Prof. Ricardo Felipe Custódio

Memorial de Atividades Acadêmicas

Documento submetido a Universidade Federal de Santa Catarina como requisito para a promocao de Professor Associado, classe D, para Professor Titular da Carreira do Magisterio Superior, classe E, de acordo com a Resolucao Normativa No 40/CUn-UFSC/2014 e Portaria No 982/MEC/2013, de 03/10/2013.

Universidade Federal de Santa Catarina – UFSC

Departamento de Informática e de Estatística (INE)

Florianópolis, SC, Brasil

2017

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

ABIN	Agência Brasileira de Inteligência
CASNAV	Centro de Análises de Sistemas Navais
CEPESC	Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações
Certi	Centros de Referência em Tecnologias Inovadoras
CPqD	Centro de Pesquisa e Desenvolvimento em Telecomunicações
FINEP	Financiadora de Estudos e Projetos
HSM	Hardware Security Module
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ITA	Instituto Tecnológico da Aeronáutica
ITI	Instituto Nacional de Tecnologia da Informação
LabCAS	Laboratório de Computação Algébrica e Simbólica
LabGES	Laboratório de Tecnologias de Gestão
LabSEC	Laboratório de Segurança em Computação
RNP	Rede Nacional de Ensino e Pesquisa
UDESC	Universidade do Estado de Santa Catarina
UFSC	Universidade Federal de Santa Catarina

Sumário

Parte I

Preliminares

1 Identificação

Professor Ricardo Felipe Custódio, engenheiro (1985), mestre (1990) em Engenharia Elétrica pela Universidade Federal de Santa Catarina (UFSC) e doutor em Ciência da Computação (1999) pela Universidade Federal do Rio Grande do Sul. Foi professor substituto do Departamento de Engenharia Elétrica da UFSC no período de Novembro de 1991 a Agosto de 1992. Foi professor da Universidade do Estado de Santa Catarina (UDESC) de Agosto de 1992 a Abril de 1994, quando se transferiu para a UFSC. Fez estágio pós-doutoral em Certificação Digital na George Washington University, USA, nos anos de 2005 e 2006. Atualmente é professor do Departamento de Informática e de Estatística (INE) e supervisor do Laboratório de Segurança em Computação (LabSEC) da Universidade Federal de Santa Catarina. É membro permanente do Programa de Pós-graduação em Ciência da Computação (PPGCC) tendo orientado mais de 50 trabalhos de mestrado e teses de doutorado. É autor de mais de 80 artigos científicos, publicados em encontros científicos e revistas nacionais e internacionais. Tem realizado pesquisa científica e tecnológica na áreas de criptografia, com ênfase no documento eletrônico seguro, na gestão do ciclo de vida de chaves criptográficas e, mais recentemente, tem se dedicado a teoria e aplicações de corpos finitos.

2 Trajetória Acadêmica

Apresento o Memorial de Atividades Acadêmicas (MAA), instrumento para minha avaliação em exigência da Resolução Normativa Nº 40/CUn/2014, de 27 de maio de 2014, com alterações promovidas pela Resolução normativa Nº 69/CUn, de 31 de maio de 2016, documento de caráter descritivo, analítico, quantitativo e qualitativo, em que coloco em destaque os fatos marcantes e méritos acadêmicos de minha trajetória como docente, o qual apresentarei em defesa pública.

A Figura 1 mostra uma visão macro da minha formação acadêmica e os principais marcos relacionados às minhas atividades como estudante, professor e pesquisador.

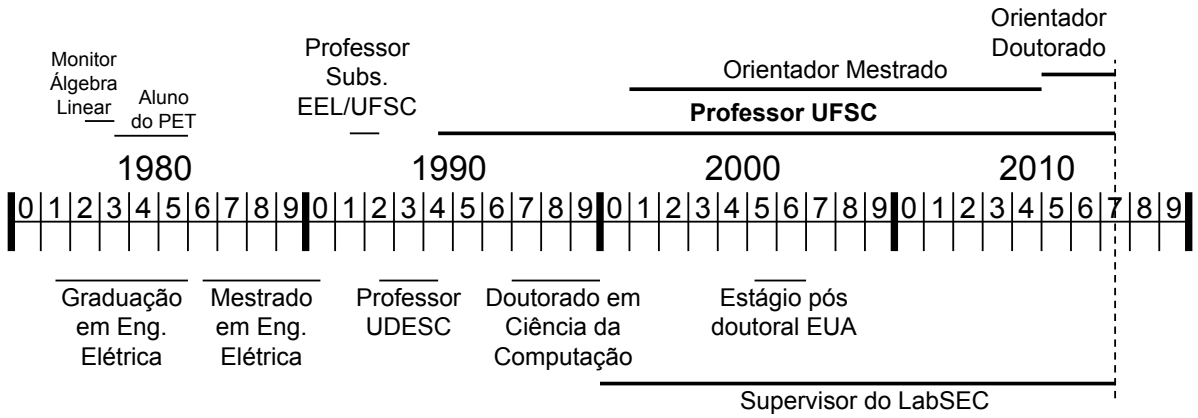

Figura 1: Linha do Tempo Acadêmica.

Conforme ilustra a figura, a década de 1980 foi dedicada aos cursos de graduação e mestrado em Engenharia Elétrica. Logo após fazer a disciplina de Álgebra Linear, encantei-me pelo assunto, e fui escolhido por um processo de seleção para me tornar monitor dessa disciplina na UFSC. Essa foi a minha primeira experiência como tutor. Em seguida entrei no Programa Especial de Treinamento (PET) promovido pela CAPES. Fiquei nesse programa até me formar engenheiro eletricista. Logo após finalizar a graduação, iniciei o meu mestrado no programa de pós-graduação em engenharia elétrica. O meu trabalho foi na área de processamento digital de sinais e estive vinculado ao Laboratório de Instrumentação Eletrônica (LINSE) do Departamento de Engenharia Elétrica da UFSC. O meu trabalho de mestrado consistiu na proposição de um codificador de sinais de voz, baseado na resposta ao multi-pulso (CUSTÓDIO, 1990).

A primeira metade da década de 1990 foi dedicada ao início de minha carreira como professor. A decisão já estava tomada em relação a minha vocação para ser professor e pesquisador. Decidi então submeter-me a concursos públicos para o ingresso na carreira de magistério superior. Inicialmente fui professor substituto no Departamento de Engenharia

Elétrica da UFSC. Em seguida, passei em um concurso para ser professor no Departamento de Ciência da Computação da Universidade do Estado de Santa Catarina (UDESC). Na UDESC, além de ministrar aulas, trabalhei na revisão do plano de informatização da universidade, no projeto da rede de comunicação de dados e no treinamento de técnicos administrativos.

Entretanto, o meu desejo era ser professor na UFSC, o qual prestei concurso e ingressei em Abril de 1994, tendo sito lotado no Departamento de Informática e Estatística (INE). Logo após o meu ingresso na UFSC, participei de forma ativa na construção do Laboratório de Computação Algébrica e Simbólica (LabCAS), onde fui incumbido de preparar um curso sobre o sistema de computação algébrica MAPLE (BREGMAN; ACHIM; AHAD, 1992).

Em 1996, após o estágio probatório obrigatório, fui avaliado pela comissão de avaliação de desempenho constituída pela portaria 08/INE/95 e sem nada que pudesse desabonar a aprovação para minha progressão funcional, fui contratado em caráter permanente por esta instituição.

Após essa primeira avaliação, rigorosamente fui progredindo na carreira de magistério superior, considerando o tempo mínimo exigido pela legislação, tendo sempre obtido pontuação em relação aos processos de avaliação, consideravelmente acima do esperado.

A segunda metade dessa mesma década foi dedicada ao doutoramento em Ciência da Computação. Eu ingressei em 1997 no Programa de Pós-Graduação em Computação (PPGC) da Universidade Federal do Rio Grande do Sul (UFRGS). O meu trabalho consistiu em estudar séries temporais caóticas através dos expoentes de Lyapunov. Eu desenvolvi um método para se determinar todo o espectro de Lyapunov e apliquei este método como uma técnica de detecção de diferentes sons pulmonares. O trabalho foi teórico e prático. A parte teórica foi, a partir de um modelo matemático usando um sistema de equações diferenciais ordinárias, propor um algoritmo para a extração dos expoentes de Lyapunov. A parte prática foi a implementação de um sistema de análise de sons pulmonares usando os expoentes de Lyapunov. Os principais resultados do trabalho estão na tese de doutorado (CUSTÓDIO, 1999) e em um artigo publicado em uma revista (OLIVEIRA; ROQUE; CUSTÓDIO, 1999).

Já as décadas de 2000 e 2010 foram dedicadas ao ensino de graduação e pós-graduação, à pesquisa científica e tecnológica e à construção do Laboratório de Segurança em Computação (LabSEC) o qual eu utilizei para a formação de alunos de graduação, mestrado e mais recentemente, alunos de doutorado. Também me dediquei à realização de atividades de extensão nessas duas décadas.

Desde meu ingresso na carreira acadêmica, tenho ministrado diversas disciplinas, seminários e cursos, tanto em nível de graduação quanto em nível de pós-graduação. Tam-

bém tenho realizado atividades de extensão, onde se pode destacar a minha participação no processo de informatização da Universidade do Estado de Santa Catarina (UDESC) e no desenvolvimento da plataforma criptográfica para a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Ao longo de minha carreira como pesquisador, tenho tido a honra de ter sido convidado para participar de bancas de avaliação de concursos para professores e bancas examinadoras de trabalhos de mestrado e doutorado.

Destaco, ainda como atividade administrativa a supervisão e coordenação dos laboratórios, Laboratório de Computação Algébrica e Simbólica (LabCAS) no ano de 1999/02 a 2000/01 e do Laboratório em Segurança da Computação (LabSEC) com início em 2000/02 até a presente data.

Creio oportuno descrever como foi criada a área de segurança computacional na UFSC. Quando retornei do meu doutorado, e a partir de consulta aos meus colegas à época, concluímos que deveríamos, de alguma forma, aplicar a nossa expertise em matemática simbólica, em teoria e aplicações de computação. Acreditávamos que dessa forma, poderíamos contribuir para a melhoria da qualidade, tanto dos nossos cursos de graduação quando os de pós-graduação em computação. Foi então que optamos pela criptografia e suas aplicações.

A criptografia exige profundos conhecimentos de matemática discreta e as aplicações são inúmeras, destacando-se, por exemplo, a segurança computacional e a assinatura digital de documentos eletrônicos.

Foi uma grande oportunidade para nós. Várias universidades no Brasil e no exterior estavam aprimorando os currículos dos cursos de computação, e entre as melhorias, estavam incluindo, como obrigatório, a disciplina de segurança computacional.

Assim, o nosso primeiro desafio foi criar e ministrar um curso de segurança computacional e criptografia na pós-graduação. Optamos por iniciar pela pós-graduação, com o objetivo de entendermos bem a nova área, e também poder iniciar alguns projetos de pesquisa científica e tecnológica. Após dois semestres consecutivos de cursos de segurança na pós, propomos uma disciplina optativa sobre segurança computacional na graduação. A disciplina foi um sucesso entre os alunos, que lotavam o curso, mesmo sendo optativo. Na primeira oportunidade que tivemos para modificar o currículo do nosso curso de graduação, incluímos a disciplina de segurança computacional com obrigatória.

Concomitantemente, criamos o grupo de pesquisa em segurança computacional e o laboratório de segurança em computação para abrigar os professores e alunos interessados em estudar, pesquisar e desenvolver projetos na área de segurança computacional. Como em qualquer universidade brasileira, não havia recursos para a instalação de um laboratório e também espaço físico disponível para tal. Assim, após conversas com a direção da

universidade, acordamos que a melhor alternativa seria a construção de um novo edifício para abrigar o laboratório que estava nascendo.

A partir de uma consulta pública sobre a implantação da Infraestrutura de Chaves Públicas Brasileira, tomei conhecimento sobre a necessidade de se criar, no Brasil, um centro de pesquisa e inovação tecnológica na área de certificação digital e suas aplicações. Aproveitei a oportunidade, e visitei o Instituto Nacional de Tecnologia da Informação (ITI), o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), a Financiadora de Estudos e Projetos (Finep), a Rede Nacional de Ensino e Pesquisa (RNP), o Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD) e outras agências que poderiam estar interessadas em investir na construção do nosso laboratório da UFSC. Por fim, em um esforço conjunto entre várias entidades, conseguimos recursos para construir um ambiente seguro (Sala Cofre) e também um prédio, para abrigar o nosso laboratório. A contrapartida seria que ficaríamos responsáveis pelas pesquisas e pelo desenvolvimento tecnológico, que ao final culminasse no desenvolvimento de uma plataforma criptográfica nacional, voltada à gestão confiável do ciclo de vida de certificados digitais.

O projeto de desenvolvimento da plataforma criptográfica foi batizado de *João de Barro*. Além da UFSC, participaram do projeto as seguintes instituições: Centro de Análises de Sistemas Navais (CASNAV), Instituto Tecnológico da Aeronáutica (ITA), Agência Brasileira de Inteligência (ABIN), Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC) e a Financiadora de Estudos e Projetos (FINEP).

Cada uma dessas entidades desempenhou um papel diferente para a consolidação do projeto. Ao longo de 2005, o CASNAV especificou os requisitos do João de Barro que foram entregues às outras instituições para que cada uma desenvolvesse os módulos de acordo com sua área de competência. Entre 2005 até agosto de 2006, o software foi projetado e consolidado pela UFSC.

No final de 2007, dada a necessidade imediata de emissão do novo par de chaves da ICP-Brasil, foi firmado um acordo de cooperação com a Rede Nacional de Estudo e Pesquisa (RNP) para a utilização do hardware desenvolvido pela UFSC para essa instituição.

Adotamos com estratégia, na UFSC, o envolvimento de alunos de graduação e de pós-graduação focados nos mais diversos desafios que, em conjunto, pudessem integrar a plataforma criptográfica. Após algum tempo, iniciamos o desenvolvimento dos sistemas computacionais, incluindo hardware e software, que iriam constituir a plataforma criptográfica. Paralelamente, construímos a sala cofre e o prédio para abrigar o nosso grupo de pesquisa.

Foi com grande alegria que, finalmente, em 2008, apresentamos o resultado final

do nosso trabalho. Os sistemas computacionais (software e hardware) ficaram prontos e foram implantados na Sala Cofre da Presidência da República, em Brasília, e também na Sala Cofre do Serviço Federal de Processamento de Dados (Serpro), no Rio de Janeiro. O Brasil passou a contar com uma solução nacional, desenvolvida em uma universidade brasileira. Cabe salientar que era muito importante que tal desenvolvimento fosse feito, uma vez que tal sistema precisava ser confiável e passível de auditoria.

Os principais resultados desse grande projeto foram:

1. Construção de um Ambiente Seguro (Sala Cofre) na UFSC;
2. Construção de um prédio para abrigar o Laboratório de Segurança em Computação (LabSEC);
3. Mais de 30 trabalhos de conclusão de cursos de graduação e trabalhos de mestrado orientados;
4. Vários artigos científicos publicados em encontros científicos e revistas especializadas, nacionais e internacionais;
5. Um hardware criptográfico, conhecido como Hardware Security Module (HSM), totalmente concebido na UFSC, para a gestão confiável do ciclo de vida de chaves criptográficas. Esse equipamento foi transferido para a iniciativa privada e hoje é um produto de sucesso, sendo utilizado por inúmeras empresas públicas no Brasil e no exterior.
6. Três sistemas de gerenciamento do ciclo de vida de certificados digitais: um para Autoridades Certificadoras Raiz; um para Autoridades Certificadoras Intermediárias; e um para Autoridades Certificadoras Finais.

