Estado do Ceará
Poder Judiciário
Tribunal de Justiça
Comitê Gestor de Segurança da Informação
Anexo VI

PJSETIN2015004 – Implantação do Programa de Segurança Corporativa da Informação no âmbito do Poder Judiciário do Estado do Ceará

06/NSI06/CGSI/TJCE – **Norma de gestão de riscos – Metodologia de Gestão de Riscos de Segurança da Informação**

1. FINALIDADE

Este documento tem por finalidade apresentar a Metodologia de Gestão de Riscos em Segurança da Informação para o Poder Judiciário do Estado do Ceará, bem como descrever os procedimentos correlatos ao referido Processo.

2. CAMPO DE APLICAÇÃO

- Poder Judiciário do Estado do Ceará.

3. DEFINIÇÕES

- **Aceitação do risco** – É a decisão de concordar com o risco, considerando-se as limitações para seu tratamento.

- **Probabilidade** – É a possibilidade da vulnerabilidade (Controle não implementado) ser explorada pelas ameaças.

- **Relevância** – É o grau de importância do Ativo para o negócio do Poder Judiciário do Estado do Ceará, considerando os componentes de negócio que ele apoia.

- **Risco residual** – É o risco remanescente após o tratamento do risco.

- **Severidade** – É a consequência, na segurança da informação, caso as ameaças explorem a vulnerabilidade nos aspectos de confidencialidade, integridade e disponibilidade.

- **Tratamento do risco** – É o processo de seleção e implementação de medidas de controle de segurança da informação no intuito de reduzir um risco de determinado ativo.

4. CONSIDERAÇÕRES INICIAIS

- A implantação da Metodologia de Gestão de Riscos de Segurança da Informação busca identificar as necessidades da organização em relação aos requisitos de segurança da informação, bem como.

- Convém que a Metodologia de Gestão de Riscos de Segurança da Informação esteja alinhada ao Planejamento Estratégico do Poder Judiciário do Estado do Ceará e o Plano Estratégico de Tecnologia da Informação - PETI do Poder Judiciário do Estado do Ceará e também, com o processo maior de Gestão de Riscos corporativos, se esse existir.

- A Gestão de Riscos de Segurança da Informação, objeto desta Metodologia, está limitada ao escopo das ações de Segurança da Informação e tais ações compreendem apenas as medidas de proteção dos ativos de informação, conforme definido nesta Metodologia.

5. DIRETRIZES

- Neste capítulo estão descritas as diretrizes da Gestão de Riscos de Segurança da Informação, que são as declarações de alto nível sobre como esse processo será utilizado nas atividades de trabalho do Poder Judiciário do Estado do Ceará.

- As diretrizes descritas nesta norma estão em conformidade com a ABNT NBR ISO 31000:2009 - Gestão de riscos – Princípios e diretrizes. A utilização de um modelo baseado em padrões e metodologias formalizados, reconhecidos internacionalmente, é capaz de se adequar às estratégias, iniciativas e estrutura organizacional do Poder Judiciário do Estado do Ceará, além de atender às exigências dos órgãos reguladores e fiscalizadores da administração pública.

- As diretrizes gerais da Metodologia de Gestão de Riscos de Segurança de SI deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do Poder Judiciário do Estado do Ceará, além de estarem alinhadas à respectiva Política de Segurança da Informação do Poder Judiciário do Estado do Ceará.

- O processo de Gestão de Riscos de Segurança da Informação deve ser contínuo.

- Os riscos de Segurança da Informação devem ser identificados, aceitos ou tratados.

- As decisões estratégicas de Segurança da Informação serão baseadas nos níveis de exposição aos riscos.

- A adoção das boas práticas de Governança de Segurança da Informação é uma forma sistemática, estruturada e oportuna de mitigar os riscos da gestão das informações com o objetivo de alcançar e manter a transparência, a qualidade e a segurança das informações do Poder Judiciário do Estado do Ceará.

6. RESPONSABILIDADES

6.1. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO

- Aprovar o nível desejável de risco de SI para o Poder Judiciário do Estado do Ceará.

- Aprovar os investimentos nos controles de segurança da informação para tratamento dos riscos identificados.

6.2. SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO (SETIN)

- Divulgar a Metodologia de Gestão de Riscos de SI no âmbito do Poder Judiciário do Estado do Ceará.

- Gerenciar e garantir a execução da norma de Gestão de Riscos de SI no âmbito do Poder Judiciário do Estado do Ceará.

6.3. GERENCIAS DE GOVERNANÇA, SISTEMAS INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO DA SETIN E GERENCIA DE INFORMÁTICA DO FÓRUM CLÓVIS BEVILÁQUA

- Definir e coletar indicadores para avaliar a efetividade da Metodologia de Gestão de Riscos de SI.

- Identificar oportunidades de melhorias no processo.

- Aprovar, acompanhar e dar condições para implementação do Plano de Tratamento do Risco de SI nos ativos de sua responsabilidade.

6.4. SERVIÇO DE SEGURANÇA DA INFORMAÇÃO

- Administrar a ferramenta de Gestão de Riscos do Poder Judiciário do Estado do Ceará.

- Definir o contexto interno e externo da Gestão de Riscos de SI.

- Propor escopos para a análise e avaliação de riscos de SI.

- Analisar, avaliar e acompanhar o tratamento dos riscos de Segurança da Informação, identificadas.

- Fornecer ao Comitê Gestor de SI informações para aprovação do nível de risco.

- Elaborar o Plano de Tratamento de Risco de SI.

- Acompanhar a implementação do Plano de Tratamento de Risco de SI

- Aprovar os riscos residuais.

- Comunicar riscos às partes interessadas.

6.5. GESTORES DO PODER JUDICIÁRIO DO ESTADO DO CEARÁ

- Acompanhar e dar condições para implementação do Plano de Tratamento do Risco nos ativos de sua responsabilidade.

