



## Comitê Gestor de Segurança da Informação e Comunicação - CGSIC

### Ata da 1ª Reunião de 2019 - CGSIC (04 e 05/04/2019)

#### 1. Identificação da Reunião

Descrição	Data e Hora	Local	Coordenador
1ª Reunião de 2019	04/04/2019 às 13:30 05/04/2019 às 09:00	Sala do Secretário Geral da Presidência no Prédio sede do TRT 16ª Região	SOLANGE CRISTINA PASSOS DE CASTRO CORDEIRO

#### 2. Objetivo da Reunião

Apresentar a minuta da revisão do Processo de Gestão de Riscos de Segurança da Informação e apresentar os principais conceitos da Lei de Proteção de Dados Pessoais (Lei LEI N° 13.709, DE 14 DE AGOSTO DE 2018) e impactos dela no âmbito do TRT16.

#### 3. Membros Presentes

Nome	Função
Noredim Oliveira Reuter Ribeiro Neto	Secretário-Geral da Presidência
Sílvia Maria Pontes de Castro	Secretária de Administração
Fernanda Cristina Muniz Marques	Assessora da Diretoria-Geral
Stanley Araujo de Sousa	Chefe da Seção de Segurança da Informação

#### 4. Pauta da Reunião

- Análise da minuta da revisão do Processo de Gestão de Risco em Segurança da Informação;
- Apresentação da Lei Geral de Proteção de Dados Pessoais.

#### 5. Discussão dos Itens da Pauta

##### Item da Pauta: Minuta da revisão do Processo de Gestão de Riscos de Segurança da Informação

- 5.1. Stanley Araújo iniciou a reunião apresentando a Portaria GP nº 779/2017 que define o atual processo de Processo de Gestão de Riscos de Segurança da Informação;
- 5.2. Stanley Araújo fez uma explanação das principais mudanças propostas pela revisão do processo, destacando a inclusão da dimensão Relevância, que grau de impacto do Ativo ser afetado por uma ameaça, o quão importante é o ativo para o escopo em análise;
- 5.3. Após debates, o Comitê manifestou-se favoravelmente à aprovação da minuta;

##### Item da Pauta: Exposição dos principais conceitos da Lei geral de Proteção de Dados Pessoais

- 5.4. Stanley Araújo apresentou, surgimento e prazos da Lei de Proteção dos Dados Pessoais (Lei nº 13.709/2018) e contextualizou o crescimento da internet e do nível de tratamento de dados com a introdução aos conceitos iniciais da lei de proteção de dados;
- 5.5. Stanley Araújo fez uma breve exposição sobre a quem a lei se aplica e suas exceções e comentou sobre os fundamentos dela;
- 5.6. Em seguida, Stanley Araújo apresentou o conceitos de Dado Pessoal, Dado Sensível e Dado Anonimizado para iniciar a conceitualização do tratamento de dados e os principais agentes que participam desse processo e a agência que regulamenta (ANPD);
- 5.7. Exposição e breve comentário sobre os princípios para a coleta e tratamento de dados associando às bases legais para a realização de tratamento de dados. Ressalva dos artigos que mais impactam nas atividade do TRT16 mencionando o direito do titular dos dados e as sanções as quais o TRT16, como órgão público, está suscetível.
- 5.8. Abordou-se o conceito e a estrutura mínima do Relatório de Impacto além de apresentar o curso de Introdução à Lei Brasileira de Proteção de Dados disponível em [escolavirtual.gov.br](http://escolavirtual.gov.br).
- 5.9. Após o fim da exposição, deu-se início aos comentários e sugestões. O comitê deliberou por recomendar a Presidência a criação de um Grupo de Trabalho Multidisciplinar a fim de realizar uma



## Comitê Gestor de Segurança da Informação e Comunicação - CGSIC

Ata da 1ª Reunião de 2019 - CGSIC (04 e 05/04/2019)

avaliação e elaborar um plano de conformidade à Lei de Proteção de Dados Pessoais no âmbito do Tribunal Regional do Trabalho da 16ª Região.

5.10. Ademais, o Comitê sugeriu que o Grupo de Trabalho seja composto por, no mínimo, representantes da:

- 5.10.1. Diretoria-Geral;
- 5.10.2. Secretaria de Administração;
- 5.10.3. Controle Interno;
- 5.10.4. Assessoria Jurídica;
- 5.10.5. Coordenadoria de Tecnologia da Informação e Comunicação;
- 5.10.6. Seção de Apoio ao PJe-JT;
- 5.10.7. Seção de Segurança da Informação;

### 6. Assinaturas

Nome	Data	Assinatura
Noredim Oliveira Reuter Ribeiro Neto	22/04/19	
Sílvia Maria Pontes de Castro	15/04/19	
Fernanda Cristina Muniz Marques	15/04/19	
Stanley Araujo de Sousa	09/04/19	



