de comparar as fragilidades descobertas com as mostradas pelo projeto.

Embora todos os trabalhos citados acima tenham contribuído para a elaboração deste, nenhum deles retrata a criação de três Políticas de Segurança da Informação (PSI) com foco na OWASP *TOP* 10 2021 e a utilização de um *software* de gerenciamento de projetos que auxilia no desenvolvimento de projetos de maneira segura seguindo as PSIs criadas.

4 REFERENCIAL TEÓRICO

4.1 SEGURANÇA DA INFORMAÇÃO

De acordo com Hintzbergen (2018) a Segurança da Informação é a proteção contra ameaças que podem vir a surgir e tem o intuito de garantir a continuidade dos negócios minimizando os riscos. Ela é alcançada por meio do uso de controles, como por exemplo políticas, que visam assegurar que objetivos de segurança e da empresa sejam cumpridos. Seus pilares são a confidencialidade, disponibilidade e integridade.

Sendo a confidencialidade o acesso às informações e dados restritos apenas a pessoas autorizadas previamente. A disponibilidade o acesso à informação a qualquer momento que precisar, por pessoas autorizadas. E a integridade a garantia de que a informação está completa, íntegra e de que não foi modificada em nenhum momento por pessoas não autorizadas. (HINTZBERGEN, 2018)

4.2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

De acordo com a *High Security Center*, empresa provedora de soluções em cibersegurança,

> a Política de Segurança da Informação (PSI) pode ser definida como um documento que reúne um conjunto de ações, técnicas e boas práticas para o uso seguro de dados empresariais. Em outras palavras, é um manual que determina as medidas mais importantes para certificar a segurança de dados da organização.
>
> Para facilitar o entendimento, pode-se dizer que o PSI funciona como o código de conduta interno de um negócio, no qual é estabelecido como os profissionais devem agir, o que é permitido e o que é proibido fazer e quais atitudes devem ser tomadas no caso de uma emergência (HSC Brasil, 2018).

4.3 OWASP

A OWASP (Open Web Application Security Project) é uma fundação que colabora para melhorar a segurança de *software*s, sem fins lucrativos e conta com a ajuda de membros de todos os lugares do mundo por meio de projetos *open source* que buscam cada dia mais aprimorar a segurança da informação. (OWASP, 2023)

4.4 OWASP *TOP* 10

A OWASP *TOP* 10 é um documento de conscientização da fundação OWASP, que publica a cada triênio uma lista com as 10 vulnerabilidades *web* mais populares nesse período, apresentando a visão geral de cada uma e como se prevenir, visando alertar e orientar os desenvolvedores *web*. Com a adoção desse documento nas empresas é possível minimizar esses riscos citados no desenvolvimento de suas aplicações *web* futuras. (OWASP Top Ten, 2023)

4.5 LGPD

A Lei Nº 13.709, chamada de Lei Geral de Proteção de Dados ou LGPD, foi sancionada em 14 de agosto de 2018 e entrou em vigor em 2020. De acordo com o *site* oficial do Planalto,

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (PLANALTO, 2018).

4.6 IEC

De acordo com o *site* oficial da IEC,

> Fundada em 1906, a IEC (*International Electrotechnical Commission*) é a organização líder mundial na preparação e publicação de normas internacionais para todas as tecnologias elétricas, eletrônicas e relacionadas. Estes são conhecidos coletivamente como “eletrotecnologia” (IEC, 2023).

No Brasil, o Comitê Brasileiro de eletricidade, eletrônica, iluminação e telecomunicações (COBEI) é o responsável pelo Comitê Nacional Brasileiro da IEC. (COBEI, 2023)

4.7 ISO/IEC 27001:2013

A ISO 27001 é uma norma internacional padrão para a implementação de um sistema de gerenciamento de segurança da informação. Ela tem como princípio geral, a adoção de processos e requisitos que visam mitigar e monitorar o risco da organização, melhorando o sistema de gerenciamento de segurança da informação. É possível obter uma certificação ISO 27001, caso a organização cumpra com os princípios que são propostos na norma (ISO/IEC 27001:2013).

4.8 ISO/IEC 27002:2013

A ISO 27002 é uma norma internacional que apoia a implantação do Sistema de Gestão de Segurança da Informação (SGSI), com foco em boas práticas (OSTEC, 2016), e de acordo com o *site* da ISO,

> A ISO/IEC 27002:2013 fornece diretrizes para padrões de segurança da informação organizacional e práticas de gerenciamento de segurança da informação, incluindo a seleção, implementação e gerenciamento de controles levando em consideração o(s) ambiente(s) de risco de segurança da informação da organização (ISO/IEC 27002:2013).

4.9 SDLC

O Ciclo de vida de desenvolvimento de *software* é um processo usado para projetar e criar *softwares*, ele descreve as tarefas necessárias para criação e implantação do *software*. É utilizado para minimizar riscos, por meio do planejamento antecipado. Com essa metodologia é possível dividir o desenvolvimento do *software* em fases especificas, são elas: planejamento, projeto, implementação, teste, implantação e manutenção. O SDLC também possui alguns modelos, em cada modelo as fases do SDLC são divididas em ordens variadas e o modelo é escolhido de acordo com o objetivo específico de cada projeto. (AWS, 2023).

4.10 AMEAÇA

É a possibilidade de um incidente indesejado, que pode resultar em prejuízos (HINTZBERGEN, 2018).

4.11 CONTROLE

Medida de segurança para o tratamento de um risco específico, essas medidas podem ser políticas, diretrizes, determinadas práticas preestabelecidas e procedimentos direcionados (HINTZBERGEN, 2018).

4.12 INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

É um evento ou um conjunto de eventos indesejados que pode comprometer e afetar a segurança da informação (HINTZBERGEN, 2018). Pode ser ocasionado de forma acidental, por meio do envio de informações para o destinatário errado ou de forma intencional, por meio do furto de um dispositivo de armazenamento de dados ou por meio do ataque de sequestro de dados (*ransomware*). A exploração de uma vulnerabilidade existente não tratada, pode resultar em um incidente de segurança (ANPD, 2023).

4.13 VULNERABILIDADE

É uma fraqueza existente que pode vir a ser explorada e prejudicar a segurança da informação na empresa. (HINTZBERGEN, 2018).

5 METODOLOGIA

Este trabalho é uma pesquisa de natureza exploratória e descritiva. Para sua execução, foi analisado e estudado conteúdos científicos com foco em Segurança da Informação (HSC Brasil, 2018), Fundamentos de Segurança da Informação com base na ISO 27001 e na 27002 (HINTZBERGEN, 2018), na norma ISO 27001 (ISO/IEC 27001: 2013), Políticas de Segurança da Informação (DODT, 2020), OWASP Top Ten (OWASP Top 10: 2021), na lei LGPD (PLANALTO, 2018), Desenvolvimento Seguro (MONTANHEIRO, 2018), funcionamento de uma empresa de desenvolvimento de *Software* (HANASHIRO, 2019), ciclo de vida do *software* (CRONAPP, 2020) (MACORATTI, 2020) e demais assuntos mencionados no decorrer do trabalho.

De acordo com o OWASP TOP 10 2021, selecionou-se as vulnerabilidades A04: *Design* Inseguro e na A07: Falhas na Identificação e Autenticação e, com foco nelas foram elaboradas três Políticas de Segurança da Informação, sendo elas: Política Geral de Segurança da Informação para aplicações *web*, Política de Implementação do SDLC (Ciclo de Vida de Desenvolvimento de *Software*) e a Política para Identificação e Autenticação Segura.

Optou-se por utilizar o *software GanttProject*, para exemplificar o gerenciamento de um projeto de desenvolvimento de *software* de acordo com as políticas de segurança criadas, de maneira a contribuir para a segurança da informação. O *software* utilizado é *open source*, está disponível para *desktop,* tem a opção de armazenamento e compartilhamento em nuvem, tendo este um pequeno custo, a depender da quantidade de usuários, sendo o mesmo de utilização intuitiva.

Essa pesquisa optou por utilizar o *software GanttProject* para gerenciar o projeto a ser desenvolvido, considerando que:

- Por meio do *software GanttProject* o responsável, diretor ou pessoa designada, deve gerenciar o projeto a ser desenvolvido;
- O gerente de projetos, deve primeiramente criar as tarefas que serão necessárias, em seguida adicionar os responsáveis por elas através do seu *e-mail* corporativo, determinar o prazo para o cumprimento da tarefa, e demais informações que forem necessárias;

- Os responsáveis pelas tarefas devem cumpri-las no tempo determinado, utilizando os recursos do *software GanttProject* para se dividirem, se comunicarem e terem ciência de cada etapa do projeto e seu prazo final;
- O *GanttProject Cloud* é um serviço de colaboração ao *GanttProject*, e nele é possível distribuir acesso ao projeto com os outros colaboradores através da nuvem e ter acesso à versões anteriores do mesmo.

6 DESENVOLVIMENTO

Neste capítulo apresenta-se a aplicação desta pesquisa.

6.1 POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO PARA APLICAÇÕES *WEB*

Código: PGSIAW **Emissão:** 01/07/2022 **Versão:**1.0

Classificação: Uso interno e externo

Aprovado por: Nome do diretor da empresa

Introdução

A empresa tem como missão desenvolver *softwares* e aplicações *web* seguras, com alto desempenho e qualidade, gerando satisfação aos clientes e demais usuários.

A empresa reconhece que o produto final fornecido ao cliente deve ser totalmente íntegro e o mais seguro possível a fim de resolver as demandas requisitadas.

Dessa forma, a empresa estabelece sua Política Geral de Segurança da Informação para aplicações *web* alinhada as ISOs 27001 e 27002, como parte fundamental e primordial de seu sistema de gestão coorporativo. O objetivo desta é garantir a proteção das informações da empresa, de seus colaboradores e clientes por meio de regras e orientações estabelecidas.

Propósito

O principal propósito desta política é estabelecer normas de Segurança da Informação que sejam seguidas durante todo o processo de desenvolvimento do *software*, que ajude a eliminar todas as vulnerabilidades que poderiam surgir sem o cumprimento da política, com foco nas vulnerabilidades relacionadas ao: A04 *Design* Inseguro e a A07 Falhas de Autenticação e Identificação da OWASP TOP 10, a fim de que se obtenha um *software* que atenda a todos os requisitos desejados pelo cliente, e que seja confiável e seguro.

Orientar os colaboradores quanto à adoção de controles e adequação ao que se fizer necessário por meio das políticas.

Proteger as informações da empresa e dos clientes e produzir um *software* seguro, a fim de que se preserve os três principais pilares da segurança da informação: confidencialidade, integridade e disponibilidade.

Se prevenir de vulnerabilidades que possam surgir e colocar em risco o projeto, desenvolvimento e implementação do *software*, ainda assim, estar atento e pronto para intervir em possível caso de incidente de segurança da informação, revertendo a situação.

Escopo

Essa política de segurança se aplica a todos os colaboradores da empresa, independente da área atuante, desde programadores, gerentes de segurança da informação, prestadores de serviço, ex-prestadores de serviços, ex-colaboradores, todos que possuíram, possuem e que possam vir a possuir algum vínculo com a empresa no futuro.

Diretrizes

O objetivo da Gestão de Segurança da Informação da empresa é definir, revisar e manter as políticas de segurança e garantir que todas as exigências sejam cumpridas e seguidas, evitando impactos à segurança da empresa, colaboradores, fornecedores e clientes.

A Presidência e o Comitê Gestor de Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação na empresa. Com isso adotam todas as medidas necessárias para garantir que a política seja comunicada e entendida por todos dentro e fora da empresa que tenham vínculos com a mesma.

É política da empresa:

- Criar, implantar, seguir e revisar as políticas, normas e procedimentos de segurança da informação, garantindo que os pilares da segurança da informação sejam seguidos;
- Proporcionar o acesso às políticas, normas e procedimentos de segurança a todos que tenham vínculo com a empresa;
- Assegurar a conscientização das práticas de segurança da empresa, para todos os que tenham algum vínculo com a organização;

- Seguir todos os requisitos de segurança da informação exigidos por regulamentações, leis e/ou cláusulas contratuais;
- Documentar tudo o que ocorre na empresa, desde o planejamento antes de iniciar o projeto até a entrega e manutenção do mesmo;
- Tratar e resolver todos os incidentes de segurança da informação que possam ocorrer, registrando, investigando as causas, corrigindo e comunicando às autoridades quando necessário;
- Garantir a continuidade do negócio independente dos fatores que ocorrerem, por meio de planos de continuidade;
- Revisar, monitorar e melhorar a Gestão de Segurança da Informação de acordo com os objetivos de segurança da organização sempre que necessário.

Papéis e Responsabilidades

- **TODOS OS FUNCIONÁRIOS DA EMPRESA:**
  - É responsabilidade de todos os colaboradores da empresa:
    - Ler, compreender e assinar o Apêndice A – Termo de Uso de Compromisso e Responsabilidade para Colaboradores, assumindo a responsabilidade pelo cumprimento de todas as PSIs da empresa;
    - Respeitar e cumprir todas as normas e deveres presentes nesta e nas demais políticas;
    - Colaborar com sugestões de melhorias nas políticas de segurança de acordo com o que for notado;
    - Informar ao Comitê Gestor de Segurança da Informação, ou à alta direção qualquer evento que viole ou possa vir a violar esta Política.

- **COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO – CGSI**
  - O Comitê Gestor de Segurança da Informação é formado por meio da participação de um representante da diretoria, um gerente de projetos, um desenvolvedor, um analista de testes, um administrador de banco de

dados, e outros que se julgar necessários, estes tendo por responsabilidade tratar de questões ligadas à segurança da informação.

- É responsabilidade do CGSI:
  - Analisar e propor a aprovação de políticas e normas visando a segurança da informação;
  - Garantir que todos os recursos fundamentais para se fazer cumprir a PGSIAW e as Políticas existentes estejam disponíveis para os colaboradores;
  - Divulgar a PGSIAW e as Políticas, realizando ações necessárias para que todos tenham ciência da segurança da informação na empresa;
  - Realizar uma auditoria antes de liberar o produto final para o uso.

- **GERENTE DE PROJETOS**
  - É responsabilidade do Gerente de Projetos:
    - Entender o produto que será desenvolvido, conversando com o cliente e mantendo contato com ele sempre que necessário;
    - Criar as tarefas relacionadas ao desenvolvimento de cada projeto e disponibilizar o acesso ao *Ganttproject* a todos os envolvidos pelo desenvolvimento do projeto em questão;
    - Identificar e avaliar ameaças à segurança da informação e propor alterações nas políticas. Quando aprovada as propostas, implantar medidas corretivas para reduzir riscos;
    - Estabelecer o prazo de entrega do produto de acordo com o andamento da equipe;
    - Obedecer e cumprir as Políticas de Segurança da Informação.

- **ARQUITETO DA INFORMAÇÃO**
  - É responsabilidade do Arquiteto da Informação:
    - Desenhar a estrutura do projeto que será desenvolvido visando a usabilidade e a acessibilidade dos usuários;

- Utilizar ferramentas para criar um protótipo que facilite apresentar tanto aos desenvolvedores como ao cliente como o *software* ou *site* ficará;
- Utilizar o *Ganttproject* para melhor gerenciamento do projeto, informando início e fim de sua etapa;
- Obedecer e cumprir as Políticas de Segurança da Informação.

- **DESIGNER**
  - É responsabilidade do *Designer*:
    - Trabalhar junto com o Arquiteto da Informação;
    - De acordo com o protótipo feito pelo Arquiteto da Informação, o *Designer* define como os componentes da interface deverão ser, cores, tipografia, espaçamentos, tamanho, ícones e demais detalhes visuais necessários;
    - Utilizar o *Ganttproject* para melhor gerenciamento do projeto, informando início e fim de sua etapa;
    - Obedecer e cumprir as Políticas de Segurança da Informação.

- **DESENVOLVEDOR / PROGRAMADOR**
  - É responsabilidade do Desenvolvedor / Programador:
    - Escrever os códigos do programa que está sendo desenvolvido de acordo com o projeto que foi lhe passado;
    - Utilizar o *Ganttproject* para melhor gerenciamento do projeto, informando início e fim de sua etapa;
    - Obedecer e cumprir as Políticas de Segurança da Informação.

  - Desenvolvedor *Front-end*:
    - Escreve os códigos da parte visual, passados pelo Arquiteto da Informação e o *Designer*;
    - Utilizar o *Ganttproject* para melhor gerenciamento do projeto, informando início e fim de sua etapa;
    - Obedecer e cumprir as Políticas de Segurança da Informação.

- Desenvolvedor *Back-end*:
  - Escreve os códigos que ficarão no servidor, lidando com as regras de negócios e também os códigos que farão a ligação do *front-end* com o Banco de Dados;
  - Utilizar o *Ganttproject* para melhor gerenciamento do projeto, informando início e fim de sua etapa;
  - Obedecer e cumprir as Políticas de Segurança da Informação.
- Desenvolvedor *FullStack*:
  - Escreve os códigos do *Front-end* e também do *Back-end*;
  - Utilizar o *Ganttproject* para melhor gerenciamento do projeto, informando início e fim de sua etapa;
  - Obedecer e cumprir as Políticas de Segurança da Informação.

- **ANALISTA DE TESTES**
  - É responsabilidade do Analista de Testes:
    - Conhecer as regras de negócio do *software* desenvolvido e testar todo o *software*, analisar se todos os requisitos estão sendo cumpridos e verificar se há alguma vulnerabilidade, caso encontre vulnerabilidades deve identificar a causa e relatar para que os programadores façam as devidas correções;
    - Utilizar o *GanttProject* para melhor gerenciamento do projeto, informando início e fim de sua etapa;
    - Obedecer e cumprir as Políticas de Segurança da Informação.

- **ADMINISTRADOR DE BANCO DE DADOS (DBA)**
  - É responsabilidade do Administrador de Banco de Dados:
    - Criar a estrutura do Banco de Dados;
    - Cuidar do Banco de Dados, realizando *backups* e atualizações, garantindo a segurança e integridade dos dados;
    - Utilizar o *GanttProject* para melhor gerenciamento do projeto, informando início e fim de sua etapa;
    - Obedecer e cumprir as Políticas de Segurança da Informação.

Revisões

Esta política é revisada trimestralmente, ou quando se fizer necessário.

Gestão da Política

A Política Geral de Segurança da Informação para aplicações *web* é aprovada pelo Comitê Gestor de Segurança da Informação, e pela diretoria da empresa.

A presente política foi aprovada no dia 10/07/2022.

_____

_____

ASSINATURA DO(S) PRESIDENTE(S) DA EMPRESA

6.2 POLÍTICA DE IMPLEMENTAÇÃO DO SDLC (Ciclo de Vida de Desenvolvimento de *Software*)

Código: PSI01 **Emissão:** 01/07/2022 **Versão:** 1.0

Classificação: Uso interno

Aprovado por: Nome do diretor da empresa

Introdução

A norma de segurança da informação PSI01 complementa a PGSIAW-Política Geral de Segurança da Informação para aplicações w*eb*, definindo as diretrizes para a escolha e implementação do Ciclo de Vida de Desenvolvimento de *Software*, como uma das práticas para se ter melhor controle, segurança e evitar a vulnerabilidade: A04 - *Design* Inseguro, que faz parte das 10 vulnerabilidades mais frequentes dos últimos anos do projeto OWASP TOP 10 2021.

Propósito

Estabelecer diretrizes para a escolha e implementação de um Ciclo de Vida de Desenvolvimento de *Software* para guiar os projetistas e desenvolvedores ao longo de todo o processo de desenvolvimento do *software* da maneira mais segura possível.

Escopo

Essa política de segurança se aplica a todos os colaboradores da empresa, desde programadores, gerentes de segurança da informação, prestadores de serviço, ex-prestadores de serviços, ex-colaboradores, todos que possuíram e possuem algum vínculo com a empresa.

Diretrizes

Entender o conceito de SDLC (Ciclo de Vida de Desenvolvimento de *Software*) e as fases existentes

Cabe ao grupo de desenvolvedores, analistas, projetistas e toda a equipe entender a importância de seguir o SDLC para a segurança, organização e conclusão do projeto que será desenvolvido.

- **Fases do SDLC**:
    - **Fase de requisitos:** é a fase de levantamento de requisitos do projeto, e definição do modelo de SDLC a ser utilizado, sendo que:
        - Todos os colaboradores devem trabalhar em conjunto nesta fase de levantamento de requisitos;
        - Os requisitos são tudo o que deve ter no projeto a ser desenvolvido;
        - Nesta fase deve-se definir a modelagem de ameaças, padrões de *design* e arquitetura de referência que serão seguidos durante todo o Ciclo de Vida de Desenvolvimento do *Software*;
        - Nesta fase, após o levantamento dos requisitos e da definição da modelagem do sistema, deve-se criar um documento que indique os tipos de ataques que cada recurso a ser desenvolvido estará propenso a sofrer para maior atenção e segurança na hora de desenvolver tal recurso. É importante saber o cenário que o sistema será executado para entender e prever antecipadamente, quais os tipos de ataque que ele pode vir a receber, assim utilizando-se de estratégias e técnicas seguras para impedi-los de terem sucesso;
        - O modelo de SDLC escolhido deve ser seguido e obedecido durante todo o projeto.
    - **Fase de projeto:** é a fase de prototipação, *design* da arquitetura e interface:
        - Os responsáveis por essa fase, engenheiros de *software,* arquitetos da informação, *designers* e projetistas devem se atentar aos padrões de projetos, modelagem de ameaças, arquitetura de referência, e demais métodos e recursos seguros, para que os responsáveis pela implementação, já iniciem suas tarefas, seguindo as normas de segurança adotadas;
        - Deve-se ater às normas e leis que podem influenciar nesse projeto principalmente a norma internacional ISO 27001 e a lei nacional LGPD.