6.6. ÁREA RESPONSÁVEL PELA IMPLANTAÇÃO DOS CONTROLES DE SEGURANÇA DA INFORMAÇÃO

- Implementar os controles de segurança da informação sob suas responsabilidades relacionadas no Plano de Tratamento de Risco de SI.

7. DESCRIÇÃO DA METODOLOGIA

7.1. METODOLOGIA DE GESTÃO DE RISCOS DO PODER JUDICIÁRIO DO ESTADO DO CEARÁ

A Metodologia de Gestão de Riscos de SI permite identificar os riscos que podem causar impacto negativo nas atividades operacionais e administrativas do Poder Judiciário do Estado do Ceará.

Consiste na aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.

7.2. VISÃO GERAL METODOLOGIA DE GESTÃO DE RISCOS

Segue abaixo o fluxograma da Gestão de Riscos de acordo com a ABNT NBR ISO 31000:2009 – Gestão de riscos – Princípios e diretrizes.

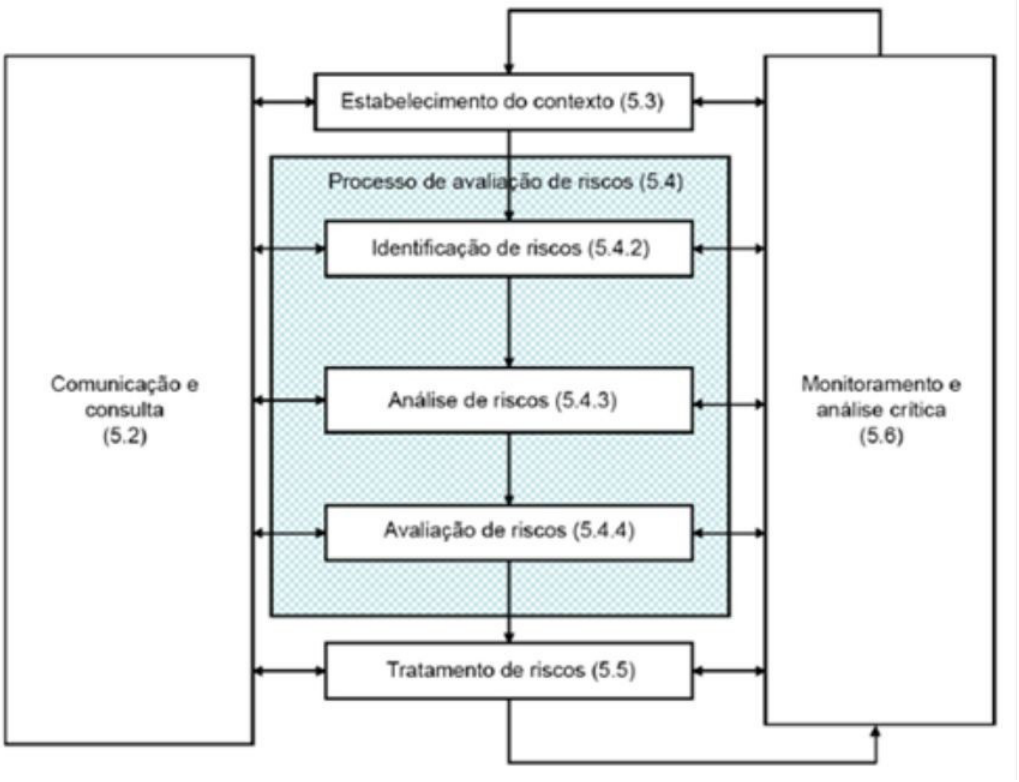

Figura 1

De modo geral, a Metodologia é um conjunto sequencial de ações ou atividades particulares com a finalidade de alcançar um determinado objetivo. Pode ser composto de uma ou mais entradas, que são processadas, retornando uma ou mais saídas.

O processo será dividido em subprocessos, que por sua vez poderão também ser subdivididos em outros subprocessos denominados etapas ou fases.

A Metodologia de Gestão de Risco é composta por 6 (seis) subprocessos a seguir descritos: definição de contexto, identificação dos riscos, análise e avaliação de risco, tratamento de risco, aceitação de riscos, comunicação de risco e monitoração e análise crítica, conforme ilustrado na figura 2.

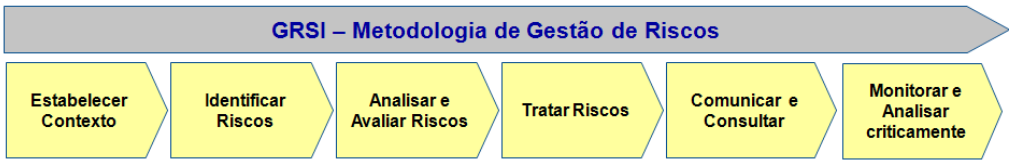

Figura 2 – Visão Geral da Metodologia de Gestão de Riscos

7.2.1 Subprocesso "ESTABELECER CONTEXTO"

Contexto é um conjunto de circunstâncias que se relacionam de alguma forma com um determinado acontecimento. É a situação geral ou o ambiente a que está sendo

referido um determinado assunto, neste caso a análise e avaliação de riscos. Denomina-se contextualização a atividade de mapear todo o ambiente que envolve o evento sob análise.

Este subprocesso é composto de 3 (três) etapas, a saber: identificar as informações sobre o contexto interno e externo, definir os critérios da Gestão de Risco e, por último, mapear os ativos de informação, conforme ilustrado na figura 3.