---

# **Processo de Gestão de Riscos de Segurança da Informação**

---

2019



# Processo de Gestão de Riscos de Segurança da Informação

---

## Sumário

1. Objetivo.....	3
2. Aplicabilidade.....	3
3. Referências Normativas.....	3
4. Termos e Definições.....	3
5. Papéis e Responsabilidades.....	4
6. Critérios para avaliação de risco.....	5
7. Processo de Gestão de Riscos.....	7
ANEXO I - Fluxo do Processo de Gestão de Riscos.....	10
ANEXO II - Tarefas do Processo de Gestão de Riscos.....	11



# Processo de Gestão de Riscos de Segurança da Informação

---

## 1. Objetivo

Este documento tem como objetivo estabelecer o processo de Gestão de Riscos de Segurança da Informação (GRSI) no âmbito do Tribunal Regional do Trabalho da 16ª Região (TRT16).

A gestão de risco consiste no processo de planejar, organizar, dirigir e controlar os recursos humanos e materiais de uma organização, no sentido de minimizar ou aproveitar os riscos e incertezas sobre essa organização.

Espera-se, com esse artefato, tornar a gestão de riscos do TRT16 mais eficaz, buscando ampliar a probabilidade de cumprimento da missão institucional; melhorar a governança; estabelecer uma base confiável para a tomada de decisão e o planejamento; e melhorar a eficácia e eficiência operacional.

## 2. Aplicabilidade

O processo de Gestão de Riscos tem aplicabilidade em todas as unidades organizacionais do TRT16.

## 3. Referências Normativas

A elaboração do processo descrito por este documento utilizou como referência as seguintes normas:

- ISO/IEC 31000:2018;
- ABNT NBR ISO/IEC 27005:2011;
- ABNT NBR ISO/IEC GUIDE 73:2005.

## 4. Termos e Definições

- **Ameaça:** causa potencial de um incidente indesejado que pode resultar em dano para a organização;
- **Ativo:** qualquer recurso que tenha valor para a organização e cujo risco precisa ser controlado;
- **BPMN:** Acrônimo de Business Process Modeling Notation. Notação gráfica que descreve a lógica dos passos de um processo de negócio. É um padrão internacional de modelagem que permite modelar o processo de uma maneira unificada e padronizada;
- **Contexto Externo:** é o ambiente externo no qual a organização se situa e busca atingir seus objetivos (ambiente cultural, financeiro, regulatório, econômico, entre outros);
- **Contexto Interno:** é o ambiente interno no qual a organização busca atingir seus objetivos (governança, estrutura organizacional, políticas, normas, objetivos, diretrizes, cultura organizacional, entre outros);
- **Controle:** ação, medida ou dispositivo utilizado para tratar o risco;





## Processo de Gestão de Riscos de Segurança da Informação

- **Evento de Segurança da Informação:** ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;
- **Impacto (ou consequência):** uma das consequências da ocorrência de um evento. Ocasiona mudança adversa no nível obtido dos objetivos. Corresponde ao produto da Severidade e da Relevância;
- **Nível de risco:** magnitude do risco, expressa em termos da combinação das suas severidades, suas relevâncias e de suas probabilidades;
- **Probabilidade:** possibilidade de concretização de uma ameaça;
- **PSR:** Valor obtido da multiplicação entre a Probabilidade, a Severidade e a Relevância.
- **Relevância:** grau de impacto do Ativo ser afetado por uma ameaça, o quão importante é o ativo para o escopo em análise. A relevância deve ser atribuída durante o levantamento dos ativos;
- **Risco de segurança da informação:** possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos. É medido em função da combinação das suas severidades, suas relevâncias e de suas probabilidades;
- **Risco Residual:** Risco remanescente após o tratamento de risco ter sido implementado. O risco residual pode conter riscos não identificados;
- **Severidade:** medida do grau em que um Ativo será afetado, caso as ameaças explorem a(s) vulnerabilidade(s);
- **Segurança da Informação:** Preservação da confidencialidade, integridade e disponibilidade da informação;
- **TIC:** Tecnologia da Informação e Comunicações;
- **Vulnerabilidade:** fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

### 5. Papéis e Responsabilidades

Na Tabela 1 estão descritos os papéis e as responsabilidades relacionadas ao Processo de Gestão de Riscos de Segurança da Informação do TRT16.

Papel	Responsabilidades
<b>Presidência do Tribunal</b>	<ul style="list-style-type: none"><li>• Analisar as deliberações relacionados à Gestão de Riscos e decidir sobre possíveis providências;</li><li>• Aprovar o Processo de Gestão de Riscos de Segurança da Informação;</li></ul>
<b>Comitê Gestor de Segurança da Informação e Comunicação</b>	<ul style="list-style-type: none"><li>• Deliberar sobre as principais diretrizes e temas relacionados à Gestão de Riscos de Segurança da Informação;</li><li>• Submeter o Processo de Gestão de Riscos da Segurança da Informação e suas revisões para</li></ul>