É preciso esclarecer que o hardware criptográfico foi resultado de um Grupo de Trabalho, denominado Infraestrutura de Chaves Públicas para o Ensino e a Pesquisa (GT ICPEDU), financiados pela RNP. Esse foi mais um projeto que desenvolvemos no LabSEC. Como resultado desse projeto, tem-se:

1. Um sistema de gerenciamento do ciclo de vida de certificados digitais para a ICPEDU;
2. Um HSM;
3. Um sistema para a emissão automática de certificados digitais para correio eletrônico seguro (E-mail Seguro);
4. Um sistema de emissão de certificados digitais integrados a Federação Café;
5. Vários artigos científicos publicados.

Por fim, vale mencionar o projeto Cartório Virtual. Esse projeto, antes de mais nada, foi concebido como forma de motivar e de inspirar os alunos e professores a buscarem desafios práticos, relacionados à segurança da informação, que pudessem vir a ser alvos de investigação científica e tecnológica. Como resultado desse projeto, destacamos as pesquisas que foram feitas no sentido de se entender o ciclo de vida de documentos eletrônicos. Em termos de produtos, desenvolvemos a Protocoladora Digital de Documentos Eletrônicos, cujo projeto e tecnologia foi transferida para a iniciativa privada e hoje é um produto de sucesso de uma empresa nacional.

A Parte II desse documento apresenta as principais atividades e resultados obtidos em minha trajetória acadêmica. O texto foi dividido em capítulos, conforme a sugestão da Resolução Normativa Nº 40/CUn/2014, de 27 de maio de 2014. Por fim, acrescento em anexo, documentos que comprovam a meu percurso acadêmico.

3 Resumo do Desempenho Acadêmico

Este capítulo apresenta um resumo do desempenho acadêmico, em termos das atividades relacionadas no Artigo 5º. da Portaria nº. 981, de 3 de outubro de 2013, do Ministério da Educação.

Tabela 1: Resumo do Desempenho Acadêmico

Item	Atividade	Resumo
I	Atividades de ensino e orientação, nos níveis de graduação e/ou mestrado e/ou doutorado e/ou pós-doutorado.	Em todos os semestres, desde o ingresso na UFSC, foram ministradas, em média, duas disciplinas na graduação, à exceção dos períodos de afastamento para formação. A Seção 1.1 na página 19 lista todas as disciplinas ministradas. A Seção 1.2, página 21, lista as disciplinas ministradas na pós-graduação. Foram orientados 61 trabalhos de conclusão de curso de graduação. A Seção 1.3, na página 21 detalha os trabalhos orientados. Foram orientados 52 trabalhos de mestrado e doutorado, conforme detalha a Seção 1.4 na página 27.
II	Atividades de produção intelectual, demonstradas pela publicação de artigos em periódicos e/ou publicação de livros/capítulos de livros e/ou publicação de trabalhos em anais de eventos e/ou de registros de patentes/softwares e assemelhados; e/ou produção artística, demonstrada também publicamente por meios típicos e característicos das áreas de cinema, música, dança, artes plásticas, fotografia e afins.	Durante o período como professor da UFSC, procurou-se publicar artigos científicos para divulgar os trabalhos realizados. De forma resumida foram: • Livros Publicados: 1 • Capítulos de Livros: 3 • Artigos Científicos em Anais de Congressos: 70 • Artigos em Revistas: 12 • Softwares sem Registro: 17 • Produtos Tecnológicos: 7 A descrição detalhada da produção intelectual está apresentada no Capítulo 2, na página 32.
III	Atividades de extensão, demonstradas pela participação e organização de eventos e cursos, pelo envolvimento em formulação de políticas públicas, por iniciativas promotoras de inclusão social ou pela divulgação do conhecimento, dentre outras atividades.	Preocupação constante desde o ingresso como professor na UFSC foi a realização de atividades de extensão universitária. Procurou-se participar de encontros científicos, ajudar na organização de eventos, ministrar cursos, contribuir com documentos para a melhoria de políticas públicas e ajudar entidades, principalmente governamentais, na execução de atividades de tecnologia de informação consideradas complexas. O Capítulo 3, na página 45 lista as principais atividades de extensão realizadas no período avaliado.

IV	Coordenação de projetos de pesquisa, ensino ou extensão e liderança de grupos de pesquisa.	Como supervisor do LabSEC e líder do grupo de pesquisa de mesmo nome no CNPq, certificado pela UFSC, tenho realizado uma série de ações relacionadas a coordenação de projetos de pesquisa, ensino e extensão, conforme é apresentado no Capítulo 4, página 47. Essas ações culminaram no reconhecimento nacional e internacional do nosso grupo de pesquisa como de excelência na área de segurança computacional, em particular em criptografia e suas aplicações.
V	Coordenação de cursos ou programas de graduação ou pós-graduação.	Sempre tive como preocupação contribuir com a coordenação dos cursos de graduação e de pós-graduação, seja através de minha participação voluntária em comissões, ou através de participação nos órgãos colegiados. Detalhes no Capítulo 5, página 50.
VI	Participação em bancas de concursos, de mestrado ou de doutorado.	Foram um total de 83 bancas de mestrado e 8 de doutorado, sendo uma de doutorado na Alemanha. O Capítulo 6, na página 51 detalha as bancas do qual se fez parte ao longo da vida acadêmica.
VII	Organização e/ou participação em eventos de pesquisa, ensino ou extensão.	Ao longo da carreira acadêmica procurei organizar vários eventos científicos com o objetivo de promover a área de segurança computacional. Destaca-se o *Third International Conference on Cryptology and Information Security in Latin America* (Latincrypt 2014). O Capítulo 7, página 59 detalha os eventos que coordenei, alguns em cooperação com renomados professores.
VIII	Apresentação, a convite, de palestras ou cursos em eventos acadêmicos.	Ao longo da carreira acadêmica, eu fui convidado para ministrar muitas palestras em encontros científicos. O Capítulo 8.1, página 60, contém uma lista de algumas das palestras proferidas, bem como de cursos de curta duração ministrados.
IX	Recebimento de comendas e premiações advindas do exercício de atividades acadêmicas.	Ao longo de minha carreira fui homenageado formalmente em três ocasiões: Em 2003 pela ITA, na forma de uma menção honrosa por minha contribuição no simpósio de segurança da informação que era realizado regularmente nessa instituição; Em 2011, pelo ITI, pela minha contribuição para a ICP-Brasil; e em 2012, pela ALESC/Certi por minha contribuição para o desenvolvimento tecnológico de Santa Catarina. O Capítulo 9, página 64 traz maiores detalhes dessas homenagens.
X	Participação em atividades editoriais e/ou de arbitragem de produção intelectual e/ou artística.	Tenho procurado participar de forma ativa de comitês de programa de avaliação de artigos científicos em eventos na área da segurança da informação. Ao longo de minha carreira, participei de 22 eventos científicos avaliando artigos submetidos. O Capítulo 10, página 66 lista em detalhes cada um dos encontros científicos em que participei como avaliador.

XI	Assessoria, consultoria ou participação em órgãos de fomento à pesquisa, ao ensino ou à extensão.	A minha participação consiste na avaliação de projetos de pesquisa submetidos a agências de fomento. O Capítulo 11, página 68 detalha a minha participação.
XII	Exercício de cargos na administração central e/ou colegiados centrais e/ou de chefia de unidades/setores e/ou de representação.	A minha participação na administração na UFSC da-se através da supervisão do Laboratório de Segurança em Computação (LabSEC) e da participação nos colegiados dos cursos de graduação em computação e sistemas de informação e também no colegiado delegado do curso de pós-graduação em Ciência da Computação.

Parte II

Memorial de Atividades Acadêmicas: Detalhamento

1 Atividades de Ensino e Orientação

1.1 Ensino de Graduação

Iniciei as minhas atividades como docente na Universidade Federal de Santa Catarina em 1994, tendo sido lotado no Departamento de Informática e de Estatística. Desde então tenho ministrado diversas disciplinas para os cursos: Engenharias, Ciência da Computação e Sistemas de Informação.

Tabela 2: Disciplinas Graduação

Semestre	**Código**	**Disciplina**	**Créditos**
1994.1	INE5202	Cálculo Numérico em Computadores	4
1994.2	INE5202	Cálculo Numérico em Computadores	4
1995.1	INE5202	Cálculo Numérico em Computadores	4
	INE5207	Cálculo Numérico para Engenharia Elétrica	4
1995.2	INE5202	Cálculo Numérico em Computadores	4
	INE5305	Eletrônica para Computação	4
1996.1	INE5202	Cálculo Numérico em Computadores	4
1996.2	INE5202	Cálculo Numérico em Computadores	4
1999.2	INE5202	Cálculo Numérico em Computadores	4
	INE5207	Cálculo Numérico para Engenharia Elétrica	4
2000.1	INE5207	Cálculo Numérico para Engenharia Elétrica	4
	INE5372	Teoria da Computação	2
2000.2	INE5207	Cálculo Numérico para Engenharia Elétrica	4
	INE5351	Tópicos Especiais em Arquitetura de Computadores I	3
2001.1	INE535	Tópicos Especiais em Arquitetura de Computadores I	3
	INE5382	Introdução à Computação	6
2001.2	INE5351	Tópicos Especiais em Arquitetura de Computadores I	3
	INE5382	Introdução à Computação	3
2002.1	INE5351	Tópicos Especiais em Arquitetura de Computadores I	3
	INE5602	Introduçõa à Informática	4
2002.2	INE5351	Tópicos Especiais em Arquitetura de Computadores I	3
	INE5382	Introdução à Computação	6
2003.1	INE5383	Desenvolvimento de Sistemas Orientados a Objetos	6
	INE5386	Segurança em Computação	4
2003.2	INE5386	Segurança em Computação	4
2004.1	INE5383	Desenvolvimento de Sistemas Orientados a Objetos	3
2004.2	INE5383	Desenvolvimento de Sistemas Orientados a Objetos	6

2005.1	INE5383	Desenvolvimento de Sistemas Orientados a Objetos	6
	INE5605	Desenvolvimento de Sistemas Orientados a Objetos I	2
2006.2	INE5386	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2007.1	INE5386	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2007.2	INE5386	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2008.1	INE5386	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2008.2	INE5386	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2009.1	INE5386	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2009.2	INE5386	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2010.1	INE5429	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2010.2	INE5429	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2011.1	INE5429	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2011.2	INE5429	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2012.1	INE5429	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
	INE5449	Tópicos Especiais em Aplicações Tecnológicas II	4
2012.2	INE5429	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2013.1	INE5429	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2013.2	INE5429	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2014.1	INE5429	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2014.2	INE5429	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4
2015.1	INE5429	Segurança em Computação	4
	INE5601	Fundamentos Matemáticos da Informática	4

1.2 Ensino de Pós-Graduação

Em três de maio de 1999 fui credenciado como professor permanente do Curso de Pós-Graduação em Ciências da Computação da UFSC, dando início as minhas atividades de orientação de mestrado e ministração de disciplinas regulares ou de tópicos especiais avançados nesse programa de pós-graduação. A Tabela 3 lista o conjunto de disciplinas que foram ministradas.

Tabela 3: Disciplinas de Pós-Graduação

Trimestre	**Código**	**Disciplina**	**Créditos**
1999.3	INE410098	Tópicos Especiais em Redes de Computadores: Criptografia e Segurança em Redes de Computadores	3
	INE6906000	Criptografia e Segurança em Redes de Computadores	3
2000.1	INE6906000	Criptografia e Segurança em Redes de Computadores.	3
2000.3	INE6401000	Arquitetura de Redes de Computadores	
2001.1	INE410066	Segurança em redes de Computadores	3
2002.2	INE410066	Segurança em redes de Computadores	3
2008.2	INE410012	Tópicos Especiais em Computação Paralela e Distribuída: Special Aspects of Distributed Embedded Real-Time Systems	3
	INE6904000	Infraestrutura de Chaves Públicas	3
2009.2	INE410007	Tópicos Avançados em Infraestrutura de Chaves Públicas	3
2010.3	INE410007	Tópicos Avançados em Infraestrutura de Chaves Públicas	3
2011.2	INE6904000	Infraestrutura de Chaves Públicas	3
2012.3	INE410093	Tópicos Especiais em Computação	3
2013.2	INE410120	Tópicos Especiais em Computação: Infraestrutura de Chaves Públicas e Aplicações.	3
2014.2	INE410120	Tópicos Especiais em Computação: Infraestrutura de Chaves Públicas e Aplicações.	3
2015.1	INE410120	Tópicos Especiais em Computação: Infraestrutura de Chaves Públicas e Aplicações.	3

1.3 Orientações em Nível de Graduação

Desde que retornei do meu doutorado, procurei orientar trabalhos de conclusão de curso. Inicialmente alunos do curso de Ciência da Computação e posteriormente, também, alunos do curso de Sistemas de informação. A maioria dos meus orientandos desenvolvia trabalhos dos laboratórios que eu coordenei. Inicialmente o Laboratório de Computação Algébrica e Simbólica (LabCAS) e posteriormente o Laboratórios de Segurança em Computação (LabSEC). Na maioria das vezes, como forma de incentivo, eu procurei por

agências de fomento ou empresas que pudessem financiar esses alunos. Quase a totalidade desse alunos fizeram seus trabalhos tendo bolsas de iniciação científica ou de extensão. Assim esses alunos puderam se dedicar integralmente aos estudos e ao desenvolvimento de seus trabalhos. Foi uma atividade muito enriquecedora, pois permitiu-me maior aproximação dos alunos, onde muitos deles vieram a ser alunos de Pós-Graduação em nível de mestrado e doutorado sob minha orientação. Um total de 61 trabalhos de conclusão de curso de graduação foram orientados. As declarações que disponibilizo, comprovam minhas orientações nesta atividade.

1. Ricardo Vieira Losso. Protocoladora Digital de Documentos Eletrônicos. 2000.2. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

2. Antônio Cesa da Silveira Júnior. Protocoladora Digital de Documentos Eletrônicos. 2000.2. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

3. Fabiano Castro Pereira. OSTRACON: Sistema de Votação Digital Segura Através da Internet. 2001.1 Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

4. Carlos Eduardo Mazzi. OSTRACON: Sistema de Votação Digital Segura Através da Internet. 2001.1 Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);.

5. Juliano Vieceli. Consulta de Processos no Tribunal de Justiça do Estado de Santa Catarina via Dispositivos WAP. 2001. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

6. Cristiano Freccia. Consulta de Processos no Tribunal de Justiça do Estado de Santa Catarina via Dispositivos WAP. 2001.1. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

7. Marcelo Digiácomo Chryssovergis. Emissão de Certidão de Nascimento na WEB. 2001.1. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

8. Jean Everson Martina. Emissão de Certidão de Nascimento na WEB. 2001.1. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

9. Fauze Valério Polpeta. Sistema Seguro de Atendimento ao Cliente via WEB. 2002.01. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

10. Iomani Engelmann Gomes. Validação de Certificados Digitais. 2002. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

11. André Theodoro Carlucci. Fax Seguro. 2003. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

12. Bruno Maluche Neto. Validação de Certificados Digitais. 2003. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);.