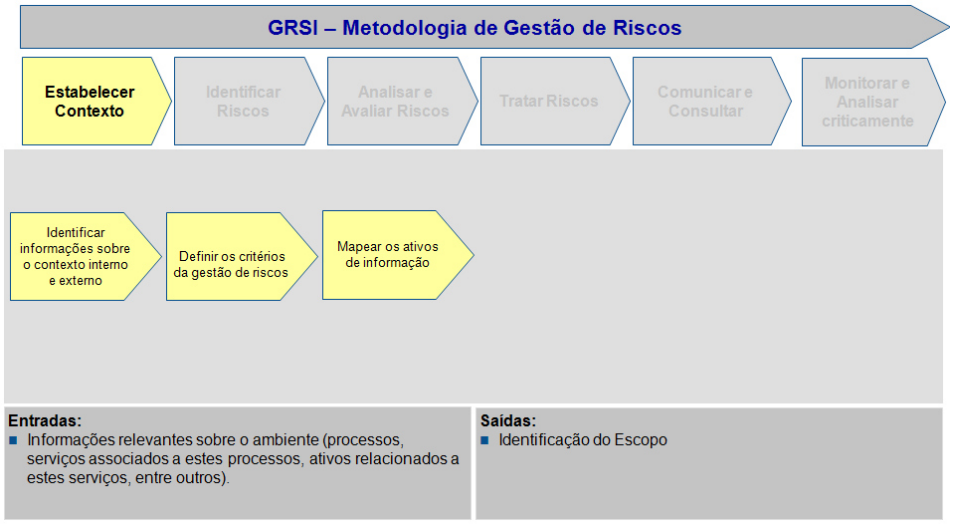

Figura 3 - Subprocesso "Estabelecer Contexto"

Responsável: Serviço de Segurança da Informação

Nas atividades que envolvem a Gestão de Riscos de Segurança da Informação, o estabelecimento do contexto é a parte inicial e tem como objetivo permitir o conhecimento do ambiente da organização.

Contextualização é a atividade de mapeamento de todo o ambiente que envolve o evento em análise.

Além de identificar o contexto interno e externo da organização, os critérios da gestão de riscos deverão ser identificados e os ativos de informação mapeados.

Para identificar as informações sobre o contexto interno e externo, deverá ser realizada uma análise no ambiente do Poder Judiciário do Estado do Ceará pela equipe de analistas de segurança da informação, identificando os elementos que caracterizam a Organização e que contribuem para o seu desenvolvimento.

No que tange à etapa de definição de critérios da Gestão de Riscos, é importante ressaltar que os critérios fazem parte da Metodologia de Gestão de Riscos e são a forma e o valor (pesos) com que os riscos e impactos serão valorados.

Quanto à etapa de identificação dos ativos, deve ser feita em um nível de detalhamento que permita o fornecimento de informações adequadas e suficientes para a análise e avaliação de riscos. Devem ser listados os ativos de informação considerados

críticos para o Poder Judiciário do Estado do Ceará e, também, uma lista de componentes organizacionais que este ativo suporta.

A ferramenta utilizada para a identificação dos ativos de informação que farão parte do escopo da análise e avaliação de riscos no Poder Judiciário do Estado do Ceará será o Módulo Risk Manager®. Também será organizada toda a análise e avaliação dos ativos de informação do escopo, por intermédio do Mapa de Governança, conforme exemplo abaixo na figura 04.

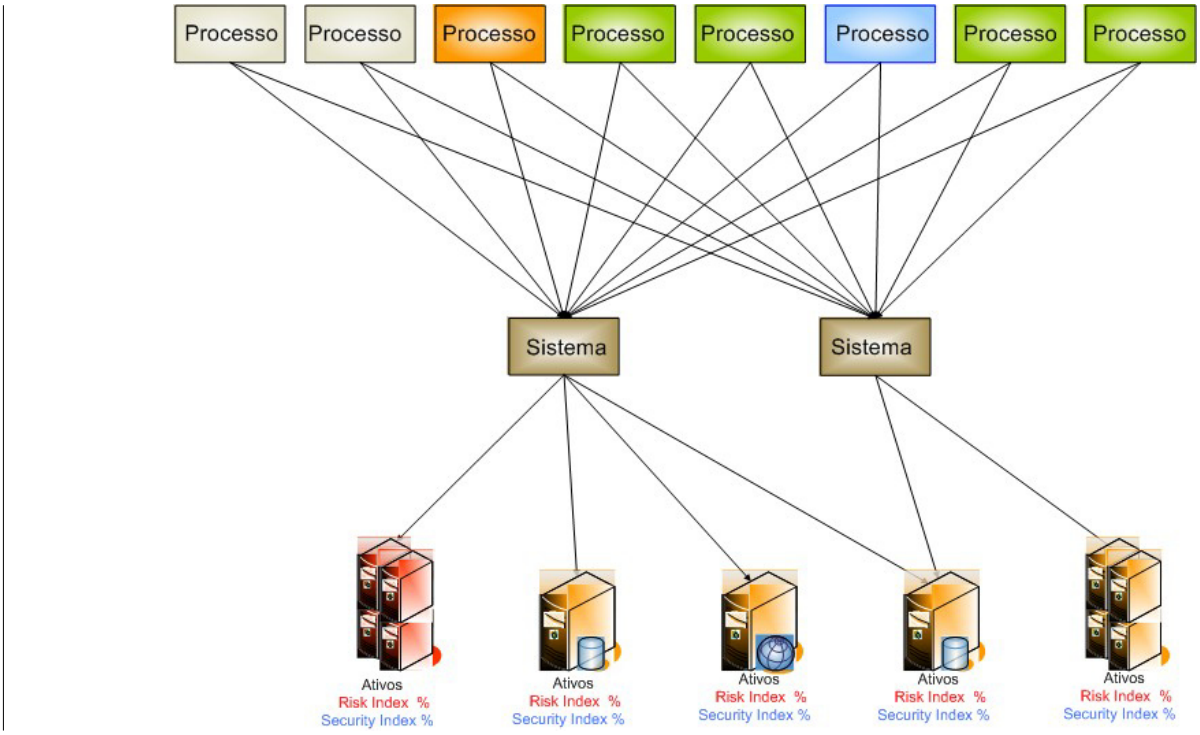

Figura 4 – Exemplo do Mapa de Governança com os ativos de informação do escopo da análise e avaliação de riscos.