- **Fase de implementação:** é a fase de codificação do projeto na linguagem de programação definida, de acordo com o que foi planejado nas fases anteriores:
  - Os programadores devem seguir corretamente todo o projeto recebido, com todas as orientações descritas, seguindo os padrões e convenções de codificação indicados para a linguagem utilizada e caso tenha dúvidas deve-se procurar os responsáveis pela fase anterior do projeto;
  - Ficar atento às questões relacionadas a autenticação segura, seguindo a PSI02 - Política para identificação e autenticação Segura (a seguir).
- **Fase de testes:** aplicação de testes para verificar possíveis falhas na implementação, que servirão para nortear possíveis correções.
  - Testadores de *softwares* ou Analistas de Qualidade devem testar todas as possíveis formas de ataque que podem colocar em risco a segurança do *software* desenvolvido, pesquisar quais são as principais ferramentas automatizadas para invasão de sistemas, e testá-las, se prevenindo e assim diminuindo as chances de invasões.
  - Deve-se ater ao prazo estabelecido para a entrega desta fase.
- **Fase de produção:** implantação do *software* já concluído e funcionando.
  - Nesta etapa, os profissionais devem entregar o *software* já em funcionamento e com as devidas instruções de uso aos seus clientes.
- **Fase de manutenção:** nesta fase o *software* deve ser atualizado de acordo com as manutenções necessárias para o aprimoramento deste e de acordo com o surgimento de atualizações de segurança de *frameworks* e bibliotecas utilizadas no desenvolvimento da aplicação.
  - Os responsáveis pela manutenção são os programadores, e toda a equipe em sua determinada área. Ao alterar-se algo na aplicação, deve-se repassar a alteração a todos, para atualizarem o projeto de acordo com as mudanças na aplicação.

Escolha do SDLC (Ciclo de Vida de Desenvolvimento de *Software*)

Cabe ao grupo de desenvolvedores, analistas, projetistas e toda a equipe levantar os requisitos do projeto e em seguida analisar e escolher, de acordo com o projeto, o melhor modelo de Ciclo de Vida de Desenvolvimento de *Software* dentre os disponíveis e conhecidos tais como:

- **Modelo Cascata:** nesse modelo o processo de desenvolvimento é dividido em fases separadas e sequenciais, só se começa a próxima etapa quando finalizar a etapa anterior. A primeira etapa é a análise, em seguida projeto, codificação, testes e por último implementação. Na Figura 54, é apresentado um exemplo deste modelo, através do gráfico *Gantt*.
- **Modelo Incremental:** cada parte do projeto é desenvolvida separadamente, porém ao mesmo tempo e depois de finalizadas são integradas. Quando finalizada cada etapa uma amostra é apresentada para o cliente, para assim alterar algo que o cliente sugeriu antes da finalização do projeto. Na Figura 51, é apresentado um exemplo deste modelo, através do gráfico *Gantt*.
- **Modelo Evolutivo:** esse modelo é parecido com o modelo incremental, a cada etapa uma amostra é dividida com o cliente e de acordo com as demandas do cliente o desenvolvedor vai evoluindo o projeto. Os requisitos desse projeto são levantados no decorrer da evolução do projeto, de acordo com o que o cliente solicitar. Esse modelo depende das demandas do cliente. Nas Figuras 52 e 53, é apresentado um exemplo deste modelo, através do gráfico *Gantt*.
- **Modelo Espiral:** nesse modelo o *software* é desenvolvido de acordo com um ciclo de atividades e então é liberado para uso, porém ele continua em evolução, melhorando recursos e sempre liberando novas versões no final de mais um ciclo. Na Figura 50, é apresentado um exemplo deste modelo, através do gráfico *Gantt*.

Papéis e Responsabilidades

- **GERENTE DE PROJETOS E EQUIPE**
    - É responsabilidade do gerente de projetos juntamente com toda a equipe que realizará o projeto:
        - Definir os requisitos do projeto.

- **GERENTE DE PROJETOS**
    - É responsabilidade do gerente de projetos:
        - Definir o modelo que será usado para o Ciclo de Vida de Desenvolvimento do *Software*, de acordo com os requisitos necessários para cada projeto;
        - Revisar periodicamente se o SDLC adotado está sendo cumprido corretamente e com as devidas medidas de segurança.

- **TODA A ESQUIPE DE COLABORADORES**
    - É responsabilidade de toda a equipe que realizará o projeto:
        - Cumprir todas as regras estabelecidas no modelo do SDLC adotado;
        - Zelar pela integridade, confiabilidade e disponibilidade do *software* desenvolvido e cumprir sua parte no projeto com total dedicação.

Revisões

Esta norma é revisada trimestralmente, ou quando se fizer necessário.

Gestão da Norma

A norma **PSI01** é aprovada pelo Comitê Gestor de Segurança da Informação, e pela diretoria da empresa.

A presente norma foi aprovada no dia 10/07/2022.

_____

_____

ASSINATURA DO(S) PRESIDENTE(S) DA EMPRESA

6.3 POLÍTICA PARA IDENTIFICAÇÃO E AUTENTICAÇÃO SEGURA

Código: PSI02 **Emissão:** 18/08/2022 **Versão:** 1.0
Classificação: Uso interno
Aprovado por: Nome do diretor da empresa.

Introdução

A Norma de segurança da informação PSI02 complementa a Política Geral de Segurança da Informação para aplicações *web*, definindo as diretrizes para mitigar falhas de identificação e autenticação, como uma das práticas para se ter melhor segurança, controle e evitar a vulnerabilidade: A07 - Falhas de Autenticação e Identificação, que faz parte das 10 vulnerabilidades mais frequentes dos últimos anos de acordo com o projeto OWASP TOP 10 2021.

Propósito

Estabelecer diretrizes para guiar os projetistas e desenvolvedores no planejamento e posterior desenvolvimento de uma aplicação segura e confiável principalmente com relação a identificação e autenticação segura de usuários, evitando assim muitas vulnerabilidades que poderiam surgir devido a uma fraca implementação nessa área.

Escopo

Essa política de segurança se aplica a todos os colaboradores da empresa, desde programadores, gerentes de segurança da informação, prestadores de serviço, antigos prestadores de serviços, ex-colaboradores, todos que possuíram e possuem algum vínculo com a empresa.

Diretrizes

Com o objetivo de se obter um produto final íntegro, disponível e confiável, pilares da segurança da informação, uma das medidas que se deve tomar é seguir rígidas práticas na hora de planejar e implementar a autenticação e identificação dos usuários. As medidas fundamentais a serem tomadas são:

- **Autenticação de 02 fatores:**
    - É imprescindível a implementação da autenticação de 02 fatores, tendo como regra a obrigação da utilização pelos usuários. Com isso, evita-se o sucesso de ataques automatizados de preenchimento de credenciais, ataques de força bruta e ataques de reutilização de credenciais roubadas. Segundo a Microsoft, 99,9% dos ataques a contas podem ser evitados usando a autenticação de 02 fatores (MICROSOFT, 2023);
    - Indicação de *software* para utilização dos usuários: *Authy* e *Google Authentication*.
- **RegEx (Expressões Regulares)**:
    - É fundamental a implementação de RegEx na hora do desenvolvimento, para identificar e recusar senhas padrões (12345/admin) ou fracas na criação de um usuário, na troca de senha de um usuário, ou na recuperação de senha de um usuário.
- **Verificação de senhas fracas:**
    - Não usar senhas padrões composta por combinações numéricas sequenciais;
    - Testar senhas novas ou alteradas na lista das 10.000 piores senhas;
    - Definir políticas de complexidade, tamanho e rotação de senha com as diretrizes 800-63b do Instituto Nacional de Padrões e Tecnologia (NIST) na seção 5.1.1 para segredos memorizados ou também outras políticas de senha modernas baseadas em índices reais.
- **Recuperação de Senha:**
    - A validação para a recuperação e mudança de senha deve ser rigorosa e segura evitando-se perguntas padrões e garantindo que o caminho para a recuperação de senha seja protegido contra ataques de enumeração de contas.

- **Falhas no *login:***
    - Limitar tentativas de *login* com falha, bloqueando por um tempo as tentativas, para evitar ataques de força bruta e demais ataques, alertando o usuário através do *e-mail* cadastrado;
    - Registrar todas as falhas no *login* e informar aos administradores quando algo sair fora do normal.
- **Gerenciador de Sessão de Usuário/ *Token* de Autenticação:**
    - Utilizar um gerenciador de sessão integrado e seguro do lado do servidor que gere um ID de sessão aleatório após a realização do *login*;
    - O identificador de sessão não deve ficar na URL;
    - Deve-se implementar funções para que as sessões de usuário e *token* de autenticação sejam invalidados imediatamente após o *logout* ou após um certo período de inatividade.
- **Gerenciador de Senhas:**
    - É necessário recomendar ao usuário a utilização de um *software* para gerenciamento de senhas. Um *software* gratuito, *open source* que pode-se recomendar é o *Bitwarden*;
    - O *bitwarden* é um gerenciador de senhas baseado na nuvem e com ele é possível criar senhas, cadastrar *logins* de *sites* e autopreencher o usuário e senha em vários *sites*. É possível acessar o *bitwarden* por meio de seu *site* oficial na *web* e também através das extensões existentes para navegadores.

Papéis e Responsabilidades

- **DESENVOLVEDOR**
    - É responsabilidade do(a) desenvolvedor(a) seguir e implementar todas as etapas e métodos descritos nesta política ao desenvolver o *software*, resultando assim em um *software* protegido e atento às falhas de identificação e autenticação.

Revisões

Esta norma é revisada trimestralmente, ou quando se fizer necessário.

Gestão da Norma

A norma **PSI02** é aprovada pelo Comitê Gestor de Segurança da Informação, e pela diretoria da empresa.

A presente norma foi aprovada no dia 18/08/2022.

_____

_____

ASSINATURA DO(S) PRESIDENTE(S) DA EMPRESA

6.4 UTILIZAÇÃO DO *GANTTPROJECT* SIMULANDO UM PROJETO DE DESENVOLVIMENTO DE *SOFTWARE*

O uso de *software*s de gerenciamento de projetos ao desenvolver um projeto é indispensável, pois com ele é possível organizar a distribuição de tarefas entre os colaboradores, definição de prazos, acompanhar o andamento das tarefas, entre outras funções que auxiliam a execução do projeto do início ao fim, garantindo ainda uma maneira de minimizar os riscos. Nessa pesquisa utilizou-se o *software* de gerenciamento de projeto *GanttProject* para nortear o projeto de desenvolvimento de um *software* para *web* com foco na vulnerabilidade A04-*Design* Inseguro e A07-Falhas de identificação e autenticação, do projeto OWASP TOP 10 2021. Sendo assim, ao definir um modelo de Ciclo de Vida de Desenvolvimento do *Software,* já é possível montar o projeto no *software* de gerenciamento de projetos *GanttProject* e iniciar o desenvolvimento do *software*.

Podemos ver por meio das figuras a seguir, a utilização do *software GanttProject* simulando um projeto de desenvolvimento de *software web*, seguindo as políticas de segurança da informação criadas neste trabalho, a saber PGSIAW, PSI01 e PSI02.

Após feito o *download* e instalado o *software GanttProject* em sua máquina pelo link: https://www.ganttproject.biz/, iniciamos a criação do projeto. Na Barra de Menus, clique em Projeto e depois em Novo, como pode-se ver na Figura 1.

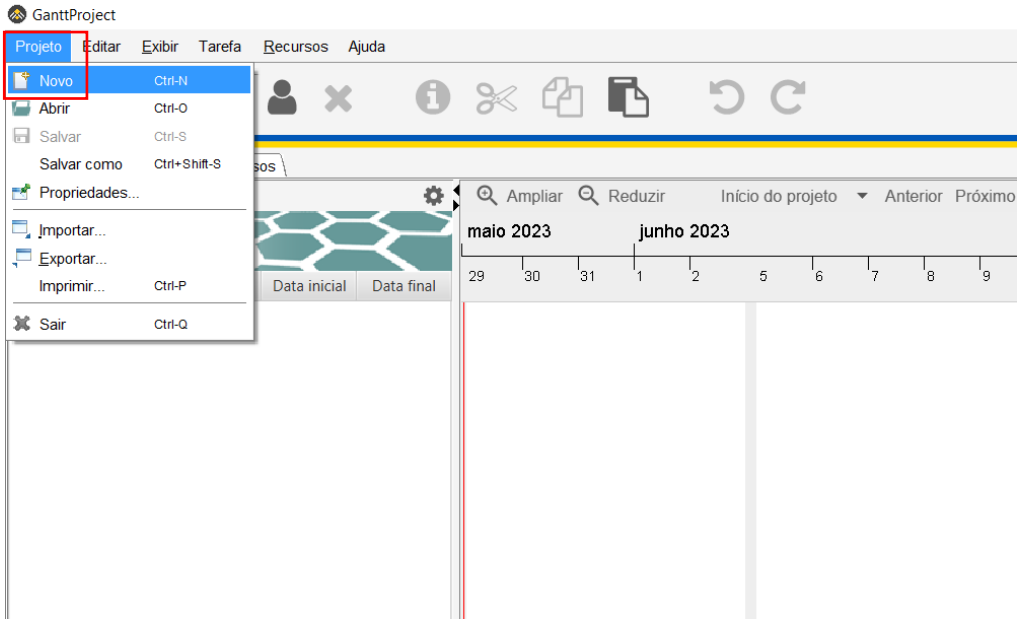

Figura 1 - Criação de um novo projeto no *GanttProject*.

Para criar um novo projeto, dê um nome ao mesmo e preencha mais alguns dados, conforme mostra a Figura 2.

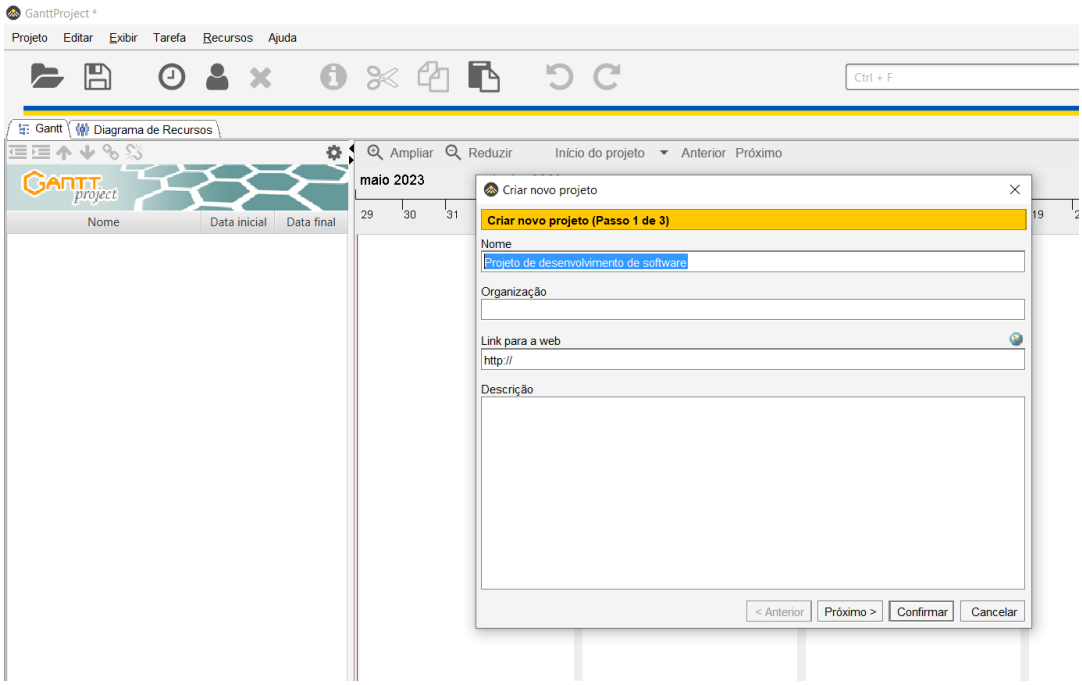

Figura 2 - Criação de um nome para o projeto.

Após confirmar o nome para o novo projeto, é necessário escolher o domínio do projeto conforme a Figura 3. Para essa configuração, marque as funções Padrão e Desenvolvimento de *Software*. Após a implantação será disponíbiliza-se várias funções relacionadas ao respectivo desenvolvimento de *software*.

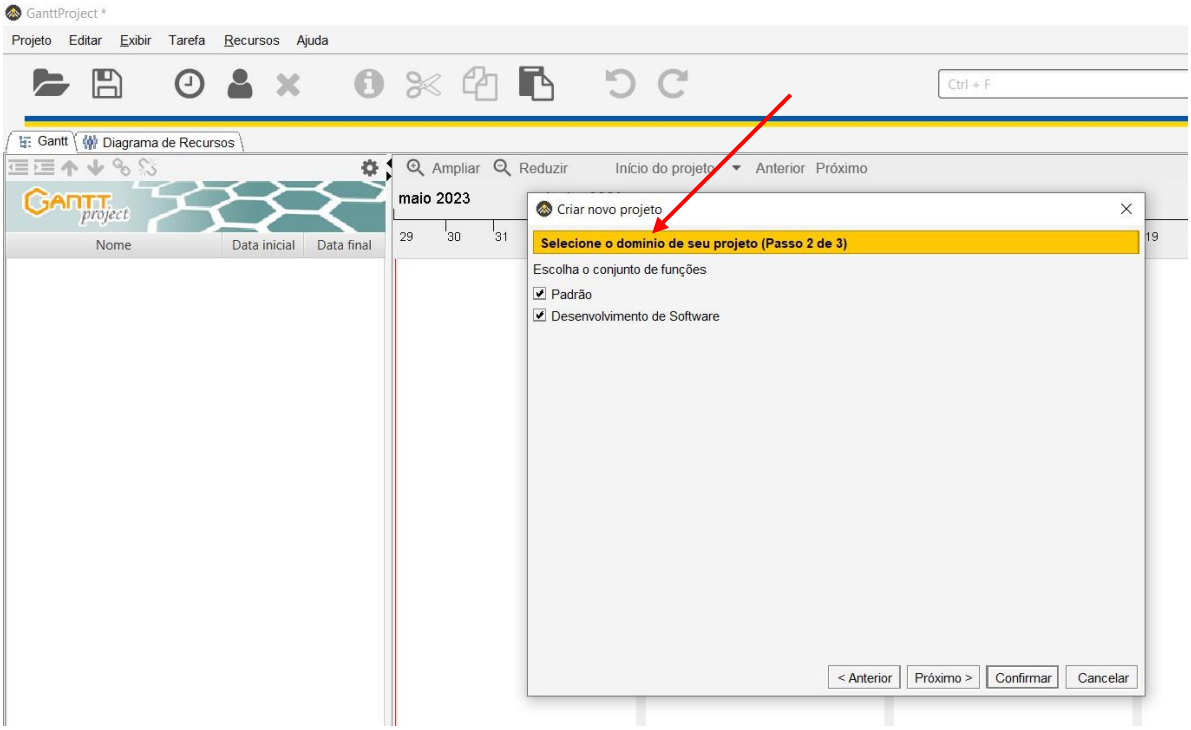

Figura 3 - Selecionando o domínio do projeto.

Após selecionar os dois conjuntos de funções e clicar em Próximo, é o momento de configurar alguns ajustes sobre a realização de tarefas aos fins de semana e feriados, conforme a Figura 4, onde optou-se por não executar nenhuma tarefa nessas datas, conforme o calendário de feriados disponível no *GanttProject* com intervalo de 2017 a 2022 do Brasil.

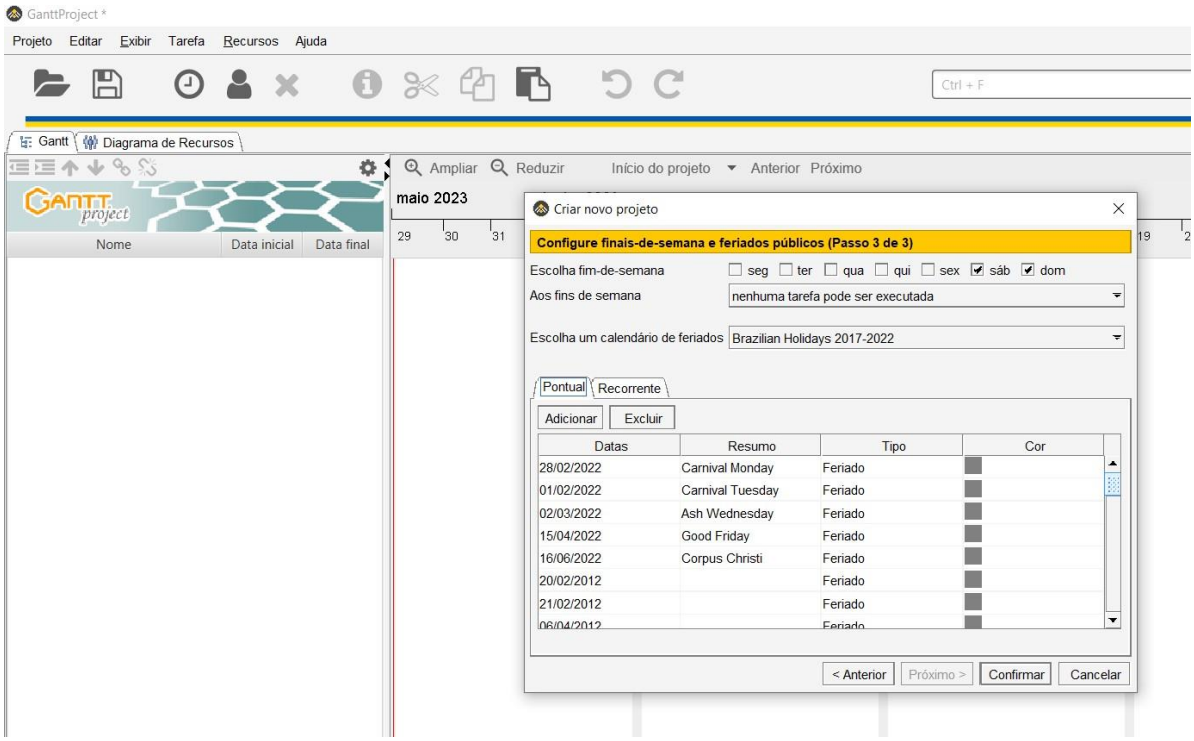

Figura 4 - Configurando finais de semana e feriados.

Após criado e configurado o projeto, é o momento de começar a criar os colaboradores. Para isso, na Barra de Menus, clique em Recursos e em seguida clicar em Novo Recurso.