13. Carlos Francisco Tatara. S2Card. 2003. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

14. Victor Simas Silva. Sistema de Compras Seguro. 2003. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

15. Iuri Campana. Sistema de Compras Seguro. 2003. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

16. Marcos Aurélio Dias. Auditoria Interna e Externa da Protocolizadora Digital de Documentos Eletrônicos. 2003. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

17. Cleyton André Pires. Auditoria Interna e Externa da Protocolizadora Digital de Documentos Eletrônicos. 2003. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

18. Giovane Pasa. Implementação de um sistema seguro de auditoria de publicidade na WEB. 2003. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

19. Fernando José Karl. Implementação de um sistema seguro de auditoria de publicidade na WEB. 2003. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

20. Túlio V. Duarte Christofoletti. Cupom Fiscal Seguro. 2004. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

21. Roberta Cavalcanti de Brito. Cupom Fiscal Seguro. 2004. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

22. Vitor Claudino dos Santos. Sincronização seguro de relógios na Internet. 2004. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

23. Bruno Leonardo Martins de Melo. Sincronização seguro de relógios na Internet. 2004. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

24. Rodrigo Muller Pons. Formulários Eletrônicos Seguros. 2004. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

25. Marcelo Carlomagno Carlos. Formulários Eletrônicos Seguros. 2004. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

26. Rafael Despindola Correa. Sistemas de Gerenciamento de Conteúdo para Web: Uma Avaliação dos Principais Tipos de Wikis. 2005.1. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

27. João Antônio N. Ramos Neto. Sistemas de Gerenciamento de Conteúdo para Web: Uma Avaliação dos Principais Tipos de Wikis. 2005.1. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);.

28. Leandro Amâncio. Autoridade de Aviso. 2004. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

29. Eduardo Bruno Hadlich. Autoridade de Aviso. 2004. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

30. José Manuel Ramírez Núñez. IBE aplicado à Criptografia Temporal. 2004. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

31. Luciana Schmitz. Implantação Webmail Seguro. 2004. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

32. Eduardo Juquem. Implantação Webmail Seguro. 2004. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

33. Túlio Cicero Salvaro de Souza. Aplicações embarcadas para gerenciamento de chaves criptográficas. 2005. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

34. Fabio Antonio Rodrigues. Sistema de Denúncia Anônima Segura. 2004.1. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

35. Jeandré Monteiro Sutil. Implementando Novas Abordagens para a Troca do Par de Chaves de Autoridades Certificadoras. 2005. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

36. Eduardo Ruhlan. JOpenSC: Uma interface gráfica para OpenSC. 2004.1. Trabalho de Conclusão de Curso. (Graduação em Ciências da Computação) - (UFSC);

37. Evandro Araujo de Sousa. Software para Assinatura Digital. 2005.1 Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

38. Leonardo Schmitz da Costa. Autoridade Certificadora Temporal. 2006. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

39. Glauco Israel Rebello Bondan. Autoridade Certificadora Temporal. 2006. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

40. Guilherme Steinmann. Infra-estrutura de Chaves Públicas Temporal. 2006. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

41. Geovani Ferreira da Cruz. Infra-estrutura de Chaves Públicas Temporal. 2006. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

42. José Carlos Kuerten Minuzzo. Interface para Autenticação Universal de Home Banking com Certificação Digital. 2007. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

43. Rogério Bodemuller Júnior. Sistema de Gerenciamento de Certificados Digitais. 2007. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

44. Jonathan Gehard Kohler. Contribuições ao Sistema de Gerenciamento do ciclo de Vida de Certificados Digitais da Infraestrutura de Chaves Públicas para Pesquisa e Ensino (SGCI). 2007. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

45. André Luiz Cardoso. Uma Ferramenta para Obtenção on-line de Certificados Digitais para Uso de Smartcards em Aplicações Java ME. 2007. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

46. Thiago Acordi Ramos. Preservação de Longo Prazo de Documentos Eletrônicos na CNSEC. 2007. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

47. Nelson da Silva. Preservação de Longo Prazo de Documentos Eletrônicos na CNSEC. 2007. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

48. Michel Zanini. Formulários Eletrônicos. 2007. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

49. Rogério José Hoffmann. Assinatura Digital de documentos pertinentes aos processos de instituições públicas. 2008. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

50. Cristian Thiago Moecke. Assinatura Digital de Documentos Eletrônicos na ICP-Brasil. 2008. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

51. Leonardo Albuquerque Menti. Auditoria em Unidade Certificadora. 2008. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

52. Davi Garcia Pereira. Assinatura Digital de Documentos Eletrônicos em Dispositivos Móveis. 2009. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

53. Hendri Nogueira. Infraestrutura de Autenticação Única em Instituições de Ensino e Pesquisa Brasileiras. 2010. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

54. Victor Daniel Müller. Desenvolvimento de aplicações sob o paradigma da computação em nuvem com ferramentas Google. 2010. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

55. Tiago Estevão De Rolt. Sistema Gerenciador de Ciclo de vida de Certificados de Atributos. 2010. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

56. Felipe Menegola Blauth. Framework para Padronização do Acesso a Cartões Inteligentes. 2011. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

57. Vicente Silveira Inácio. Framework LibPKI. 2011. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

58. Alex Sandro da Silva Pereira. Aplicabilidade das políticas ICP-Brasil no padrão de assinatura PAdES. 2011. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

59. Lucas Vinícius da Rosa. Gestão segura de certificados A1 para assinatura digital de documentos eletrônicos. 2011. Trabalho de Conclusão de Curso. (Graduação em Ciência da Computação) - (UFSC);

60. Bruno Imhof. Prescrição de Medicamento Controlado por Certificação Digital. Início: 2011. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Universidade Federal de Santa Catarina.

61. Maurício Simões de Oliveira. Modelagem e implementação do software de uma Autoridade de Registro para ICP-Brasil. Início: 2011. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Universidade Federal de Santa Catarina.

1.4 Orientações em Nível de Pós-Graduação

1.4.1 Orientações de Mestrado

Desde que eu obtive o meu doutorado e fui credenciado pelo Programa de Pós-graduação em Ciência da Computação, tenho orientado alunos de mestrado. Mais recentemente, quando foi criado o programa de doutorado, passei também a orientar trabalhos de doutorado. Até o ano 2015, foram 51 trabalhos orientados, dando uma média de um pouco mais de 3 alunos por ano. A maioria desses alunos seguiram carreira acadêmica, alguns deles ingressando em programas de doutorado. Esta é a lista de alunos que orientei desde o ano 2000:

1. Laurentino Augusto Dantas. ECN: Protocolo Criptográfico para Emissão de Certidões de Nascimento na WEB. 2000. Dissertação (Mestrado em Ciências da Computação) - UFSC.

2. Mehran Misaghi. Avaliação de Modificações do Cifrador Caótico de Roskin. 2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

3. Marco André Lopes Mendes. Modelo Simplificado do Cifrador RC6. 2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

4. João Luiz Francalacci Rocha. Proteção de Software por Certificação Digital. 2001. 111 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

5. Marcelo Luiz Brocardo. I2AC: Um protocolos criptográfico para crédito seguro. 2001. 120 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

6. Augusto Jun Devegili. Farnel: Uma Proposta de Protocolo Criptográfico para Votação Digital. 2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

7. Raquel Aparecida Pegoraro. Segurança no Comércio Eletrônico. 2002. Dissertação (Mestrado em Ciências da Computação) - UFSC.

8. Felipe Pompeo Pereira. Sistema de Assinatura Digital utilizando Impressão Digital. 2002. 101 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

9. Enrico Golfetto Masella. Sistema de Votação Digital Seguro via Internet. 2002. 101 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

10. Handerson Koerich. Sistema seguro de atendimento ao cliente via WEB. 2002. 101 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

11. Glauco Vinícios Scheffel. Segurança na Avaliação não Presencial. 2002. 156 f. Dissertação (Mestrado em Ciências da Computação) - UFSC..

12. Dejane Luiza Bortoli. O Documento Eletrônico no Ofício de Registro Civil de Pessoas Naturais. 2002. 131 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

13. Charles Christian Miers. Modelo Simplificado do AES. 2002. 126 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

14. Maria Eloisa Mignoni. Políticas e Declaração de Práticas de Certificação Digital para a UFSC. 2002. 159 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

15. Amauri Sant'Anna Ghisleri. Sistema Seguro de Atendimento ao Cliente: Garantia da Qualidade de Serviço. 2002. 118 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

16. Marco Antônio Torrez Rojas. Utilização de Algoritmos Genéticos no Projeto de Caixas-S para Cifradores de Bloco Simétricos. 2002. Dissertação (Mestrado em Ciências da Computação) - UFSC.

17. Luciano Ignaczak. Um novo modelo de Infra-estrutura de Chaves Públicas para uso no Brasil utilizando aplicativos com o código fonte aberto. 2002. Dissertação (Mestrado em Ciências da Computação) - UFSC.

18. Ana Karina Dourado Salina de Oliveira. Geradores de Números Randômicos Caóticos. 2002. Dissertação (Mestrado em Ciências da Computação) - UFSC.

19. Adriana Elissa Notoya. IARSDE - Infra Estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos: Validade do documento eletrônico por tempo indeterminado. 2002. 104 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

20. Roberto Samarone dos Santos Araújo. Protocolos Criptográficos para Votação Digital. 2002. Dissertação (Mestrado em Ciências da Computação) - UFSC.

21. Everton Schonardie Pasqual. IDDE - Uma Infra-estrutura para a Datação de Documentos Eletrônicos. 2002. 95 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

22. Amauri Sant'Anna Ghisleri. Sistema Seguro de Atendimento ao Cliente: Garantia da Qualidade de Serviço. 2002. Dissertação (Mestrado em Ciências da Computação) - UFSC.

23. Denise Bendo Demétrio. Infra-estrutura e Protocolação Digital de Documentos Eletrônicos. 2003. Dissertação (Mestrado em Ciências da Computação) - UFSC.

24. Vanessa Costa. Análise da Confiança do Sistema de Protocolação Digital de Documentos. 2003. Dissertação (Mestrado em Ciências da Computação) - UFSC.

25. Juliano Fontoura Kazienko. Assinatura Digital de Documentos Eletrônicos através da Impressão Digital. 2003. Dissertação (Mestrado em Ciências da Computação) - UFSC.

26. Débora Cabral. Uma análise da segurança da urna eletrônica brasileira. 2003. Dissertação (Mestrado em Ciências da Computação) -UFSC.

27. Paulo Sérgio Ribeiro. Comunicação Anônima Segura em Grupo. 2003. Dissertação (Mestrado em Ciências da Computação) - UFSC.

28. Luciana Rita Guedes Ghisleri. Um Protocolo Criptográfico para Marketing Seguro na Web. 2003. Dissertação (Mestrado em Ciências da Computação) -UFSC..

29. Fernando Cézar de Oliveira Lopes. Sistema de Denúncia Anônima Segura. 2003. Dissertação (Mestrado em Ciências da Computação) - UFSC.

30. Fernando Carlos Pereira. Protocolos Criptográficos para Selar e Lacrar Documentos Eletrônicos Aplicados a Sistemas de Compras Seguro. 2003. Dissertação (Mestrado em Ciências da Computação) - UFSC.

31. Ernesto Hermann Warnecke. G-DEF - Protocolo Criptográfico para Geração de Documento Eletrônico Fiscal nas Operações entre Empresas. 2003. Dissertação (Mestrado em Ciências da Computação) - UFSC.

32. Fabiano Castro Pereira. Estudo e Implementação de Redes de Comunicação Anônima e aplicação ao Sistema de Votação Digital OSTRACON. 2004. 111 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

33. Carlos Eduardo Mazzi. ECFV - Emissor de Cupom Fiscal Virtual. 2005. Dissertação (Mestrado em Ciências da Computação) -UFSC.

34. Jean Everson Martina. Provedor de Serviços Criptográfico para Infra-estrutura de Chaves Públicas e suas Aplicações. 2005. 140 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

35. Marcelo Carlomagno Carlos. Topologias Dinâmicas de infra-estrutura de Chaves públicas. 2007. Dissertação (Mestrado em Ciências da Computação) - UFSC.

36. Juliano Romani. Integração e Serviços de Relógio para Infra-estrutura de Chaves Pública. 2008. Dissertação (Mestrado em Ciências da Computação) - Universidade Federal de Santa Catarina, Financiadora de Estudos e Projetos. UFSC.

37. Túlio Cícero Salvaro de Souza. Aspectos Técnicos e Teóricos da Gestão do Ciclo de Vida de Chaves Criptográficas no OPenHSM. 2008. Dissertação (Mestrado em Ciências da Computação) - UFSC.

38. Martín Augusto Gagliotti Vigil. Infraestrutura de Chaves Públicas Otimizadora. 2010. Dissertação (Mestrado em Ciências da Computação) - UFSC.

39. Nelson da Silva. Preservação por Longo Prazo de Assinaturas Digitais. 2011. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

40. Thiago Acórdi Ramos. Preservação do Sigilo e Autenticidade de Documentos Eletrônicos por Longo Prazo. 2011. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

41. Jonathan Gehard Kohler. Gestão de Políticas e de Algoritmos Criptográficos na Integração de Infraestrutura de Chaves Públicas. 2011. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

42. Jeandré Monteiro Sutil. Gestão Segura de Múltiplas Instâncias de uma mesma Chave de Assinatura em Autoridades Certificadoras. 2011. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

43. Cristian Thiago Moecke. NBPKI - Uma ICP baseada em Autoridades Notariais. 2011. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

44. Eduardo dos Santos. Autenticação Multifator em Sistemas Computacionais. 2012. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

45. Dayana Pierina Brustolin Spagnuelo. Protocolo Flexível de Autenticação Multifator: Estudo de caso para Ambientes de Telemedicina. 2013. Dissertação (Mestrado em Ciências da Computação) - UFSC.

46. Lucas Gonçalves Martins. Autoridades Certificadoras Online. 2013. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

47. André Bereza Júnior. Gerência de Chaves em Dispositivos Criptográficos. 2013. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

48. Felipe Carlos Werlang. Assinatura Digital com Reconhecimento de Firma: Um Modelo de Assinatura Digital Centrado no Usuário. 2014. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

49. Hendri Nogueira. Aprimoramento da Privacidade em Infraestruturas de Chaves Públicas Centradas no Usuário e Baseada em Notários. 2014. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

50. Thaís Bardini Idalino. Using combinatorial group testing to solve integrity issues. 2015. Dissertação (Mestrado em Ciências da Computação) - UFSC.

51. Gustavo Souza Banegas. Pentanômios Irredutíveis sobre GF(2m) para redução modular eficiente. 2015. Dissertação (Mestrado em Ciências da Computação) - UFSC.

1.4.2 Orientações de Doutorado

Nesses anos todos, só tive a oportunidade de co-orientar um aluno de doutorado. Assim que o nosso programa de doutorado foi criado, eu iniciei minhas atividades de orientação de alunos de doutorado.

