Collaborative Approach to Security Risk Management Information

Maicon Balke, Lisandra M. Fontoura, Luís A. L. Silva

Programa de Pós-Graduação em Informática
Universidade Federal de Santa Maria – UFSM
Santa Maria, Brasil
{maiconbalke, lisandramf, silva.luisalvaro}@gmail.com

Abstract – Risk management is one of the main management processes of security information since it aims to identify, analyze, evaluate and control risks that are due to security information. To utilize users´ experiences in this process, the utilization of collaborative tasks allows one to exploit argumentative interactions between project participants that are involved in the development of risk management debates regarding security information. The goal of this paper is to propose an argumentation-based collaborative approach to deal with such risk management of security information. The approach aims to guarantee that activities defined in a security risk management process are executed accordingly. In it, a set of rules is proposed to ensure that the final security risk management debate is complete and consistent with the arguments presented by participants of a security software project. This communication protocol is tailored to a process of security risk management that was particularly defined from the ISO / IEC 27005. The protocol allows users to structure and control risk discussions developed by debate participants using a web-based tool called RD System. Through this system, a case study was developed to validate the approach proposed in this work.

Keywords- Risk Security Management, Collaboration, Dialogue Games, Argumentation.

I. INTRODUÇÃO

Segundo o Federal Information Security Management Act (FISMA) [1], segurança da informação se refere a proteger os sistemas de informação e as informações contra acesso não autorizado ou uso indevido dessas informações. As atividades relacionadas à segurança da informação têm como objetivo identificar e eliminar as vulnerabilidades de sistemas de computador ou redes de computadores. Porém, os problemas de muitas organizações na implementação de segurança da informação estão relacionados com a dificuldade em definir o que deve ser protegido, qual o nível de proteção necessário e quais ferramentas devem ser utilizadas [2].

A priorização das ações em segurança da informação e a falta de exploração das atividades de gestão de risco de segurança de informação (GRSI) podem ser consideradas duas das maiores dificuldades na gestão de segurança [3]. Normalmente, existe uma ideia de que tudo em segurança é importante, mas comumente não existem recursos financeiros para tratamento de todos os riscos. Em 2012, foi realizado um estudo pela empresa Kaspersky [4], no qual foram entrevistadas 3300 organizações em 22 países, incluindo o Brasil. O resultado do estudo traz a informação de que, para 42% dos entrevistados, a importância dos problemas com crimes virtuais, como roubo de dados, exposição de dados importantes, entre outros, deve aumentar nos próximos anos.

Se a estimativa estiver correta, existirão ainda mais problemas e, como consequência destes, poderão ocorrer eventos que afetarão a integridade, disponibilidade e confiabilidade dos ativos organizacionais. Por esse motivo, torna-se necessário o uso de uma sistemática para identificar os possíveis riscos de segurança de informação em projetos de Tecnologia de Informação e para elaborar um plano de gerenciamento de riscos descrevendo as ações a serem tomadas durante o projeto para manter os fatores de risco sob controle [5]. Além disso, é importante a colaboração entre os membros da equipe do projeto visando englobar diferentes visões, compartilhar conhecimento e experiências e fomentar uma discussão sobre riscos de segurança. É importante que pessoas de diferentes níveis organizacionais, tais como gerentes e desenvolvedores participem do processo decisório, pois o conhecimento acerca de um projeto geralmente encontra-se disperso em diferentes fontes.

Atualmente, muitas organizações utilizam o desenvolvimento distribuído de software [6][7]. Neste tipo de desenvolvimento, diferentes equipes podem trabalhar em diferentes locais, com diferentes fusos horários, dificultando a realização de reuniões presenciais ou videoconferência. Ferramentas de colaboração assíncronas possibilitam a participação de membros que atuam em equipes distribuídas geograficamente [7].

Técnicas de argumentação, assim como sistemas de argumentação típicos, conforme descrito em [8] e [9], podem ser usadas para facilitar a organização e a compreensão de um diálogo, e dessa forma, auxiliar no desenvolvimento de discussões assíncronas. No cenário de técnicas de argumentação, optou-se por usar jogos de diálogo [10] no desenvolvimento deste trabalho. Em especial, jogos de diálogo descrevem como organizar a troca de argumentos em uma discussão, por meio da definição de um protocolo de comunicação [10]. Entre outras características, essa estrutura de representação de conhecimento visa identificar e representar passos significativos de interação humana que são típicos de diálogos [11].

Um dos problemas relacionados a utilização de jogos de diálogos em tarefas de aquisição e representação de argumentos em discussões colaborativas é a produção de discussões muitas vezes incoerentes, onde argumentos apresentados podem estar incompletos. Estas podem levar a equipe do projeto a tomar decisões não acertadas, principalmente por não seguir um processo sistemático de gerenciamento de riscos de segurança da informação. Para

garantir que as atividades típicas de gerenciamento de riscos de segurança sejam exploradas nestes cenários de discussão colaborativa que é organizado por um jogo de diálogo, este trabalho formaliza e estrutura discussões de riscos de segurança da informação com base nas atividades descritas na norma ISO/IEC 27005. Essa norma foi escolhida porque ela descreve um processo sistemático de segurança da informação. Além disso, visando garantir a obtenção de uma discussão completa e bem estruturada neste problema de aplicação foram propostas regras para validação da consistência de discussões realizadas. As regras têm como objetivo garantir que todas as atividades descritas em um processo de gerenciamento de riscos, elaborado a partir da ISO/IEC 27005, sejam executadas em uma ordem pré-definida. Um sistema web para apoiar as discussões de riscos – Risk Discussion system (RD system) – é utilizado com o propósito de gerenciar protocolos e interações entre os *stakeholders*, assim disponibilizando um ambiente colaborativo para discussões de riscos de segurança. As discussões de riscos são registradas em uma memória e validadas por meio de um conjunto de regras.

A principal contribuição deste trabalho é a proposta de um protocolo para jogos de diálogos visando atender as necessidades de uma discussão colaborativa de riscos de segurança da informação. Este protocolo utiliza um processo para garantir que a colaboração seja realizada de forma consistente auxiliando os gestores na tomada de decisões sobre riscos de segurança. Para satisfazer este objetivo foram definidos um protocolo de debate, um processo de debate baseado na ISO/IEC 27005 e um conjunto de regras de validação da discussão.