## Processo de Gestão de Riscos de Segurança da Informação

	<p>aprovação pela Presidência do Tribunal;</p> <ul style="list-style-type: none"><li>• Aprovar os critérios de riscos (apetite a risco, graus de impacto, graus de probabilidade e classificação de riscos);</li></ul>
<b>Seção de Segurança da Informação</b>	<ul style="list-style-type: none"><li>• Elaborar o Processo de Gestão de Riscos de Segurança da Informação;</li><li>• Gerir e executar o Processo de Gestão de Riscos de Segurança da Informação;</li><li>• Auxiliar na elaboração dos Planos de Tratamento de Riscos;</li><li>• Acompanhar a execução dos planos de ação;</li><li>• Realizar o monitoramento e a análise crítica do Processo de Gestão de Riscos de Segurança da Informação, propondo ajustes e medidas preventivas e proativas;</li><li>• Disseminar cultura voltada para identificação e tratamento de riscos;</li><li>• Fornecer consultoria interna em gestão de riscos;</li><li>• Comunicar os riscos às partes interessadas.</li></ul>

Tabela 1- Papéis e Responsabilidades

### 6. Critérios para avaliação de risco

Os critérios de riscos são parâmetros estabelecidos para avaliar a magnitude dos riscos, a fim de que seja possível quantificar o impacto negativo na busca da obtenção de resultados esperados pelo TRT16 em sua missão institucional.

Para efeito deste processo, definiu-se como metodologia para a análise de risco a forma proposta pela norma ABNT NBR ISO 31000:2018, a qual define o nível do risco em termos da combinação dos impactos, de suas probabilidades e relevância.

Serão utilizadas escalas qualitativas para estimar a probabilidade, a relevância e severidade. Tais escalas encontram-se representadas nas Tabela 2, Tabela 3 e Tabela 4.

Peso	Valor	Probabilidade
5	Muito Alta	Probabilidade > 95%
4	Alta	65% < Probabilidade <= 95%
3	Média	35% < Probabilidade <= 65%
2	Baixa	5% < Probabilidade <= 35%



## Processo de Gestão de Riscos de Segurança da Informação

1	Muito Baixa	0% < Probabilidade <= 5%
---	-------------	--------------------------

Tabela 2- Critérios de Probabilidade

Peso	Valor	Descrição
5	Muito Alto	Impacto máximo nos objetivos do processo avaliado, sem possibilidade de recuperação.
4	Alto	Impacto significativo nos objetivos do processo avaliado, com possibilidade remota de recuperação.
3	Médio	Impacto mediano nos objetivos do processo avaliado, com possibilidade de recuperação.
2	Baixo	Impacto mínimo aos objetivos do processo avaliado. São facilmente remediáveis.
1	Muito Baixo	Impacto insignificante nos objetivos do processo avaliado. Dispensa qualquer medida de reparação.

Tabela 3- Critérios de Relevância

Peso	Valor	Descrição
5	Muito Alto	Afeta serviços prestados pelo TRT16 causando indisponibilidade dos sistemas que auxiliam suas atividades e perda de bens de extrema importância.
4	Alto	Afeta significativamente os serviços do TRT16, com possibilidade remota de recuperação.
3	Médio	Afeta os serviços de maneira mediana, tendo a possibilidade de recuperação.
2	Baixo	Não afeta as atividades do TRT16, não sendo tão vital o seu tratamento, porém é preciso controlar pra evitar a elevação do risco.
1	Muito Baixo	Não afeta as atividades do TRT16, não sendo tão vital o seu tratamento.

Tabela 4- Critérios de Severidade

Na Tabela 5, a seguir temos os possíveis valores resultado do produto entre a Severidade e a Relevância.

Severidade	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Relevância				





## Processo de Gestão de Riscos de Segurança da Informação

Tabela 5 - Possíveis valores do produto Severidade x Relevância

Para finalizar o modelo PSR, os resultados da tabela anterior são multiplicados pelo fator Probabilidade, gerando a Tabela 6 com a distribuição dos possíveis valores de risco:

Probabilidade	5	5	10	15	20	25	30	40	45	50	60	75	80	100	125
	4	4	8	12	16	20	24	32	36	40	48	60	64	80	100
	3	3	6	9	12	15	18	24	27	30	36	45	48	60	75
	2	2	4	6	8	10	12	16	18	20	24	30	32	40	50
	1	1	2	3	4	5	6	8	9	10	12	15	16	20	25
		1	2	3	4	5	6	8	9	10	12	15	16	20	25
Severidade x Relevância															

Tabela 6 - Possíveis valores do produto Probabilidade x Severidade x Relevância

NÍVEL DE RISCO	PSR	%
Muito Alto	De 60 a 125	$40 < NR \leq 100$
Alto	De 32 a 50	$24 < NR \leq 40$
Médio	De 15 a 30	$9,6 < NR \leq 24$
Baixo	De 06 a 12	$4 < NR \leq 9,6$
Muito Baixo	De 01 a 05	$NR \leq 4$

Tabela 7 - Critérios de Risco – Prioridade para tratamento de riscos

O TRT16 classifica como risco aceitável os níveis que apresentem PSR Muito Baixo ou Baixo, assim devendo tratar os riscos Médio, Alto e Muito Alto, sendo responsabilidade do Gestor da Seção de Segurança da Informação averiguar cada caso.