1. Júlio da Silva Dias. Confiança no Documento Eletrônico. 2004. 150 f. Tese (Doutorado em Engenharia de Produção) - Universidade Federal de Santa Catarina, Conselho Nacional de Desenvolvimento Científico e Tecnológico.

2 Atividades de Produção Intelectual

Este capítulo contém a lista de livros, capítulos de livros, artigos publicados em anais de congressos, artigos publicados em periódicos, programas de computador sem registro, produtos tecnológicos desenvolvidos.

2.1 Publicação de Livro

1. Nelson da Silva; Custódio, R. F.; SILVA, R. P. E.; Thiago Acórdi Ramos . Central Notarial de Serviços Eletrônicos Compartilhados. 1. ed. São Caetano do Sul, SP: Yendis, 2007. v. 1. 106p .

2.2 Capítulos de Livros

1. Werlang, Felipe Carlos; Custódio, Ricardo Felipe; Vigil, Martín A. G. Lecture Notes in Computer Science. 834. ed. Springer Berlin Heidelberg, 2014.
2. Araújo, R. S. S.; Custódio, R. F.; Graaf, Jeroen Antonius Maria Van de . A Verifiable Voting Protocol based on Farnel. In: David Chaum;Markus Jakobsson;Ron Rivest;Peter Ryan;Josh Benaloh;M. Kutylowski;Ben Adida. (Org.). Towards Trustworthy Elections. Baltimore: Springer, 2010, v. , p. 274-288.
3. Custódio, R. F.; Notoya, Adriana Elissa; Pereira, Fernando Carlos . Infra-estrutura de Chaves Públicas e Aplicações. In: SBC. (Org.). XII Escola Regional de Informática da SBC. : , 2004, v. 1, p. 62-92.

2.3 Texto Integral em Anais de Congressos

Desde que eu ingressei na carreira de professor, tenho procurado participar de encontros científicos, não somente como ouvinte, mas de forma ativa, principalmente através da submissão e apresentação de artigos científicos. Tais artigos descrevem os resultados dos meus trabalhos de desenvolvimento científicos e tecnológico. Foram um total de 70 artigos publicados em anais de congressos científicos desde 1994, o que constitui uma média de 3 artigos por ano.

1. Custódio, R. F.; Borba, M. P. Método da Interação Dinâmica para a Determinação de Zeros de Funções. In: XVII Congresso Nacional de Matemática Aplicada e Computacional, 1994, Vitória - ES, 1994. v. 2. p. 549-553.

2. Peters. Sergio; Custódio.R.F; Eger, Rita; Mendonça, Nelcy. A Computação Algébrica no Ensino. In: IX Congresso Nacional de Matemática Aplicada e Computacional, 1996, Goiânia - GO, 1996.v. 2. p. 176- 354.

3. Custódio, R. F.; Barone, D. A. C. Atomic Decomposition with Genetic Algorithms. In: 1997 International Symposium on Nonlinear Theory and its Applications, 1997, 1997. v. 2. p. 1285-1288.

4. Roque, W. L.; Oliveira, L. P. L.; Custódio, R. F.; Valliatti, H. Time-Dependent Fractal Dimension of Lung Sounds. In: The 23rd International Conference on Lung Sounds, 1998, Boston. International Conference on Lung Sounds, 1998. v. 1.

5. Roque, W. L.; Oliveira, L. P. L.; Custódio, R. F. Identifying Lung Sound Patterns through Lyapunov Exponent Estimations. In: Congresso Nacional de Matematica Aplicada e Computacional, 1999. Congresso Nacional de Matematica Aplicada e Computacional, 1999. v. 1.

6. Roque, W. L.; Heimfarth, T.; Spengler, T.; Valliatti, H.; Custódio, R. F.; Oliveira, L. P. L. PulSA: A System to Support Lung Sound Analysis. In: The 23rf International Conference on Lung Sounds, 1999. The 23rf International Conference on Lung Sounds, 1999. v. 1.

7. Oliveira, L. P. L.; Custódio, R. F.; Roque, W. L. Negative Lyapunov Exponent Estimations in Non Chaotic Data Time Series. In: Nonlinear Dynamics of Electronic Systems - NDES99, 1999, Dresden. NDES99 - Nonlinear Dynamics of Electronic Systems, 1999. v. 1.

8. Oliveira, L. P. L.; Custódio, R. F.; Roque, W. L. Use of Lyapunov Exponents for Pattern Recognition in Lung Sounds. In: VIII Workshop on Nonlinear Dynamics of Eletronic Systems, 2000, Catânia. Proceedings of VIII Workshop on Nonlinear Dynamics of Eletronic Systems, 2000.

9. Rocha, J. L. F.; Custódio, R. F. Proteção de Software por Certificação Digital. In: Simpósio de Segurança em Informática, 2001, São José dos Campos - SP. SSI 2001, 2001. v. 1. p. 17-26.

10. Notoya, Adriana Elissa; Custódio, R. F. Aspectos Tecnológicos para a Validade Jurídica da Cópia Impressa de um Documento Eletrônico. In: SEMINC - Semana de Informática de Cascavel, 2001, Cascavel. SEMINC 2001, 2001. v. 1. p. 92-96.

11. Pasqual, E. S.; Dias, Júlio da Silva; Custódio, R. F. Um Novo Método para Datação de Documentos Eletrônicos. In: SEMINC - Semana de Informática de Cascavel, 2001, Cascavel. SEMINC 2001, 2001. v. 1. p. 31-36.

12. Custódio, R. F.. Infra-estrutura de chaves públicas. In: Simpósio de Segurança em Informação, 2001, São José dos Campos - SP. 3o. Simpósio de Segurança em Informação, 2001. v. 1. p. 1-50.

13. Zancanella, Luiz Carlos; Custódio, R. F.; Freitas, D. S. Fundamentos de Criptografia. In: IX Escola de Informática da SBC - Sul, 2001, Passo Fundo, São José, Maringá. IX Escola de Informática da SBC-Sul. Por Alegre: SBC, 2001. v. 1. p. 175-198.

14. Pasqual, E. S.; Dias, Júlio da Silva; Custódio, R. F. A New Method for Digital Time-Stamping of Electronic Documents. In: FIRST Conference on Computer Security Incident Handling & Response 2002, 2002, Hawaii, USA. 14th Anual FIRST Conference on Computer Security Incident Handling & Response 2002, 2002. v. 1. p. 1-8.

15. Kazienko, J. F.; Pereira, F. P.; Custódio, R. F. Assinatura Digital de Documentos Eletrônicos através da Impressão Digital. In: XII Seminário Regional de Informática, 2002, Santo Ângelo. XII Seminário Regional de Informática, 2002. v. 1. p. 1-8.

16. Notoya, Adriana Elissa; Custódio, R. F. IARSDE: Infra-estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos. In: The International Symposium on Document Technologies, 2002, São Paulo. The International Symposium on Document Technologies, 2002. v. 1. p. 1-8.

17. Custódio, R. F.. Tecnologias para a Segurança da Informação: Infra-estrutura de Chaves Públicas. In: IV Escola de Informática Norte da SBC, 2002, Palmas, Belém e Macapá. EIN/Ecoinfo 2002, 2002. v. 1. p. 203-230.

18. Notoya, Adriana Elissa; Custódio, R. F. Uma Proposta Para Garantia da Validade do Documento Eletrônico por Tempo Indeterminado. In: IV Simpósio Segurança em Informática, 2002, São José dos Campos, SP. SSI 2002 - IV Simpósio Segurança em Informática, 2002. v. 1. p. 1-8.

19. Ribeiro, P. S.; Custódio, R. F. Um Protocolo Criptográfico para Comunicação Anônima Segura. In: II Workshop de Segurança de Sistemas Computacionais, 2002, Búzios, Rio de Janeiro. WSeg 2002, 2002. v. 1. p. 97-104.

20. Custódio, R. F.; Araújo, R. S. S.; Devegili, A. J. Farnel: Um protocolo Criptográficos para Votação Digital. In: II Workshop de Segurança de Sistemas Computacionais, 2002, Búzios, Rio de Janeiro. WSeg 2002, 2002. v. 1. p. 113-120.

21. Arantes, J. A.; Westphall, Carlos Becker; Custódio, R. F. Modelo Analítico para Avaliar Plataformas Cliente/Servidor e Agentes Móveis Aplicados à Gerência de

Redes. In: 20o. Simpósio Brasileiro de Redes de Computadores, 2002, Búzios, Rio de Janeiro. SBRC 2002, 2002. v. 1. p. 1-8.

22. Arantes, J. A.; Westphall, Carlos Becker; Custódio, R. F. Client/Server and Mobile Agent Paradigms - An Analytical Model for Performance Evaluation. In: Colloque Francophone sur la Gestion de Réseuax et Service, 2003, Fortaleza (CE), 2003, Fortaleza. Colloque Francophone sur la Gestion de Réseuax et Service, 2003, Fortaleza (CE), 2003. v. 1. p. 329-344.

23. Pereira, Fernando Carlos; Custódio, R. F.; Notoya, Adriana Elissa . Protocolo Criptográfico para Envio de Propostas em Processos de Compras. In: V Simpósio Segurança em Informática, 2003, São José dos Campos, SP. Anais do V SSI 2003, 2003. v. 1. p. 90-103.

24. Costa, Vanessa; Custódio, R. F.; Dias, Júlio da Silva; Rolt, Carlos Roberto de . Protocolação Digital de Documentos Eletrônicos. In: I Fórum sobre Segurança, Privacidade e Certificação Digital, 2003, Brasília. I Fórum sobre Segurança, Privacidade e Certificação Digital, 2003. v. 1. p. 1-12.

25. Costa, Vanessa; Custódio, R. F.; Dias, Júlio da Silva; Rolt, Carlos Roberto de . Confiança na Tempestividade dos Documentos Eletrônicos: Auditoria da Protocolação Digital. In: V Simpósio Segurança em Informática, 2003, São José dos Campos, SP. Anais Eletrônicos do SSI'2003, 2003. v. 1. p. 100-109.

26. Dias, Júlio da Silva; Custódio, R. F.; Demétrio, D. B.; Rolt, Carlos Roberto de . Reliable Clock Synchronization for Electronic Documents. In: LANOMS 2003 - IEEE Latin American Network Operations and Management Symposium, 2003, Foz do Iguaçu. Anais do IEEE LANOMS 2003, 2003. v. 1. p. 38-45.

27. Dias, Júlio da Silva; Custódio, R. F.; Rolt, Carlos Roberto de . Sistema Seguro para Assinatura de Documentos Eletrônicos. In: Conferência IADIS Ibero Americana WWW/Internet 2003, 2003. Anais do IADIS WWW/internet 2003, 2003. v. 1. p. 97-102.

28. Dias, Júlio da Silva; Custódio, R. F.; Rolt, Carlos Roberto de . Assinatura Confiável de Documentos Eletrônicos. In: Workshop em Segurança de Sistemas Computacionais - WSeg, 2003, Natal, RN. WSeg-2003, 2003. v. 1. p. 103-112.

29. Pereira, F. C.; Custódio, R. F. Ostracon: Um Sistema de Votação Digital pela Internet. In: Workshop em Segurança de Sistemas Computacionais - WSeg, 2003, Natal, RN. SBRC-2003, WSeg-2003, 2003. v. 1. p. 95-102.

30. Dias, Júlio da Silva; Custódio, R. F.; Demétrio, D. B. Sincronização Segura de Relógio para Documentos Eletrônicos. In: Simpósio Brasileiro de Redes de Computadores, 2003, Natal - RN. SBRC 2003, 2003. v. 2. p. 585-598

31. Custódio, R. F.; Dias, Júlio da Silva; Pereira, Fernando Carlos; Notoya, Adriana Elissa . Módulo Cifrador de Documentos Eletrônicos. In: IV Workshop em Segurança de Sistemas Computacionais, 2004, Gramado. WSeg 2004 - IV Workshop em Segurança de Sistemas Computacionais, 2004. v. 1.

32. Dias, Júlio da Silva; Martina, Jean Everson; Custódio, R. F.; Freitas, Daniel Santana de . Execução Segura de Assinaturas Confiáveis em Documentos Eletrônicos. In: Simpósio Brasileiro de Redes de Computadores, 2004, Gramado. SBRC 2004, 2004. v. 1. p. 101-114.

33. Carlos, M. C.; Custódio, R. F. Tornando uma infra-estrutura de chaves publicas dinâmica. In: Simpósio Segurança em Informática - SSI, 2006, São José dos Campos, SP. SSI 2006, 2006.

34. Araújo, R. S. S.; Custódio, R. F.; A. Wiesmaier; T. Takagi . An Electronic Scheme for the Farnel Paper-Based Voting Protocol. In: 4th International Conference on Applied Cryptography and Network Security (ACNS'06), 2006, Singapore. 4th International Conference on Applied Cryptography and Network Security (ACNS'06), 2006. v. 1.

35. Pereira, Fernando Carlos; Fraga, Joni da Silva; Custódio, R. F. Self-adaptable and Intrusion Tolerant Certificate Authority for Mobile Ad Hoc Networks. In: International Conference on Advanced Information Networking and Applications, 2007, Ginowan City. AINA2008 - The 22nd IEEE International Conference on Advanced Information Networking and Applications, 2007.

36. Araújo, R. S. S.; Custódio, R. F.; Graaf, Jeroen Antonius Maria Van de . A Verifiable Voting Protocol based on Farnel. In: IAVoSS Workshop On Trustworthy Elections, 2007, Ottawa, CANADA. IAVoSS Workshop On Trustworthy Elections (WOTE 2007), 2007.

37. Martina, Jean Everson; Salvaro, Túlio; Custódio, R. F. OpenHSM: An Open key life cycle protocol for Public Key Infrastructure's Hardware Security Modules. In: European PKI Workshop: Theory and Practice (EuroPKI'07), 2007, Mallorca, Espanha. 2007 European PKI Workshop: Theory and Practice (EuroPKI'07), 2007.

38. Pereira, Fernando Carlos; Fraga, Joni da Silva; Notoya, Adriana Elissa; Custódio, R. F. Autoridade Certificadora Dinâmica para Redes Ad Hoc Móveis. In: Simpósio

Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), 2007, Belém. 25o. Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), 2007.

39. Custódio, R. F.; Dias, Júlio da Silva; Pereira, Fernando Carlos; Notoya, Adriana Elissa. Temporal Key Release Infrastructure. In: 6th Annual PKI R&D Workshop, 2007, Gaithersburg - MD, USA. 6th Annual PKI R&D Workshop, 2007.

40. Carlos, M. C.; Custódio, R. F.; Sutil, Jeandré M. Good practices for Long-Term Key Management in a Public Key Infrastructure. In: 11th IEEE International Conference on Computational Science and Engineering - Workshops, 2008, São Apulo. CSEWORKSHOPS '08: Proceedings of the 2008 11th IEEE International Conference on Computational Science and Engineering - Workshops, 2008. v. 1. p. 141-148.

41. Pereira, Fernando Carlos; Fraga, Joni da Silva; Custódio, R. F. Self-adaptable and Intrusion Tolerant Certificate Authority for Mobile Ad Hoc Networks. In: 22nd IEEE International Conference on Advanced Information Networking and Applications (AINA2008), 2008, Ginowan. Proceedings of 22nd IEEE AINA 2008, 2008. v. 1. p. 705-712.