O artigo está organizado da seguinte forma: na Seção 2 são apresentados conceitos relacionados a gestão de riscos de segurança da informação, argumentação e jogos de diálogos em um contexto colaborativo. Na Seção 3 é apresentada a abordagem colaborativa para gerenciamento de riscos de segurança da informação. Na Seção 4 é apresentado um estudo de caso e na Seção 5 são apresentados os trabalhos relacionados. Na Seção 6 discutidas as considerações finais e trabalhos futuros.

II. FUNDAMENTAÇÃO TEÓRICA

Nesta seção é apresentada uma fundamentação teórica sobre gerenciamento de riscos de segurança da informação e jogos de diálogos, os quais fundamentam ao trabalho proposto.

A. Gerenciamento de riscos de segurança da informação

Gerenciamento de risco de segurança tem como objetivo principal a redução de riscos e a proteção de ativos organizacionais [12]. Este gerenciamento busca a aplicação coordenada de meios financeiros para minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos. Em geral, o objetivo é um conjunto de princípios e práticas que visa identificar, analisar e tratar riscos que possam vir a ocorrer, impactando negativamente os ativos da organização[1].

A análise de risco é definida como o uso sistemático de informações para identificar fontes e para estimar a probabilidade e impacto do risco. Esta análise é composta pela identificação de ativos, vulnerabilidades, ameaças e consequências. Se a análise de risco não for realizada corretamente, a seleção de contramedidas falhará e o processo de gestão de risco não será bem sucedido [13]. A análise do risco envolve definir a probabilidade de uma ameaça atacar com sucesso um ativo por meio de uma vulnerabilidade particular deste ativo. Assim, a determinação do risco depende da análise de ativos, vulnerabilidades e ameaças [2].

É preciso também compreender que cada novo controle introduzido para tratar um risco específico produz um risco residual e pode introduzir surgimento ou desaparecimento de novos riscos. Diante desse cenário complexo para a segurança, mais especificamente, a gestão da segurança organizacional, pelo menos três atividades podem ser identificadas e executadas nesta ordem[14]:

- Levantamento do perfil de riscos de segurança da organização;
- Adoção de controles de segurança compatíveis com o perfil de riscos da organização;
- Reavaliação.

Diferentes métodos de gestão de riscos de segurança da informação foram criados, tais como: como NIST 800-39 [2], AS / NZS 4360[15], ISO/IEC 27005. Atualmente, a norma ISO / IEC 27005 é bastante utilizada para implementar sistemas de gestão de segurança da informação pelo fato de fornecer orientações detalhadas sobre a implementação de suas atividades e de como adaptá-las a diferentes tipos de organização (de pequeno a grande porte) [16]. Já outros metodos como a NIST 800-39 estabelecem métodologias que centralizam o gerenciamento em torno do patrimônio como NIST 800-39[17].

A norma AS / NZS 4360[15] fornece às organizações um processo básico de gestão de risco de segurança da informação, o qual facilita sua aplicabilidade. Mas esse gerenciamento não se aplica a ambientes mais complexos, nos quais será necessário o apoio de outras normas [18].

A ISO/IEC 27005 fornece diretrizes para o gerenciamento de riscos de segurança da informação e dá sustentação aos conceitos especificados na ISO 27001:2005 [17], além de auxiliar na implementação e certificação de tais sistemas de gestão. De acordo com a norma, o processo de gestão de riscos é composto pelas seguintes atividades:

- Definição do contexto: visa definir o escopo e limites do processo de GRSI;
- Análise e avaliação de riscos: visa identificar, estimar e avaliar os riscos;
- Tratamento do risco: envolve definir as ações de tratamento do risco de maneira mais eficiente e com menor custo;
- Aceitação do risco: envolve registrar formalmente a aprovação de planos de tratamento do risco.
- Comunicação do risco: envolve transmitir informações referentes aos riscos a todas as partes interessadas.
- Monitoramento e análise crítica de riscos: tem como objetivo identificar eventuais mudanças no contexto, certificando também que o processo e suas atividades relacionadas permaneçam apropriados durante todo o processo de gestão de riscos.

B. Argumentação

Técnicas de argumentação têm como princípio o ato de usar argumentos para explicar ou justificar um ponto de vista apresentado por um agente, seja esse humano ou

computacional. Argumentos são declarações que podem ou não ser verdadeiras em um ponto da discussão, visto que essas declarações devem considerar o auxílio (ou apoio) ou o questionamento (ou contra-argumento) de outros argumentos [19]. Modelos de argumentação alternativos [20] também têm sido explorados no desenvolvimento de sistemas inteligentes de apoio à solução de problemas em diferentes aplicações de argumentação. Nestas aplicações, um processo de argumentação, no qual é desenvolvido um debate entre agentes, pode ser organizado por meio da exploração de um modelo de jogo de diálogo [8][9].

Em um cenário colaborativo de diálogo, a construção de uma fala diz respeito ao modo com que afirmações podem ser capturadas e combinadas. Assim, a definição da sintaxe de um protocolo de jogo de diálogo geralmente envolve a especificação de possíveis locuções que os agentes podem utilizar e quais são os movimentos típicos entre locuções utilizadas pelos agentes. Um dos principais benefícios de um modelo deliberativo é a sua capacidade de fornecer um cenário padronizado para as interações que ocorrem entre participantes envolvidos em tais discussões colaborativas [5].

A utilização de jogos de diálogo e regras adicionais em discussões colaborativas é uma forma de garantir a organização e coerência dos diálogos [22]. Isso tende a evitar problemas e perda do controle da ordem em que os argumentos são inseridos na discussão, o que poderia vir a dificultar a compreensão do significado dos argumentos utilizados pelos participantes [23]. Ou seja, um conjunto de regras de combinações é descrito por combinações que expressam a forma como estas locuções podem ser executadas (por exemplo, que locução pode ser usada como resposta a determinadas locuções). Para contemplar tais combinações, o modelo proposto por Walton[24] para "esquemas de argumentação" discute como dois ou mais participantes podem produzir uma discussão envolvendo argumentos bem formados e completos os quais podem levar a conclusões melhor fundamentadas ou sólidas.