### 7. Processo de Gestão de Riscos

O modelo adotado pelo TRT16 para o gerenciamento de riscos pautou-se na norma ISO 31000:2018. A Figura 1 apresenta a visão geral do processo.

## Processo de Gestão de Riscos de Segurança da Informação

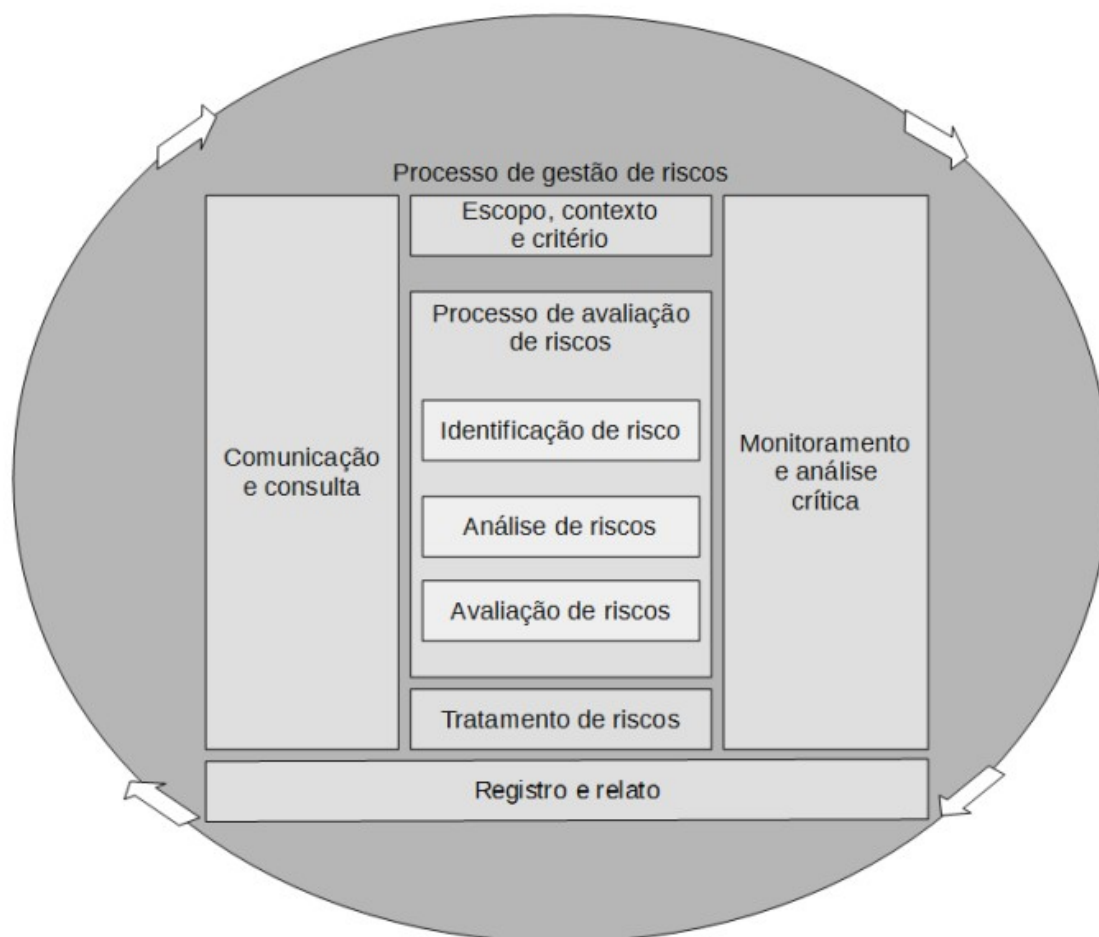


Figura 1 - Processo de Gestão de Risco ABNT NBR ISO 31000:2018

O processo engloba os seguintes elementos:

- Estabelecimento do escopo, do contexto e do critério;
- Avaliação de riscos (identificação, análise e avaliação de riscos);
- Tratamento de riscos;
- Comunicação e consulta;
- Monitoramento e análise crítica;
- Registro e relato.

O fluxo processo de Gestão de Risco do TRT16 encontra-se desenhado em BPMN no Anexo I.



## Processo de Gestão de Riscos de Segurança da Informação

---

As tarefas previstas pelo Processo de Gestão de Riscos de Segurança da Informação do TRT16 estão especificadas no Anexo II.