A Figura 5 mostra a criação dos colaboradores que irão trabalhar no projeto de desenvolvimento do *software web*, sendo necessário configurar a Guia Geral com as seguintes informações: nome, telefone, *e-mail*, função e taxa de pagamento.

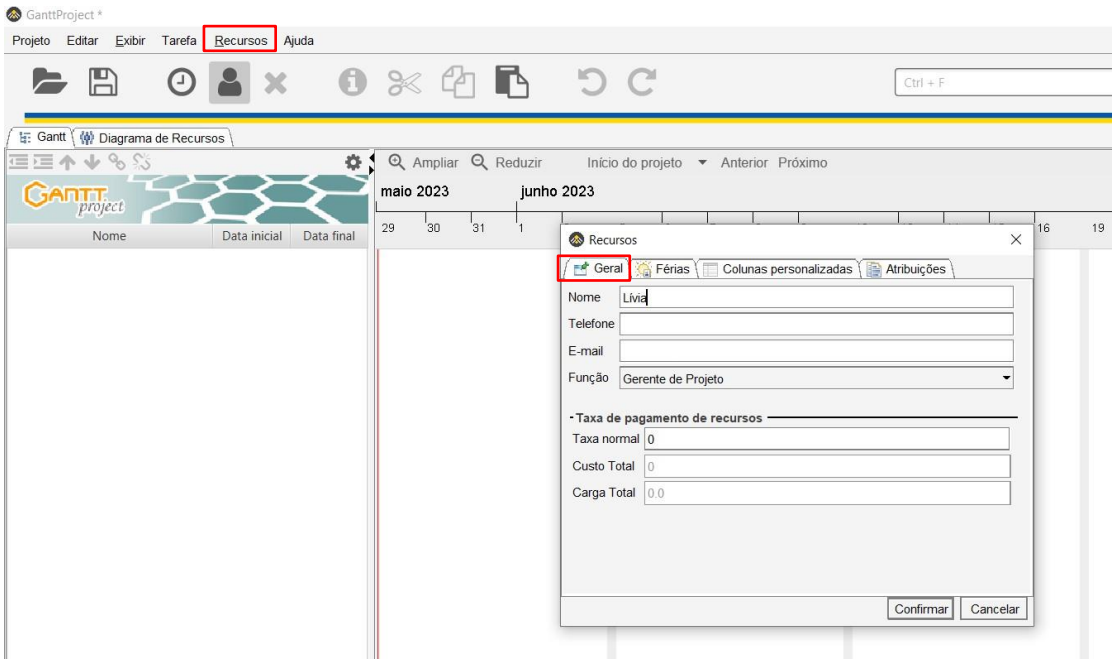

Figura 5 - Criação e personalização dos colaboradores.

Na Figura 6, podemos ver três colaboradores já criados, com suas respectivas funções.

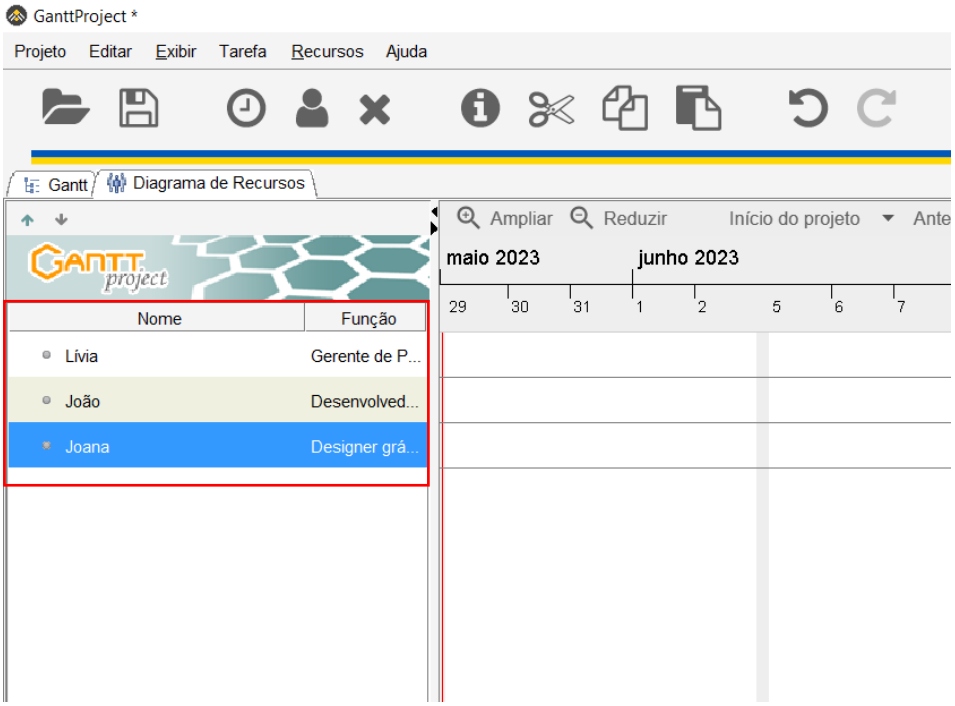

Figura 6 - Lista de colaboradores criados.

Na Figura 7 é possível ver a criação de novas funções para os colaboradores, caso alguma função necessária não esteja predefinida. Para isso deve-se ir em Projeto, na Barra de Menus, em seguida em Propriedades, e após isso, em Função da pessoa. Após adicionar a nova função deve-se confirmar e então a nova função estará disponível para ser adicionada aos colaboradores.

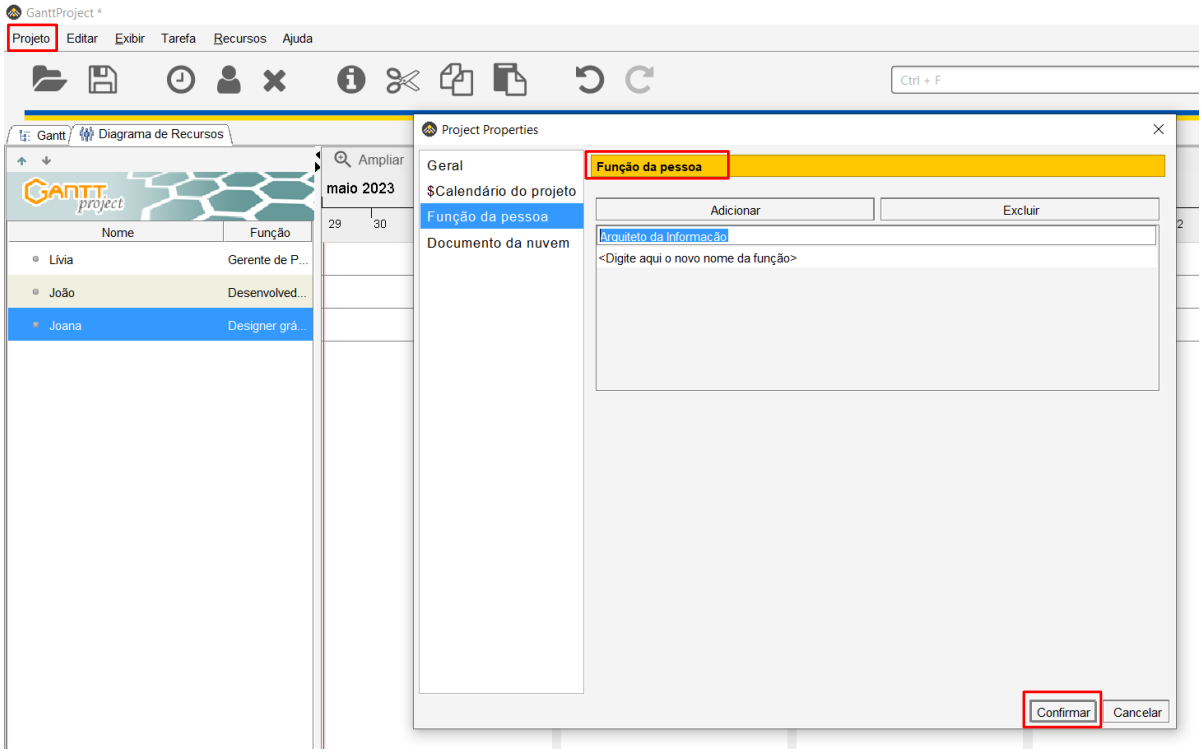

Figura 7 - Criação de novas funções.

Na Figura 8, podemos ver que a função criada na Figura 7, já está disponível para ser utilizada nos colaboradores.

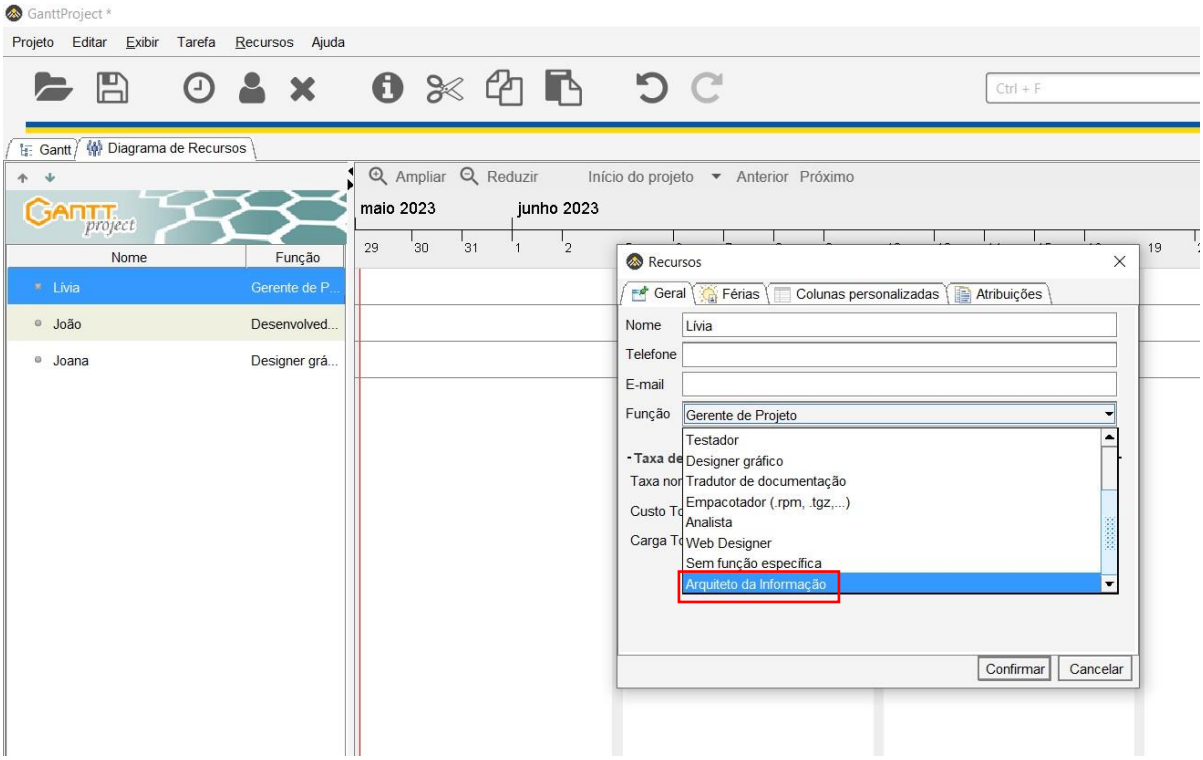

Figura 8 - Nova função: Arquiteto da Informação, disponível para uso.

Após a criação de todos os recursos, que são os colaboradores, é iniciada a criação das tarefas, conforme Figura 9. Para isso, na Barra de Menus clique na opção Tarefas.

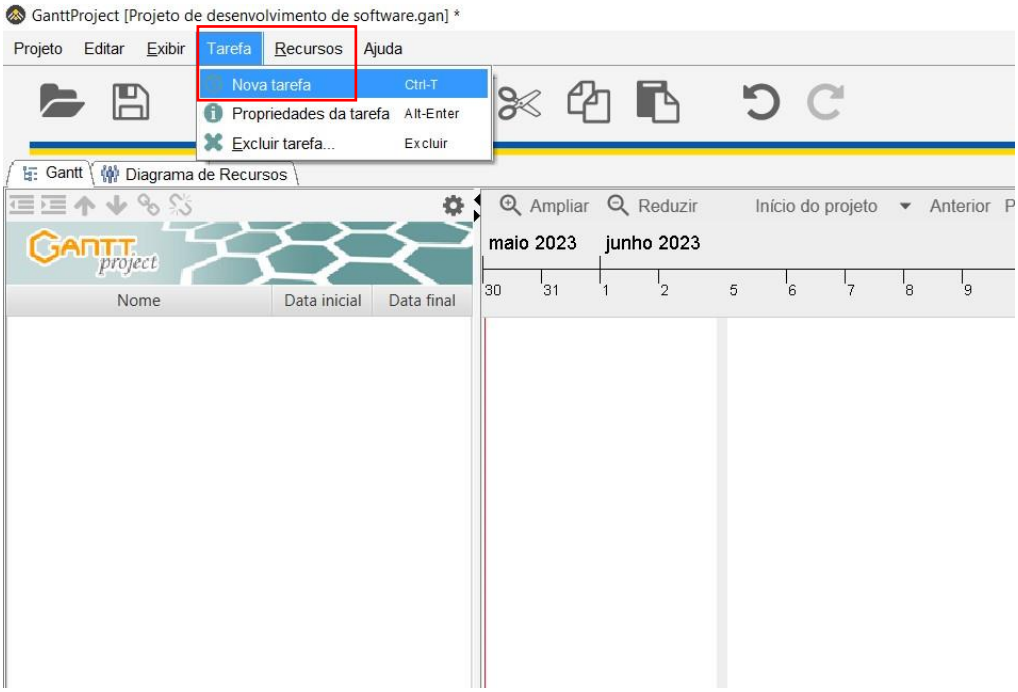

Figura 9 - Criação de nova tarefa.

Nesta etapa, deve-se criar cada tarefa levando em conta todo o desenvolvimento do *software*, do início ao fim e o modelo do SDLC escolhido. É necessário preencher as Propriedades de acordo com o que é exigido por cada tarefa, conforme vemos na Figura 10.

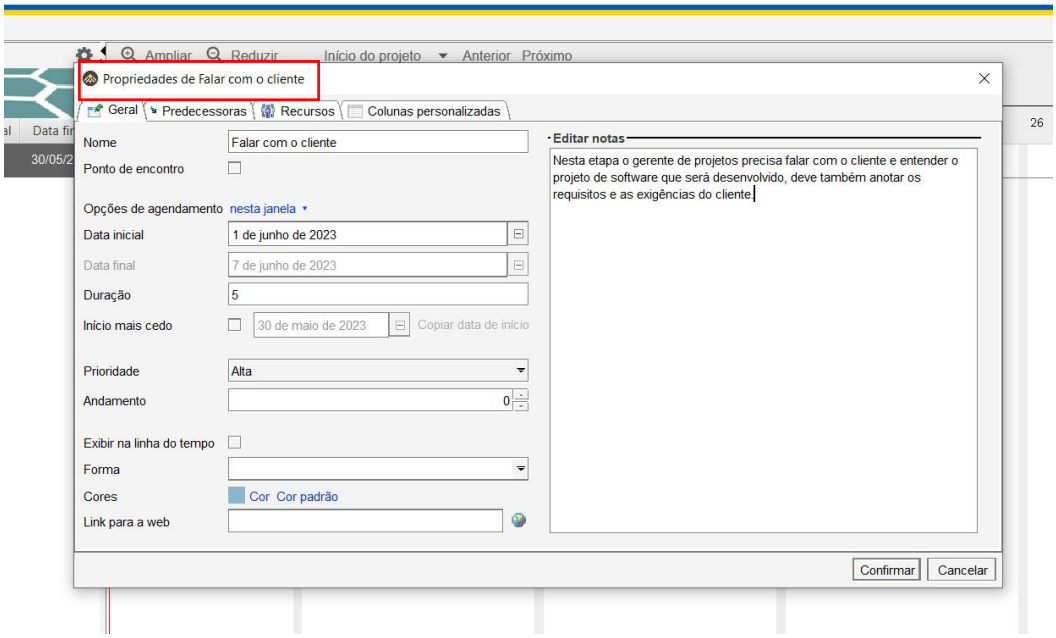

Figura 10 - Definição das propriedades da tarefa.

No Menu de Propriedades, ao ir em Recursos, é possível selecionar o colaborador responsável pela tarefa criada, conforme vemos na Figura 11.

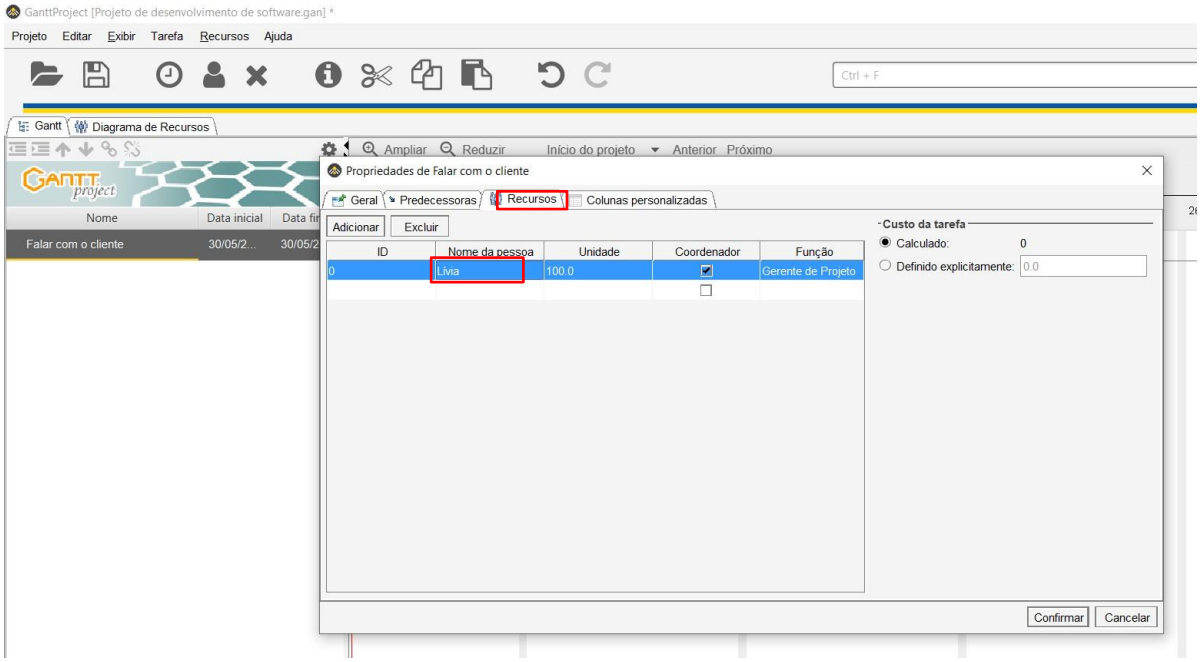

Figura 11 - Adicionando colaborador responsável pela tarefa.

Após a criação de mais tarefas é necessário definir dependências umas das outras de acordo com o modelo do Ciclo de Vida de Desenvolvimento do *Software* (SDLC) escolhido para o projeto. Nessa simulação optou-se pelo Modelo Cascata, que é o modelo mais utilizado. Para isso deve-se dar duplo clique sobre a tarefa para

abrir suas propriedades, em seguida clicar em predecessoras, e conforme mostra a Figura 12, podemos selecionar a tarefa predecessora da tarefa em questão e clicar em confirmar.

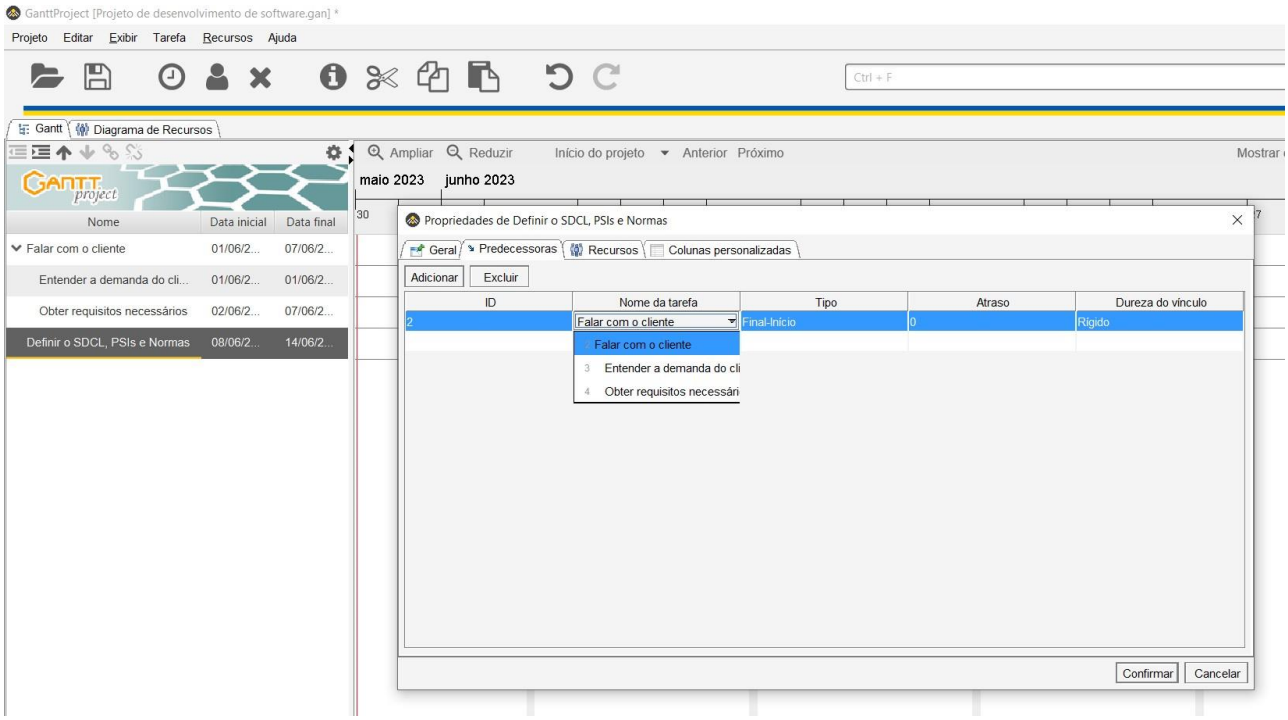

Figura 12 - Definindo uma tarefa predecessora.