7.2.1.1 Entradas e saídas do subprocesso "Estabelecer Contexto"

Entradas:

➢ Informações relevantes sobre o ambiente (processos, serviços associados a estes processos, ativos de informação relacionados a estes serviços, entre outros).

Saídas:

➢ Identificação do Escopo

➢ Mapa da Governança

7.2.2 Subprocesso "IDENTIFICAR RISCOS"

Convém que o Serviço de Segurança da Informação apoiado por áreas estratégicas do Poder Judiciário do Estado do Ceará (SETIN, GERENCIA DE INFORMÁTICA DO FCB, SEPLAG, CGSI etc) identifique as fontes de risco, áreas de impactos, eventos (incluindo mudanças nas circunstâncias) e suas causas e consequências

potenciais. A finalidade desta etapa é gerar uma lista abrangente de riscos baseada nestes eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos.

Convém que a identificação inclua todos os riscos, estando suas fontes sob o controle do Poder Judiciário do Estado do Ceará ou não, mesmo que as fontes ou causas dos riscos possam não ser evidentes.

O Poder Judiciário do Estado do Ceará aplicará ferramentas e técnicas de identificação de riscos que sejam adequadas aos seus objetivos e capacidades e aos riscos enfrentados. Informações pertinente e atualizadas são importantes na identificação de riscos. Convém que incluam informações adequadas sobre os fatos por trás dos acontecimentos, sempre que possível. Convém que pessoas com um conhecimento adequado sejam envolvidas

Este subprocesso é composto de 3 (três) etapas, a saber: identificar as ameaças envolvidas; as vulnerabilidades existentes nos ativos de informação; e os controles de Segurança da Informação já implantados, conforme ilustrado na figura 5.

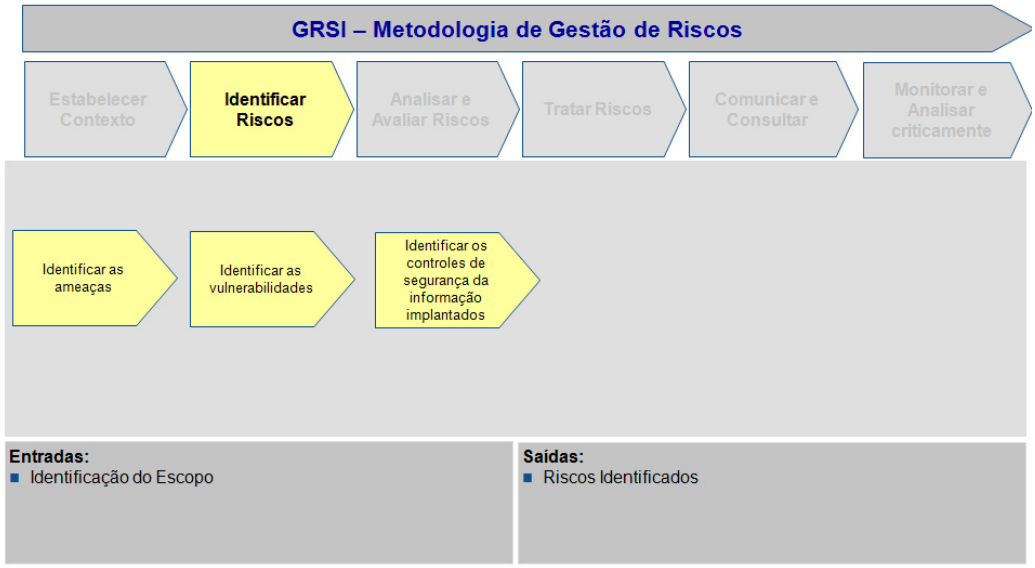

Figura 5 – Subprocesso "Identificar Riscos"

Responsável: Serviço de Segurança da Informação apoiado por áreas estratégicas do Poder Judiciário do Estado do Ceará (SETIN, GERENCIA DE INFORMÁTICA DO FCB, SEPLAG, CGSI etc.

Devem-se identificar todas as ameaças que podem causar impacto no escopo da análise e avaliação de Riscos, pois são essas ameaças identificadas que podem explorar as vulnerabilidades causando prejuízo para os processos de negócio do Poder Judiciário do Estado do Ceará.

Uma ameaça tem o potencial de comprometer os ativos de informação e, por isso também os processos de negócio do Poder Judiciário do Estado do Ceará. Ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais.

Convém que todas as fontes das ameaças acidentais, quanto as intencionais, sejam identificadas. Uma ameaça pode surgir de dentro ou fora do Poder Judiciário do Estado do Ceará. Algumas ameaças podem afetar mais de um ativo de informação. Nesses casos, elas podem provocar impactos diferentes, dependendo de quais ativos são afetados.

Deve-se identificar as vulnerabilidades que podem se exploradas por ameaças para comprometer os ativos de informação e os processos de negócio do Poder Judiciário do Estado do Ceará.

Vulnerabilidades podem ser identificadas nas seguintes áreas: Organização (TJCE, unidades administrativas e judiciais), em pessoas, processos e procedimentos, rotinas de gestão, recursos humanos, ambiente físico, configuração do sistema de informação, hardware, software ou equipamentos de comunicação e dependência de entidades externas.

Deve-se identificar os controles de segurança da informação, implantados e os planejados.

Convém que a identificação dos controles existentes seja realizada para evitar custos e trabalho desnecessários, por exemplo: na duplicação de controles. Além disso, enquanto os controles existentes estão sendo identificados, convém que seja feita uma verificação para assegurar que eles estão funcionando corretamente. Um controle que não funcione como esperado pode provocar o surgimento de vulnerabilidades.