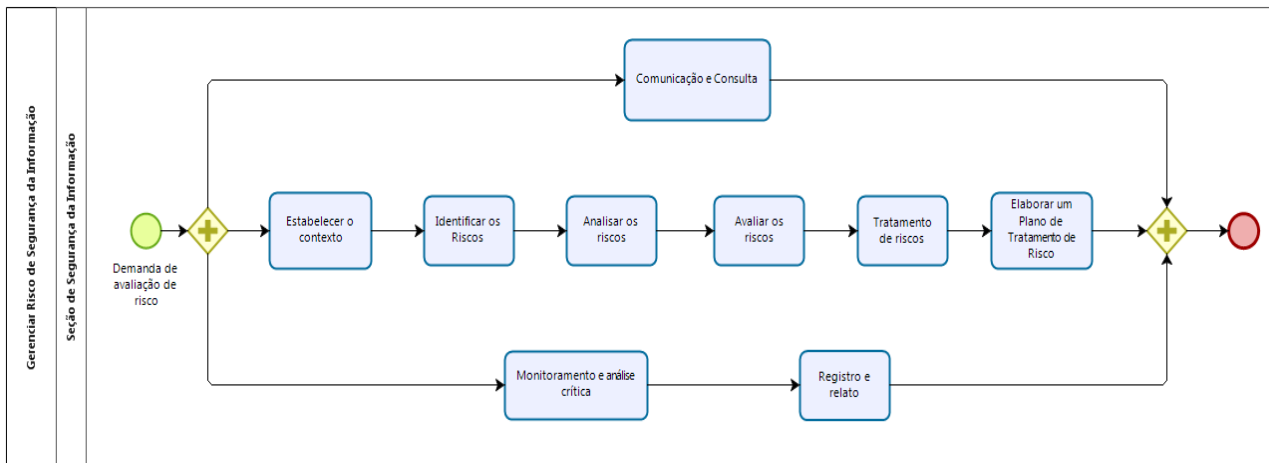
Destaca-se que a participação das outras unidades da área de TIC (Desenvolvimento de Sistemas, Governança de TIC, Infraestrutura de Comunicação, Relacionamento com o Cliente e Apoio ao PJe-JT) e do Comitê Gestor de Segurança da Informação e Comunicação são indispensáveis para o sucesso na gestão dos riscos.

As unidades de TIC participarão das atividades sempre que os riscos envolverem as suas respectivas áreas de atuação. E o Comitê Gestor de Segurança da Informação e Comunicação será instado a validar e aprovar os artefatos produzido ao longo do processo quando for necessário o estabelecimento de diretrizes com aplicabilidade em todo Tribunal.



# Processo de Gestão de Riscos de Segurança da Informação

## ANEXO I - Fluxo do Processo de Gestão de Riscos



Powered by  
**bizagi**  
Modeler



## Processo de Gestão de Riscos de Segurança da Informação

### ANEXO II - Tarefas do Processo de Gestão de Riscos

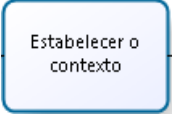
	<b>Estabelecer o contexto</b>
<b>Objetivo:</b> Estabelecer o contexto externo e interno para apoiar o Processo de Gestão de Riscos de Segurança da Informação.	
<b>Entradas:</b> Todas as informações relevantes sobre a organização para a definição do contexto da gestão de riscos.	
<b>Descrição da atividade:</b> <ul style="list-style-type: none"><li>Definir os critérios básicos para a gestão de riscos, tais como critério de avaliação de riscos, critério de impacto e critérios de aceitação do risco;</li><li>Estipular os objetivos a serem alcançados. Por exemplo: conformidade legal, preparação de um plano de resposta a incidentes, etc.;</li><li>Definir o escopo — descrição dos limites do projeto, sua abrangência, seus resultados e entregas.</li></ul>	
<b>Metodologia:</b> Analisar os contextos interno e externo buscando o apoio do processo de Gestão de Riscos de Segurança da Informação.	
<b>Responsável:</b> Unidades de TIC.	
<b>Saída:</b> Especificação dos critérios básicos, o escopo e os limites do processo de gestão de riscos.	

Tabela 8 - Tarefa Estabelecer o contexto



## Processo de Gestão de Riscos de Segurança da Informação

Identificar os Riscos

### Identificar os Riscos

#### Objetivo:

Encontrar, reconhecer e iniciar o registro dos riscos com o objetivo de identificar o que poderia acontecer ou quais situações poderiam afetar o alcance dos objetivos do TRT16.

#### Entradas:

- Contexto dos riscos (critérios básicos, o escopo e os limites, e a organização do processo de gestão de riscos);
- Lista dos ativos relacionados aos riscos;
- Informações do histórico e de incidentes passados;
- Documentação dos controles, planos de implementação do tratamento do risco.