42. Salvaro, Túlio; Martina, Jean Everson; Custódio, R. F. Audit and Backup Procedures for Hardware Security Modules. In: 7th Symposium on Identity and Trust on the Internet (IDtrust 2008), 2008, Gaithersburg, MD, USA. Proceedings of the 7th symposium on Identity and trust on the Internet, 2008. v. 238. p. 89-97.

43. Custódio, R. F.; Vigil, Martín Augusto Gagliotti; Romani, J.; Pereira, Fernando Carlos; Fraga, Joni da Silva . Optimized Certificates ? A New Proposal for Efficient Electronic Document Signature Validation. In: EuroPKI2008, 2008, Trondheim, Norway. Fifth European PKI Workshop, 2008. v. 1. p. 49-59.

44. Martina, Jean Everson; Salvaro, Túlio; Custódio, R. F. Ceremonies Design for PKI's Hardware Security Modules. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2009, Campinas. SBSeg 2009. Porto Alegre: SBC, 2009.

45. Semprebom, T.; Montez, Carlos Barros; Moraes, R. A. R.; Vasques, Francisco; Custódio, R. F. Distributed DBP: A (m,k)-firm Based Distributed Approach for QoS Provision in IEEE 802.15.4 Networks. In: IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2009, Palma de Mallorca, Spain. 14th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2009. p. 1-8.

46. Vigil, Martín Augusto Gagliotti; Custódio, R. F.; Moraes, R. A. R. Infra-estrutura de Chaves Públicas Otimizada: Uma ICP de Suporte a Assinaturas Eficientes para Documentos Eletrônicos. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2009, Campinas. IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2009. p. 129-142.

47. Rafael T. Souza Jr.; Custódio, R. F.; Viviane Bertol . Propostas para apoiar a preservação documental de longo prazo na ICP-Brasil. In: V Congreso Iberoamericano de Seguridad Informática, 2009, Montevideo, Uruguay. CIBSI 2009 - V Congreso Iberoamericano de Seguridad Informática. Montevideo: Universidad de la República, 2009. v. 1. p. 61-72.

48. Martina, Jean Everson; Salvaro, Túlio; Custódio, R. F. Ceremonies Formal Analysis in PKI?s Context. In: International Symposium on Privacy and Security Applications, 2009, Vancouver. International Symposium on Privacy and Security Applications (PSA09), 2009. v. 1. p. 1-10.

49. Thiago Acórdi Ramos; Lung, Lau Cheuk; Jonathan Gehard Kohler; Custódio, R. F. An Infrastructure for Long-term Archiving of Authenticated and Sensitive Electronic Documents. In: 7th European Workshop on Public Key Services, Applications and Infrastructures, 2010, Atenas, Greece. Lecture Notes on Computer Science. Boston,: Springer Verlag in the Lecture Notes in Computer Science, 2010. v. 339. p. 1-8.

50. Moecke, C. T.; Custódio, R. F.; Jonathan Gehard Kohler; Carlos, M. C. Uma ICP baseada em certificados digitais autoassinados. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2010, Fortaleza. X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2010. p. 91-104.

51. Costa, Robson; Portugal, Paulo; Vasques, Francisco; Moraes, R. A. R.; Custódio, R. F. A Coordination Layer to Handle Real-Time Communication in Wi-Fi Networks with Uncontrolled Traffic Sources. In: Local Computer Networks, 2011, Bonn. 36th Annual IEEE Conference on Local Computer Networks, 2011. p. 263-266.

52. Hendri Nogueira; Custódio, R. F.; Moecke, C. T.; Wangham, Michelle Silva . Using Notary Based Public Key Infrastructure in Shibboleth. In: Workshop de Gestão de Identidades, 2011, Brasília. I WGID, 2011.

53. Werlang, Felipe Carlos; Custódio, R. F.; Araújo, R. S. S. Electronic Documents with Signature Constraints. In: Workshop de Gestão de Identidades, 2011, Brasília. I WGID, 2011.

54. Silverio, Anderson Luiz; Jonathan Gehard Kohler; Custódio, R. F. Análise e implementação de um protocolo de gerenciamento de certificados. In: Workshop de

Trabalhos de Iniciação Científica e de Graduação, 2011, Brasília. WTICG 2011, 2011.

55. Nelson da Silva; Thiago Acórdi Ramos; Custódio, R. F. Carimbos do Tempo Autenticados para a Preservação por Longo Prazo de Assinaturas Digitais. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2011, Brasília. XI SBSEG, 2011.

56. dos Santos, Eduardo; Martina, Jean Everson; Custódio, Ricardo Felipe . Towards a Formal Verification of a Multi-factor Authentication Protocol Using Automated Theorem Provers, 2012. p. 84-91.

57. Carlos, M. C.; Martina, Jean Everson; Price, Geraint; Custódio, R. F. A Proposed Framework for Analysing Security Ceremonies. In: International Conference on Security and Cryptography, 2012, Rome. Proceedings of the International Conference on Security and Cryptography. p. 440.

58. Vigil, Martín Augusto Gagliotti; Custódio, Ricardo Felipe . Cleaning up the PKI for Long-term Signatures. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2012, Curitiba. XII SBSeg 2012, 2012.

59. Vigil, Martín Augusto Gagliotti; Moecke, C. T.; Custódio, R. F.; Volkamer, Melanie . The Notary Based PKI. A Lightweight PKI for Long-term Protection of Digital Documents. In: EuroPKI 2012, 2012, Pisa. 9th European PKI Workshop: Research and Applications, 2012.

60. Wangenheim, von Aldo; Custódio,R. F. Assinatura digital de laudos médicos: um assunto ainda não resolvido. Revista da Associação Médica Brasileira, 2013. p.209-2012.

61. Nogueira, Henri; Souza, R. L.; Custódio, R. F. A Privacy-Enhanced User-Centric Identity and Access Management Based on Notary. In: International Conference on Systems and Networks Communications (ICSNC 2013), 2013, Venice. The Eighth International Conference on Systems and Networks Communications, 2013. p. 159-164.

62. Lopes de Souza, Rick; Lung, Lau Cheuk; Custódio, Ricardo Felipe . Multi-factor Authentication in Key Management Systems. In: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2013, Melbourne. 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. p. 746.

63. Spagnuelo, Dayana. P. B.; Martina, J. E.; Custódio, R. F.; Andrade, Rafael . Multi-Factor Authentication in Telemedicine Systems. In: The Fifth International Conference on eHealth, Telemedicine, and Social Medicine, 2013, Nice. eTELEMED 2013 : The Fifth International Conference on eHealth, Telemedicine, and Social Medicine, 2013. p. 114.

64. Carlos, Marcelo Carlomagno; Martina, Jean Everson; Price, Geraint; Custódio, Ricardo Felipe . An updated threat model for security ceremonies. In: the 28th Annual ACM Symposium, 2013, Coimbra. Proceedings of the 28th Annual ACM Symposium on Applied Computing - SAC '13. New York: ACM Press. p. 1836.

65. Martins, Lucas Gonçalves; Custódio, R. F. Implementation of Trust Metrics in X.509 Public Key Infrastructure. In: International Conference on Emerging Security Information, Systems and Technologies, 2013, Barcelona. The Seventh International Conference on Emerging Security Information, Systems and Technologies, 2013.

66. Martins, Lucas Gonçalves; Custódio, R. F. Sistema Gerenciador de Certificados Digitais: Um modelo para governo eletrônico. In: Workshop de Computação Aplicada em Governo Eletrônico, 2013, João Pessoa. IX Simpósio Brasileiro de Sistemas de Informação, 2013.

67. Silvério, Anderson Luiz; Custódio, Ricardo F.; Carlos, M. C.; MELLO, R. S. Efficient Data Integrity Checking for Untrusted Database Systems. In: International Conference on Advances in Databases, Knowledge, and Data Applications, 2014, Chamonix. The Sixth International Conference on Advances in Databases, Knowledge, and Data Applications, 2014. p. 118-124.

68. Souza, R. L.; Netto, H. V.; Lung, Lau Cheuk; Custódio, R. F. CloudSec - Um Middleware para Compartilhamento de Informações Sigilosas em Nuvens Computacionais. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2014, Belo Horizonte. VIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2014.

69. Souza, R. L.; Netto, H. V.; Lung, Lau Cheuk; Custódio, R. F. SSICC: Sharing Sensitive Information in a Cloud-of-Clouds. In: International Conference on Systems, 2014, Nice. ICONS 2014, The Ninth International Conference on Systems, 2014. v. 1. p. 185-191.

70. Brocardo, Marcelo Luiz; Custódio, Ricardo Felipe; Rolt, Carlos Roberto de; Dias, Júlio da Silva; Traore, Issa . Sharing Privacy Information in Credit Analysis Environment. In: 2015 Ninth International Conference on Complex, Intelligent, and

Software Intensive Systems (CISIS), 2015, Santa Catarina. 2015 Ninth International Conference on Complex, Intelligent, and Software Intensive Systems, 2015. p. 491-496.

2.4 Artigos Publicados em Periódicos

Também foram publicados artigos em periódicos científicos. Foram publicados no total 12 artigos.

1. Oliveira, L. P. L.; Roque, W. L.; Custódio, R. F. Lung Sound Analysis with Time-Dependent Fractal, v. 10, p. 1419-1423, 1999.

2. Rover, A. J.; Custódio, R. F.; Bortoli, D. L. Cartório Virtual: uma experiência na emissão de certidão de nascimento.. Revista do Curso de Direito das Faculdades Jorge Amado, Salvador, v. 1, n.1, p. 143-162, 2001.

3. Lopes, Fernando Cézar de Oliveira; Custódio, R. F. Denúncia Anônima Segura. Revista do IST, Joinville - SC, v. 1, n.1, p. 50-53, 2004.

4. Arantes, J. A.; Westphall, Carlos Becker; Custódio, R. F.; Chaves, Shirlei A. Analytical Model to Evaluate the Performance of Mobile Agents in a Generic Network Topology. Journal of Network and Systems Management, v. 18, p. 357-373, 2010.

5. Moraes, Ricardo; Portugal, Paulo; Vasques, Francisco; Custódio, R. F. Assessment of the IEEE 802.11e EDCA Protocol Limitations when Dealing with Real-Time Communication. EURASIP Journal on Wireless Communications and Networking, v. 2010, p. 1-15, 2010.

6. Nobre, Luiz Felipe; von Wangenheim, Aldo; Custódio, Ricardo Felipe . Autenticação digital de documentos médicos: encontramos a solução?. RB. Radiologia Brasileira (Impresso), v. 44, p. V-VI, 2011.

7. Nogueira, H.; Custódio, R. F.; Martina, J. E. An Attribute-Based Public Key Infrastructure. International Journal of Computer Science and Information Security, v. 11, p. 11-18, 2013.

8. Von Wangenheim, A.; Custódio, R. F.; Martina, Jean Everson; Giuliano, Isabela de Back; Andrade, Rafael . Digital authentication of medical records: have we found a solution?. Revista da Associação Médica Brasileira, v. 59, p. 209-212, 2013.

9. Martina, J. E.; dos Santos, Eduardo; Carlos, Marcelo Carlomagno; Price, Geraint; Custódio, R. F. An adaptive threat model for security ceremonies. International Journal of Information Security, v. 14, p. 103-121, 2015.

10. Idalino, Thaís Bardini; Moura, Lúcia; Custódio, Ricardo Felipe; Panario, DANIEL . Locating modifications in signed data for partial data integrity. Information Processing Letters (Print), v. 115, p. 731-737, 2015.

11. Perin, L.P.; Custódio, R.; Panario, D.; Wang, Q. Formulas for p^{th} root computations in finite fields of characteristic p. Electronics Letters (Online), v. 52, p. 117-119, 2016.

12. Brocardo, Marcelo Luiz; Rolt, Carlos Roberto de; Dias, Júlio da Silva; Custódio, Ricardo Felipe; Traore, Issa . Privacy information in a positive credit system. International Journal of Grid and Utility Computing, v. 8, p. 61, 2017.

2.5 Programa de computador sem registro

Procurou-se também, sempre que se julgou oportuno, desenvolver sistemas computacionais que pudessem mostrar os resultados de algum trabalho proposto. Eis a lista de programas de computador que não foram registrados:

1. Custódio, R. F.. Time Series Analysis System (TSAS). 1997.

2. Custódio, R. F.. Pulmonary System Analyzer (PulSA). 1999.

3. Custódio, R. F.; Dias, Júlio da Silva; SILVEIRA JÚNIOR, A. C. LabSECSigner. 2000.

4. Custódio, R. F.; Dias, Júlio da Silva; Bortoli, D.; DANTAS, L. A.; Martina, Jean Everson; CHRYSSOVERGIS, M. D. Cartório Virtual. 2000.

5. Custódio, R. F.. Protocoladora Digital de Documentos Eletrônicos (PDDE). 2000.

6. Araújo, R. S. S.; Custódio, R. F. OSTRACON: Sistema de Votação Digital Seguro para a Internet. 2002

7. Custódio, R. F.; Martina, Jean Everson; Salvaro, Túlio; Vigil, Martín Augusto Gagliotti; Bereza, André . OpenHSM - Sistema gerenciador do ciclo de vida de chaves privadas em ambiente embarcado. 2005.

8. Custódio, R. F.; Carlos, M. C.; Moecke, C. T.; Werlang, Felipe Carlos; Martins, Lucas Gonçalves . Ywapa - Um Sistema de Gerência de Certificados Digitais para Autoridades Certificadoras Raiz. 2008.

9. Custódio, R. F.; Moecke, C. T.; Martins, Lucas Gonçalves; Werlang, Felipe Carlos . Ywyra - Um Sistema de Gerência de Certificados de ACs Intermediárias. 2009.

10. Custódio, R. F.; Guerra Junior, Armindo Antônio . Assinador Digital Web ICP-Brasil. 2010

11. Custódio, R. F.; HOHLER, J. G.; Vigil, Martín Augusto Gagliotti . Autoridade Certificadora de Correio Eletrônico. 2010.

12. Custódio, R. F.; Bereza, André; Sutil, Jeandré M.; Gallo Filho, Roberto Alves . ASI-HSM. 2010.

13. Custódio, R. F.; Jonathan Gehard Kohler . Módulo Público de ICP. 2011

14. Vigil, Martín Augusto Gagliotti; Werlang, Felipe Carlos; Ferraro, Lucas; Custódio, R. F. Políticas de Assinatura Digital e Listas de Políticas Aprovadas em CAdES e XAdES para o Padrão Brasileiro de Assinatura Digital no âmbito da Infraestrutura de Chaves Públicas Brasileira. 2011

15. Vigil, Martín Augusto Gagliotti; Werlang, Felipe Carlos; Custódio, R. F.; Ferraro, Lucas . Assinador de Documentos Eletrônicos Minimalista do Padrão Brasileiro de Assinatura Digital. 2011.

16. Custódio, R. F.; Vigil, Martín Augusto Gagliotti; Ferraro, Lucas . Biblioteca de Códigos de Referência de Assinatura Digital. 2011.

17. Custódio, R. F.; Werlang, Felipe Carlos; Hohler, J. G.; Martins, Lucas Gonçalves . Hawa - Um sistema de autoridade certificadora final. 2011.