7.2.2.1 Entradas e saídas do subprocesso “Identificar Riscos”

Entradas:

- Identificação do Escopo

Saídas:

- Riscos Identificados

7.2.3 Subprocesso “ANALISAR E AVALIAR RISCOS”

Este subprocesso visa produzir os dados que auxiliarão na decisão sobre quais riscos serão tratados e quais formas de tratamento serão empregadas. Também se subdivide em duas etapas, a saber: análise e avaliação dos riscos, conforme ilustrado na figura 6.

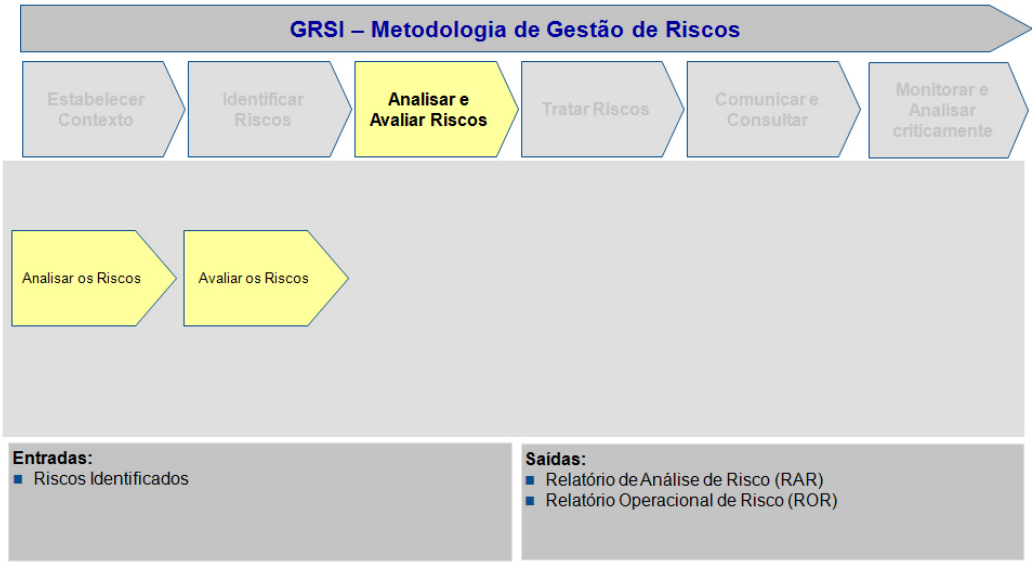

Figura 6 - Subprocesso "Analisar e Avaliar Riscos"

Responsável: Serviço de Segurança da Informação apoiado por áreas estratégicas do Poder Judiciário do Estado do Ceará (SETIN, GERENCIA DE INFORMÁTICA DO FCB, SEPLAG, CGSI, etc.

A ferramenta utilizada para análise de risco no Poder Judiciário do Estado do Ceará será o Módulo Risk Manager®. Esta é uma metodologia de cálculo de Risco aderente às normas ABNT NBR ISO/IEC 27005:2011, ABNT NBR ISO 31000:2009 e ISO Guide 73:2009. A metodologia utilizada no Módulo Risk Manager® permite que o cálculo do risco seja aplicável a elementos tecnológicos, de ambiente físico, processo e pessoas do Poder Judiciário do Ceará.

O Módulo Risk Manager® utiliza um método de Análise de Riscos qualitativa que calcula um índice ("rating") denominado **PSR®** (**P**robabilidade, **S**everidade e **R**elevância). Este índice define o Risco para cada Controle ausente encontrado na Análise. Da fórmula do Risco: **RISCO = PROBABILIDADE X IMPACTO**

No Módulo Risk Manager®, o valor do impacto no negócio é atendido pelas duas variáveis S e R, Severidade e Relevância respectivamente, e esta fórmula do Risco é calculada então pela seguinte equação:

RISCO = PROBABILIDADE X SEVERIDADE X RELEVÂNCIA

O Módulo Risk Manager® considera que a ausência de Controle de Segurança da Informação representa uma ou mais vulnerabilidades associadas ao Controle. Caso não exista a vulnerabilidade associada à falta de um Controle específico em algum ambiente, então o Controle deve ser considerado como Não Aplicável – N/A.

Em conformidade com a ISO Guide 73:2009, que define o risco como "a combinação da probabilidade de um evento e sua consequência", o Módulo Risk Manager® considera para cálculo do risco um índice (PSR®) que representa a estimativa destes fatores.

Este valor PSR® representa o grau de risco associado à ausência de um controle, sendo calculado pela equação Risco = Probabilidade x Severidade x Relevância, onde os fatores da Probabilidade e Severidade são pontuados durante as análises técnicas, e a Relevância pontuada considerando-se a visão do negócio, em termos da relevância do ativo de informação para o Poder Judiciário do Estado do Ceará.

Assim, o Risco associado a cada Controle ausente é calculado multiplicando-se os três fatores básicos, e o resultado é um valor numérico entre 1 e 125, com seu nível variando conforme o resultado desta multiplicação:

Nível de Risco	Valores Possíveis PSR®
Muito Baixo	1, 2, 3, 4, 5,6
Baixo	8, 9, 10, 12, 15,16
Médio	18, 20, 24, 25, 27,30
Alto	32, 36, 40, 45, 48,50
Muito Alto	60, 64, 75, 80, 100,125

O PSR® representa o índice para o cálculo do Risco no Módulo Risk Manager®. Para os ativos de informação, o seu índice de Risco é o resultado da soma algébrica do PSR® dos Controles ausentes em seus componentes.

O PSR® de um ativo de informação é o resultado da soma dos PSR® de seus Controles não implementados.

Apesar de o risco técnico (binômio Probabilidade e Severidade) da ausência do Controle ser importante para os gestores de tecnologia, para a análise e avaliação de riscos e, consequentemente, para a Segurança da Informação, o que importa é considerar o Risco ao negócio como fator de priorização de ações (pois considera o fator Relevância do Ativo).