Após isso sua data inicial e data final já são atualizadas automaticamente e o gráfico *gantt* passa a mostrar a sequência correta de acordo com as dependências, conforme mostra a Figura 13.

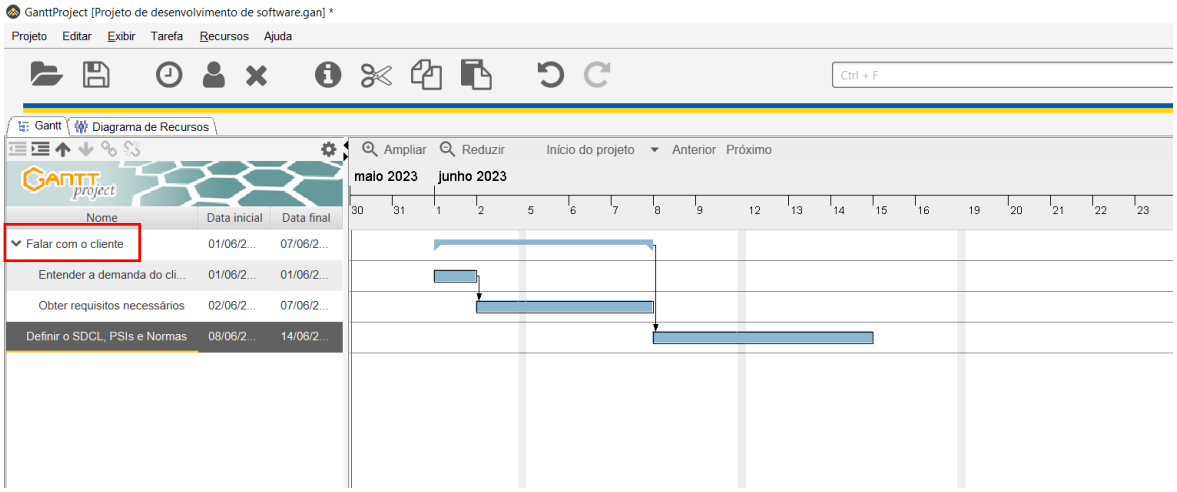

Figura 13 - Gráfico *gantt* de acordo com tarefas criadas até o momento.

É possível adicionar tarefas dentro de um conjunto de tarefas caso necessário, como é mostrado na Figura 13. Existem duas tarefas que fazem parte da tarefa Falar com o cliente, são as tarefas: Entender a demanda do cliente e Obter requisitos necessários. No gráfico de *gantt* podemos ver que as duas tarefas estão dentro da primeira. Essa organização é útil para detalhar melhor o projeto.

Após incluir todos os recursos e todas as tarefas no *software* de acordo com o projeto, podemos observar na Figura 14, que temos acesso ao gráfico *gantt* de todo o projeto.

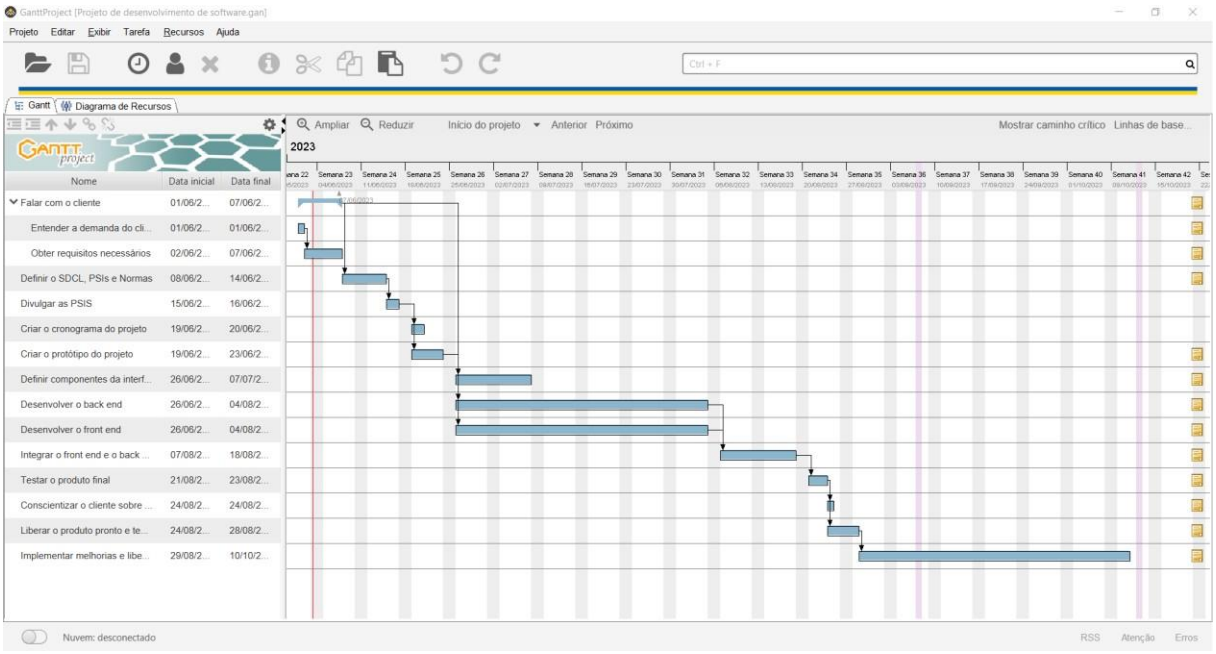

Figura 14 - Gráfico *gantt* de todo o projeto.

Também é possível ver o diagrama de recursos de todo o projeto, como mostra o diagrama da Figura 15. O diagrama exibe o período em que cada colaborador vai estar ocupado com suas tarefas de acordo com o estabelecido pelo projeto criado.

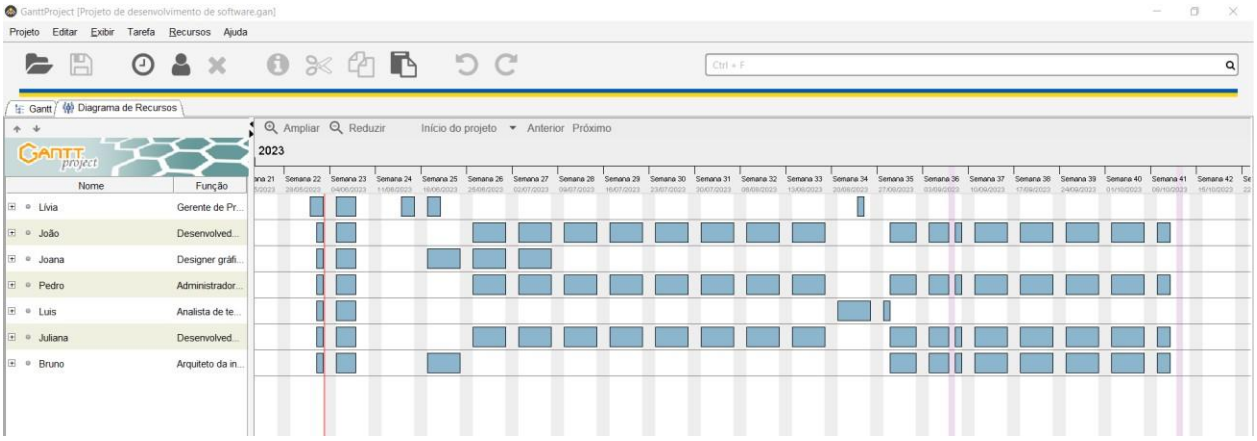

Figura 15 - Diagrama de recursos de todo o projeto.

Além do gráfico *gantt* e do seu diagrama de recursos, é gerado automaticamente o gráfico PERT. Para isso deve-se ir na Barra de Menus, na aba Exibir e clicar em Gráfico PERT conforme Figura 16.

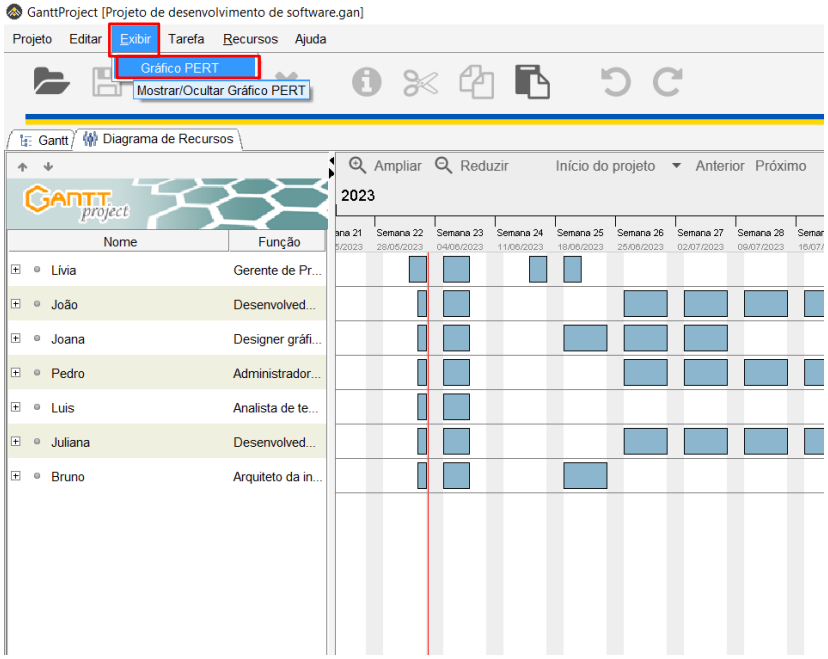

Figura 16 - Exibir gráfico PERT.

No Gráfico PERT é possível ver claramente e de maneira simples o mapeamento do projeto, com suas tarefas, datas de início e fim de cada tarefa e suas dependências, como é apresentado na Figura 17.

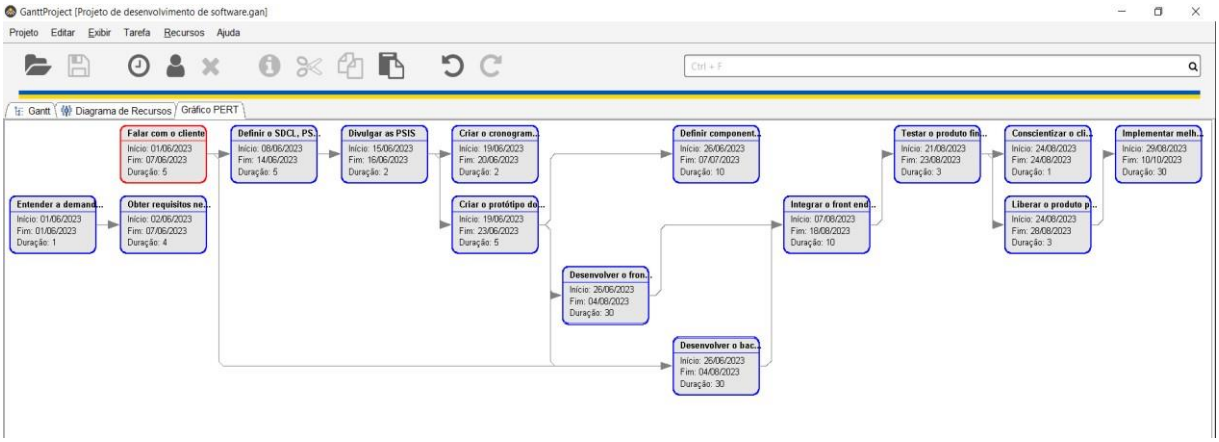

Figura 17 - Gráfico PERT.

Caso seja necessário exportar o projeto, ao clicar em Projeto na Barra de Menus e em Exportar, é possível exportar o projeto para: arquivo *Microsft Project*, relatório HTML, relatório PDF, arquivo de imagem, e arquivos separados por vírgula, conforme mostra a Figura 18.

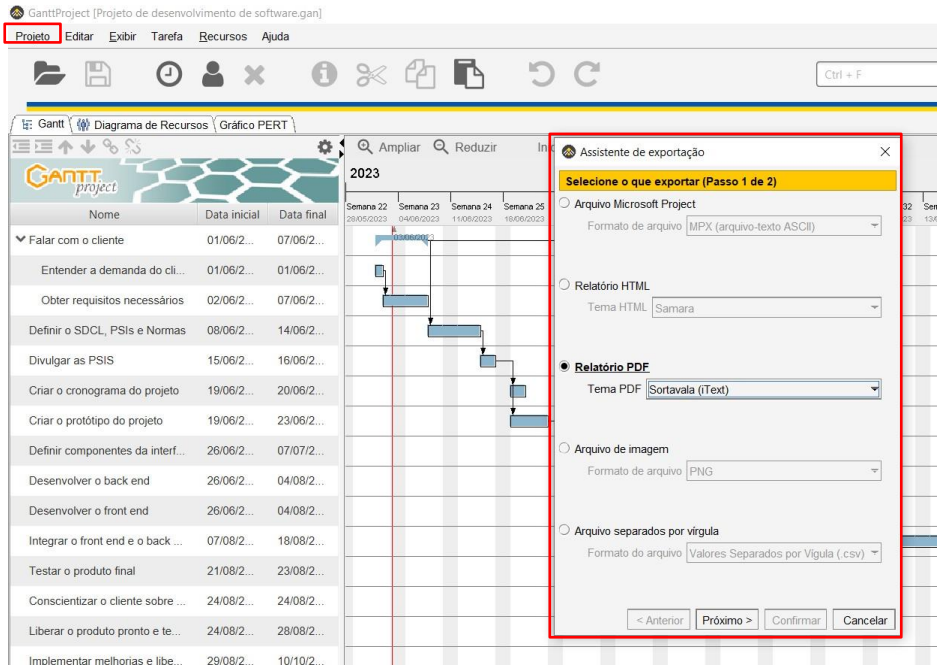

Figura 18 - Formas de exportação do projeto.

6.5 UTILIZAÇÃO DO *GANTTPROJECT CLOUD* SIMULANDO UM PROJETO DE DESENVOLVIMENTO DE *SOFTWARE*

É importante também que ao utilizar um *software* de gerenciamento de projetos seja possível compartilhar o projeto com os outros colaboradores. Para isso, é necessário criar um *login* no *GanttProject Cloud*, que pode ser acessado pelo *link*: https://ganttproject.cloud/.

Como vemos na Figura 19, podemos fazer o *login* pela conta *Google*, ou com algum *e-mail*.

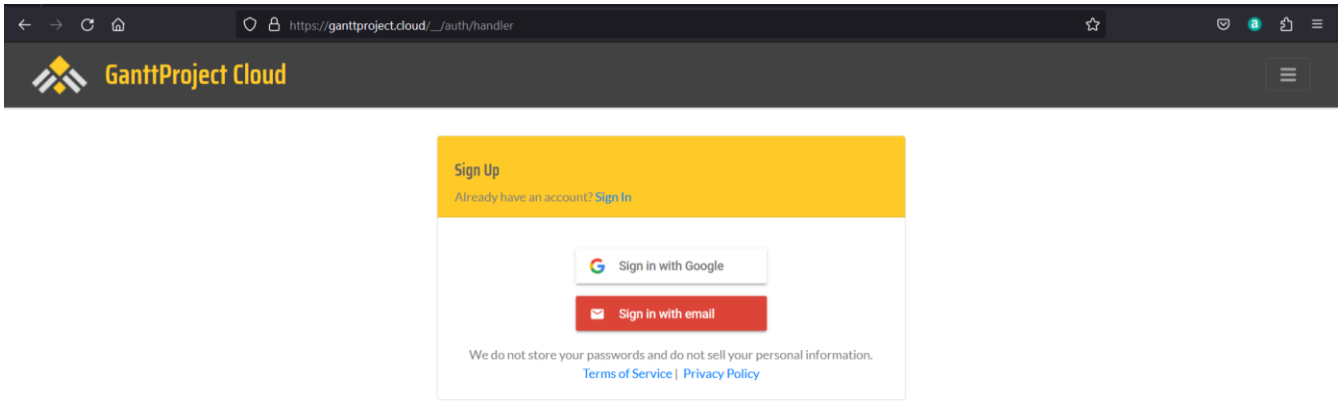

Figura 19 - Criando uma conta no *GanttProject Cloud*.

Feito o cadastro no *GanttProject Cloud*, é hora de conectar o projeto feito no *GanttProject* na nuvem. Para isso no *software*, na Barra de *Status*, localizada no canto inferior esquerdo clique no botão Nuvem desconectado, conforme Figura 20.

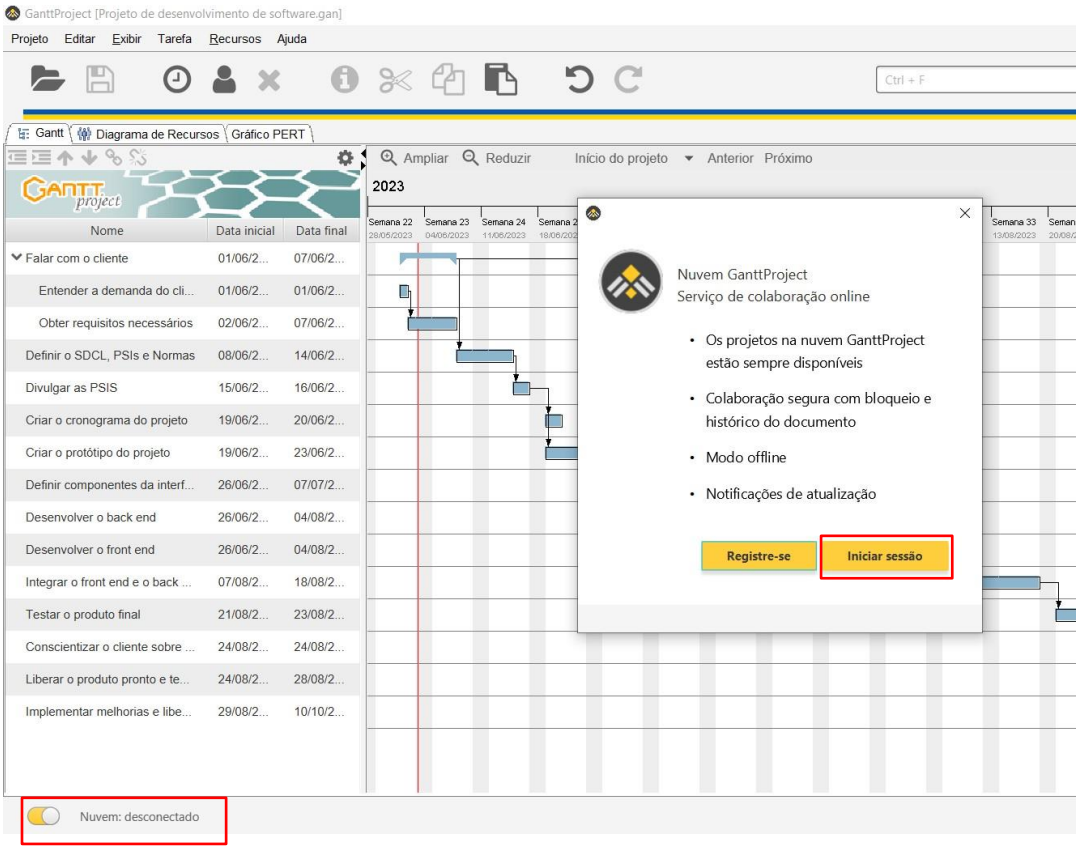

Figura 20 - Conectando o *software GanttProject* no *GanttProject Cloud*.

Ainda na Figura 20, clique em iniciar sessão, pois já foi criada a conta no *GanttProject Cloud*. Automaticamente o navegador padrão é aberto e precisamos definir a validade do *token* de autenticação. Nesse caso definiu-se: Até *GanttProject* ser fechado. Após isso deve-se clicar em: Garantir acesso, conforme mostra a Figura 21.

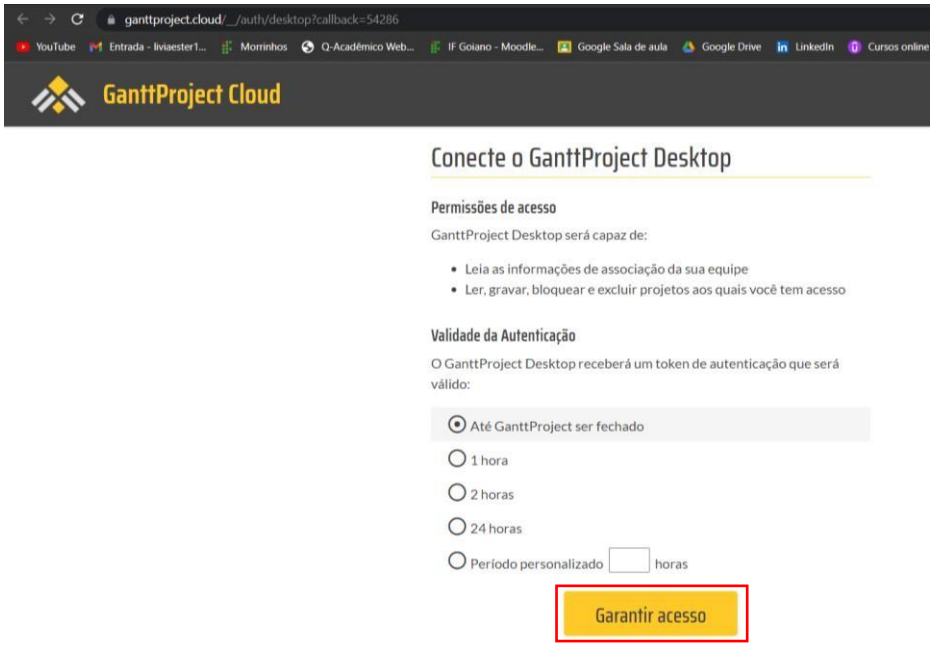

Figura 21 - Definindo a validade do *token* de autenticação.

Sempre que acabar o prazo de validade do *token* de autenticação, será necessário gerar um novo *token* para conseguir o acesso ao projeto no *GanttProject Cloud*.