#### Descrição da atividade:

- Identificação de ativos – realizar o levantamento dos ativos que estão dentro do escopo estabelecido. Além disso, é necessário listar os serviços/sistemas relacionados aos ativos identificados;
- Identificação de ameaças – realizar o levantamento das ameaças que tem potencial de comprometer ativos, identificando as suas fontes;
- Identificação de controles existentes – realizar o levantamento dos mecanismos administrativos, físicos ou operacionais capazes de tratar a ocorrência de um incidente de segurança existentes no TRT16;
- Identificação de vulnerabilidades – realizar o levantamento das vulnerabilidades que podem ser exploradas por ameaças para comprometer os ativos ou a organização. Essas vulnerabilidades podem ser das seguintes áreas: organização; processos e procedimento; rotinas de gestão; recursos humanos; ambiente físico; configuração do sistema de informação; hardware, software ou equipamento de comunicação; dependência de entidades externas;
- Identificação das consequências – realizar o levantamento do prejuízo ou das consequências para o TRT16 que podem decorrer de um cenário de incidente. Um cenário de incidente é a descrição de uma ameaça explorando as vulnerabilidades.





## Processo de Gestão de Riscos de Segurança da Informação

### **Metodologia:**

Conjunto de ações necessárias para levantamento, detalhamento e estruturação dos componentes de negócio, das ameaças e dos ativos (processos, tecnologias, ambientes e pessoas) que podem impactar os objetivos, missão ou atividades finalísticas do TRT16.

É importante que todos os ativos sob o escopo sejam inventariados. Essa atividade pode ser executada por meio de reuniões entre as equipes envolvidas. A partir disso, é necessário que os ativos e suas características (incluindo suas interdependências) sejam listadas. Essa lista de ativos deve ser revalidada ao final da atividade, garantindo que o escopo possui todos os ativos necessários para indicar os índices de riscos corretos.

### **Responsável:**

Unidades de TIC.

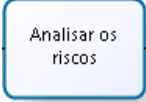
### **Saída:**

- Lista de ativos cujos riscos precisam ser controlados;
- Lista de processos de negócios relacionados aos ativos;
- Lista de ameaças com a identificação do tipo e da fonte das ameaças;
- Lista de todos os controles existentes;
- Lista de vulnerabilidades associadas aos ativos, ameaças e controles;
- Lista de cenários de incidentes com suas consequências;

*Tabela 9 - Tarefa Identificar os riscos*



## Processo de Gestão de Riscos de Segurança da Informação

	<b>Analisar os riscos</b>
<b>Objetivo:</b> Diz respeito ao entendimento do risco, com a definição das consequências e probabilidades para eventos identificados de risco. Com essa análise, busca-se o levantamento de informações que contribuam com a tomada de decisões estratégicas sobre os riscos e a forma mais adequada e rentável de tratamento.	
<b>Entradas:</b> <ul style="list-style-type: none"><li>• Lista de cenários de incidentes com suas consequências, incluindo a identificação de ameaças, vulnerabilidades, ativos afetados e consequências para os ativos e processos do negócio.</li></ul>	
<b>Descrição da atividade:</b> <ul style="list-style-type: none"><li>• Avaliação das consequências – avaliar os impactos sobre os negócios do TRT16 levando-se em conta as consequências de uma violação de segurança da informação. As consequências poderão ser expressas em função de critérios financeiros, técnicos, humanos, do impacto nos negócios, dentre outros;</li><li>• Avaliação da probabilidade dos incidentes – avaliar a probabilidade de ocorrência de incidentes em cada cenário e seus impactos;</li><li>• Determinação do nível de risco – realizar a mensuração do nível de risco para todos os incidentes considerados com o uso dos resultados obtidos pela avaliação das consequências e avaliação de probabilidade.</li></ul>	
<b>Metodologia:</b> Criação de questionários ou <i>checklists</i> que contenham as particularidades para cada um dos ativos do escopo.  Os questionários devem ser capazes de identificar as ameaças e vulnerabilidades associadas a cada ativo de informação, a probabilidade de ocorrência das ameaças, a severidade dos possíveis danos associados, assim como a relevância do ativo de informação para o escopo em análise.	



## Processo de Gestão de Riscos de Segurança da Informação

<p>Durante a fase de Análise, obtém-se a estimativa de Risco a que está submetido cada ativo, pelo produto dos seguintes atributos:</p> <ul style="list-style-type: none"><li>• <b>Probabilidade</b> da vulnerabilidade ser explorada por uma ameaça;</li><li>• <b>Severidade</b> das consequências da vulnerabilidade ser explorada;</li><li>• <b>Relevância</b>, que significa o grau de impacto do Ativo ser afetado por uma ameaça, o quão importante é o ativo para o escopo em análise. A relevância deve ser atribuída durante o levantamento dos ativos. Ela é obtida do cadastro de ativos e corresponde ao atributo "valor" do ativo.</li></ul>
<p><b>Responsável:</b></p> <p>Unidades de TIC.</p>
<p><b>Saída:</b></p> <ul style="list-style-type: none"><li>• Lista de consequências avaliadas referente a um cenário de incidente;</li><li>• Probabilidade dos cenários de incidentes;</li><li>• Lista de riscos com níveis de valores designados.</li></ul>