A Matriz a seguir segue como referência para se estabelecer uma pontuação adequada para cada um dos fatores do PSR®. É importante frisar que esta matriz serve como instrumento de sintonia do senso comum, de forma a substituir avaliações subjetivas por critérios mais objetivos para cada um dos fatores do PSR®, transformando-os em valores de 1 a 5.

PSR				
	PROBABILIDADE A ocorrência da vulnerabilidade ser explorada pelas ameaças:	SEVERIDADE A conseqüência da vulnerabilidade ser explorada pelas ameaças:	RELEVÂNCIA O comprometimento da segurança do ativo:	
5	É quase certa (≥ 95%)	Afetará extremamente a segurança	Pode afetar toda a empresa e os prejuízos serão extremamente altos	MUITO ALTA
4	É muito provável (65% ≤ P < 95%)	Afetará muito gravemente a segurança	Pode afetar um ou mais negócios da empresa e os prejuízos serão muito altos	ALTA
3	É provável (35% ≤ P < 65%)	Afetará gravemente a segurança	Pode afetar uma parte do negócio da empresa e os prejuízos serão razoáveis	MÉDIA
2	É improvável (5% ≤ P < 35%)	Afetará pouco a segurança	Pode afetar uma parte pequena e localizada do negócio da empresa e os prejuízos serão baixos	BAIXA
1	É muito improvável (< 5%)	Quase não afetará a segurança	Pode afetar uma parte muito pequena e localizada do negócio da empresa e os prejuízos serão desprezíveis	MUITO BAIXA

Figura 7 – Matriz de Probabilidade X Severidade X Relevância

A etapa de avaliação de riscos tem por objetivo comparar os níveis de riscos identificados na fase anterior com os critérios de avaliação e aceitação de riscos e obter uma lista de riscos ordenados por prioridade.

Após a emissão dos relatórios, o Serviço de Segurança da Informação apoiado por áreas estratégicas do Poder Judiciário do Estado do Ceará (SETIN, GERENCIA DE INFORMÁTICA DO FCB, SEPLAG, CGSI, etc.) avalia e verifica se o nível de risco está dentro dos padrões definidos no contexto interno e externo para a análise e avaliação de riscos para cada um dos ativos de informação que estão no escopo determinado.

7.2.3.1 Entradas e saídas do subprocesso "Analisar e Avaliar Riscos"

Entradas:

- Riscos Identificados

Saídas:

- Relatório de Análise de Risco (RAR) onde é apresentado, de forma consolidada, o resultado da análise do nível atual do risco dos ativos do Poder Judiciário do Estado do Ceará e os riscos encontrados nos componentes de negócio, bem como, a consolidação por tipo de ativo de informação.

- Relatório Operacional de Risco (ROR), onde é apresentado o detalhamento das ações e controles que devem ser implementados para eliminar ou mitigar os riscos.

7.2.4 Subprocesso "TRATAR RISCOS"

Este subprocesso visa relacionar os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos na definição de escopo, detalhados na figura 6.

É importante ressaltar que se recomenda a implantação dos controles de segurança da informação descritos no Plano de Tratamento de Riscos de acordo com as melhores práticas de gestão de mudanças para não ocasionar possíveis incidentes na implantação dos controles de segurança da informação.

Este subprocesso é composto de 4 (três) etapas, a saber: determinar a forma de tratamento dos riscos, obter parecer do proprietário do ativo de informação, gestão de mudanças e identificar os riscos residuais, conforme ilustrado na figura 8.

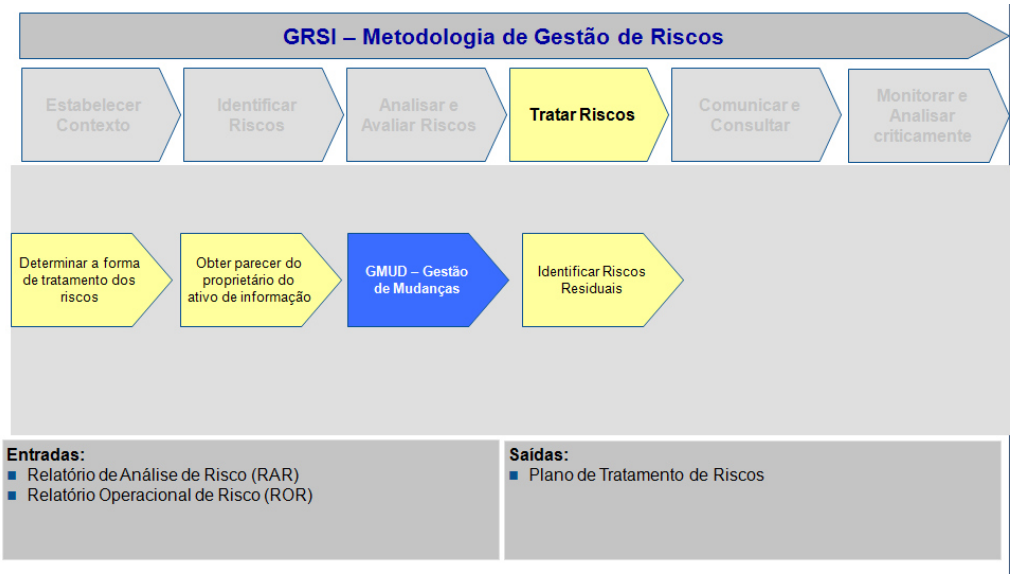

Figura 8 – Subprocesso "Tratar Riscos"

Responsável: Serviço de Segurança da Informação apoiado por áreas estratégicas do Poder Judiciário do Estado do Ceará (SETIN, GERENCIA DE INFORMÁTICA DO FCB, SEPLAG, CGSI, etc).

Em relação ao subprocesso "Determinar a forma de tratamento de risco", para cada risco identificado deverá ser informada a ação de tratamento. Com a utilização da ferramenta Módulo Risk Manager® toda as informações de tratamento para cada risco identificado estão descritas detalhadamente no Relatório Operacional de Risco (ROR).