E então já é possível voltar para o *GanttProject*, conforme vemos na Figura 22.

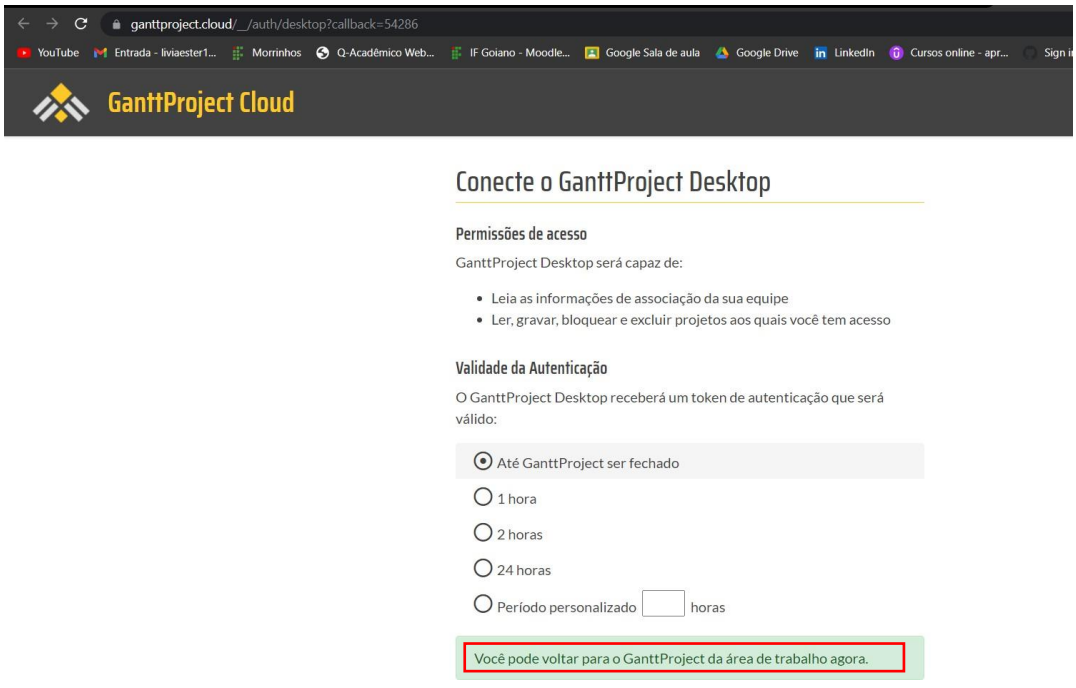

Figura 22 - Validade do *token* definida.

Ao voltar para o *software* podemos ver que ele já está conectado na nuvem, conforme mostra a Barra de *Status* na Figura 23.

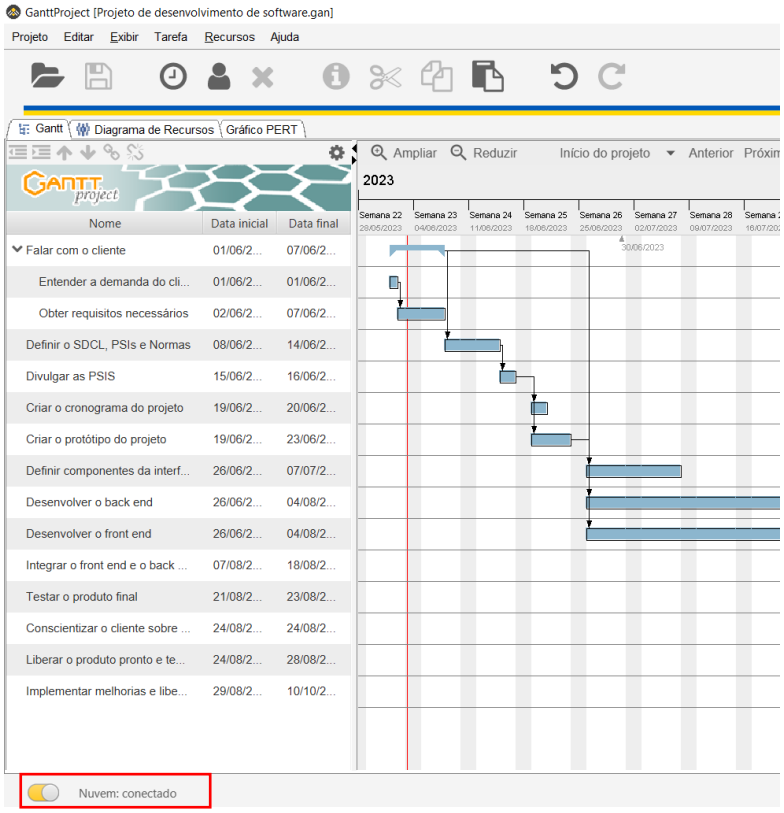

Figura 23 - Nuvem: conectado.

De volta ao *GanttProject Cloud*, é preciso criar um novo time, onde é possível incluir os colaboradores, para eles terem acesso ao projeto. Optou-se pelo nome: Projeto de Desenvolvimento de *Software*, que é o mesmo nome do projeto no *software GanttProject*, conforme Figura 24.

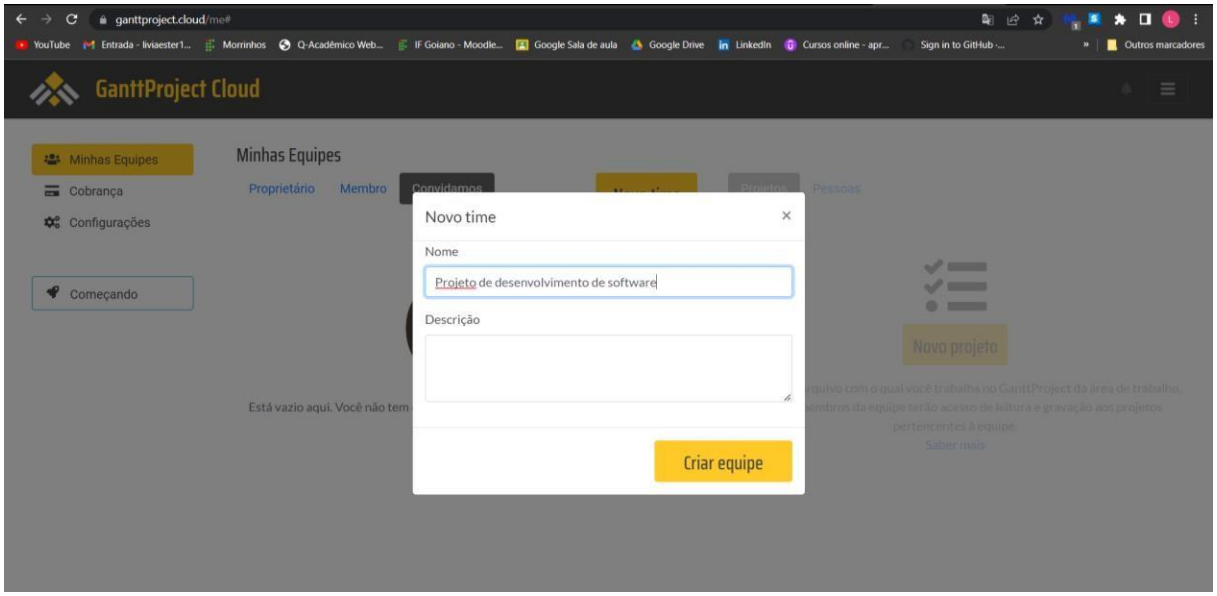

Figura 24 - Novo time no *GanttProject Cloud*.

Antes de adicionar os colaboradores no time para terem acesso ao projeto, é preciso passar este projeto do *software* para o *GanttProject Cloud*. Após clicar em Projeto, na Barra de Menus no canto superior esquerdo e em seguida em Salvar como, deve-se clicar em Nuvem *GanttProject.* Em seguida já podemos ver a pasta com o nome da equipe criada na etapa anterior, como mostra a Figura 25. Após isso clicamos na pasta Projeto de desenvolvimento de *software* e em seguida em Salvar. Feito isso o projeto já estará salvo no *GanttProject Cloud*, dentro da pasta criada anteriormente.

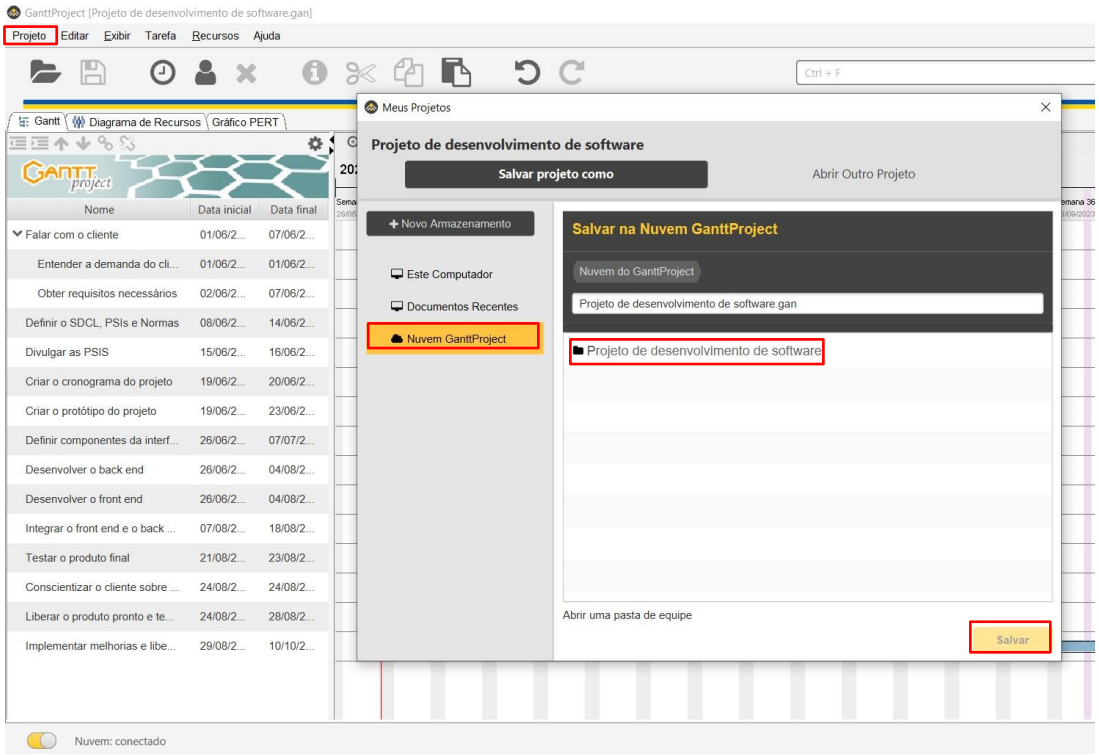

Figura 25 - Salvando o projeto do *Software* na Nuvem *GanttProject*.

Conforme a Figura 26, pode-se ver que o Projeto de desenvolvimento de *software.gan*, que é o projeto criado no *software*, já está conectado com o *GanttProject Cloud*.

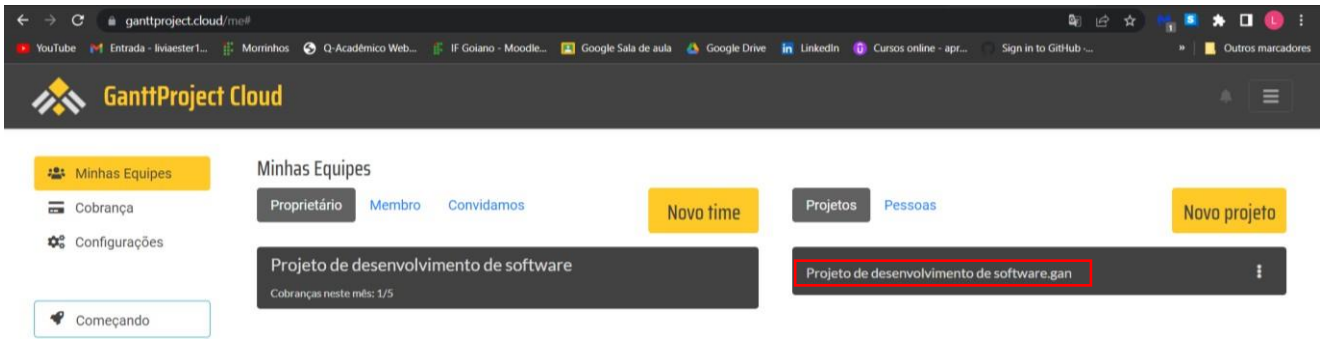

Figura 26 - Projeto de desenvolvimento de software.gan.

O próximo passo é convidar as pessoas da equipe de desenvolvimento para se tornarem membros do projeto no *GanttProject Cloud*. Sendo assim, deve-se clicar em Pessoas, após isso já são automaticamente puxados os *e-mail*s cadastrados nas pessoas pelo *Software*, como podemos ver na Figura 27, onde já aparecem João e Joana com seus respectivos *e-mails*, como candidatos.

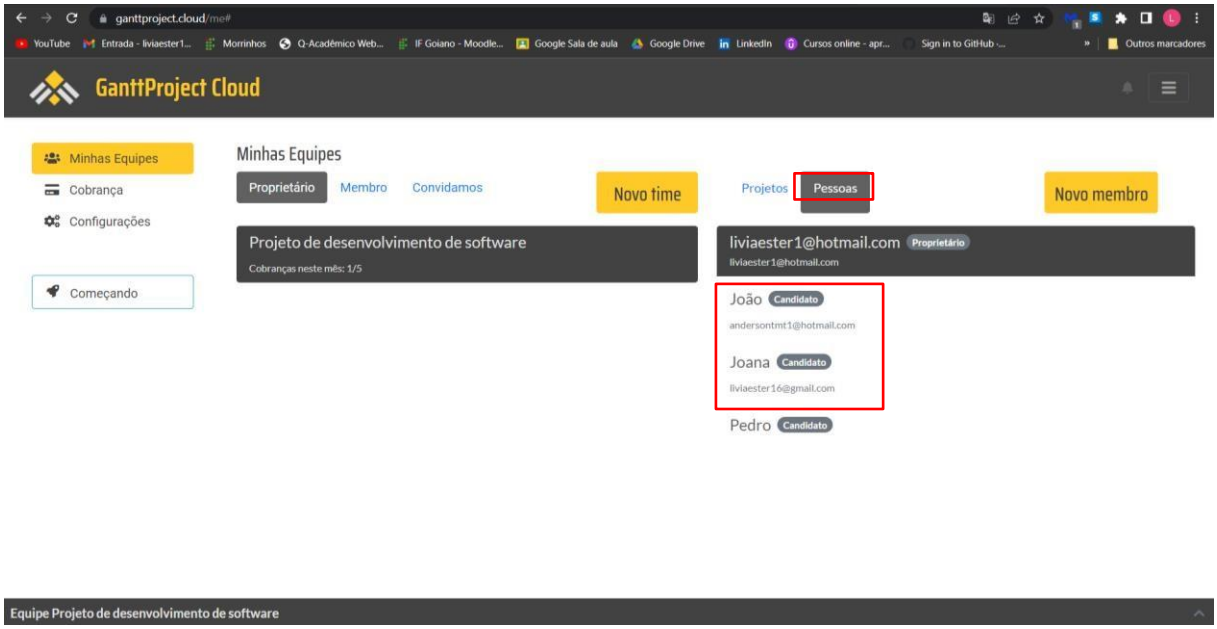

Figura 27 - Convidar pessoas para o projeto.

Para convidar a pessoa, é preciso clicar no ícone que aparece ao ir com o *mouse* sobre o nome da pessoa. Após isso é necessário preencher o nome e *e-mail* da pessoa e clicar em Enviar convite, conforme vemos na Figura 28.

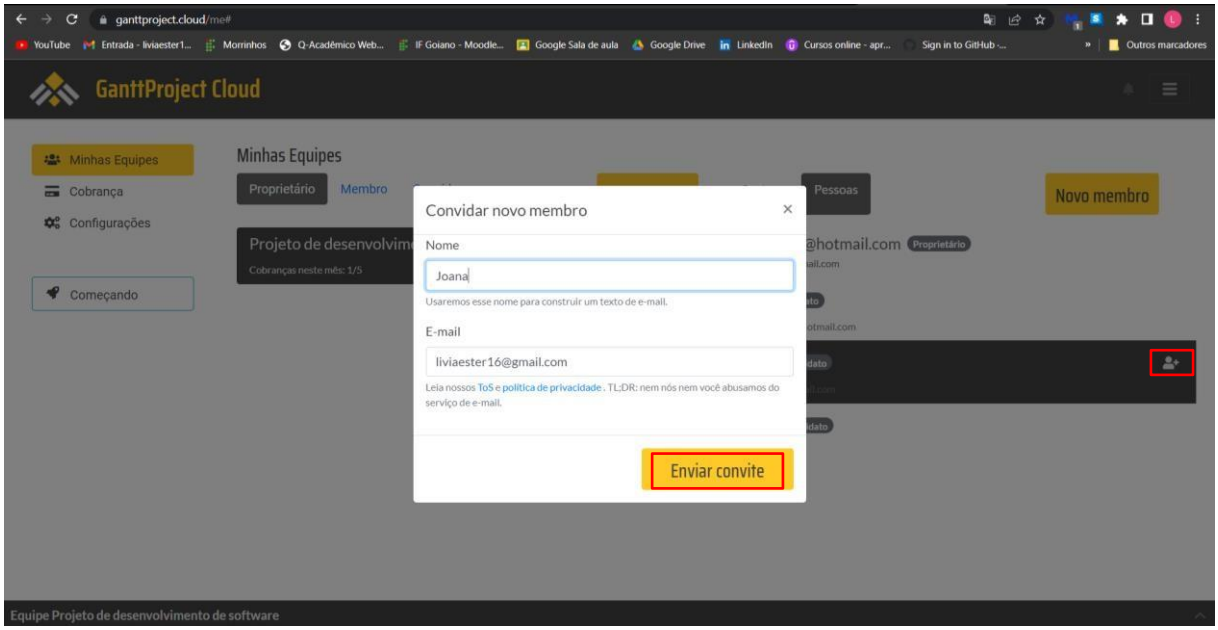

Figura 28 - Enviar convite.

6.6 UTILIZAÇÃO DO *GANTTPROJECT CLOUD* A PARTIR DE OUTRA MÁQUINA PARA OUTROS USUÁRIOS TEREM ACESSO AO PROJETO

A partir de outra máquina, é possível ver que o convite foi recebido no *e-mail* indicado. O próximo passo é acessar o *link* disponibilizado no *e-mail,* conforme mostra a Figura 29.

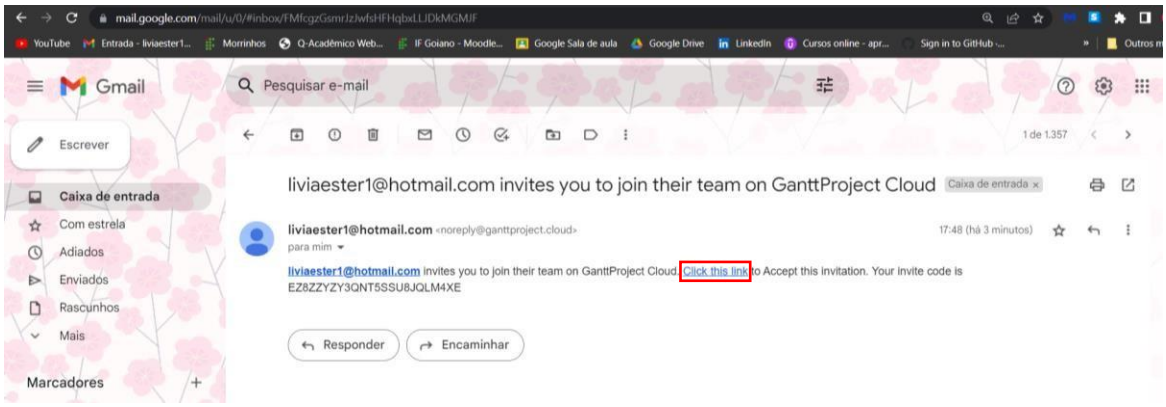

Figura 29 - Convite recebido no *e-mail*.

Ao acessar o *link* e já com o *login* do outro usuário conectado no *GanttProject Cloud*, é feito o redirecionamento para essa página do *GanttProject Cloud* conforme mostra a Figura 30, onde é possível visualizar o projeto.

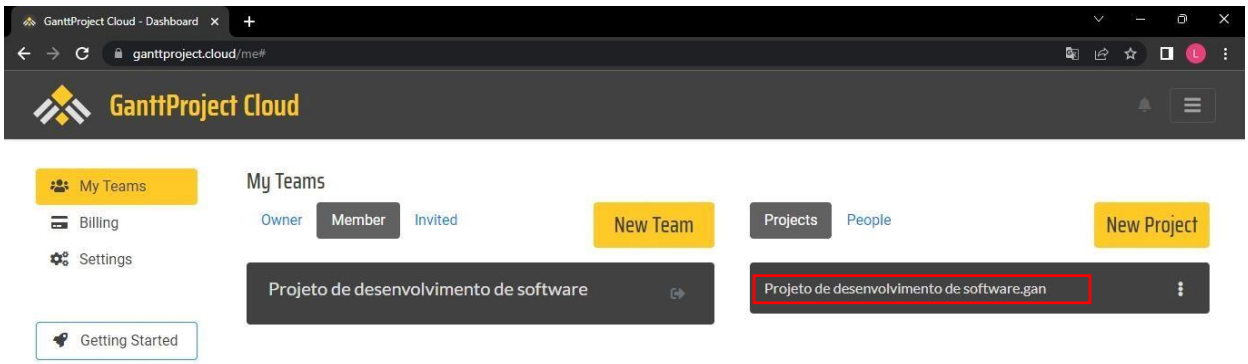

Figura 30 - Acesso ao projeto no *GanttProject Cloud* através de outra máquina.

Após conectado o usuário ao projeto através do *GanttProject Cloud*, é preciso abrir o *software* na máquina do usuário e conectar o *software* na nuvem, por meio da Barra de *Status* no lado inferior esquerdo, conforme Figura 20. Em seguida é necessário clicar em Projeto na Barra de Menus no canto superior esquerdo, clicar em

abrir, e clicar em Nuvem *GanttProject.* Feito isso, já é possível visualizar a pasta do projeto, conforme Figura 31.