Tabela 10 - Tarefa Analisar os riscos



## Processo de Gestão de Riscos de Segurança da Informação


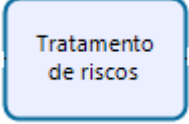
	<b>Avaliar os riscos</b>
<b>Objetivo:</b> Compreender a natureza do risco a fim de auxiliar a tomada de decisão sobre ações futuras.	
<b>Entradas:</b> Lista de riscos com níveis de valores designados e critérios para a avaliação de riscos.	
<b>Descrição da atividade:</b> Consiste em comparar os níveis de riscos estimados com critérios de riscos definidos pelo TRT16, a fim de determinar a ação mais adequada a ser tomada em relação ao risco, identificando quais riscos necessitam ser tratados e quais terão prioridade no tratamento.	
<b>Metodologia:</b> Tomar decisões sobre qual risco necessita de tratamento ou aceitação, bem como sua prioridade, com base nos resultados obtidos na Análise de Riscos considerando o contexto mais amplo do risco, incluindo o exame de quão tolerável são os riscos a serem assumidos. Para isso, com as informações sobre os processos de negócio da organização e os ativos que os suportam, deve-se: <ul style="list-style-type: none"><li>• Priorizar os riscos – os ativos que possuem os maiores níveis de risco (PSR) serão priorizados em termos de recursos e proteções.</li><li>• Ter maior conhecimento sobre os riscos e avaliar as melhores soluções de proteção, considerando seu custo-benefício.</li></ul>	
<b>Responsável:</b> Unidades de TIC.	
<b>Saída:</b> Lista de riscos priorizados, de acordo com os critérios de avaliação de riscos, em relação aos cenários de incidentes que podem levar a esses riscos.	

Tabela 11 - Tarefa Avaliar os riscos



## Processo de Gestão de Riscos de Segurança da Informação

	<b>Tratamento de riscos</b>
<b>Objetivo:</b> Estabelecer medidas para tratamento dos riscos visando a minimização dos impactos nos ativos do TRT16.	
<b>Entradas:</b> Lista de riscos com níveis de valores designados e critérios para a avaliação de riscos.	
<b>Descrição da atividade:</b> Consiste em comparar os níveis de riscos estimados com critérios de riscos definidos pelo TRT16, a fim de determinar a ação mais adequada a ser tomada em relação ao risco, identificando quais riscos necessitam ser tratados e quais terão prioridade no tratamento.	
<b>Metodologia:</b> O tratamento dos riscos consiste em reduzir, evitar, transferir ou reter o risco, observando: <ul style="list-style-type: none"><li>• A eficácia das ações de Segurança da Informação e Comunicações já existentes;</li><li>• As restrições organizacionais, técnicas e estruturais;</li><li>• Os requisitos legais; e</li><li>• A análise custo/ benefício.</li></ul> <b>Reduzir o risco</b> – implantar controles de proteção que reduzam o risco do ativo; <b>Evitar o risco</b> – uma forma de tratamento de risco na qual a alta administração decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco; <b>Transferir o risco</b> – é a decisão de compartilhar os riscos com outras entidades. A implantação do tratamento pode ser feita por um seguro que cubra as consequências, ou pela mudança do ativo para outro local ou empresa que cubra eventuais prejuízos; <b>Retter o risco</b> (aceitar) – não há implantação de controles, caso o nível do risco atenda aos critérios de aceitação do risco. O tratamento do risco pode ser iniciado quando nas fases de análise e avaliação forem fornecidas informações suficientes para determinar as ações necessárias para reduzir os riscos a níveis aceitáveis. Esta fase envolve a identificação dos controles previamente avaliados, além da preparação e	



## Processo de Gestão de Riscos de Segurança da Informação

<p>implantação das ações em planos de tratamento. Esses planos visam à redução dos riscos para os níveis aceitáveis e podem ter opções no tratamento de eventos internos e externos.</p> <p>Na gestão de tratamento dos riscos avaliados é importante estabelecer critérios para priorizar o tratamento dos riscos, considerando a tabela PSR.</p>
<p><b>Responsável:</b></p> <p>Unidades de TIC.</p>
<p><b>Saída:</b></p> <p>Lista de riscos e seus respectivos tratamento, de acordo com os critérios de avaliação de riscos, em relação aos cenários de incidentes que podem levar a esses riscos.</p>