2.6 Produtos Tecnológicos

Desde o início de minha carreira acadêmica, tem sido uma preocupação constante, não somente os aspectos teóricos da computação, mas também as aplicações. O desenvolvimento de produtos, resultados de trabalhos científicos, mostrou-se de grande valia para os alunos que participaram dos projetos e para as instituições que se beneficiaram desses produtos.

Entre os produtos desenvolvidos, destaca-se o Módulo de Segurança Criptográfica (HSM). Este equipamento, resultado de vários projetos de pesquisa, culminou num produto inédito no Brasil. O HSM foi transferido para a iniciativa privada e tem sido adotado por diversas empresas públicas e privadas, não somente no Brasil, mas também em outros países. No Brasil, destaca-se o uso do nosso equipamento como principal plataforma criptográfica da Autoridade Certificadora Raiz da Infraestrutura de Chaves Públicas Brasileira.

A seguir tem-se uma lista dos principais produtos dos quais eu fui responsável direto pelo seu desenvolvimento.

1. Custódio, R. F.; Araújo, R. S. S. OSTRACON: Sistema de Votação Digital Segurança na Internet. 2001.

2. Custódio, R. F.; Pasqual, E. S. Protocoladora Digital de Documentos Eletrônicos. 2001.

3. Custódio, R. F.; Pereira, Fernando Carlos; Notoya, Adriana Elissa. Sistema Gerenciador de Certificados Digitais. 2007.

4. Custódio, R. F.; Dahab, Ricardo; Graaf, Jeroen Antonius Maria de; Martina, Jean Everson; Salvaro, Túlio; SANTOS, Eduardo dos. Hardware Criptográfico para infraestrutura de Chaves Públicas (HSM). 2007.

5. Bereza, André; Custódio, R. F.; Rick Lopes de Souza; Paulo Henrique de Moraes; Hendri Nogueira . Módulo de Segurança Criptográfica ASI-HSM. 2006.

6. Custódio, R. F.; Dahab, R.; Graaf, Jeroen Antonius Maria Van de; Martina, Jean Everson; Salvaro, Túlio; Santos, Eduardo dos . Hardware Criptográfico para Infraestrutura de Chaves Públicas (HSM). 2007.

7. Custódio, R. F.; Pereira, Fernando Carlos; Notoya, Adriana Elissa . Sistema Gerenciador de Certificados Digitais. 2007.

3 Atividades de Extensão

3.1 Assessoria, Consultorias e Perícias

Um preocupação constante foi o desenvolvimento de atividades de extensão. A atividade de extensão tornou-se muito importante para aproximar os professor, pesquisadores e alunos da realidade do mercado. Foi possível através dessas atividades, entender problemas reais e propor soluções inovadoras. Algumas desses soluções acabaram se tornando produtos inovadores no mercado brasileiro e internacional.

1. Participação como consultor de Informática no processo de informatização da UDESC. 1995.

2. Treinamento do núcleo de informática da Universidade do Extremo Sul Catarinense (UNESC) em Gerência e Administração de Redes de Comunicação de Dados. 1996.

3. Consultoria ad hoc - Análise de mérito técnico científico das propostas submetidas ao Programa RHAE- Programa de Capacitação de Recursos Humanos para Atividades Estratégicas. 1999.

4. Membro da Comissão para elaboração do Projeto para o Atendimento do Programa de Capacitação Tecnológica-PCT2 da Motorola na área de Ciência da Computação.1999.

5. Integração da Universidade do Oeste de Santa Catarina - UNOESC à Internet através da Rede Catarinense de Ciência e Tecnologia - RCT. 2000.

6. Consultor na área de informática em diversas instituições, estaduais e interestaduais, tais como: Universidade do Sul de Santa Catarina - UNISUL, UDESC, UNOESC. 2000.

7. Consultoria - Suporte à elaboração do Projeto de Implantação do novo curso de Sistemas de Informação. em especial nas de ferramentas computacionais de apoio ao ensino das diversas disciplinas propostas no Centro Educacional Exponencial S/A - CEESA. 2000.

8. Suporte a coordenação para implantação de um novo curso de Sistemas de Informação na Faculdade Exponencial S/A. 2001.

9. Consultoria - Elaboração de um modelo de Gestão e Tecnologia da Informação, para Secretaria da Fazenda do Estado de Santa Catarina. 2001.

10. Membro da Comissão para a Coordenação do Projeto para o Atendimento do Programa de Capacitação Tecnológica (PCT2) da Motorola nas áreas de Engenharia de Software e Firmware. 2001.

11. Participação no Programa de Capacitação Tecnológica - PCT - SW. 2001.

12. Consultor Científico no V Encontro de Atividade Científicas da Universidade de Londrina e Arapongas (UNOPAR). 2002.

13. Prestação de Serviço Especializado de Suporte Técnico de Software de Gerenciamento de Certificado Digital . Serviço de Federal de Processamento de Dados - SERPRO. 2008. (Participação Prof. Sérgio Peters e Pro. Ricardo Alexandre Reinaldo de Moraes.

14. Prestação de Serviço Especializado de Suporte Técnico de Software de Gerenciamento de Certificados Digital. Serviço Federal de Processamento de Dados (SERPRO). 05/09/2008 a 04/09/2009.

15. Suporte a Infraestrutura de Chaves Públicas para Ensino e Pesquisa. Rede Nacional de Ensino e Pesquisa (RNP). 01/09/2010 a 30/08/2011.

16. Auditoria no Sistema Eletrônico de Processos. Tribunal de Justiça do Maranhão - TJM.2011.

17. Suporte a Infraestrutura de Chaves Públicas para Ensino e Pesquisa. Rede Nacional de Ensino e Pesquisa (RNP). 01/09/2013 a 01/09/2014.

18. Suporte a Infraestrutura de Chaves Públicas para Ensino e Pesquisa. Rede Nacional de Ensino e Pesquisa (RNP). 01/09/2013 a 01/09/2014.

19. Consultoria para apoio ao desenvolvimento sob Ywapa e Ywyra. Valid Certificadora Digital Ltda. 01/03/2012 a 18/09/2013.

4 Coordenação de Projetos

Este capítulo contém uma lista de projetos de pesquisa e de extensão dos quais participei ativamente desde que ingressei na carreira acadêmica nessa universidade.

4.1 Participação em Grupos de Pesquisa

O professor Ricardo Custódio é líder do grupo de pesquisa LabSEC[1], devidamente registrado e certificado no diretório de grupos de pesquisas do CNPq. Também está vinculado ao grupo de pesquisa LabGES, liderado pelo professor Carlos Roberto De Rolt, da Universidade do Estado de Santa Catarina (UDESC).

4.2 Coordenação e Participação em Projeto de Pesquisa

1. Desenvolvimento de uma infraestrutura, para a criação de um ambiente chamado cartório digital. Câmara Brasileira de Comércio Eletrônico - CAMARA-NET. Período: 02/01/2008 a 28/02/2010.

2. Manutenção de Aprimoramento dos Softwares Ywapa e Ywyra. Instituto Nacional de Tecnologia da Informação (ITI). Período: 01/10/2009 a 30/12/2010.

3. Padrão Brasileiro de Assinatura Digital - Implementação de Referência. Colégio Notarial do Brasil (CNB). Período: 01/08/2009 a 31/03/2011.

4. Proposta de Implementação de um Sistema Online Gerenciador de Certificados Digitais Finais, Autoridade Certificadora, Autoridade de Registro, Modelo Público. 01/05/2011 a 30/11/2012.

4.3 Coordenação e Participação em Projeto de Extensão

A Tabela 4 lista os projetos de extensão universitária que foram coordenados.

Tabela 4: Coordenação e Participação em Projetos de Extensão

Título	**Instituição**	**Período**
João de Barro	Instituto Nacional de Tecnologia da Informação (ITI)	2003 - 2008

[1] dgp.cnpq.br/dgp/espelhogrupo/1660457225829962

Gestão Estratégica da Tecnologia da Informação e da Comunicação (TIC)		20/04/2006 a 13/07/2006
Elaboração de Substitutivo ao Projeto ANOREG de Modernização Cartorial	Associação Nacional dos Notários e Registradores - ANOREG	16/10/2006 a 14/11/2006
Auditoria da Eleição interna para Diretoria, Conselho Deliberativo e Conselho Fiscal da Fundação CODESC de Seguridade Social - FUSESC.	Fundação de Ensino de Engenharia de Santa Catarina - FEESC.	01/10/2005 a 30/06/2006
Projeto Sala Cofre, Software e procedimentos do Módulo Criptográfico-MSC para ICP-Brasil.	Associação Nacional dos Notários e Registradores - ANOREG	01/01/2005 - ????
Projeto Sala Cofre, Software e procedimentos do Módulo Criptográfico-MSC para ICP-Brasil.	Instituto Nacional de Tecnologia da Informação (ITI) e Financiadora de Estudos e Projetos (FINEP)	01/01/2005 a 30/06/2008
Projeto Sala Cofre, Software e procedimentos do Módulo Criptográfico-MSC para ICP-Brasil.	Instituto Nacional de Tecnologia da Informação (ITI) e Financiadora de Estudos e Projetos (FINEP)	01/07/2008 a 30/06/2009
Revisão e validação do Padrão Brasileiro de Assinatura Digital.	Instituto Nacional de Tecnologia da Informação (ITI)	01/07/2009 a 30/11/2009
Manutenção de Aprimoramento dos Sistemas Ywapa/Ywyra v. 3.0.	Instituto Nacional de Tecnologia da Informação - ITI	11/12/2012 a 11/12/2013
Atualização e Manutenção no Sistema de Gerenciamento de Certificados(SGC) versões softwares Ywapa/Ywyra. 1º aditivo.	Instituto Nacional de Tecnologia da Informação - ITI	03/01/2011 a 30/04/2012
Certificado de Identificação Móbile para Acesso Seguro a Ambientes de Telessaúde e Telemedicina	FINEP	27/01/2011 a 27/09/2013
Desenvolvimento Conjunto de Pesquisa Aplicada para Reconstrução do Sistema de Gerenciamento de Certificados do SERPRO (SGCS) Versão Online	Serviço de Processamento de Dados (SERPRO)	01/03/2012 a 31/08/2014
Desenvolvimento de uma Infraestrutura, para a Criação de um Ambiente Chamado Cartório Digital *Criação de um Ambiente Chamado Cartório Digital*	Câmara Brasileira de Comércio Eletrônico (Camara-Net)	01/03/2011 a 29/02/2012

Desenvolvimento do Softwares Assinador de Referência versão 2.0 Verificador de Conformidade e Gerador de Políticas.	Instituto Nacional de Tecnologia da Informação (ITI)	03/09/2012 a 03/03/2014
Sistema Gerenciador de Certificados de Atributos (SGCA)	Instituto Nacional de Tecnologia da Informação (ITI)	03/12/2012 a 02/07/2014
Manutenção de Aprimoramento dos Softwares Ywapa/Ywyra.	Instituto Nacional de Tecnologia da Informação (ITI)	03/01/2011 a 31/12/2011
Padrão Brasileiro de Assinatura Digital - Implementação de Referência.	Colégio Notarial do Brasil	01/11/2011 a 31/10/2013
Projeto Bry Cloud	Bry Tecnologia Ltda.	06/08/2012 a 02/05/2015
Proposta de Implementação de um Sistema Online Gerenciador de Certificados Digitais Finais.	Instituto Nacional de Tecnologia da Informação (ITI)	01/05/2011 a 30/11/2012
Manutenção dos Códigos de Referência do Padrão Brasileiro de Assinatura Digital.	Instituto Nacional de Tecnologia da Informação (ITI)	09/02/2015 a 09/02/2016
Assinador PAdES ICP-Brasil Bry	Bry Tecnologia	01/04/2015 a 01/06/2017

5 Coordenação de Cursos e Representações

Desde o início de minha carreira acadêmica, tenho procurado contribuir na coordenação de cursos seja participando de comissões ou mesmo dos colegiados delegados.

6 Participação em Bancas

Este capítulo apresenta a lista a participação em bancas de mestrado e doutorado ao longo da vida acadêmica. Foram um total de 83 bancas de mestrado e 8 de doutorado, sendo uma de doutorado na Alemanha.

6.1 Bancas de Mestrado

1. Julíbio David Ardigo O Desenvolvimento da Comunidade Virtual: Polígrafo Computadorizados para Sinais Biomédicos. 1994. Dissertação (Mestrado em Engenharia de Produção) - UFSC.

2. Antônio Luiz Fernandes. Sistema de Backup de Dados Digitais baseado em Gravador de Vídeo VHS. 1991. Dissertação (Mestrado em Engenharia Elétrica) - Universidade Federal de Santa Catarina.

3. Ricardo Alexandre Reinaldo de Moraes. Resolução de Modelos Matemáticos pelo Método dos Elementos Finitos em Geometrias Não-convexas. 1999. Dissertação (Mestrado em Ciências da Computação) - UFSC.

4. Tais Freire da Silva Costa. Avaliação Analítica do Uso de Agentes Móveis na Gerência de Redes. 1999. Dissertação (Mestrado em Ciências da Computação) -UFSC.

5. Daniela Barreiro Claro. Integração de Bases de Dados Utilizando Mobilidade de Código.2000. Dissertação (Mestrado em Ciências da Computação) -UFSC.

6. Daniela Vanassi de Oliveira. Mobilidade em Gerência de Redes. 2000. Dissertação (Mestrado em Ciências da Computação) - UFSC.

7. Maurílio Alves Martins da Costa. Avaliação Analítica de Desempenho do Uso do IPv6. 1999. Dissertação (Mestrado em Ciências da Computação) - UFSC.

8. André Barros de Sales. Medidas de latência em Ambientes de Processamento de Alto Desempenho. 2000. Dissertação (Mestrado em Ciências da Computação) - UFSC

9. Marcelo Luiz Brocardo. Protocolo Para Transação de Crédito Seguro Criptográfico. 2000. Dissertação (Mestrado em Ciências da Computação) - UFSC.

10. Marco André Lopes Mendes. Modelo Simplificado para o Cifrador RC6.2000.2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

11. Mehran Misaghi. Criptossistemas Caóticos. 2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

12. Kathia Regina Lemos Jucá. Aspectos de Segurança em Sistemas de Agentes Móveis. 2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

13. Adriana Elissa Notoya. IARSDE - Infra Estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos: Validade do documento eletrônico por tempo indeterminado. 2002. Dissertação (Mestrado em Ciências da Computação) - UFSC.

14. Abiel Roche Lima. Gerência da largura de banda para garantir QOS adaptável em Rede sem fio Ad Hoc. 2000. Dissertação (Mestrado em Ciências da Computação) - UFSC.

15. Laurentino Augusto Dantas. Protocolo Criptográfico Para a Emissão de Certidão de Nascimento na WEB.2001.Dissertação (Mestrado em Ciências da Computação) - UFSC.

16. Glauco Vinícius Scheffel. Avaliação não Presencial Segura da Aprendizagem.2002. Dissertação (Mestrado em Ciências da Computação) - UFSC.

17. João Luiz Francalacci Rocha. Proteção de Software por Certificação Digital. 2000. Dissertação (Mestrado em Ciências da Computação) - UFSC.