III. UMA ABORDAGEM COLABORATIVA PARA GERENCIAMENTO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

A exploração de um jogo de diálogo para o desenvolvimento de tarefas de gerenciamento de riscos de segurança da informação permite que participantes discutam de forma colaborativa os riscos inerentes à segurança da informação em projetos de software. Nesse debate, os participantes podem expressar a sua opinião sobre vulnerabilidade, ameaças e riscos envolvendo os ativos. Além disso, podem ser elaborados planos para tratamento de riscos identificados na discussão para que estes possam ser prevenidos, minimizados ou eliminados. Esse processo de diálogo organizado por um jogo de diálogo tem um claro contraste com uma discussão colaborativa realizada de forma *ad hoc*, onde os participantes de determinado debate poderão chegar a discussões incoerentes, inconsistentes e muitas vezes incompletas. Desse modo, a adoção de processos sistemáticos torna-se adequada por garantir que determinados passos de debate sejam devidamente seguidos em uma sequência pré-definida. É sabido que decisões tomadas a partir de discussões que não seguem corretamente um protocolo podem chegar a conclusões equivocadas e gerar inconsistências no processo como um todo [22]. Desta forma, a abordagem proposta visa estabelecer um processo para discussão de riscos de segurança de informação baseado na norma ISO/IEC 27005. O protocolo descreve um conjunto de locuções e regras de interação entre as locuções. Para garantir a consistência e completude do processo são estabelecidas regras de consistência da discussão, visando garantir que todas as etapas da discussão sejam executadas de forma consistente.

A. Protocolo para colaboração em riscos de segurança da informação

Para a construção de um protocolo de gerenciamento colaborativo de riscos de segurança, é necessário descrever as locuções, que podem ser: iniciação, finalização, gerais ou específicas e regras de interação entre locuções. As locuções que determinam o início e o término da discussão são mostradas na Tabela 1. Locuções gerais são aquelas que os participantes usam de forma geral para fomentar a discussão, tais como: perguntar, pedir opinião, argumentar contra, argumentar a favor; assim como apresentado em [25][26]. Locuções específicas são relacionadas ao domínio do problema a ser tratado na locução. No caso deste trabalho, o domínio é GRSI e as locuções foram definidas a partir da norma ISO/IEC 27005.

A partir da análise desta norma, atos de locução foram definidos para cada atividade proposta pela ISO. Para cada atividade foi definido um conjunto de locuções que possibilitam aos participantes da discussão executar as atividades previstas pela norma.

O foco principal da discussão é a análise, avaliação e o tratamento dos riscos. Essas atividades são executadas no início de cada projeto, na etapa de planejamento. A definição das locuções se deu da seguinte forma: para cada atividade descrita na norma ISO/IEC-27005 foi analisada quais locuções seriam necessárias para que a atividade fosse realizada em uma discussão de riscos. Também foram consideradas as entradas e saídas, ações e guias de implementação descritos na ISO/IEC 27005. Essas locuções são descritas na Tabela 2.

Tabela 1 – Locuções do protocolo de comunicação que determinam o início e término de uma discussão de riscos

Nome: **Iniciar Discussão** Descrição: Iniciar a discussão com uma afirmação a respeito do assunto a ser abordado no processo de gerenciamento de riscos de segurança da informação. Exemplo: *Iniciar Discussão*: Discussão do módulo de consulta.
Nome: **Terminar Discussão** Descrição: Terminar a discussão, não permitindo mais a inserção de novos argumentos no processo de gerenciamento de riscos. Exemplo: *Terminar Discussão:* Discussão finalizada.

Tabela 2 – Atos de locuções específicos para discussão das tarefas de gerenciamento de riscos de segurança da informação

Nome: **Propor Ativo** Descrição: possibilita ao participante propor um novo ativo para ser discutido. Exemplo: *Propor Ativo:* Dados Sigilosos
Nome: **Propor Valor** Descrição: possibilita ao participante propor um valor para um ativo proposto previamente. Exemplo: *Propor Valor:* de uma escala de 0 a 10 considero 7.
Nome: **Propor Impacto**

Descrição: possibilita ao participante propor um impacto para um ativo proposto previamente.
Exemplo: *Propor Impacto:* De uma escala de 0 a 10 considero que o impacto deste risco é 8.

Nome: **Propor Probabilidade**
Descrição: possibilita ao participante propor a probabilidade de uma vulnerabilidade proposta previamente.
Exemplo: *Propor Probabilidade:* A probabilidade de ser explorada é baixo.

Nome: **Propor Ameaça**
Descrição: possibilita ao participante propor uma ameaça para uma vulnerabilidade proposta previamente.
Exemplo: *Propor Ameaça:* Saturação do sistema de informação.

Nome: **Propor Vulnerabilidade**
Descrição: possibilita ao participante propor uma vulnerabilidade para um ativo proposto previamente.
Exemplo: *Propor Vulnerabilidade:* Criptografia usada para proteger dados está ultrapassada.

Nome: **Propor Risco**
Descrição: possibilita ao participante propor um risco para um ativo proposto previamente.
Exemplo: *Propor Risco:* Informações confidenciais de clientes.

Nome: **Propor Tratamento**
Descrição: possibilita ao participante propor um tratamento para um risco proposto previamente.
Exemplo: *Propor Tratamento:* Criar criptografias mais avançadas.

Nome: **Propor Consequência**
Descrição: possibilita ao participante propor uma consequência para um ativo proposto previamente.
Exemplo: *Propor Consequência*: Afeta integridade e com isso os dados podem ser divulgados ou modificados causando transtorno e prejuízo.

Nome: **Propor Controle**
Descrição: possibilita ao participante propor controles existentes para um ativo proposto previamente.
Exemplo: *Propor Controle: é usado padrão de senhas padronizados no ano de 2000.*

Em geral, argumentos em uma discussão podem ser contestados de alguma forma, sendo eles uma afirmação ou uma interrogação. Neste contexto, locuções voltadas para a captura e representação de movimentos críticos (investigatórios) de debate foram definidas e são mostradas na Tabela 3:

Tabela 3 – Atos de locuções de propósito geral que visam permitir uma discussão crítica de riscos e seus planos

Nome: **Argumentar a Favor**
Descrição: possibilita ao participante expressar argumento favorável a uma locução proposta previamente.
Exemplo:
Propor Plano: Implementar novas técnicas de criptografia
Argumentar a favor: Concordo, isso irá minimizar as chances de invasão.

Nome: **Argumentar Contra**
Descrição: possibilita ao participante expressar argumento desfavorável a uma locução proposta previamente.
Exemplo:
Propor Impacto: De uma escala de 0 a 10 considero 8.
Argumentar Contra: O impacto é 5, levando em consideração o contexto onde é discutido.