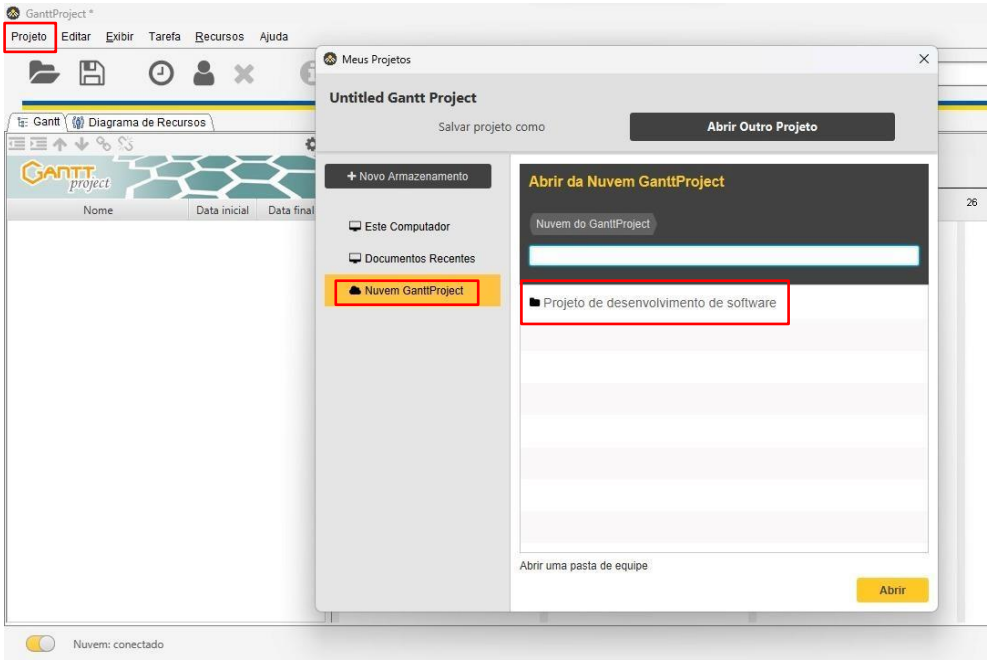

Figura 31 - Pasta do projeto criado em outra máquina.

Ao clicar na pasta do projeto, é possível ver o arquivo do projeto criado no *software*, conforme Figura 32. A seguir deve-se clicar em Abrir.

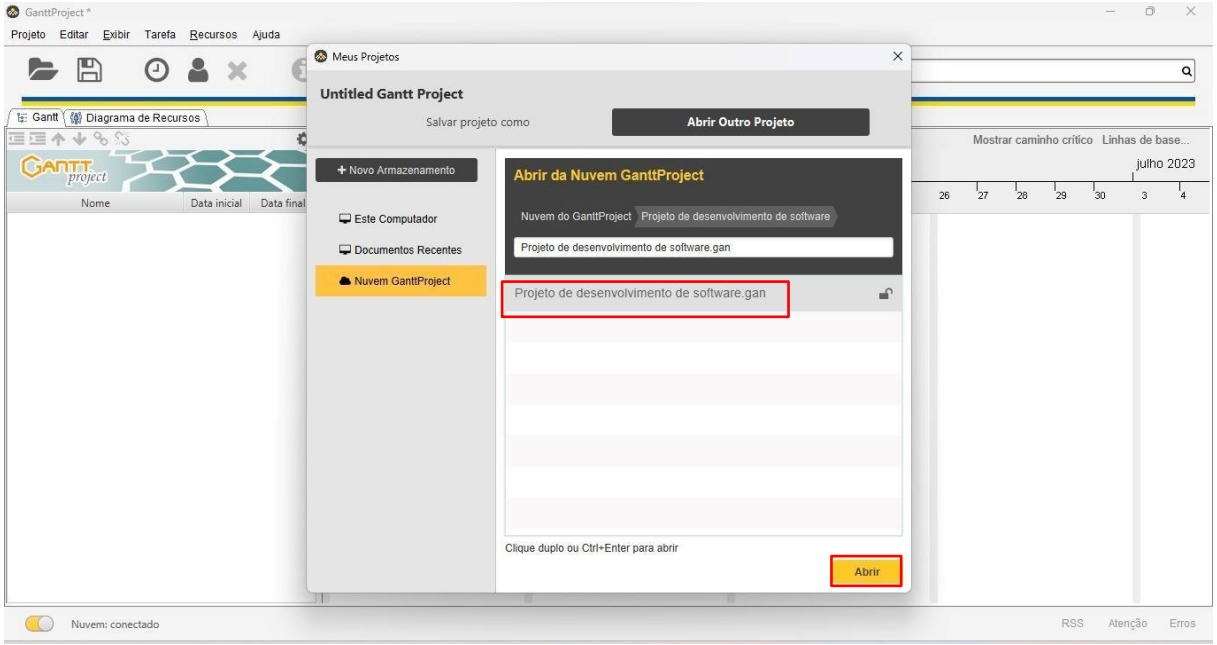

Figura 32 - Abrindo o projeto no *software* através de outra máquina por outro usuário.

Após isso, o acesso ao projeto é liberado, conforme mostra a Figura 33.

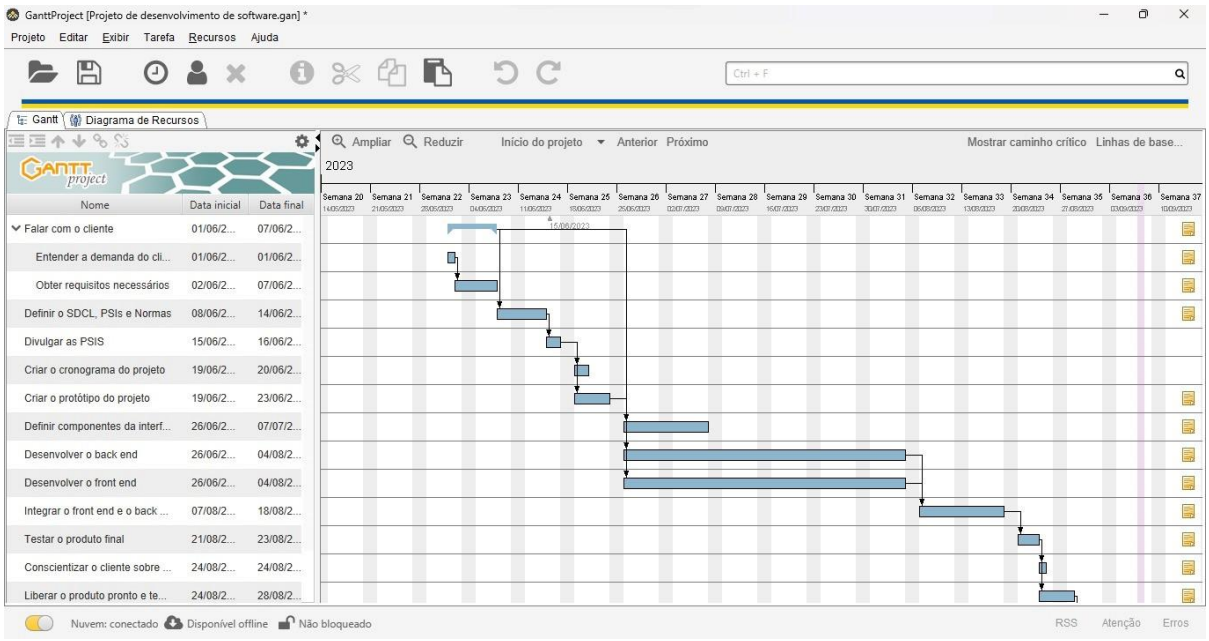

Figura 33 - Projeto aberto por outro usuário em outra máquina através do *software*.

O usuário conectado na máquina 2 agora pode alterar o projeto, criar novos colaboradores, atualizar o andamento do projeto e criar novas tarefas. Na Figura 34 vemos que o usuário criou um novo recurso com o nome Carolina. Para isso foi necessário acessar a aba Recursos na Barra de Menus, em seguida Novo recurso, e preencher as informações necessárias.

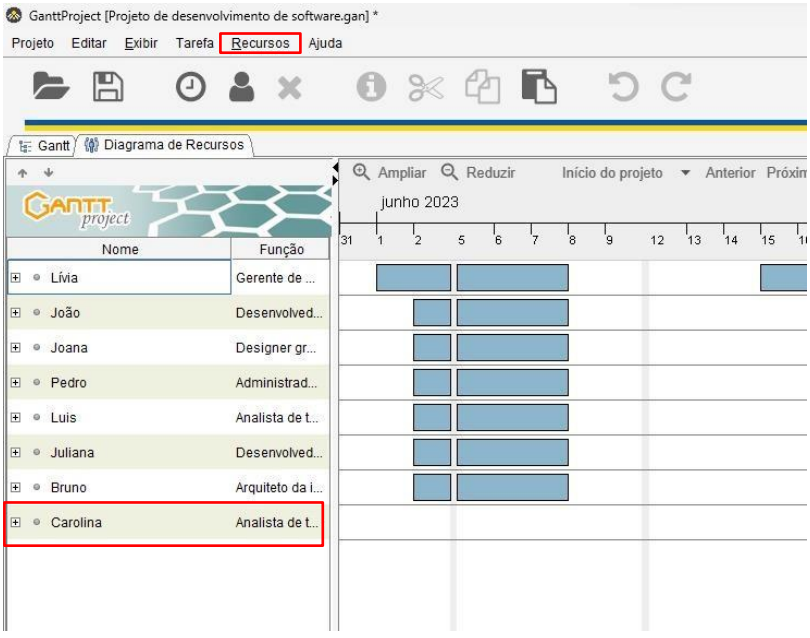

Figura 34 - Criação de novo usuário na máquina 2.

Após o usuário salvar o projeto na máquina 2, o usuário na máquina 1 será notificado de que existe uma atualização do projeto, conforme mostra a Figura 35.

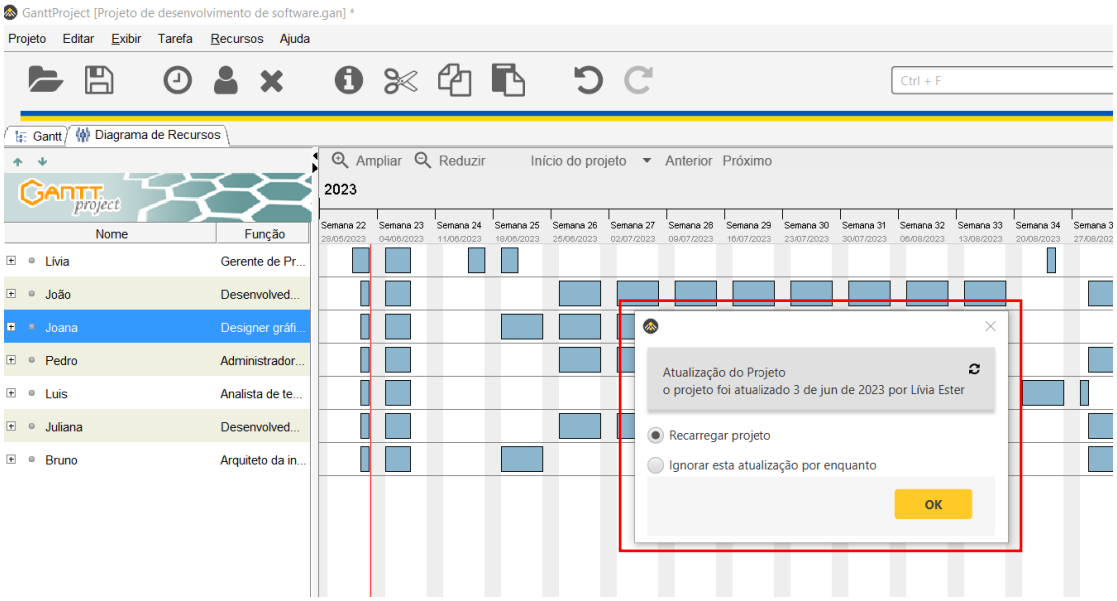

Figura 35 - Notificação de atualização do projeto na máquina 1.

A Figura 36 mostra o projeto atualizado na máquina 1 com as alterações realizadas na máquina 2. A nova integrante do projeto denominada Carolina, já está disponível na máquina 1.

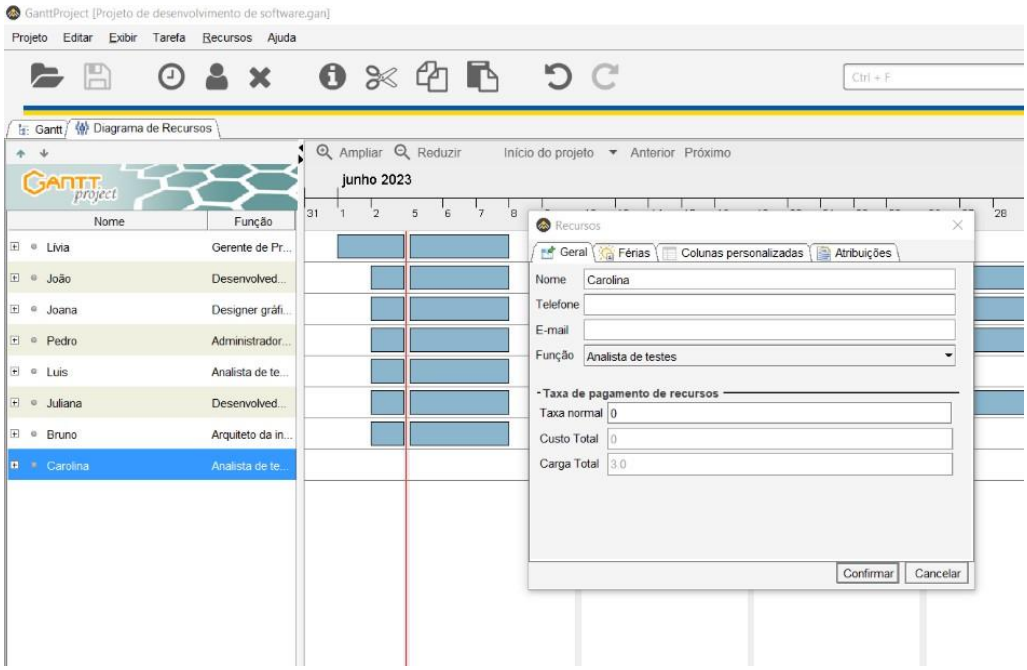

Figura 36 - Projeto atualizado na máquina 1.

Caso seja necessário, é possível bloquear alterações no projeto por determinado período, caso o gerente de projetos precise fazer alterações que não possam ser interrompidas, o ideal é bloquear o projeto. Caso o intuito do projeto seja ficar disponível só para a visualização das demais pessoas, é possível também que a pessoa responsável deixe o projeto bloqueado por várias horas, fazendo com que as outras pessoas possam apenas visualizá-lo.

Para isso é necessário acessar o *GanttProject Cloud*, em seguida clicar em Projetos, clicar sobre o Menu de Mais Opções ⋮ indicado na Figura 37 e clicar em Trancar.

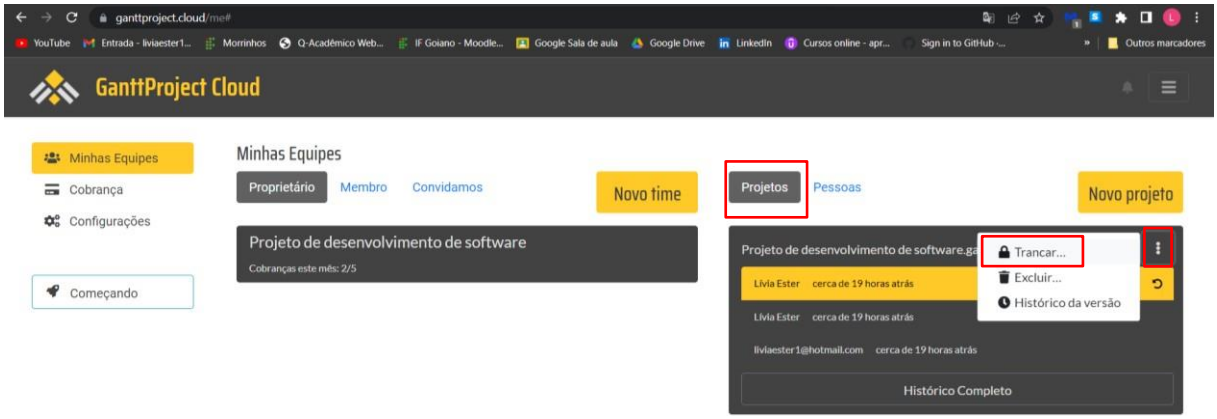

Figura 37 - Bloquear alterações no projeto.

Em seguida é o momento de selecionar a quantidade de horas que o projeto deverá permanecer bloqueado, e na sequência clicar na opção Trancar, conforme mostra a Figura 38.

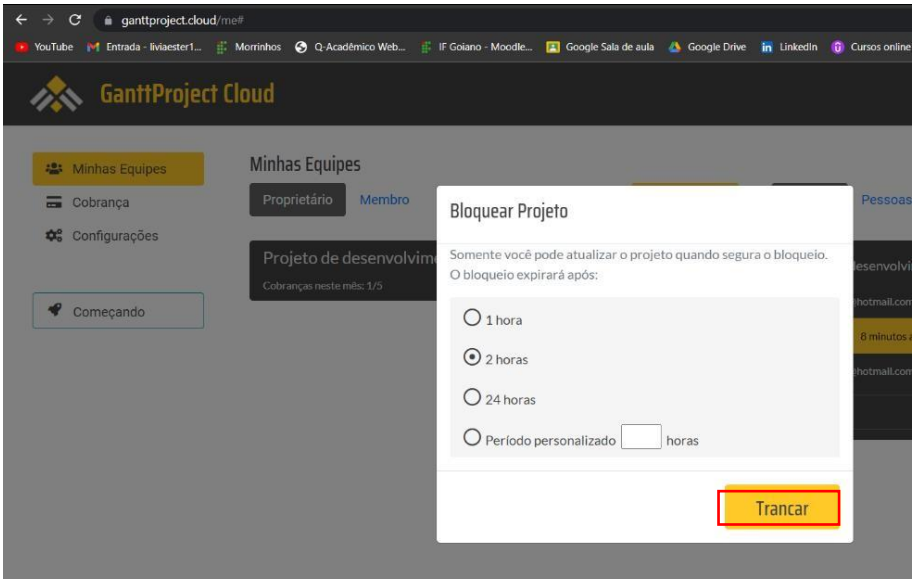

Figura 38 - Tempo para o bloqueio de alterações no projeto.

Após isso, é possível visualizar um cadeado ao lado do nome do projeto, que indica que o projeto está bloqueado para outros usuários, conforme mostra a Figura 39.

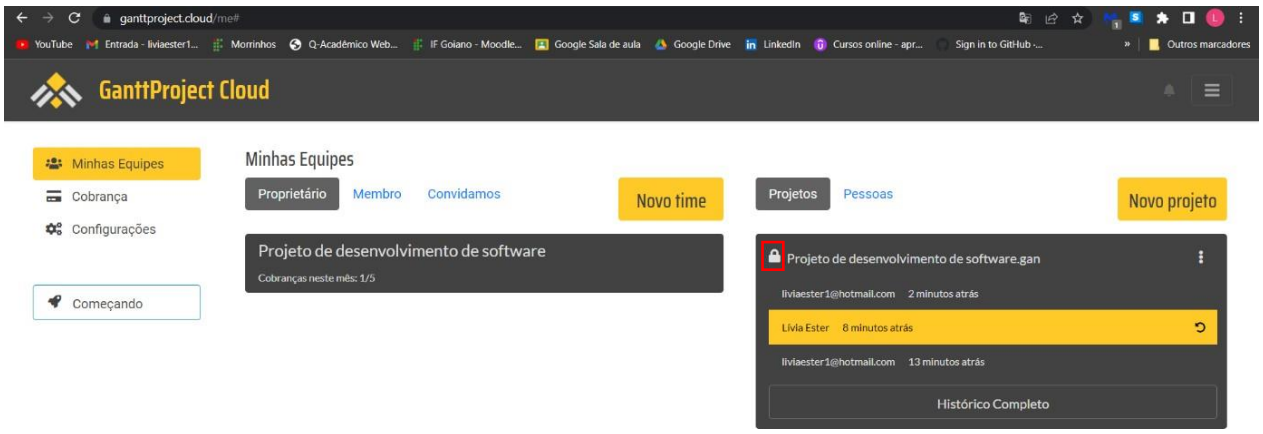

Figura 39 - Projeto bloqueado para outros usuários modificarem.

No *software*, podemos ver na Barra de Status que o projeto está bloqueado. Ao clicar sobre a palavra bloqueado, temos acesso à um menu onde é possível liberar bloqueio, manter o bloqueio já definido anteriormente no *GanttProject Cloud,* ou modificar o tempo do bloqueio, como mostra a Figura 40.