O subprocesso de tratamento de risco é realizado após os subprocessos de estabelecimento do contexto e análise/avaliação de riscos. Ao final desses subprocessos, a equipe do Serviço de Segurança da Informação deverá fazer uma análise crítica dos resultados a fim de verificar a situação dos trabalhos desenvolvidos. Caso essa análise se mostre insatisfatória, deve-se retornar ao início do processo, para ajustes.

Os Gestores do Poder Judiciário do Estado do Ceará deverão emitir parecer sobre os riscos identificados nos ativos de informações sob sua responsabilidade. Este poderá concordar ou não em relação aos riscos identificados.

Convém que os controles de segurança da informação necessários para tratar os riscos deverão ser implementados de acordo com o processo de Gestão de Mudanças dependendo da ação de tratamento escolhida.

A equipe do Serviço de Segurança da Informação apoiado por áreas estratégicas do Poder Judiciário do Estado do Ceará (SETIN, GERÊNCIA DE INFORMÁTICA DO FCB, SEPLAG, CGSI, etc) deve elaborar o Plano de Tratamento de Risco, baseado nas informações contidas no Relatório Operacional de Risco (ROR), apresentando:

- **O que?** – o controle que deve ser implementado;
- **PSR®** – o valor do risco encontrado (nível de risco);
- **Por que?** – a importância da implementação do controle;
- **Como?** – a descrição de como implementar o controle;
- **Quem?** – o responsável pela implementação do controle;
- **Quando?** – o prazo para a implementação do controle;
- **Onde?** – o local para implementação do controle;
- **Quanto custa?** – o valor em reais ou em HH (homem-hora) para a implementação do controle (opcional);
- **Justificativa** – uma explicação para a não implementação do controle.

O Poder Judiciário do Estado do Ceará utilizará a seguinte interpretação dos resultados do PSR® para o Tratamento dos Riscos:

Nível de Risco do Controle PSR®	Interpretação
Muito Alto	São Riscos inaceitáveis, e os gestores dos ativos devem ser orientados para que os eliminem imediatamente.
Alto	São Riscos inaceitáveis e os gestores dos ativos devem ser orientados para pelo menos controlá-los.
Médio	São Riscos que podem ser aceitáveis após revisão e confirmação dos gestores dos ativos, contudo a aceitação do Risco deve ser feita por meios formais.
Baixo	São Riscos que podem ser aceitáveis após revisão e confirmação dos gestores dos ativos.
Muito Baixo	São Riscos aceitáveis e devem ser informados para os Gestores dos ativos.

O Serviço de Segurança da Informação apoiado por áreas estratégicas do Poder Judiciário do Estado do Ceará (SETIN, GERÊNCIA DE INFORMÁTICA DO FCB, SEPLAG, CGSI, etc.) deverá apresentar o Plano de Tratamento de Risco para a Secretaria de Tecnologia da Informação e para o CGSI e solicitar a sua aprovação para implementação.

O Serviço de Segurança da Informação deverá enviar o Plano de Tratamento de Risco para as áreas responsáveis pela sua implementação e fazer o acompanhamento da implementação das recomendações que tratam os riscos identificados.

Uma vez implantado os controles de segurança da informação do Plano de Tratamento de Risco, é necessário identificar os riscos residuais após implementação de controles para evitar, transferir ou mitigar riscos, ou seja, após a implementação de um determinado controle, é possível que ele não seja suficiente para mitigar totalmente um risco. A diferença, isto é, a possibilidade restante da ocorrência dos riscos, após a implantação do controle para mitigá-lo caracteriza o risco residual.

7.2.4.1 Entradas e saídas do subprocesso "Tratar Riscos"

Entradas:

- Relatório de Análise de Risco (RAR)
- Relatório Operacional de Risco (ROR)

Saídas:

- Plano de Tratamento de Riscos

7.2.5 Subprocesso “COMUNICAR E CONSULTAR”

A Gestão de Riscos de Segurança da Informação pode ter diversas partes interessadas. Essas partes devem ser identificadas e seus papéis e responsabilidades delimitados. Os riscos serão comunicados para os seus respectivos responsáveis. Assim, o subprocesso de comunicar e consultar se encarrega de proporcionar essa comunicação, sendo composta de duas etapas: a primeira relativa à identificação das partes interessadas e a outra efetivamente associada à comunicação, ambas ilustradas na figura 9.

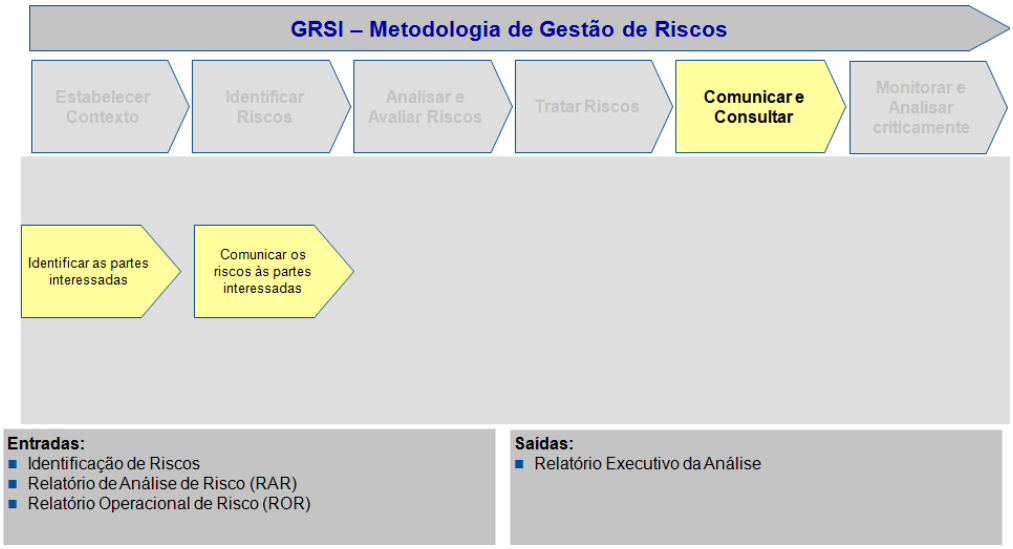

Figura 9 – Subprocesso “Comunicar e Consultar”

Responsável: Serviço de Segurança da Informação

A comunicação do risco é uma troca interativa, documentada formalmente, contínua e intencional de informações, conhecimentos e percepções sobre como os riscos devem ser gerenciados.