Nome: **Informar**
Descrição: possibilita ao participante expressar uma informação a uma locução proposta previamente.
Exemplo: *Informar:* Este tratamento será implementado.

Nome: **Perguntar**
Descrição: possibilita ao participante questionar sobre uma locução proposta previamente.
Exemplo: *Perguntar*: Este ativo é realmente importante?

Nome: **Retirar**
Descrição: possibilita ao participante a retirada de uma locução proposta previamente.
Exemplo:
Argumento contra: Esse ativo tem valor baixo.
Argumento contra: Este ativo é importante para a empresa, por isso tem um valor alto
Retirar: Ok.

Nome: **Pedir Opinião**
Descrição: possibilita ao participante pedir opinião de outros participantes referente a locução proposta previamente.
Exemplo: *Pedir Opinião:* Todos concordam que o impacto do risco é alto?

Nome: **Opinar**
Descrição: possibilita ao participante expressar opinião em relação a uma locução proposta previamente.
Exemplo: *Pedir Opinião:* Todos concordam que o impacto do risco é alto?
Opinar: Sim.

B. Processo para GRSI em uma discussão colaborativa

O processo proposto visa estruturar as atividades envolvidas em uma discussão colaborativa de riscos, garantindo que os participantes executem tais atividades em uma sequência pré-definida pelo fluxo do processo. O processo pode ser visualizado na Figura 1. Este processo foi baseado no fluxo de atividades da norma ISO/IEC 27005 e tem como foco as atividades envolvidas no planejamento de riscos inicial, que são: a análise e avaliação de riscos e o tratamento dos riscos identificados. Além do fluxo de execução, foram elaboradas regras que visam garantir a execução de todas as atividades (completude) e restrições e condições sobre as locuções (consistência).

A sequência do processo foi definida a partir dos objetivos da atividade e das entradas e saídas de cada atividade proposta pela ISO/IEC 27005.

C. Regras de combinações entre Locuções

As regras de combinação descrevem o contexto de cada ato de locução, de forma a organizar o progresso do diálogo. As regras foram classificadas nas seguintes categorias: *regras de início*, *regras de transição*, *regras internas a etapa* e *regras de finalização*, que são descritas a seguir:

- *Regra de Início:* é a regra que dará início a discussão.
- *Regra de Transição*: valida se requisitos mínimos para passar para a próxima etapa da discussão são satisfeitos. Por exemplo, para se propor um risco é necessário ter proposto uma vulnerabilidade, um controle e um valor para o ativo.
- *Regra Interna a Etapa*: verifica se a etapa foi finalizada com todos os requisitos ou somente atingiu o requisito mínimo para continuar a discussão.
- *Regra de Finalização*: valida se a discussão pode ser finalizada, isto é se todas as etapas do processo da discussão foram realizadas com sucesso.

Como exemplo de uma regra interna a etapa, pode-se especificar que é obrigatório utilizar o ato "*informar*" em resposta à locução "*perguntar*."

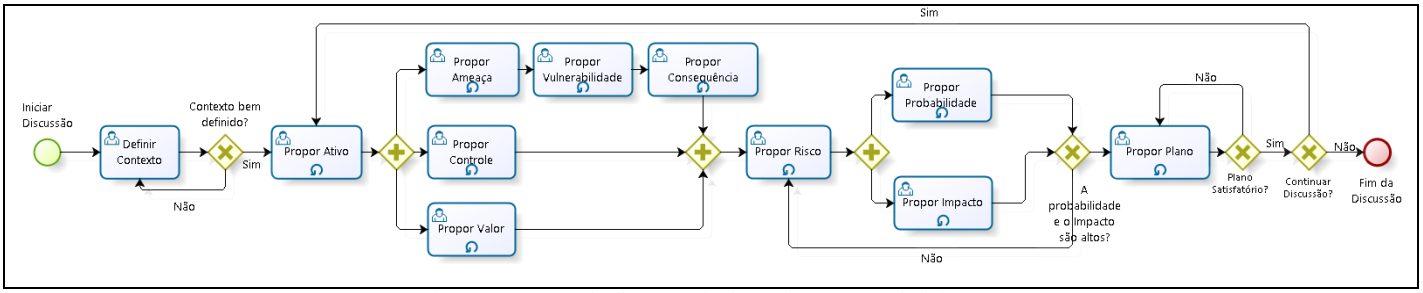

Figura 1: Processo de discussão de riscos de segurança da informação

Para que o processo seja completo, um conjunto de regras estabelecido para serem aplicada em uma discussão foi definido. Exemplos dessas regras podem ser visualizadas na Tabela 4. Como resultado da aplicação das práticas, é possível identificar atividades não executadas ou inconsistências na execução do processo. Neste caso, os participantes da discussão precisam resolver as inconsistências tornando as discussões completas, evitando transtorno em recuperações de fragmentos de discussões incompletas no futuro. Caso inconsistências identificadas não forem resolvidas, a discussão ficará com status de inconsistente.

Tabela 4 – Fragmento de regras de transição de etapa.