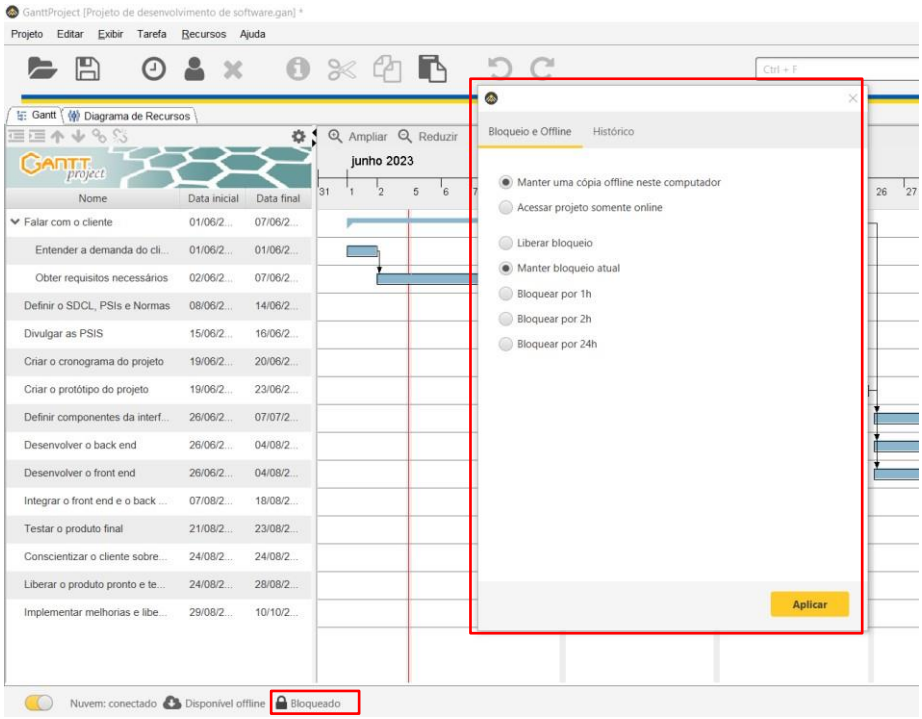

Figura 40 - Bloqueio do projeto no *software*.

Na máquina 2, quando outra pessoa tenta alterar o projeto depois deste ter sido bloqueado, aparece a mensagem exibida na Figura 41.

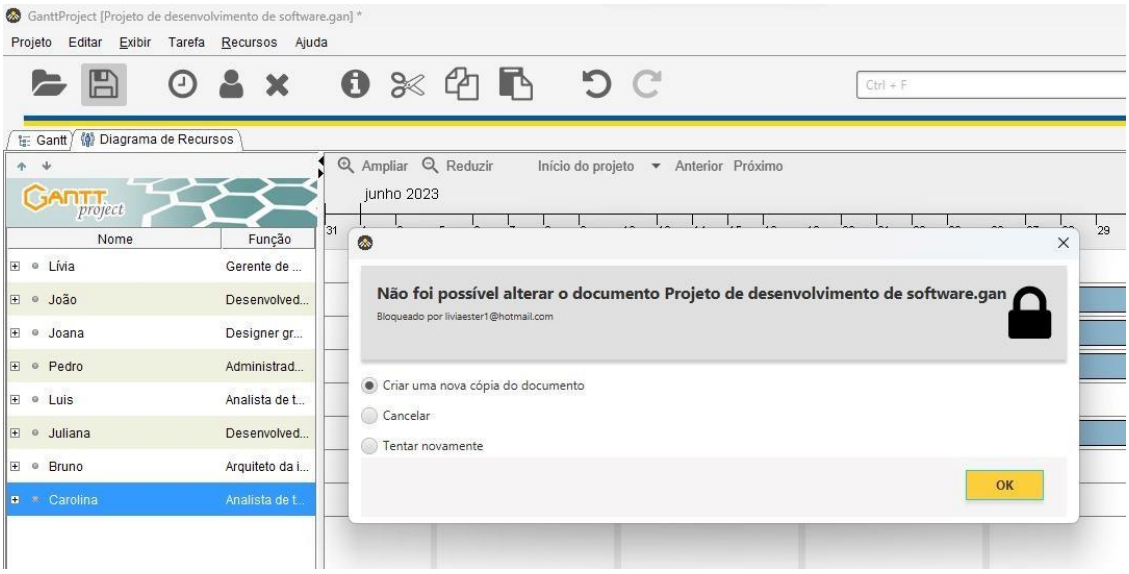

Figura 41 - Mensagem de projeto bloqueado.

Ainda na máquina 2, ao clicar sobre: Bloqueado por liviaester1@hotmail.com, é exibido a janela de bloqueio com as informações mostradas na Figura 42, inclusive a opção de mostrar notificação quando o bloqueio do projeto for liberado.

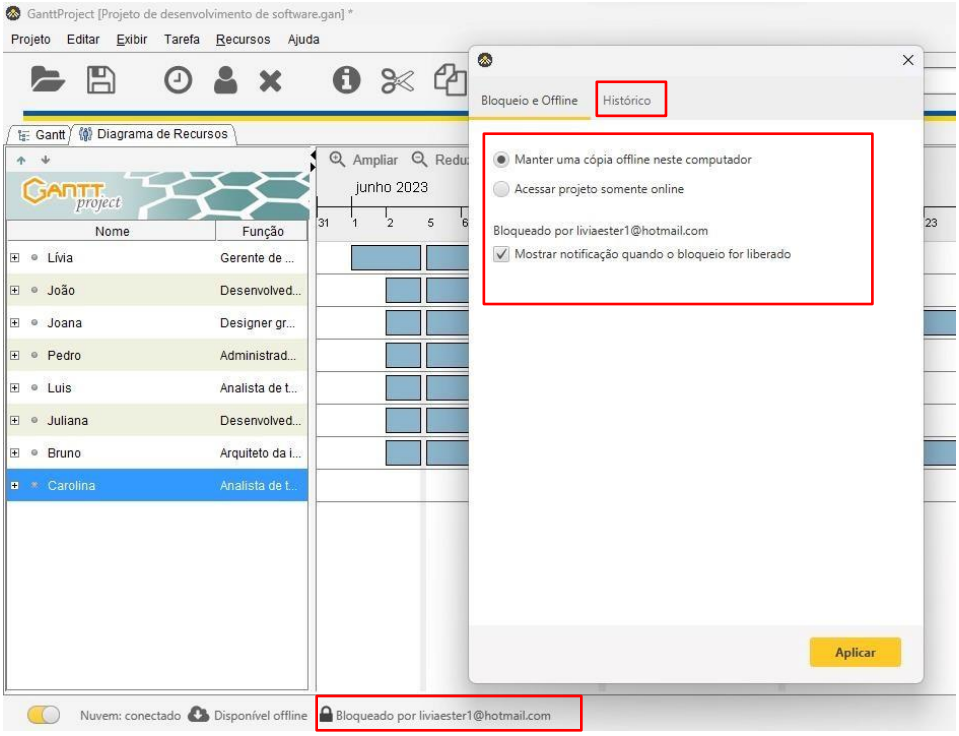

Figura 42 - Janela de bloqueio do projeto.

Ao clicar sobre Histórico, ao lado de Bloqueio e *Offline*, é exibido o histórico do projeto como mostra a Figura 43, onde é possível ter acesso às últimas versões e até mesmo obter a versão selecionada.

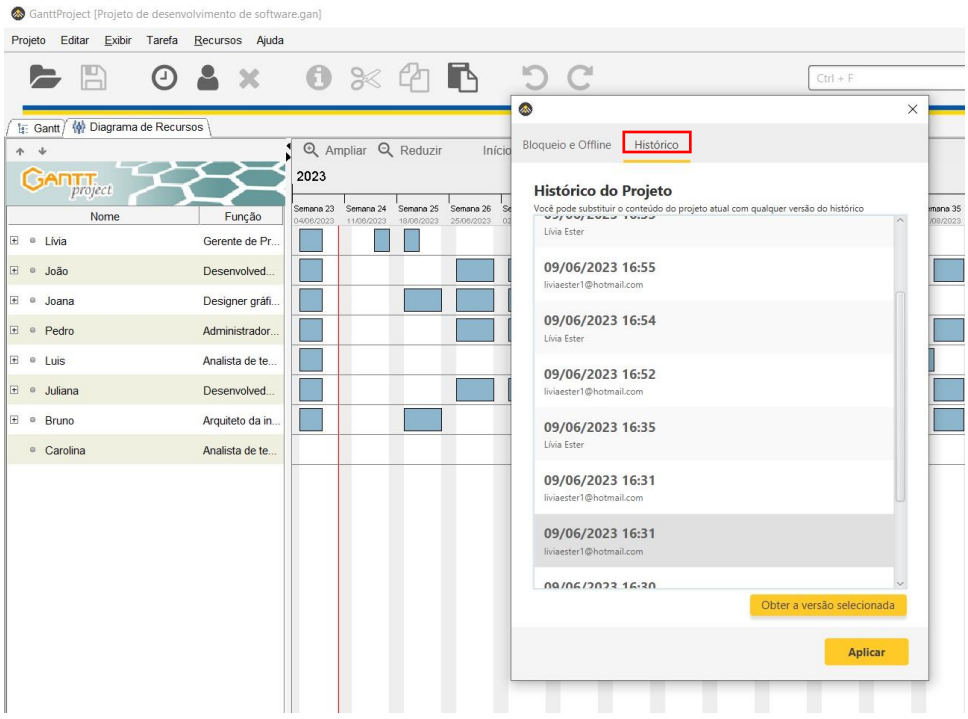

Figura 43 - Histórico do projeto no *software*.

É possível ter acesso ao histórico da versão do projeto também por meio do *GanttProject Cloud*, para isso é necessário clicar no ícone indicado, como mostra a Figura 44 e em seguida clicar em Histórico da versão.

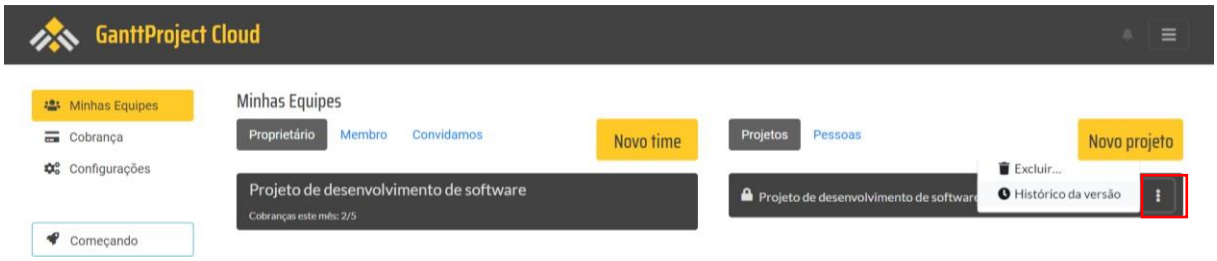

Figura 44 - Acesso ao histórico da versão do projeto no *GanttProject Cloud*.

Como mostra a Figura 45, podemos ter acesso à todas as últimas alterações do projeto e seus respectivos responsáveis.

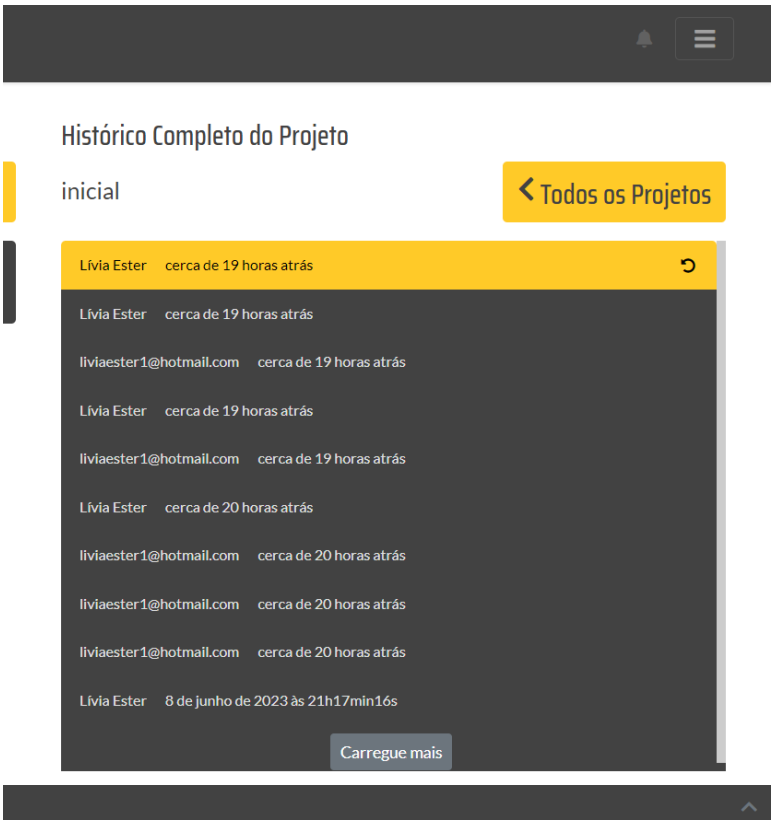

Figura 45 - Histórico completo da versão do projeto no *GanttProject Cloud*.

Além disso, com o *GanttProject Cloud* é possível reverter todo o projeto para a versão desejada, como é exibido na Figura 46.

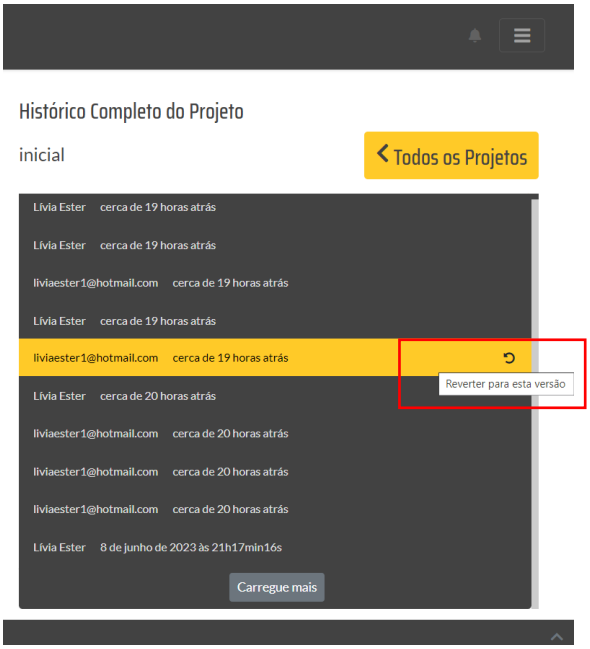

Figura 46 - Reverter o projeto para determinada versão.

O uso do *GanttProject Cloud* é gratuito para equipes com 2 membros. Equipes com mais de 2 membros devem pagar uma mensalidade de 1 euro por membro da equipe. Como podemos ver no *site* do *GanttProject Cloud* na Figura 47.

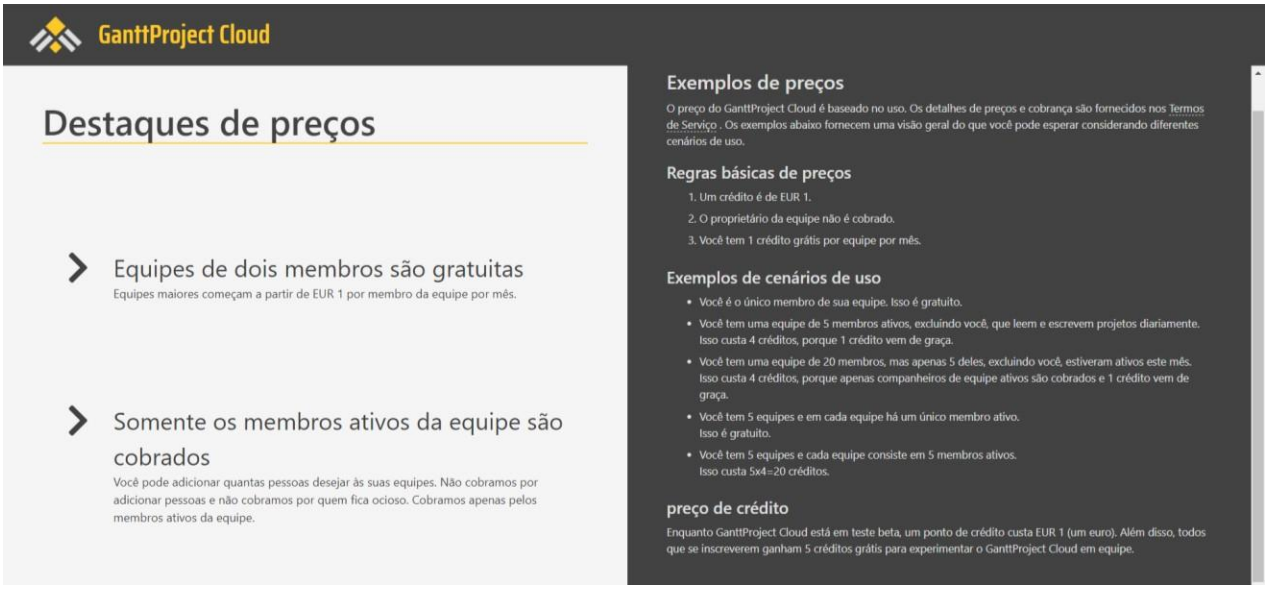

Figura 47 - Preços do *GanttProject Cloud*.

Como mostra a Figura 48, do lado esquerdo na aba cobrança, é possível visualizar os custos com o uso do *GanttProject Cloud*. Ao criar a conta no *site*, ganha-se 5,00 de crédito para testar. No caso abaixo, como há apenas 2 membros ativos

utilizando o *GanttProject Cloud*, está indicando o uso total de 2,00. Porém como até 2 membros o uso é gratuito, esse valor não aparece no total a ser pago.

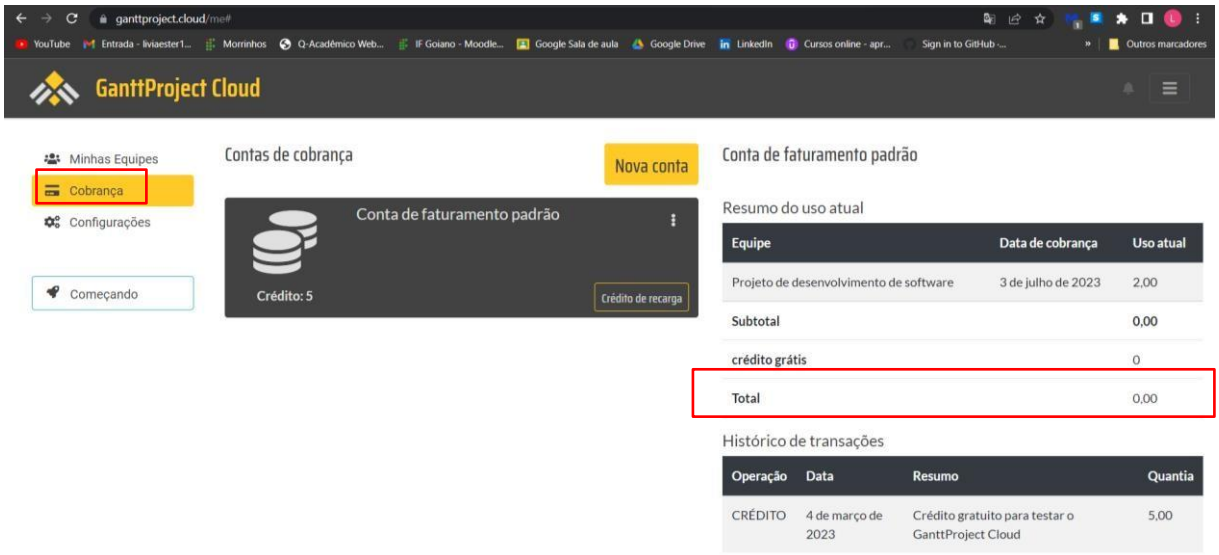

Figura 48 - Custo do *GanttProject Cloud* nesse projeto.

Para finalizar, do lado esquerdo na aba de Configurações, temos alguns dados que podem ser visualizados na Figura 49, e um deles é a possibilidade de exportar os dados das equipes, caso seja necessário.

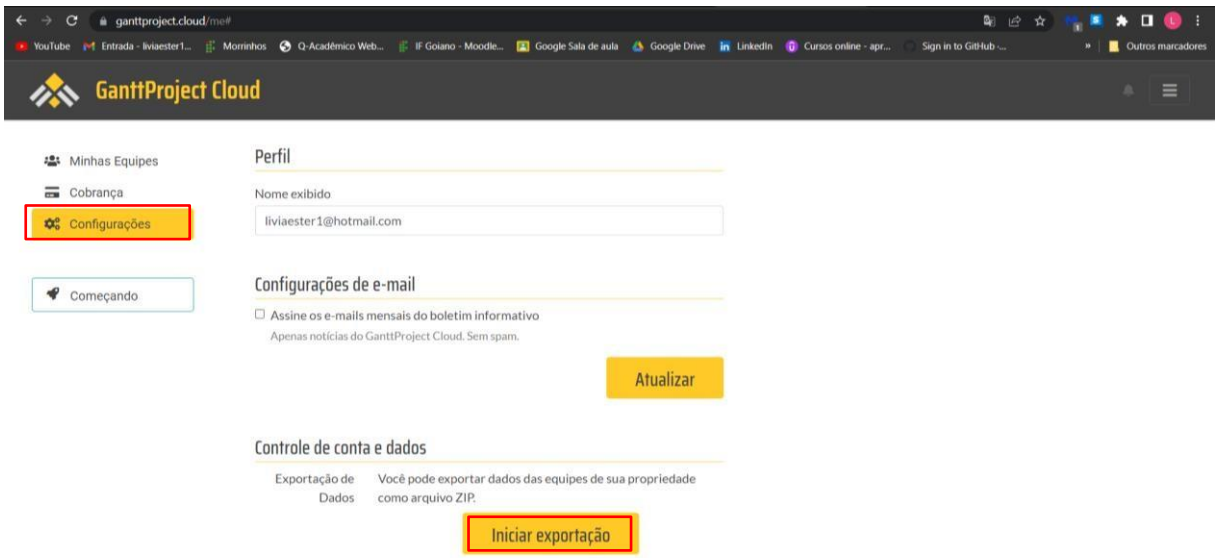

Figura 49 - Configurações do *GanttProject Cloud*.

6.7 EXEMPLOS DE UTILIZAÇÃO DE CICLO DE VIDA DE DESENVOLVIMENTO DE *SOFTWARE* (SDLC) NO *GANTTPROJECT*

Aqui apresenta-se os quatro SDLCs aplicados no *GanttProject*, conforme Figuras 50 a 54. Para esta pesquisa utilizou-se o Modelo em Cascata.

Os modelos exemplificados a seguir estão explicados no Capítulo 6.0 Desenvolvimento, no item 6.2 Política de Implementação do SDLC (Ciclo de Vida de Desenvolvimento de Software).