18. Luiz Carlos Cancelier de Olivo. Informatização do Judiciário e processo digital: limites e possibilidades a partir da recuperação da lei 9800/99. 2001. Dissertação (Mestrado em Direito) - UFSC

19. Eduardo Kessler Piveta. Framework de Suporte a AOP em Object Pascal. 2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

20. Abiel Roche Lima. Gerência da largura de banda para garantir QOS adaptável em Rede sem fio Ad Hoc. 2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

21. Augusto Jun Devegili. Farnel: Uma Proposta de Protocolo Criptográfico para Votação Digital. 2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

22. Roberto Carlos Dariva. A Segurança de Aplicações e Comércio Eletrônico na Internet. 2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

23. Anna Lúcia Anacleto Reis. Comparação SNMP x Agentes Móveis para Gerência de Redes. 2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

24. Juliana Amaral Arantes. Agentes Móveis Versus SNMP - Uma avaliação de desempenho analítica. 2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

25. Roberto Samarone dos Santos Araújo. Protocolos Criptográficos para Votação Digital. 2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

26. Everton Schonardie Pasqual. IDDE - Uma Infra-estrutura para a Datação de Documentos Eletrônicos. 2002. Dissertação (Mestrado em Ciências da Computação) - UFSC.

27. Ana Karina Dourado Salina de Oliveira. Geradores de Números Randômicos Caóticos. 2002. 0 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

28. Kathia Regina Lemos Jucá. Aspectos de Segurança em Sistemas de Agentes Móveis. 2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

29. Luciano Ignaczak. Um novo modelo de Infra-estrutura de Chaves Públicas para uso no Brasil utilizando aplicativos com o código fonte aberto. 2002. 0 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

30. Dejane Luiza Bortoli. O Documento Eletrônico no Ofício de Registro Civil de Pessoas Naturais. 2002. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

31. Maria Eloisa Mignoni. Políticas e Declaração de Práticas de Certificação Digital para a UFSC. 2002. 159 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

32. Raquel Aparecida Pegoraro. Segurança no Comércio Eletrônico. 2002. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

33. Emiliano Soares Monteiro. Autenticação e Permissão no Sistema Operacional Aurora. 2002. Dissertação (Mestrado em Ciências da Computação) - Universidade Federal de Santa Catarina.

34. Alessandro Freitas de Oliveira. Sistema de Detecção de Intrusão Baseado em Aplicação.2002. Dissertação (Mestrado em Ciências da Computação) - UFSC.

35. Guilherme Eliseu Rhoden. Detecção de Intrusão em backbones Através da Análise de Comportamento com SNMP e JAVA. 2002. Dissertação (Mestrado em Ciências da Computação) - UFSC.

36. Alexandre Briani Kieling. Implementação de um Sistema de Gerência para o Serviço Diferenciado Premium. 2002. Dissertação (Mestrado em Ciências da Computação) - UFSC.

37. Morvan Daniel Müller. Uma Solução de Autenticação Fim a Fim para o LDP (Label Distribution Protocol). 2002. Dissertação (Mestrado em Ciências da Computação) - UFSC.

38. Marco Antônio Torrez Rojas. Utilização de Algoritmos Genéticos no Projeto de Caixas-S para Cifradores de Bloco Simétricos. 2002. 0 f. Dissertação (Mestrado em Ciências da Computação) - UFSC.

39. Andréia Vergara da Silva. Uma Aplicação da Transformação Wavelet à Verificação On-Line de Assinaturas Manuscritas. 2002. Dissertação (Mestrado em Ciências da Computação) - UFSC

40. Adriano Fiorese. Avaliação de Desempenho do Uso de Agentes Móveis na Gerência de Redes Utilizando Técnicas de Medidas. 2001. Dissertação (Mestrado em Ciências da Computação) - UFSC.

41. Edison Alessandro Xavier. Aplicação de Inteligência Computacional na Gerência de Redes através da Automatização do uso de Agentes Móveis. 2003. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

42. Fernando Cézar de Oliveira Lopes. Sistema de Denúncia Anônima Segura. 2003. Dissertação (Mestrado em Ciências da Computação) - UFSC

43. Fernando Carlos Pereira. Criptografia Temporal: Aplicação Prática em Processos de Compra. 2003. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

44. Antônio Casagrande. Técnicas de Detecção de Sniffers. 2003. Dissertação (Mestrado em Computação) - Universidade Federal do Rio Grande do Sul.

45. Luciana Rita Guedes Ghisleri. Proposta de um Protocolo Criptográfico Para Auditoria de Publicidade na Web. 2003. Dissertação (Mestrado em Ciências da Computação) - UFSC.

46. Ernesto Hermann Warnecke. G-DEF - Protocolo Criptográfico para Geração de Documento Eletrônico Fiscal nas Operações entre Empresas. 2003.Dissertação (Mestrado em Ciências da Computação) - UFSC.

47. Krishnan Lage Pontes. Proposta de um Modelo de Qualidade de Serviço e Segurança para a Tecnologia de Web Services. 2003. Dissertação (Mestrado em Ciências da Computação) - Universidade Federal de Santa Catarina.

48. Genilda Oliveira Araújo. Lottuseg: Um Protocolo Seguro para Loteria Digital. 2003. Dissertação (Mestrado em Ciências da Computação) - UFSC.

49. Débora Cabral Nazário. Análise da Segurança da Urna Eletrônica e do Sistema Eleitoral Brasileiro.2003. Dissertação (Mestrado em Ciências da Computação) - UFSC.

50. Júlio da Silva Dias. Confiança no Documentos Eletrônico.2003.Dissertação (Mestrado em Ciências da Computação) - UFSC.

51. Vanessa Costa. Análise da Confiança do Sistema de Protocolação Digital de Documentos. 2003. Dissertação (Mestrado em Ciências da Computação) - UFSC.

52. Denise Bendo Demétrio. Infra-estrutura e Protocolação Digital de Documentos Eletrônicos. 2003. Dissertação (Mestrado em Ciências da Computação) - UFSC.

53. Paulo Sérgio Ribeiro. Um Protocolo Criptográfico Para Comunicação Anônima Segura em Grupo. 2003. Dissertação (Mestrado em Ciências da Computação) - UFSC.

54. Emerson Ribeiro de Mello. Redes de Confiança em Sistemas de Objetos CORBA. 2003. Dissertação (Mestrado em Engenharia Elétrica) - UFSC.

55. Juliano Fontoura Kazienko. Assinatura Digital de Documentos Eletrônicos através da Impressão Digital. 2003. Dissertação (Mestrado em Ciências da Computação) - UFSC.

56. Edmar Roberto Santana de Rezende. Segurança no Acesso Remoto VPN. 2004. Dissertação (Mestrado em Ciência da Computação) - UFSC.

57. Fabiano Castro Pereira. Técnicas Criptográficas para Anonimato em Redes de Computadores: Aplicação no Sistema de Votação Digital Ostracon. 2004. Dissertação (Mestrado em Ciências da Computação) - UFSC.

58. José Eduardo Malta de Sá Brandão. Congregação de Sistemas de Auditoria: Uma abordagem Orientada a Serviços Para Construção de Sistemas de Detecção de Intrusão de Larga Escala.2004.(Mestrado em Engenharia Elétrica) - UFSC.

59. Jean Everson Martina. Projeto de Provedores de Serviços Criptográficos Embarcados. 2005. Dissertação (Mestrado em Ciências da Computação) - UFSC

60. Carlos Eduardo Mazzi. Emissor de Cupom Fiscal Virtual. 2005. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

61. Luciana Moreira Sá de Souza. Mobsec - Adaptando Serviços de Armazenamento Seguro para Dispositivos Móveis. 2005. Dissertação (Mestrado em Engenharia Elétrica) - UFSC.

62. Alexsandra Carvalho da Silva. Uma Solução de Assinatura Digital Curta Especial Baseada em uma Variação do DSA Gerada em Dispositivo Pessoal. 2005. Dissertação (Mestrado em Ciências da Computação) - UFSC.

63. Paulo Manoel Mafra. Comunicação Segura na Composição de IDSs e seus Custos. 2006. Dissertação (Mestrado em Engenharia Elétrica) - UFSC.

64. Clytia Higa Tamashiro. Análise de Protocolos de Roteamento Anônimo para Redes Sem Fio Ad Hoc Móveis. 2007. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

65. Marcelo Carlomagno Carlos. Topologias Dinâmicas de Infra-estrutura de Chaves Públicas. 2007. Dissertação (Mestrado em Ciências da Computação) - UFSC..

66. Wylber Polonini. Validação Eficiente de Certificados Digitais. 2007. Dissertação (Mestrado em Ciência da Computação) - Universidade Estadual de Campinas.

67. Juliano Romani. Integração de Serviços de Relógio para Infra-Estrutura de Chaves Públicas. 2008. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC..

68. Túlio Cícero Salvaro de Souza. Aspectos Técnicos e Teóricos da estão do Ciclo de Vida de Chaves Criptográficas no OpenHSM. 2008. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

69. Rogério Ferreira da Cunha. Abordagens para a Escuta Legal em VoIP. 2008. Dissertação (Mestrado em Computação) - Universidade Federal Fluminense.

70. Rafael José Deitos. Otimização de Algoritmos Seguros de Programação Linear Aplicados na Geração do Plano Diretor da Cadeia Logística. 2009. Dissertação (Programa de Pós-Graduação em Engenharia de Automação e Sistemas) - UFSC.

71. Tiago da Costa. Modernização dos Serviços de Registro Público do Brasil: Proposta da Averbação Eletrônica de Penhora de Imóveis. 2009. Mestrado Profissional em Administração - Universidade do Estado de Santa Catarina - UDESC.

72. Joelson de Alencar de Degaspari. Um Sistema de Detecção de Intrusão Baseado em Rede Neural e Imunologia Artificial. 2009. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - Universidade Federal de Santa Catarina.

73. Fabrício Abrão Costa. Proposta de um Modelo para a Automação e uso do Documento Eletrônico Seguro nos Processos de Realização de Auditoria e Fiscalização da ICP-Brasil. 2010. Dissertação (Mestrado em Administração) - Universidade do Estado de Santa Catarina- UDESC.

74. Martin Augusto Gagliotti Vigil. Infraestrutura de Chaves Públicas Otimizadora. 2010. Dissertação (Mestrado em Ciências da Computação) - UFSC.

75. Jeandré Monteiro Sutil. Gestão Segura de Múltiplas Instâncias de uma mesma Chave de Assinatura em Autoridades Certificadoras. 2011. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

76. Nelson da Silva. Preservação por Longo Prazo de Assinaturas Digitais. 2011. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

77. Thiago Acórdi Ramos. Preservação do Sigilo e Autenticidade de Documentos Eletrônicos por Longo Prazo. 2011. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

78. Jonathan Gehard Kohler. Gestão de Políticas e de Algoritmos Criptográficos na Integração de Infraestrutura de Chaves Públicas. 2011. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

79. Cristian Thiago Moecke. NKPKI - Uma ICP Baseada em Autoridades Notariais. 2011. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

80. Bernardo Caraponale Magri. Assinatura Digital Rabin-Williams sem Randomização e com Prova Eficiente de Segurança. 2011. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - Universidade de São Paulo - USP.

81. Dayana Pierina Brustolin Spagnuelo. Protocolo Flexível de Autenticação Multifator: Estudo de caso para Ambientes de Telemedicina. 2013. Dissertação (Mestrado em Ciências da Computação) - UFSC.

82. Rick Lopes de Souza. Um Middleware para Compartilhamento de Documentos Sigilosos em Nuvens Computacionais. 2014. Dissertação (Mestrado em Ciências da Computação) - UFSC.

83. Thaís Bardini Idalino. Using combinatorial group testing to solve integrity issues. 2015. Dissertação (Mestrado em Programa de Pós-graduação em Ciência da Computação) - UFSC.

6.2 Bancas de Doutorado

1. Júlio da Silva Dias. Confiança no Documento Eletrônico. 2004. 150 f. Tese (Doutorado em Engenharia de Produção) - UFSC

2. Carlos Roberto de Rolt. O Desenvolvimento da Comunidade Virtual: Uma Proposta para Melhoria da Qualidade e da Comercialização de Software. 2000. Tese (Doutorado em Engenharia de Produção) - UFSC

3. Julíbio David Ardigo. Modelo de Infra-estrutura de Chaves Públicas Aplicado a Processos de Avaliação Somativa à Distância. 2004. Tese (Doutorado em Engenharia de Produção) - UFSC

4. Michelle Silva Wangham. Esquema de Segurança para Agentes Móveis em Sistemas Abertos. 2004. Tese (Doutorado em Engenharia Elétrica) - UFSC.

5. Fernando Carlos Pereira. Serviços de Segurança em Sistemas Distribuídos Dinâmicos. Exame de Qualificação de Doutorado. (Doutorado em Engenharia Elétrica) - UFSC.

6. Roberto Alves Gallo Junior. Um "Framework"para Desenvolvimento e Implementação de Sistemas Seguros Baseados em Hardware. 2012. Tese (Doutorado em Doutorado em Ciência da Computação - UNICAMP) - Universidade Estadual de Campinas.

7. Juliano Fontoura Kazienko. Armazenamento Seguro de Chaves Criptográficas em Redes de Sensores Sem Fio. 2013. Tese (Doutorado em Computação) - Universidade Federal Fluminense.

8. Martín Augusto Gagliotti Vigil. Trustworthy and Efficient Protection Schemes for Digital Archiving. 2015. Tese (Doutorado em Computação) - Technische Universität Darmstadt.

6.3 Outras Bancas

Participou-se também de algumas bancas examinadoras de concurso público para professor, destacando-se:

1. Banca Examinadora de Concurso Público. Área de conhecimento Rede de Computadores e Banco de Dados. 1995. Universidade do Estado de Santa Catarina - UDESC.

2. Banca Examinadora de Concurso Público. Para Professor Efetivo do Centro de Ciências da Administração e Sócio-Econômicas. 2010. Universidade do Estado de Santa Catarina - UDESC.

3. Banca Examinadora de Concurso Público. Para Professor Efetivo do Centro de Ciências da Administração e Sócio-Econômicas. 2011. Universidade do Estado de Santa Catarina - UDESC.

7 Organização e Participação em Eventos

7.1 Organização de Eventos

Foram vários eventos organizados ao longo da carreira docentes. A seguir, lista-se alguns desses eventos:

1. I Workshop sobre Módulos de Segurança Criptográfica, 2005. Neste evento foi apresentado o hardware criptográfico desenvolvido pelo grupo de pesquisa. Várias palestras foram proferidas por pesquisadores e alunos que participaram do desenvolvimento do equipamento;

2. II Workshop LabSEC: Plataformas Criptográficas para Infra-estrutura de Chaves Públicas e Aplicações, 2008. Este evento foi organizado para apresentar as pesquisas que estavam sendo feitas sobre plataformas criptográficas pelo grupo de pesquisa do LabSEC;

3. Participou-se da coordenação do Workshop de Gestão de Identidades Digitais (WGID 2012), que foi realizado em conjunto com o XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2012);

4. II Advanced School on Cryptology and Information Security in Latin America (AS-Crypto 2013), Florianópolis, Brasil, 17-20 October 2013. Conjuntamente com os professores Ricardo Dahab na Unicamp e professor Daniel Panario da Carleton University, coordenamos essa escola de criptografia avançada em Florianópolis. Maiores informações no link: http://www.ic.unicamp.br/ascrypto2013;

5. Third International Conference on Cryptology and Information Security in Latin America (Latincrypt 2014). Florianópolis, 2014. Professor Daniel Panario da Carleton University e eu formos os coordenadores gerais desse evento internacional, realizado no Costão do Santinho. Maiores informações no link:
http://latincrypt2014.labsec.ufsc.br/;

6. Workshop on Finite Fields, Combinatorics and Cryptographical Applications. 2015. Conjuntamente com a professora Lucia Moira da University of Ottawa e o professor Daniel Panario da Carleton University, organizou-se esse evento em Florianópolis. Maiores informações no link: http://people.math.carleton.ca/ daniel/conf/FFCCA.