Regra 1. Locução **Iniciar_Discussão(.)**: Locução: **Iniciar_Discussão**(*t, Pi*), onde t é a descrição do início da discussão, e *Pi* é qualquer participante no âmbito do diálogo. **Precondição:** Deve ter sido realizado um cadastro de Organização (*Pi*), juntamente com seu contexto. **Significado:** Permite ao participante (*Pi*) dar início a discussão de gestão de riscos colaborativo. Por exemplo: um participante propõe a discussão "Essa discussão tem como objetivo mitigar riscos do Projeto X".
Regra 2. Locução **Finalizar_Discussão(.)**: Locução: **Finalizar_Discussão**(*t, Pi*), onde t é a descrição do fim da discussão, e *Pi* é qualquer participante no âmbito do diálogo. **Precondição:** Deve existir no mínimo a locução *Iniciar_Discussão*(*t, Pi*) na discussão. **Significado:** Permite ao participante(*Pi*) finalizar a discussão de gestão de riscos colaborativo. Por exemplo: um participante propõe a locução "esta discussão foi finalizada com êxito".
Regra 3. Locução **Propor_Ativo(.):** Locução: **Propor_Ativo**(*t,Pi)*, onde *t* é a descrição do Ativo, e *Pi* é qualquer participante no âmbito do diálogo. **Precondição:** Deve ter a locução *Iniciar_Discussão(t,Pi)* por qualquer participante no âmbito do diálogo. **Resposta:** Deve haver a Locução *Pedir_Opinião(t,Pi)* como nó filho *de Propor_Ativo*(*t,Pi)* por qualquer participante no âmbito do diálogo. Bem como a Locução *Opinar(t,Pi)* como nó filho de *Pedir_Opinião(t,Pi)* pela maioria dos participante no âmbito do diálogo **Validação:** A locução *Propor_Ativo*(*t,Pi)* deverá ter a maioria das opiniões obtidas por meio da locução *Opinar(t,Pi),* tanto positivas quanto negativas. Sendo elas positivas, a proposta de ativo é considerada válida e a discussão pode continuar; caso contrário, a proposta é descartada e o usuário tem que propor um novo Ativo. **Significado:** permite a proposição de ativos em um debate de gestão de riscos colaborativo. Por exemplo: um participante da discussão pode propor "Servidor" como um ativo.
Regra 4. Locução **Propor_Impacto(.).** Locução: **Propor_Impacto**(*t,Pi)*, onde *t* é a descrição do impacto do Risco, e *Pi* é qualquer participante no âmbito do diálogo. **Precondição:** Deve ter a locução *Propor_Risco* (*t,Pi)* finalizada, inserida por qualquer participante no âmbito do diálogo. **Resposta:** Sem Validação **Validação:** A locução *Propor_Impacto* (*t,Pi)* deverá ter no máximo uma proposta válida. Caso houver mais de uma locução *Propor_Impacto* (*t,Pi)* como nó filho da locução *Propor_Risco* (*t,Pi,)* uma das propostas terá que ser descartada. **Significado:** permite a proposição do impacto causado pelo Risco discutido em um debate de gestão de riscos colaborativo. Por exemplo: um participante propõe que o Risco Acesso não autorizado, e o Impacto em uma escala de 0 a 10, tem um valor 8.

No estudo de caso apresentado neste artigo é exemplificado como essas locuções e regras são utilizadas em uma discussão de riscos de segurança.

D. RD System

O Risk Discussion system (RD system)[27] é responsável pela interpretação de um protocolo de diálogo. Desse modo, o sistema tem controle sobre as interações entre os participantes de acordo com regras de combinação entre locuções. Por exemplo, ao selecionar uma locução, o sistema habilita um grupo de outras novas locuções que antes não estavam a disposição do usuário. Neste caso, essas novas locuções só poderão ser utilizadas após a seleção pelo usuário da locução em questão, obedecendo regras de uso estipuladas pelo protocolo. As discussões são constituídas por uma locução, seguida de um texto livre digitado pelos usuários. Por exemplo, ao selecionar a locução "propose active", o participante de uma discussão pode descrever um ativo que deseja propor na discussão e, a partir desta locução, podem ser selecionadas diversas outras locuções, tais como: "propose vulnerability", "ask position", "propose plan". Como resultado, estas discussões são estruturadas em formato hierárquico de árvore. Cada locução corresponde a um nó da árvore, sendo que cada locução inserida se refere a outra locução já proposta anteriormente, sendo apresentada como um nó filho de uma locução pai. Para inserção de argumentos na discussão, basta selecionar o nó desejado (pai) e a locução disponível no

protocolo, juntamente com a apresentação de um conteúdo textual para um argumento. No final, é possível coletar discussões estruturadas, as quais podem ser sistematicamente registradas em uma memória de discussão colaborativa de riscos. Por meio do Risk Discussion system (RD system) [27], os usuários são capazes de armazenar suas discussões de risco em uma memória que contém experiências concretas de gestão de risco colaborativo. O sistema também contém recursos de consulta para esta memória, onde os usuários podem procurar determinadas locuções de gestão de riscos avançadas em discussões passadas [28], sendo que as locuções são os índices para buscar na memória de discussões de risco (por exemplo, um participante do diálogo busca uma lista de "planos propostos" em discussões passadas sobre riscos).

Para o gerenciamento das regras no processo de discussão, algumas modificações foram acrescentadas no sistema Risk Discussion system (RD system) facilitando a validação da consistência da discussão. Como parte deste trabalho, o modulo desenvolvido tem como objetivo validar a discussão com base no conjunto de regras mostrado na Tabela 3. O RD system possibilita ao usuário definir novas locuções, bem como selecionar se um usuário deseja utilizar uma determinada validação (regra) ou não em um determinado debate. Cada locução está ligada a uma determinada regra. Por exemplo, só é possível utilizar uma determinada locução se algumas locuções obrigatórias já tenham sido utilizadas pelo menos uma vez. Caso isso não aconteça, o RD system acusa esse problema durante a verificação da discussão capturada. Uma questão importante é que as regras propostas e implementadas neste sistema devem ser válidas para vários tipos de protocolos de diálogo carregados no sistema. Desta forma, usuários podem incluir novas locuções no protocolo, e o RD System permite que as regras de validação sejam personalizadas para se adaptar aos novos protocolos.

IV. ESTUDO DE CASO

Um estudo de caso foi realizado com a intenção de validar o trabalho proposto. Primeiramente, é descrito o cenário de segurança de informação fictício e, posteriormente, os resultados do estudo de caso.

A. Cenário

Uma organização busca contribuir com a segurança dos dados de clientes por meio de soluções de segurança em um banco de dados. Para garantir a integridade de dados hospedados, a organização tem de ser capaz de oferecer os serviços de segurança esperados. Esta organização possui representantes espalhados por todo o território nacional.

A missão da organização envolve atividades de servidor de dados. Neste contexto, ela visa proteger a informação de diversos tipos de ameaça para garantir a continuidade dos negócios, minimizando os danos causados por acessos indevidos a informações e maximizando o retorno dos investimentos aplicados em segurança de dados e as oportunidades de negócio. Dentre as competências relacionadas à segurança da informação desta organização, algumas podem ser citadas:

- A garantia de que a informação está acessível somente a pessoas com acesso autorizado;
- A salvaguarda da exatidão e completude da informação e dos métodos de processamento;
- A garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário;
- A garantia de que padrões são verificados e validados;
- Cumprimento de diretrizes e procedimentos operacionais necessários para garantir a segurança da informação.