MODELO ESPIRAL

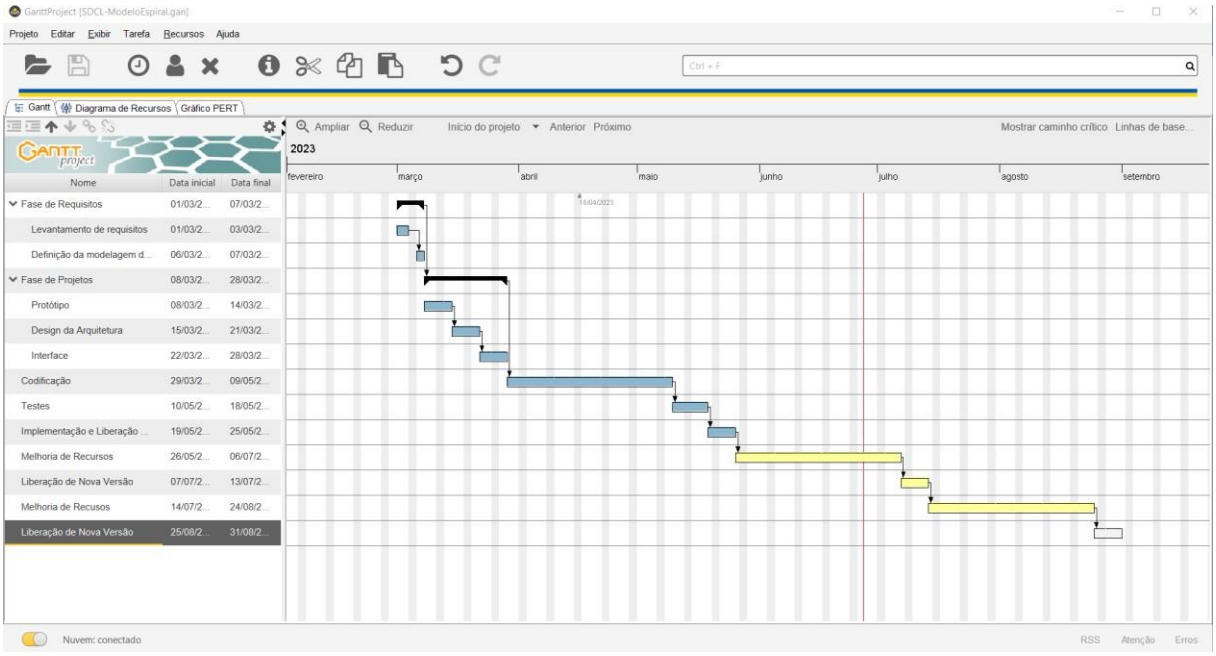

Figura 50 - Exemplo de ciclo de vida do modelo espiral.

MODELO INCREMENTAL

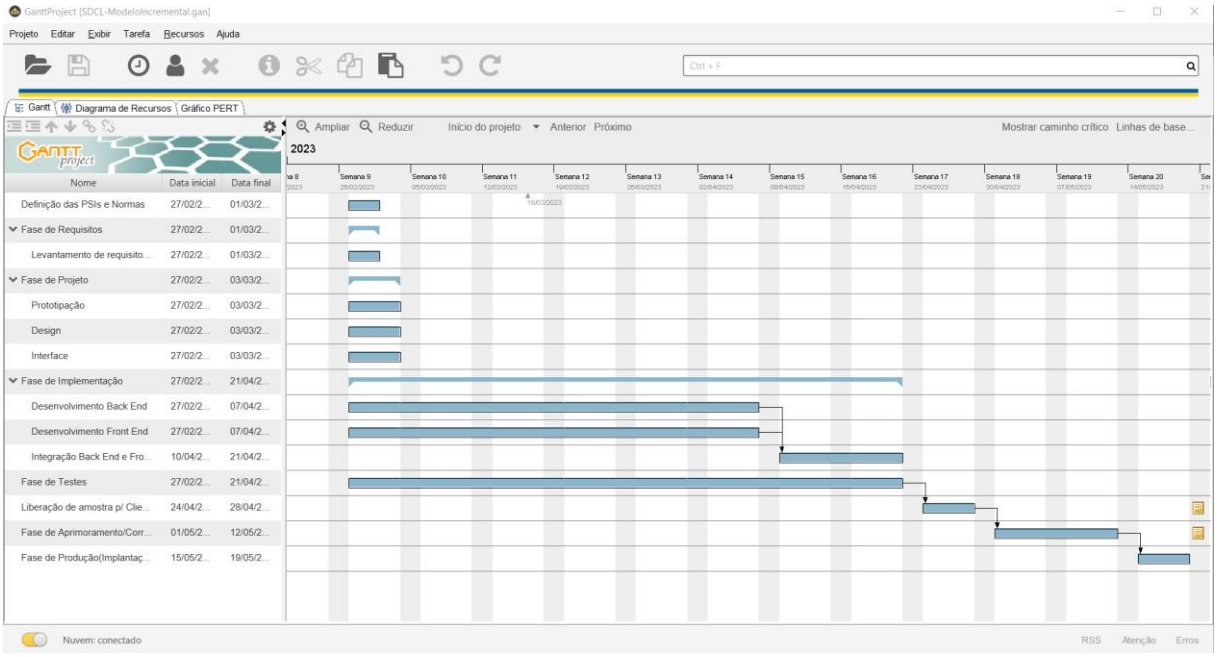

Figura 51 - Exemplo de ciclo de vida do modelo incremental.

MODELO EVOLUTIVO

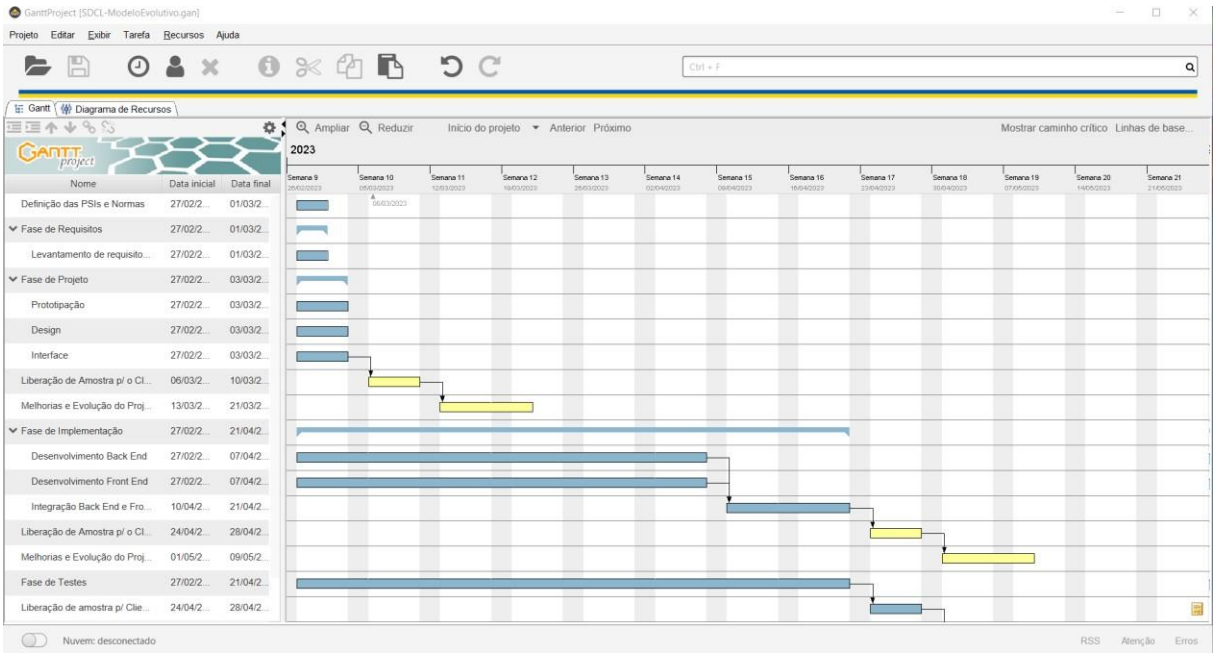

Figura 52 - Exemplo de ciclo de vida do modelo evolutivo.

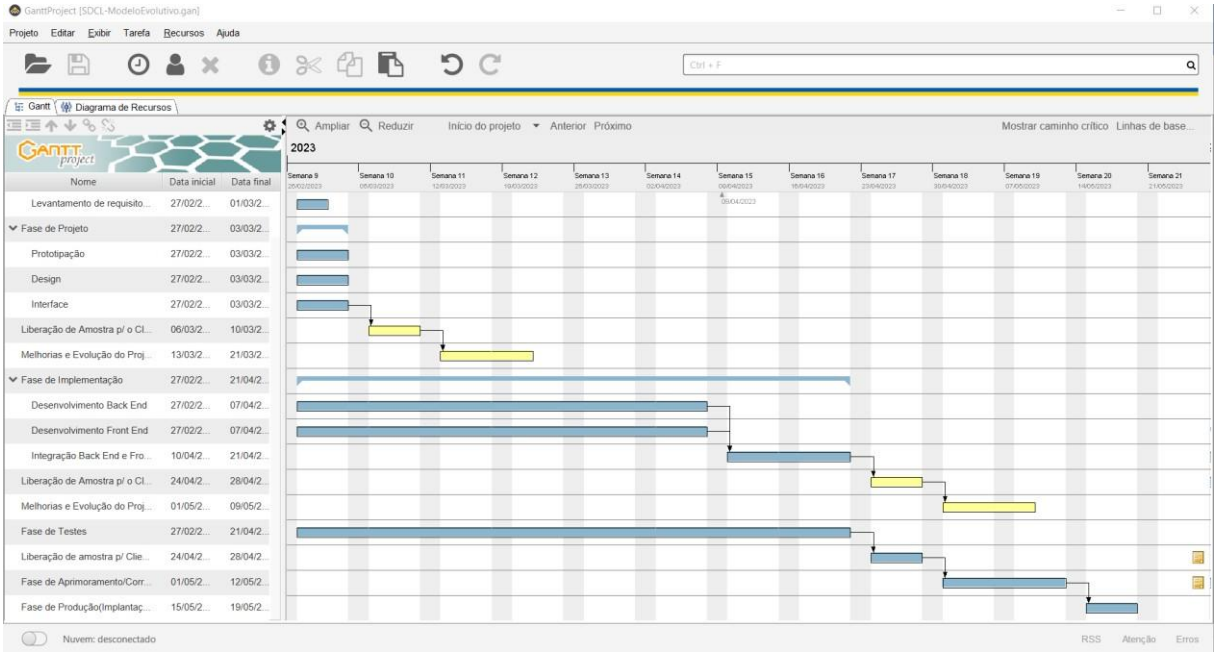

Figura 53 - Exemplo de ciclo de vida do modelo evolutivo continuação.

MODELO CASCATA

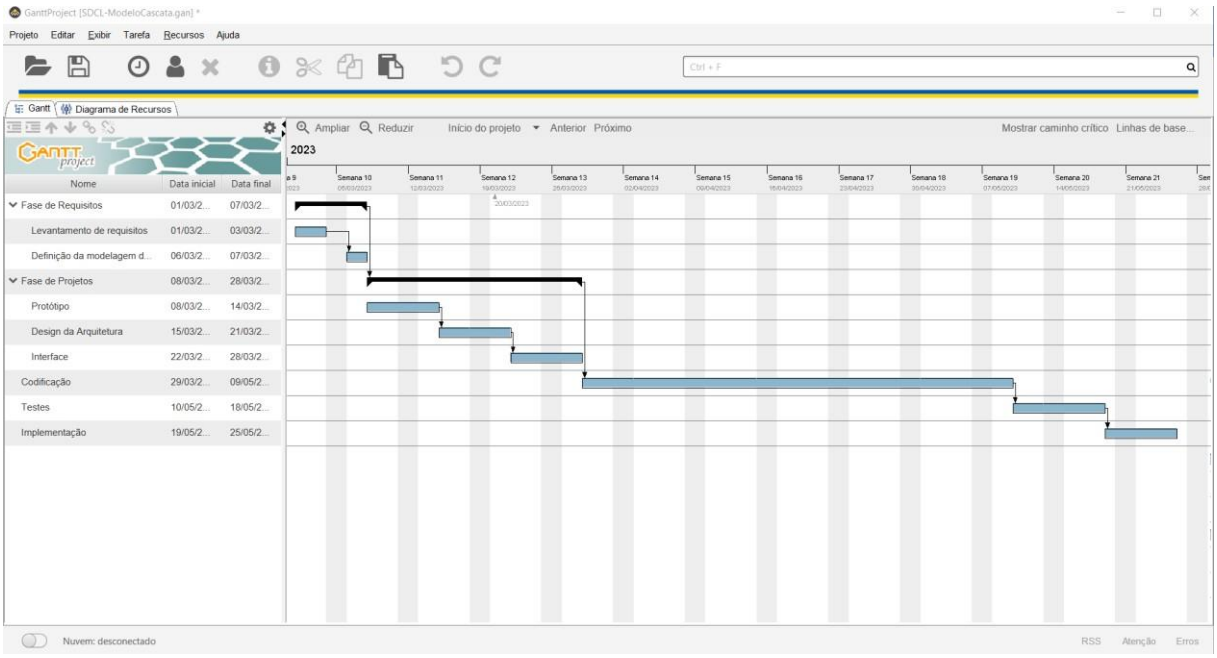

Figura 54 - Exemplo de ciclo de vida do modelo cascata.

7 CONCLUSÃO

Os esforços para o desenvolvimento de aplicações *web* seguras é um dos alicerces para disponibilizarmos, na rede mundial de computadores, produtos que garantam o mínimo de segurança para indivíduos e empresas. Com isso, toda a equipe envolvida no desenvolvimento desses projetos deve estar alinhada com foco na segurança e as Políticas de Segurança da Informação (PSI) têm se agregado de forma positiva neste cenário.

Neste trabalho foi criado e apresentado três PSIs com foco na Gerência de Projetos para o Desenvolvimento de aplicações *web* seguras. Esta pesquisa apresenta quatro Ciclos de Vida de Desenvolvimento de *Software* (SDLC), os quais norteiam que a equipe decide primeiro qual SDLC deve ser utilizado e seguido, para se ter êxito nas etapas e tarefas a serem realizadas, conforme cada PSI. As PSIs foram prototipadas por meio do *software* de gerenciamento de projetos *GranttProject.*

Com o auxílio da bibliografia correlata e execução do proposto nessa pesquisa, fica um exemplo de como a gerência de projetos, aliada a PSIs, OWASP e ISOs 27001 e 27002, podem agregar nas tomadas de decisão para a boa produtividade e desempenho de novos projetos para o desenvolvimento de aplicações *web* seguras, seja para iniciantes ou profissionais afins, que já estejam atuando no mercado de trabalho. Conclui-se que esse conhecimento contribui de forma positiva e significativa para a formação dos profissionais envolvidos com desenvolvimento de aplicações *web* seguras.

Para trabalhos futuros sugere-se criar novas PSIs explorando outras vulnerabilidades da OWASP *Top Ten* e ainda utilizar outros *softwares* de gerência de projetos como Trello, *Microsoft Project e* Primavera.

REFERÊNCIAS

ALTEFF, Fabricio Cordeiro. **APLICAÇÃO DE TÉCNICAS DE ETHICAL HACKING – DEMONSTRAÇÃO DO USO DE FERRAMENTAS E AMBIENTE DE ESTUDO PARA ACADÊMICOS OU INICIANTES EM SEGURANÇA WEB**. 2020. 68 f. TCC (Graduação) - Curso Superior de Tecnologia em Sistemas para Internet do Instituto Federal Goiano-Campus Morrinhos - GO, 2020.

ANPD. 2023. **Comunicação de incidente de segurança**. Disponível em: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis>. Acesso em: 22 jul. 2023.

AWS. 2023. **O que é SDLC?**. Disponível em: <https://aws.amazon.com/pt/what-is/sdlc/>. Acesso em: 25 jun. 2023.

COBEI. 2023. **Comitê Nacional Brasileiro da IEC.** Disponível em: <http://cobei.org.br/comite-nacional-da-iec/>. Acesso em: 23 jul. 2023.

CRONAPP, Redação. **Ciclo de vida do software: quais são as etapas e os modelos existentes?**. CRONAPP, 2020. Disponível em: <https://blog.cronapp.io/ciclo-de-vida-do-software/>. Acesso em: 24 maio. 2023.

DINIZ, Ana Laura Borsari; DINIZ, Débora Pelicano. **A ABNT NBR ISO/IEC 27701:2019 E A SEGURANÇA DA INFORMAÇÃO.** Revista Eletrônica de Computação Aplicada, Vol. 2, Nro. 2, p. 21-39, 2021.

DODT, Cláudio. **ISO 27001: Construindo Políticas de Segurança da Informação**. **Udemy, 2020.** Disponível em: <https://www.udemy.com/course/politicasegurancainformacao/>. Acesso em: 20 jun. 2023.

HANASHIRO, Akira. **Como funciona uma empresa de desenvolvimento de software?**. Treinaweb, 2019. Disponível em: <https://www.treinaweb.com.br/blog/como-funciona-uma-empresa-de-desenvolvimento-de-software>. Acesso em: 24 maio. 2023.

HINTZBERGEN, Jule; et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Rio de Janeiro: Brasport, 2018.

HSC Brasil, 2018. **Política de segurança da informação: o que é e como funciona?** Disponível em: <https://www.hscbrasil.com.br/politica-de-seguranca-da-informacao/>. Acesso em: 11 jun. 2023.

IEC. 2023. **Quem nós somos**. Disponível em: < https://www.iec.ch/who-we-are>. Acesso em: 23 jul. 2023.

ISO/IEC 27001:2013 - Os principais pontos da certificação. CCM, 2020. Disponível em: <https://blog.ccmtecnologia.com.br/post/iso-iec-27001-principais-pontos-da-certificacao>. Acesso em: 24 jun. 2023.

ISO/IEC 27002:2013 - Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Disponível em: <https://www.iso.org/standard/54533.html>. Acesso em: 23 jul. 2023.

MACORATTI, José Carlos. **O ciclo de vida do desenvolvimento de Software**. MACORATTI.NET, 2020. Disponível em: <https://www.macoratti.net/17/09/net_slcd1.htm>. Acesso em: 24 maio. 2023.

MICROSOFT. 2023. **Padrões de segurança no Azure AD.** Disponível em: <https://learn.microsoft.com/pt-br/azure/active-directory/fundamentals/security-defaults>. Acesso em: 05 ago. 2023.

MONTANHEIRO, Lucas Souza; CARVALHO, Ana Maria Martins. **Primeiros passos para o Desenvolvimento Seguro de Aplicações Web**. *In*: WORKSHOP DE TRABALHOS DE INICIAÇÃO CIENTÍFICA E DE GRADUAÇÃO - SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 18., 2018, Natal. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2018. p. 233 - 242.

NEVES, Denise Lemes Fernandes; et al. **A segurança da informação de encontro às conformidades da LGPD.** Revista Processando o Saber, Praia Grande, v.13, p. 186-198, Junho, 2021.

NITAHARA, Akemi. **Estudo mostra que pandemia intensificou uso das tecnologias digitais. Desigualdades de inclusão foram acentuadas**. Agência Brasil, Rio de Janeiro, 25 de nov. de 2021. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2021-11/estudo-mostra-que-pandemia-intensificou-uso-das-tecnologias-digitais>. Acesso em: 25 mar. 2023.

NOVAIS, Gustavo Gomes Dos Anjos; ARAÚJO, João Pedro Silva, SOUZA, Júlio Anderson Marques de. **Estudo taxonômico entre a Lei Geral de Proteção de Dados Pessoais e a ABNT NBR ISO/IEC 27001**. Orientador: Washington Fábio de Souza Ribeiro. 2020. 23f. Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) - Centro Universitário do Planalto Central Apparecido dos Santos, 2020. Disponível em: <https://dspace.uniceplac.edu.br/handle/123456789/909?mode=full>. Acesso em: 07 maio. 2022.

OLHAR DIGITAL. Conheça os golpes virtuais mais comuns na pandemia e saiba como se proteger. Olhar Digital, 2020. Disponível em: <https://olhardigital.com.br/2020/05/14/coronavirus/conheca-os-golpes-virtuais-mais-comuns-na-pandemia-e-saiba-como-se-proteger/>. Acesso em: 25 mar. 2023.

ORTEGA, F. D.; CÂMARA, C. D. **UM ESTUDO APLICADO A SEGURANÇA DE APLICAÇÕES WEB.** Revista Ubiquidade, v.4, n.2 – p. 85-125, jul. a dez. de 2021.

OSTEC. 2016. **ISO 27002: Boas práticas para gestão de segurança da informação.** Disponível em: <https://ostec.blog/padronizacao-seguranca/iso-27002-boas-praticas-gsi/>. Acesso em: 23 jul. 2023.

OWASP. 2023. Disponível em: <https://owasp.org/>. Acesso em: 30 maio. 2023.

OWASP Top 10:2021. 2021. Disponível em: <https://owasp.org/Top10/pt_BR/>. Acesso em: 07 abr. 2022.

OWASP Top Ten. 2023. Disponível em: <https://owasp.org/www-project-top-ten/>. Acesso em: 15 jun. 2023.

OWASP Top 10: 2021. **A07:2021 – Falhas de Identificação e Autenticação**. Disponível em: <https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/>. Acesso em: 28 jun. 2023.

PLANALTO, 2018. **Lei Nº 13.709 de 14 de agosto de 2018**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 15 jun. 2023.

APÊNDICE A - TERMO DE USO DE COMPROMISSO E RESPONSABILIDADE PARA COLABORADORES

Eu (nome do colaborador), afirmo que recebi as Políticas de Segurança da Informação, a saber PGSIAW, PSI01 e PSI02 da empresa e, afirmo que irei segui-las de acordo com tudo que é imposto pelas mesmas.

Sei que é meu dever e responsabilidade obedecer e apoiar o que é dito nas políticas para o bom funcionamento e segurança da empresa. É meu dever também ajudar na propagação das normas e políticas no ambiente organizacional, difundindo essa prática.

Tenho ciência de que sou responsável pelos meus atos e concordo em assumir todas as consequências que esses atos possam implicar, conforme a organização decidir.

Cidade-Estado, Dia, Mês e Ano.

_____

ASSINATURA ELETRÔNICA DO COLABORADOR