8 Apresentação de Palestras e Cursos

8.1 Palestras em Eventos como Convidado

Foram ministradas as seguintes palestras como convidado.

1. Seminário na disciplina Tópicos Especiais em Linguagens de Programação (INE 5339). Algoritmos de Computação Algébrica e Simbólica. UFSC. 1994.
2. Seminário de Computação Algébrica. Algoritmos Algébricos. UFSC. 1994.
3. III Semana da Pesquisa. UFSC. A Função de Iteração Dinâmica. Sistemas de Apoio no Ensino de Matemática. 1995.
4. Aspectos Operacionais de uma Autoridade Certificadora. 12º Seminário da Rede Nacional de Ensino e Pesquisa (RNP) de Capacitação e Inovação. 2006.
5. I Workshop de Tecnologia da Informação da IFES. Projeto ICPEDU. 2007.
6. III Jornadas de Seguridad y Firma Electrónica. Infraestructura de Certificación Electrónica para Entidades de Investigación y Enseñanza. Venezuela. 2007.
7. 6th Annual PKI R&D Workshop. Temporal Key Release Infrastructure.EUA.2007.
8. XV Congresso Notarial Brasileiro. O documento eletrônico no setor notarial: repositório legal preservação de longo prazo. 2008.
9. I Encontro em Teoria dos Códigos e Criptografia. Universidade Federal do ABC. 2010.
10. XIV Semana de Informática da UFPA. Infraestrutura de Chaves Públicas Brasileira e o Futuro da Internet .2011.
11. Seminários 2011 da Pós-Graduação. Uma ICP baseada em Autoridades Notariais. Unicamp .2011.
12. 9º Certforum - Etapa Florianópolis . Contribuição Relevante nos 10 anos da ICP-Brasil. 2011.
13. Tech Talk #9 - Tecnologias de Certificação Digital para a Segurança de Documentos Eletrônicos. 2011.
14. XI Simpósio Brasileiro - SBSEG. Carimbos do Tempo Autenticados para a Preservação por Longo Prazo de Assinaturas Digitais. 2011.

15. Workshop de Gestão de Identidade. Análise e Implementação de um Protocolo de Gerenciamento de Certificados. 2011.

16. III Workshop de Computação Aplicada em Governo Eletrônico - WCGE. Inovação Tecnológica com Certificação Digital. 2011.

17. III Padrão Brasileiro de Assinatura Digital. Notarial. Colégio Notarial do Brasil/Instituto Nacional da Tecnologia da Informação. Entrega do Novo Assinador Digital de Referência ao ITI. 2011.

18. III 1 º Workshop Sobre Propriedade Intelectual. RNP. 2011.

19. Aula Inaugural da Pós-Graduação em Segurança da Informação. Unidade Central de Educação Faem Faculdade - UCEFF. 2011.

20. XVI Simpósio de Direito Notarial. Colégio Notarial do Brasil - Seção de São Paulo - CNB/SP. 2011.

21. Ciclo de Palestras-Segurança Digital. Universidade Federal do Espírito Santo - UFES. 2011

22. VIII Conferência Internacional de Perícias em Crimes Cibernéticos - ICCyber. 2011.

23. III XIII workshop da RNP. Desafios para uma Rede de Dados Segura. Minas Gerais - MG. 2012.

24. 11th Annual On Vector Photonics Workshop. University of California. 2012.

25. Participação Primeiro Fórum RNP, espaço de debates sobre cultura digital e o papel das Tic's. I Panorama da gestão de identidade no Brasil. Brasília. 2012.

26. Escola Regional de Informática Norte 3 - II ERIN 3. Instituto Luterano de Ensino Superior - ILES. 2012.

27. Assinatura Digital de Documentos Eletrônicos com Reconhecimento de Firma. Universidade Estadual de Campinas - UNICAMP. 2012.

28. Debate FINEP. Modelo de Certificação Digital adotado no Brasil, os conceitos Básicos de infraestrutura de chaves públicas e como podem melhorar a confiança na internet. 2012.

29. III Seminário Processo de Homologação de Equipamentos ICP-Brasil. Instituto Nacional de Tecnologia da Informação - ITI. 2013

30. II Fórum RNP, espaço de debates sobre cultura digital e o papel das Tic's. Gestão de Identidade. Brasília. 2013.

31. III 41º Seminário de TIC Para Gestão Pública- SECOP. Segurança de Documentos Eletrônicos. Espírito Santo. 2013.

32. III Conferência - Terena Networking. RNP. Holanda. 2013.

33. 31º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. Painel: Desafio para uma Rede de Dados Segura. 2013.

34. 14º Workshop RNP - WRNP. Simpósio Brasileiro de Redes de Computadores. Atualizações do comitê Técnico de Gestão de Identidade. 2013.

35. 2º Congresso Iberoamericano de Investigadores y Docentes de Derecho e Informática - CIIDDI. Painel: Segurança da Informação. 2013.

36. VII Workshop de TIC das IFES. Gestão de Identidade. 2013.

37. III Workshop da RNP, painel sobre visão de futuro em GID.SBRS. Rio de Janeiro. 2015.

8.2 Cursos, Especializações e Aperfeiçoamento de Curta Duração

Participei como docente, ao longo de minha carreira, de diversos cursos de especialização e aperfeiçoamento, a fim de formar profissionais graduados em Ciência de computação ou áreas afins, em empresas e em instituições de ensino em diversas regiões do Brasil. Essas foram as principais participações:

1. Curso de Programação Maple V. dentro da disciplina de Sistemas de Computação Algébrica Pós-Graduação em Ciências da Computação. UFSC. 1995.

2. Curso Básico de Computação Algébrica. 1996

3. Curso de Calculadora HP48. 1996.

4. Definição e Organização do Papel da UDESC no contexto da Rede Catarinense de Ciência - RCT e Tecnologia.1996

5. Redefinição da Rede Local de Comunicação de Dados do CFH/UFSC.1996.

6. Ministrou a Disciplina: Segurança no Comércio Eletrônico - Convênio UFSC e Universidade de Várzea Grande - UNIVAG. 2002.

7. Minicurso: Tecnologia da Informação Segura na IV Escola de Informática Norte da Sociedade Brasileira de Computação - SBC - Universidade da Amazônia - UNAMA - Belém-PA- 2002.

8. Minicurso: Tecnologia da Informação Segura - IV Escola de Informática Norte da Sociedade Brasileira de Computação - SBC - Macapá, AP. 2002.

9. Curso de Especialização em Redes de Computadores e Sistemas Distribuídos. Joinville. 2003 e 2004.

10. Curso de Especialização em Ciência da Computação. Oeste de Santa Catarina. 2004.

11. Curso de Especialização em Segurança de Dados, em nível de Pós-Graduação na área de Ciência da Computação - Cuiabá. 2004-2005.

12. Minicurso no 17º Seminário de Capacitação e Inovação - RNP. ICPEDU: Introdução a Infraestrutura de Chaves Públicas e Aplicações. 2011.

13. Treinamento para Softwares Ywapa e Ywyra. Valid. 2011.

9 Comendas e Premiações

1. Prêmio Técio Pacitti - Siemens Menção Honrosa - Programa do SSI'2003. 5º Simpósio Segurança em Informática. Instituto Tecnológico de Aeronáutica - ITA. 2003.

2. Em 2008 fui professor homenageado pela Turma de Formandos em Computação, Turma 2008.1 (Veja Figura 2);

Figura 2: Homenagem Formandos em Computação 2008.1.

3. Em Maio de 2011, fui homenageado pelo Instituto Nacional de Tecnologia da Informação, responsável pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) pelo empenho individual para a desenvolvimento e a implantação de iniciativas voltadas para a certificação digital e para a ICP-Brasil como um todo (Veja Figura 3);

Figura 3: Homenagem 10 anos de ICP-Brasil.

4. Em Novembro de 2012, fui um dos homenageados em Seção da Assembleia Legislativa de Santa Catarina como um dos colaboradores da Fundação Centros de

Referência em Tecnologias Inovadoras (CERTI) pela minha atuação em prol do desenvolvimento tecnológico do Estado de Santa Catarina[1] (Veja Figura 4).

Figura 4: Homenagem ALESC.

[1] http://agenciaal.alesc.sc.gov.br/index.php/noticia_single/parlamento-presta-homenagem-a-fundacaeo-certi

10 Atividades Editoriais e Arbitragem de Produção Intelectual

Tenho participado de atividades editoriais e de arbitragem de produção intelectual desde o início de minha carreira acadêmica. A lista a seguir lista minhas principais participações.

10.1 Membro de Comitê de Programa Científico

1. Fórum de Certificação Digital - CertForum 2012. Florianópolis, 2012.
2. III Workshop em Segurança de Sistemas Computacionais (WSeg 2003);
3. IV Workshop em Segurança de Sistemas Computacionais (WSeg 2004);
4. WORKCOMP-SUL 2004
5. V Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2005);
6. VI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2006);
7. VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2007);
8. VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2008);
9. IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2009);
10. X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG 2010);
11. XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG 2011);
12. XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (WGID 2011);

13. XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG 2012);
14. Workshop sobre Gestão de Identidades (WGID 2012);
15. XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG 2013);
16. Workshop sobre Gestão de Identidades (WGID 2013);
17. XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG 2014);
18. Workshop sobre Gestão de Identidades (WGID 2014);
19. Workshop sobre Gestão de Identidades (WGID 2015);
20. XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG 2016);
21. Workshop sobre Gestão de Identidades (WGID 2016);
22. XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG 2017);

11 Participação de Órgãos de Fomento

Tenho feito avaliação de projetos de pesquisa submetidos à Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

12 Atividades de Administração

12.1 Supervisão em Laboratórios

Desde o retorno às minhas atividades acadêmicas, após a conclusão do doutorado, conduzi a supervisão de dois laboratórios de pesquisa e desenvolvimento, vinculados ao Departamento de Informática e de Estatística (INE) da Universidade Federal de Santa Catarina (UFSC): o Laboratório de Computação Algébrica e Simbólica (LabCAS); e o Laboratório de Segurança em Computação (LabSEC).

1. Supervisor do Laboratório de Computação Algébrica e Simbólica (LabCAS) entre os anos 1999 a 2000;

2. Supervisor do Laboratório de Segurança em Computação (LabSEC) entre os anos 2000 a 2017.

No início, no ano 2000, o LabSEC era uma pequana sala num dos corredores do antigo prédio onde estava abrigado o Departamento de Informática e de Estatística. Trabalhou-se duro para que o LabSEC tivesse uma infraestrutura adequada para o desenvolvimento de atividades de pesquisa científica e tecnológica. O LabSEC cresceu, tanto em produção tecnológica quanto em produção científica, tornando-se um centro de pesquisa e inovação de referênca na área de segurança computacional, torando-se conhecido, nacional e internacionalmente.

O LabSEC tem por objetivo estudar, pesquisar, avaliar e implementar soluções na área de segurança em computação, e em particular: criptografia; assinatura digital; segurança em sistemas computacionais; infraestrutura de chaves públicas; e protocolos criptográficos.

O LabSEC procura incentivar alunos de graduação a realizarem iniciação científica e posteriormente seu Trabalho de Conclusão de Curso (TCC) dentro de suas instalações. Posteriormente, os alunos são incentivados a realizar mestrado e doutorado. Vários egressos do LabSEC estão hoje realizando doutoramento em importantes centros de pesquisa na área de segurança computacional nos Estados Unidos e na Europa.

O laboratório tem recebido importantes recursos de agências de fomento, destacando a Finep e várias empresas público/privadas. Entre os resultados de pesquisa do laboratório destacam-se a protocoladora digital de documentos eletrônicos, a qual foi transferida para a iniciativa privada e um dispositivo criptográfico, denominado HSM, utilizado pela Autoridade Certificadora Raiz Brasileira (ICP-Brasil).

12.2 Representação em Colegiados

Como forma de contribuir para a gestão e melhoria dos cursos onde tenho ministrado aulas, tenho procurado participar como membro ativo dos seus colegiados. A seguir lista-se a minha participação como membro titular de alguns desses colegiados.

1. Membro do Colegiado do Curso de Pós-Graduação em Ciência da Computação (Representante Titular) de 1999 a 2001.
2. Membro de Colegiado do Curso de Graduação em Sistemas de Informação (Representante Titular) de 2001 a 2004.
3. Membro de Colegiado do Curso de Graduação do Curso de Graduação em Ciência da Computação (Representante Titular) de 2001 a 2004.

12.3 Outras Representações

1. Representante da Sociedade Brasileira de Computação (SBC) como membro titular no Comitê Gestor da Infraestrtutura de Chaves Públicas Brasileira deste 25 de setembro de 2008;
2. Gerência de Desenvolvimento do Site de Pós-Graduação em Ciência da Computação de acordo com o Art.6 do Regimento do Curso.1999-2001.
3. Coordenador de Turma de Mestrado Fora de Sede em Ciência da Computação - Convênio SENAC e CPGCC/UFSC.1999.
4. Membro da Comissão para elaboração de proposta de reestruturação curricular do currículo 96.1 na Área de Teoria da Computação, na Área de Matemática e na Área de Redes. 2000.
5. Membro da Comissão de Seleção dos Processos de Transferência Interna, Externa e de Retorno . Curso de Sistemas de Informação.2002.
6. Membro da Comissão de Avaliação de Estágio Probatório professor: Lau Cheuk Lung.2007.
7. Membro do Comitê Gestor da ICP-Brasil - Infra-estrutura de Chaves Públicas Brasileiras. Casa Civil . 2008.
8. Membro da Comissão para estabelecer e manter políticas de utilização de serviços de acesso e de segurança para a Rede de Computadores do INE.

Referências

BREGMAN, A.; ACHIM, A.; AHAD, P. The MAPLE software system. *Montreal, Quebec, Canada: McGill University*, 1992. Citado na página 10.

CUSTÓDIO, R. F. *Codificadores paramétricos de sinais de voz com excitação multi-pulso*. Dissertação (Mestrado) — Programa de pós-graduação em Engenharia Elétrica (PPGEEL) da Universidade Federal de Santa Catarina (UFSC), Florianópolis, Brasil, 1990. Citado na página 9.

CUSTÓDIO, R. F. *Análise Não-Linear no Reconhecimento de Padrões Sonoros: Estudo de Caso para Sons Pulmonares*. Tese (Doutorado) — Programa de Pós-Graduação em Computação (PPGC) da Universidade Federal do Rio Grande do Sul (UFRGS), 1999. Citado na página 10.

OLIVEIRA, L. P. D.; ROQUE, W. L.; CUSTÓDIO, R. F. Lung sound analysis with time-dependent fractal dimensions. *Chaos, Solitons & Fractals*, Elsevier, v. 10, n. 9, p. 1419–1423, 1999. Citado na página 10.