B. *Problema*:

As ameaças, cada vez mais especializadas e inovadoras, superam as estratégias de proteção estabelecidas na organização. Neste caso, esta organização ainda não consegue acompanhar a evolução constante de invasores. Assim, ela sofre com os custos monetários oriundos de incidentes. Portanto, é possível perceber que a organização ainda precisa se dedicar mais a definição e implantação de métodos de proteção. Por exemplo, a detecção de invasores não é efetiva e ainda há um grande desconhecimento deste serviço por parte da empresa. Baseado neste cenário, uma discussão de riscos de segurança é realizada com pessoas ligadas à segurança da informação da organização. Portanto, os participantes da discussão são membros da equipe ou partes interessadas do projeto. Sendo assim, diferentes experiências podem ser capturadas e exploradas na discussão, proporcionando uma chance maior de sucesso em aplicar tratamentos para proteger os ativos.

C. Definição do Contexto

O contexto deste problema é cadastrado no RD System, onde os gestores identificam requisitos funcionais e o contexto do projeto que está sendo discutido. Estes requisitos podem ser derivados dos objetivos de nível mais alto do sistema. Este cadastro é feito pelo gerente de projeto a fim de disponibilizar todas as informações possíveis aos demais participantes da discussão.

A Figura 2 mostra um fragmento de discussão, elaborado no RD System. Na Figura 2 pode-se visualizar algumas inconsistências e partes incompletas na discussão. Neste caso, a validação desta discussão inicia quando qualquer usuário da discussão seleciona o botão “verificar”. A partir daí, a discussão é validada com base no conjunto de regras de validação pré-estabelecido.

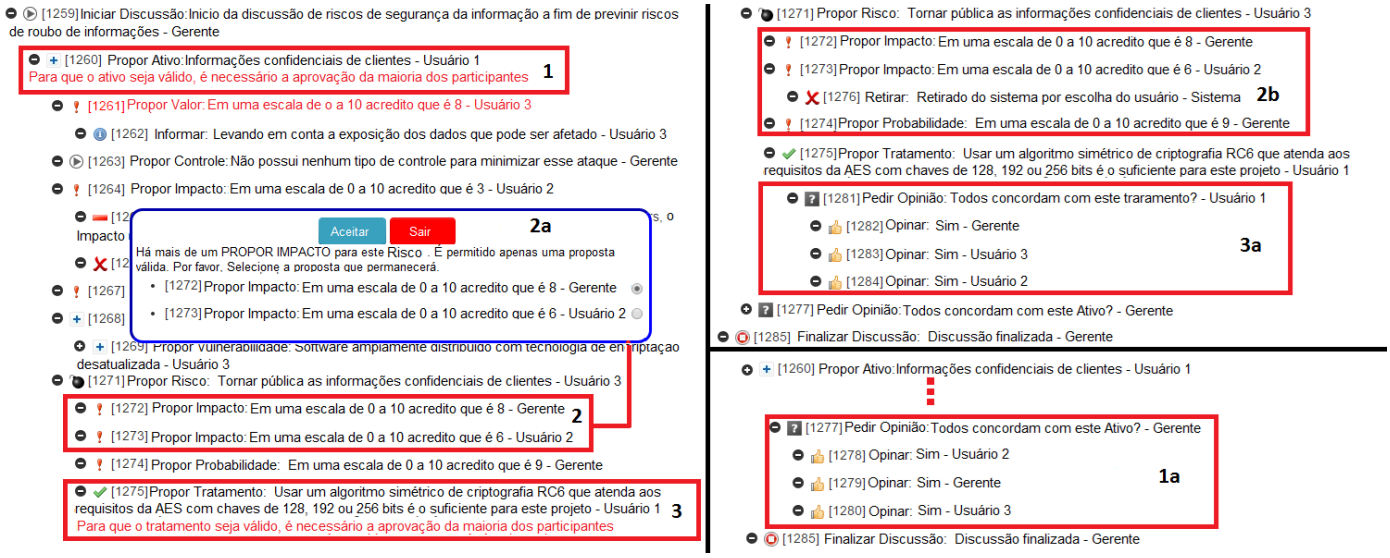

Figura 2: fragmento de uma discussão inconsistente juntamente com as correções

Na Figura 2 é exibido um fragmento da discussão sobre riscos de segurança da informação para o estudo de caso. Neste fragmento existem algumas inconsistências que são comuns em discussão que são encerradas sem que as mesmas sejam verificadas, gerando problemas de para consultas futuras.

Algumas regras propostas por esse trabalho foram aplicadas e são explicadas a seguir.

Regra 1: Validação de Ativo

- **Tipo:** completude
- **Objetivo:** determina que para um ativo ser considerado válido na discussão, a maioria dos participantes deve concordar com a proposição do ativo, ou seja, que o ativo é adequado ao contexto do projeto para o qual está sendo feito a discussão.
- **Descrição da regra:** quando a locução *Propor Ativo* é encontrada pelo algoritmo de validação, é executada a regra 3 descrita na Tabela 4 para validação. Essa regra determina que, após a proposição de um valor para o ativo, a maioria dos participantes deve opinar por meio da locução *Pedir Opinião* para que o valor do ativo seja considerado válido. No caso desta discussão, não foi utilizada a locução *Pedir Opinião*. Porém, o gerente pode usar a locução *Pedir Opinião* como nó filho de *Propor Ativo* como mostra o fragmento 1a da Figura 2. Assim, os participantes poderão opinar se o ativo é ou não válido. A partir disso, o algoritmo detecta quantas locuções *Opinar* existe na discussão e então verifica se a maioria dos participantes opinou a favor ou contra. Caso a maioria dos participantes opinou contra, o algoritmo invalida o Ativo proposto (como mostrado na Figura 2 – fragmento 1) e então terá que ser proposto um novo Ativo para a discussão.