*Tabela 12 - Tarefa Tratamento de riscos*





## Processo de Gestão de Riscos de Segurança da Informação

<div data-bbox="379 387 547 499" style="border: 1px solid blue; border-radius: 10px; padding: 5px; text-align: center;">Elaborar um Plano de Tratamento de Risco</div>	<b>Elaborar um Plano de Tratamento de Risco</b>
<b>Objetivo:</b> Criação de um plano para tratamento dos riscos identificados, o que envolve a seleção de uma ou mais ações para modificar os riscos e a implementação dessas ações.	
<b>Entradas:</b> Lista de riscos priorizadas, de acordo com os critérios de avaliação de riscos, em relação aos cenários de incidentes que podem levar a esses riscos.	
<b>Descrição da atividade:</b> Selecionar as opções de tratamento para os riscos selecionados considerando o resultado da análise/avaliação de riscos, custo esperado para implementação e benefícios previstos. Deve-se identificar a ordem de prioridade, bem como os prazos de execução. As respostas a riscos podem envolver uma ou mais das seguintes opções de tratamento: <ul style="list-style-type: none"><li>• Evitar o risco – ação para evitar totalmente o risco;</li><li>• Transferir o risco – compartilhar ou transferir uma parte do risco a terceiros;</li><li>• Mitigar o risco – reduzir o impacto ou a probabilidade de ocorrência do risco;</li><li>• Aceitar o risco – aceitar ou tolerar o risco sem que nenhuma ação específica seja tomada, pois ou o nível do risco é considerado baixo ou a capacidade da organização para tratar o risco é limitada ou o custo é desproporcional ao benefício.</li></ul>	
<b>Metodologia:</b> Elaborar um documento onde conste as medidas de tratamentos para os riscos encontrados na fase de análise e identificação de riscos.	
<b>Responsável:</b> Unidades de TIC.	
<b>Saída:</b> Plano de tratamento de riscos.	

Tabela 13 - Tarefa Elaborar um Plano de Tratamento de Risco



## Processo de Gestão de Riscos de Segurança da Informação

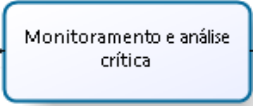
	<b>Monitoramento e Análise Crítica</b>
<b>Objetivo:</b> Trata da revisão e análise periódica da gestão de riscos, com vista ao aprimoramento contínuo desse processo pelo TRT16.	
<b>Entradas:</b> Todas as informações sobre os riscos geradas ao longo da execução das atividades do Processo de Gestão de Riscos de Segurança da Informação.	
<b>Descrição da atividade:</b> <ul style="list-style-type: none"><li>• Monitoramento e análise crítica dos fatores de risco – assegurar o controle do risco, monitorando riscos residuais e identificando novas ameaças e vulnerabilidades, assegurando a execução dos planos de tratamento dos riscos e avaliando sua eficiência e eficácia na redução dos riscos;</li><li>• Monitoramento, análise crítica e melhoria do processo de gestão de risco – garantir que o processo de gestão de riscos esteja realmente atendendo aos requisitos estratégicos do negócio.</li></ul>	
<b>Metodologia:</b> Apresentar uma rotina de revisão e análise para averiguar a eficácia na atividade de tratamento de riscos e a possibilidade de identificar novos possíveis riscos.	
<b>Responsável:</b> Unidades de TIC.	
<b>Saída:</b> Alinhamento contínuo da gestão de riscos.	

Tabela 14 - Tarefa Monitoramento e Análise Crítica



## Processo de Gestão de Riscos de Segurança da Informação

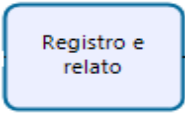
	<b>Registro e relato</b>
<b>Objetivo:</b> Documentar e relatar o processo de gestão de riscos por meios de mecanismos adequados.	
<b>Entradas:</b> Todas as informações relevantes sobre os riscos encontrados na organização.	
<b>Descrição da atividade:</b> Registrar todos os possíveis e já ocorridos riscos e relatar como foi a sua causa e consequência para assim ter um controle de medidas já preestabelecidas para combater futuros riscos utilizando o que já foi vivido.	
<b>Metodologia:</b> Utilizando os dados levantados nas tarefas de identificação e análise de riscos criar um documento que registre e relate todos os riscos identificados e suas medidas de tratamento para utilização futura.	
<b>Responsável:</b> Unidades de TIC.	
<b>Saída:</b> Documento com o registro e relato dos riscos visando o controle e melhora na tomada de decisão.	

Tabela 15 - Tarefa Registro e relato



## Processo de Gestão de Riscos de Segurança da Informação

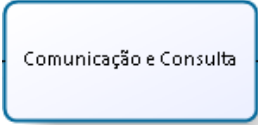
	<b>Comunicação e Consulta</b>
<b>Objetivo:</b> Compartilhamento contínuo das informações referentes aos riscos entre as partes interessadas.	
<b>Entradas:</b> Todas as informações sobre os riscos geradas ao longo da execução das atividades do Processo de Gestão de Riscos de Segurança da Informação.	
<b>Descrição da atividade:</b> Realizar a comunicação das informações produzidas ao longo da execução do processo de gestão de riscos, bem como disponibilizar essas informações para consulta, a fim de assegurar a compreensão necessária à tomada de decisão envolvendo riscos.	
<b>Metodologia:</b> Utilização de serviços digitais para disseminação das informações sobre os riscos entre as partes interessadas.	
<b>Responsável:</b> Unidades de TIC.	
<b>Saída:</b> Entendimento contínuo do Processo de Gestão de Riscos de Segurança da Informação e dos resultados obtidos.	

Tabela 16 - Tarefa Comunicação e Consulta