A comunicação é realizada entre a equipe envolvida na Gestão de Riscos e partes interessadas nas decisões dos processos de negócio que estão no contexto da análise e avaliação de riscos, por isso as partes interessadas deverão ser identificadas e documentadas.

No que se refere à comunicação dos riscos às partes interessadas, esta etapa deverá abordar com o máximo de detalhes dos riscos encontrados, informando:

- A existência da ameaça, vulnerabilidade e risco;
- A natureza e forma de ação;
- A estimativa de probabilidade;
- Sua severidade e consequências possíveis; e
- Tratamento e aceitação de riscos.

7.2.5.1 Entradas e saídas do subprocesso "Comunicar e Consultar"

Entradas:

- Identificação de Riscos
- Relatório de Análise de Risco (RAR)
- Relatório Operacional de Risco (ROR)

Saídas:

- Relatório Executivo da Análise

7.2.6 Subprocesso "MONITORAR E ANALISAR CRITICAMENTE"

Intrínseco a todo processo, a retroalimentação é necessária para corrigir e aperfeiçoar o próprio processo. Assim, este subprocesso permite detectar possíveis falhas nos resultados, monitorar os riscos, os controles de segurança da informação e verificar a eficácia do processo de Gestão de Riscos. Subdivide-se em três etapas, conforme ilustrado na figura 10.

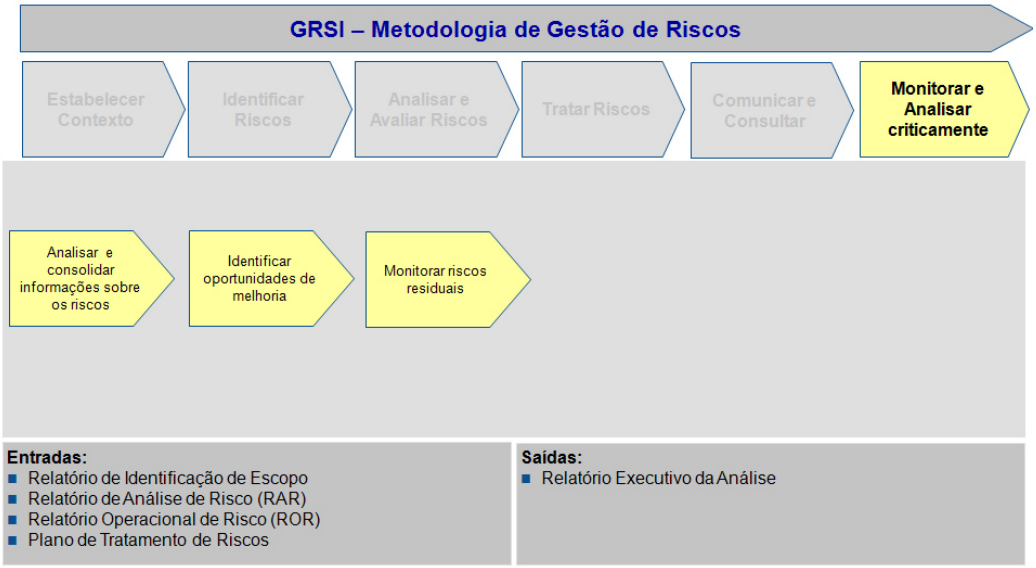

Figura 10 – Subprocesso "Monitorar e analisar criticamente"

Responsável: Gerencias de Governança, Sistemas e Infraestrutura de TI, Gerencia de Informática do Fórum Clóvis Beviláqua e Serviço de Segurança da Informação

Após o tratamento dos riscos, é necessário consolidar informações sobre o processo e identificar oportunidades de melhoria.

Na etapa de "Analisar e Consolidar Informações sobre os Riscos" deve-se identificar e quantificar os indicadores do processo no documento de Relatório Executivo da Análise.

Quanto à etapa "Identificar Oportunidades de Melhoria", deve-se analisar as informações consolidadas do processo, através dos seus indicadores, e identificar oportunidades de melhoria.

Por fim, no que se refere à etapa "Monitorar Riscos Residuais", os riscos residuais e seus fatores deverão ser monitorados.

7.2.5.1 Entradas e saídas do subprocesso "Monitorar e analisar criticamente"

Entradas:

- Identificação de Riscos
- Relatório de Análise de Risco (RAR)
- Relatório Operacional de Risco (ROR)
- Plano de Tratamento de Riscos

Saídas:

- Relatório Executivo da Análise

8. REGISTROS GERADOS

IDENTIFICAÇÃO	ARMAZENAMENTO	RECUPERAÇÃO (INDEXAÇÃO)	TEMPO DE RETENÇÃO	DISPOSIÇÃO
Relatório de Análise de Riscos - RAR	Módulo Risk Manager®.	Por assunto	5 anos	Eliminar
Relatório Operacional de Riscos - ROR	Módulo Risk Manager®.	Por assunto	5 anos	Eliminar
Painel de Controle	Módulo Risk Manager®.	Por assunto	5 anos	Eliminar
Mapa de Governança	Módulo Risk Manager®.	Por assunto	5 anos	Eliminar
Plano de Tratamento de Risco	Módulo Risk Manager®.	Por assunto	5 anos	Eliminar