Regra 2: Duplicidade de Locuções

- **Tipo:** Consistência
- **Objetivo:** tem como objetivo validar se uma locução filho aparece mais de uma vez para uma mesma locução pai, enquanto só deveria ser permitida uma única locução.
- **Descrição da Regra:** algumas locuções como propor impacto, propor probabilidade devem aparecer uma única vez para cada ativo identificado. Quando mais de uma locução deste tipo aparece, a discussão fica inconsistente, pois não é possível identificar quais dos valores propostos é o valor válido para o ativo. Para tratar desta inconsistência, o responsável poderá escolher um das locuções propostas como válida, ou poderá fomentar a discussão para que todos os participantes cheguem a um consenso e retirar manualmente o impacto(s) inválido(s). Quando a locução *Propor Impacto* é encontrada pelo algoritmo de validação, é executada a regra 4 descrita na Tabela 4 para validação. Essa regra determina que não pode haver mais de um impacto proposto para o mesmo risco. No caso dessa discussão, existe mais de um impacto proposto como mostrado na Figura 2 – fragmento 2. Quando o algoritmo de validação detecta essa inconsistência, o sistema exibe um formulário (como exibido na Figura 2 – fragmento 2a), questionando qual das locuções *Propor Impacto* deve ser considerada. Assim, o gerente escolhe o impacto válido e o outro retirado automaticamente pelo sistema incluindo a locução *Retirar* como mostrado na Figura 2 - fragmento 2b, ou pode cancelar o recurso e fomentar a discussão para que as pessoas envolvidas discutam até chegar a uma conclusão e efetuem a operação de retirar o impacto inválido manualmente.

Regra 3: Validação Propor Tratamento

- **Tipo:** completude
- **Objetivo:** determina que para que um plano de tratamento seja considerado válido é necessário que a maioria dos participantes concorde com o plano

proposto, caso contrário o plano de tratamento deve retirado e terá que ser proposto outro novamente.

- **Descrição da Regra:** quando a locução *Propor Tratamento* é encontrada pelo algoritmo de validação, é executada a regra 3 descrita na Tabela 4 para validação. Essa regra determina que, após a proposição de um tratamento para o risco, a maioria dos participantes deve opinar por meio da locução *Pedir Opinião,* para que o tratamento de minimização ou mitigação do risco seja válido. No caso desta discussão, a locução pedir opinião não foi utilizada, porém o gerente pode, usando a locução pedir opinião como nó filho de *Propor Tratamento*, pedir a opinião dos demais participantes da discussão como mostrado na Figura 2 – fragmento 3a. A partir disso, o algoritmo detecta quantas locuções *Opinar* existe na discussão e então verifica se a maioria dos participantes opinou a favor ou contra. Caso a maioria dos participantes opinou contra, o algoritmo invalida o tratamento proposto e então terá que ser proposto um novo tratamento para o risco.

V. TRABALHOS RELACIONADOS

Yuan [29] explora a ideia que a avaliação de riscos de segurança usando técnicas de argumentação pode ser formalizada como uma troca de argumentos entre assessores, os quais são especialistas em segurança e agentes de ameaças hipotéticas. Na prática, os avaliadores discutem como o sistema pode ser atacado por um agente de ameaça e os assessores defendem o sistema para verificar se a especificação satisfaz um determinado requisito de segurança. A proposta apresentada não considera técnicas de validação de discussões capturadas segundo o modelo de argumentação proposto. Este trabalho também não suporta discussões que são realizadas por equipes geograficamente distribuídas.

Franqueira *et al.* [30] exploram o uso de catálogos compartilhados de experiência em segurança para apoiar a avaliação de riscos e para orientar a argumentação de segurança na busca de respostas e fraquezas para a satisfação de requisitos de segurança. Baseia-se em dois principais conceitos propostos por Haley *et al.* [31], que são: a noção da satisfação de requisitos de segurança, bem como a utilização de argumentos divididos entre argumentos externos e internos para demonstrar a segurança do sistema. Os argumentos externos e internos estão relacionados da seguinte forma: o argumento externo formal oferece a estrutura principal que conduz a argumentação interna. Cada uma das premissas dos argumentos externos é o começo para uma lista de discussão de argumentos internos onde os participantes podem argumentar de forma informal. Ele fornece uma visão intuitiva sobre a evolução de um argumento no formato de um debate entre dois oponentes. É representado como uma estrutura de árvore de argumentos e contra-argumentos.

Prakken *et al.* [32] propõem uma abordagem de argumentação sob medida para avaliação de riscos. Ele substitui argumentos informais, propostos por Toulmin, por argumentos *aspic* em uma tentativa de formalizar o processo como um jogo de argumentação em que a equipe troca argumentos sobre como o sistema pode ser atacado e quais contra-ataques que são viáveis para o sistema. O jogo é dinâmico, os defensores podem adicionar ou remover elementos da arquitetura alvo conforme o jogo progride. Essa abordagem tem alcançado uma boa visibilidade, mas devido ao seu alto nível de formalismo, é muito difícil de usar, isto é, todos os argumentos têm de ser definidos com relação a uma base de conhecimentos utilizando uma sintaxe rigorosa. Embora o conceito de um jogo de argumentação pareça promissor, a alta sobrecarga adicionada pela estrutura lógica formal representa uma ameaça significativa para a escalabilidade e facilidade de utilização da abordagem.

Tabela 4 - Tabela comparativa dos trabalhos relacionados.

	Qual a técnica Utilizada	Quem pode usar/Suporte a equipes distribuídas	Qual forma de Validação da discussão.
Yuan [29]	Argumentação com base em vários padrões de gerenciamento de riscos de segurança, com foco em ataques e defesa	equipe de especialistas em segurança da informação. Não pode ser usado por equipes geograficamente distribuídas	O sistema não conta com técnicas de consistência e completude da discussão
Franqueira et al.[30]	Argumentação com base em catálogos compartilhados representado como uma estrutura de árvore de argumentos e contra-argumentos. Baseia-se em requisitos de segurança	Apenas dois agentes humanos. Não pode ser usado em equipes geograficamente distribuídas	O sistema não conta com técnicas de consistência e completude da discussão.
Prakken el al.[32]	Argumentação sob medida para avaliação de risco e como o sistema pode ser atacado e quais contra ataques que são viáveis para o sistema	Pode-se usar em equipes geograficamente distribuídas	O sistema não aborda este conceito
Trabalho Proposto	Argumentação utilizando a técnica de jogos de diálogos baseado no processo da norma ISO/IEC 27005	Pode ser usado por especialistas e também por pessoas com pouca experiência. Pode-se usar em equipes geograficamente distribuídas.	Propõe regras para validar a completude e a consistência da discussão.

VI. CONCLUSÃO

Este artigo apresenta uma abordagem colaborativa para a gestão de riscos de segurança da informação. Esta abordagem está fundamenta na ISO/IEC 27005. O protocolo de diálogo apresentado tem como objetivo apoiar a execução de discussões de risco e de construir uma memória de gestão de riscos. Um sistema de discussão de riscos de segurança da informação é também discutido. A principal contribuição deste

trabalho é uma abordagem de argumentação, definida como um novo jogo de diálogo, para a colaboração de gestão de riscos de segurança da informação com base na norma ISO/IEC 27005, para garantir que uma série de etapas descritas pela norma e relacionadas a GRSI sejam realizadas em uma discussão.

Um ambiente de discussão – RD System - é proposto, o qual promove o engajamento das diferentes partes interessadas na discussão. RD System possibilita a troca de informações visando melhorar a tomada de decisão em relação a identificação, análise e ações para tratamento de riscos de segurança da informação. O ambiente é centralizado na análise de opiniões e experiências dos participantes da discussão em um processo de GRSI. Outro ponto relevante é a construção de uma memória estruturada de discussão de riscos, em que coleções de dados e argumentos sobre diferentes características de riscos de segurança são analisadas e registradas.

REFERÊNCIAS

[1] O. O. F. Management, "ANNUAL REPORT TO CONGRESS : FEDERAL INFORMATION SECURITY," 2015.

[2] C. S. Division, "Managing Information Security Risk," vol. 800–39, no. March, p. 88, 2011.

[3] C. B. Haley, R. Laney, and J. D. Moffett, "Security Requirements Engineering : A Framework for Representation and Analysis Security Requirements Engineering : A Framework for Representation and Analysis," 2008.

[4] G. M. Quadrant and E. P. Platforms, "Global IT Security Risks : 2012," p. 21, 2012.

[5] O. Noroozi, A. Weinberger, H. J. a. Biemans, M. Mulder, and M. Chizari, "Argumentation-Based Computer Supported Collaborative Learning (ABCSCL): A synthesis of 15 years of research," *Educ. Res. Rev.*, vol. 7, no. 2, pp. 79–106, Jun. 2012.

[6] R. Prikladnicki and J. Audy, *Desenvolvimento Distribuído de SORFTARE*, 1st ed. 2007.

[7] E. Huzita, C. Silva, and I. Wiese, "Um conjunto de soluções para apoiar o desenvolvimento distribuído de software," pp. 101–110, 2008.

[8] P. Tolchinsky, U. Cortés, F. Caballero, A. López-navidad, H. De, and S. Creu, "Transplant Availability : Agent Deliberation," *IEEE Intel. Syst.*, p. 8, 2006.

[9] C. Reed and S. Wells, "Dialogical argument as an interface to complex debates," *Intell. Syst. IEEE*, p. 6, 2007.

[10] E. Black, K. Atkinson, and B. Katie, "Dialogues that Account for Different Perspectives in Collaborative Argumentation," pp. 867–874, 2009.

[11] M. Ning, "The actuality and countermeasure of net information safety in China," vol. 2, 2007.

[12] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," *Comput. Secur.*, vol. 44, pp. 1–15, Jul. 2014.

[13] S. Ozkan and B. Karabacak, "International Journal of Information Management Collaborative risk method for information security management practices : A case context within Turkey," *Int. J. Inf. Manage.*, vol. 30, pp. 567–572, 2010.

[14] L. Inácio, J. A. Félix, A. S. Geromel, R. S. Simião, and E. L. Jr, "Introdução à gestão de riscos de segurança da informação," 2011.

[15] A. Z. Standard, "Standards Australia and Standards New Zealand. AS/NZS 4360:2004," 2004.

[16] A. Leitner, F. H. O. O. E. F, E. Gmbh, and I. Schaum, "ARiMA - a new approach to implement ISO / IEC 27005," *IEEE Intel. Syst.*, pp. 1–6, 2009.

[17] G. Wangen, "A Comparison between Business Process Management and Information Security Management," vol. 2, pp. 901–910, 2014.

[18] P. Shedden and T. Ruighaver, "Risk management standards – the perception of ease of use," pp. 1–13, 2006.

[19] B. Moulin, H. Irandoust, and M. Bélanger, "Explanation and Argumentation Capabilities : Towards the Creation of More Persuasive Agents," pp. 169–222, 2002.

[20] T. Benchcapon and P. Dunne, "Argumentation in artificial intelligence," *Artif. Intell.*, vol. 171, no. 10–15, pp. 619–641, Jul. 2007.

[21] P. Mcburney and S. Parsons, "Argumentation in Artificial Intelligence," pp. 261–280, 2009.

[22] P. McBurney and S. Parsons, "Dialogue Games for Agent Argumentation," 2009.

[23] O. Scheuer, F. Loll, N. Pinkwart, and B. M. McLaren, "Computer-supported argumentation: A review of the state of the art," *Int. J. Comput. Collab. Learn.*, vol. 5, no. 1, pp. 43–102, Jan. 2010.

[24] D. Walton, *The New Dialectic: Conversational Contexts of Argument*. University of Toronto Press, Scholarly Publishing Division, 1988.

[25] F. S. Severo, R. C. B. Pozzebon, L. M. Fontoura, and L. A. L. Silva, "Argumentation-Based Risk Management," 2007.

[26] H. Prakken, "Formal systems for persuasion dialogue," vol. 00, pp. 1–26, 2006.

[27] F. S. Severo, L. M. Fontoura, and L. A. L. Silva, "A Dialogue Game Approach to Collaborative Risk Management," *SEKE*, 2013.

[28] N. L. R. Machado, L. A. L. Silva, M. Lisandra, and J. A. Campbell, "Case-based Reasoning for Experience-based Collaborative Risk Management."

[29] T. Yuan, "Collaborative argumentation on the web - a dialogue game approach," pp. 161–165, 2013.

[30] V. N. L. Franqueira, T. T. Tun, Y. Yu, R. Wieringa, and B. Nuseibeh, "Risk and Argument : A Risk-Based Argumentation Method for Practical Security," pp. 239–248, 2011.

[31] C. B. Haley, R. Laney, and J. D. Moffett, "Security Requirements Engineering : A Framework for Representation and Analysis," vol. 34, no. 1, pp. 133–153, 2008.

[32] H. Prakken, D. Ionita, and R. Wieringa, "Risk assessment as an argumentation game," vol. 8143, pp. 1–17, 2013.

[33] S. E. Toulmin, *The Uses of Argument*. 1958.