

Gestão de Riscos e Continuidade de Serviços de TIC – Teoria & Prática

Proposta de Curso n. 2025.08.03

1. Ementa

A capacitação em Gestão de Riscos e Continuidade dos Serviços de TIC (Tecnologia da Informação e Comunicação) tem como intuito apresentar os pilares e os principais componentes da governança corporativa, bem como a sua vinculação com a Gestão de Riscos.

Neste contexto, serão abordadas as etapas para à implantação da gestão de continuidade de negócios e das normas de segurança da informação na gestão dos processos de TIC, vinculados à manutenção e restauração da continuidade dos serviços de TIC.

Para tanto, serão utilizados normativos instituídos por órgãos de controle externo, como o Conselho Nacional de Justiça (CNJ), Conselho de Justiça Federal (CJF), bem como do próprio Tribunal Regional Federal da 5ª. Região (TRF5) e pelos conceitos emanados pelas normas ABNT NBR ISO 22301, 22313, 27005 e 31000, que constituem o arcabouço o qual possibilitará aos participantes a execução das atividades das oficinas.

Com a realização desta capacitação espera-se atingir os seguintes objetivos:

1. Atendimento às orientações emanadas pelos órgãos de controle e às boas práticas de governança de TIC.
2. Elaboração de minuta do Escopo do Plano de Continuidade de Negócios (PCN) com identificação dos cenários, partes interessadas e demais componentes do PCN.
3. Elaboração de minuta Business Impact Analysis (BIA) para seguintes serviços de TIC: SEI, PJe 2.0, Esparta-Precatório, Folha de Pagamento e o site institucional do TRF5.
4. Elaboração de minuta Plano de Tratamento do Risco Ataque Cibernético para os serviços indicados no item 3.
5. Modelagem do Processo de Gestão de Incidentes.
6. Elaboração de Planos de Gestão de Incidentes para o cenário de ocorrência de ataque cibernético para os serviços indicados no item 3.
7. Elaboração de estratégias para comunicação, visando subsidiar a alta administração quando da materialização de riscos que provoquem descontinuidade dos serviços de TIC.
8. Elaboração de minuta de Plano de Tratamento do Risco para serviços de TIC, considerando as ocorrências dos seguintes cenários: desastres naturais, sabotagem, greve e/ou falência de fornecedores, paralisação de transportes, falhas no fornecimento de energia, água e comunicação em nuvem.
9. Elaboração de Planos de Gestão de Incidentes dos serviços de TIC em caso de ocorrência de cenários relacionados no item 8.

Gestão de Riscos e Continuidade de Serviços de TIC – Teoria & Prática

Proposta de Curso n. 2025.08.03

2. Conteúdo Programático

O conteúdo programático do módulo teórico encontra-se detalhado na tabela a seguir. A previsão das atividades a serem desenvolvidas nas oficinas poderá ser adequada às peculiaridades do órgão, sempre com o intuito de alinhar as expectativas quanto aos artefatos a serem elaborados nesta capacitação.

TÓPICOS
<ul style="list-style-type: none"> Principais conceitos da Governança corporativa: pilares, agentes e estrutura.
<ul style="list-style-type: none"> Papel da Gestão de Riscos, na estrutura de governança.
<ul style="list-style-type: none"> Processo de Gestão de Riscos conforme a norma ABNT NBR ISO 31000 Contexto geral, específico, identificação, análise, avaliação e tratamento de riscos.
<ul style="list-style-type: none"> Importância de um Sistema de Continuidade de Negócios (SGCN) para as organizações.
<ul style="list-style-type: none"> Normas balizadoras de um SGCN – ABNT NBR ISO 22301.
<ul style="list-style-type: none"> Estrutura de um SGCN.
<ul style="list-style-type: none"> Estrutura organizacional recomendada para o SGCN.
<ul style="list-style-type: none"> Política de Continuidade de Negócios.
<ul style="list-style-type: none"> Planejamento de um SGCN – Serviços, atividades, ativos, fornecedores e pessoas de TIC – Escopo do SGCN.
<ul style="list-style-type: none"> Conceitos básicos: RPO, RTO, MBCO, MTPD.
<ul style="list-style-type: none"> Cenários de riscos de continuidade de negócios.
<ul style="list-style-type: none"> Objetivos de Continuidade de Negócios.
<ul style="list-style-type: none"> Definição de responsabilidades em um SGCN.
<ul style="list-style-type: none"> Business Impact Analysis.
<ul style="list-style-type: none"> Estrutura do Plano de Gestão de Incidentes.
<ul style="list-style-type: none"> Estrutura do Plano de Continuidade Operacional.
<ul style="list-style-type: none"> Estrutura do Plano de Recuperação de Desastre.
<ul style="list-style-type: none"> Estrutura do Plano de Administração de Crise.
<ul style="list-style-type: none"> Estrutura do Plano de Teste e Validação.

Gestão de Riscos e Continuidade de Serviços de TIC – Teoria & Prática

Proposta de Curso n. 2025.08.03

Após a realização do módulo teórico, o curso contempla a realização de oficinas conforme detalhamento na tabela a seguir.

A distribuição dos participantes nas oficinas se dará conforme a sua atuação nas atividades previstas nos referidos workshops.

SUGESTÃO DE OFICINAS PARA 2025	
<p>OFICINA 1 - ESCOPO SGCN</p> <p>Elaboração da declaração de escopo do SGC no âmbito dos serviços de TIC, com definição de cenários, identificação de partes interessadas, critérios de avaliação e análise de impacto no negócio (BIA) dos serviços de TIC.</p>	4 horas
<p>OFICINA 2 - TRATAMENTO RISCOS – CENÁRIO ATAQUE CIBERNÉTICO</p> <p>Elaboração de Plano de Tratamento de Riscos para os serviços: SEI, PJe 2.0, Esparta-Precatório, Folha de Pagamento e o site institucional do TRF5.</p> <ul style="list-style-type: none"> • Estabelecimento do contexto específico. • Análise das causas e consequências dos eventos de riscos relacionados com continuidade de negócios (cenários). • Avaliação dos riscos (classificação). • Levantamento dos controles existentes e de controles a serem implementados. • Cálculo do risco residual. 	12 horas
<p>OFICINA 3 - GESTÃO DE INCIDENTE EM CASO DE OCORRÊNCIA DE ATAQUE CIBERNÉTICO</p> <p>Modelagem do processo e elaboração de Plano de Gestão de Incidente para os serviços de TIC: SEI, PJe 2.0, Esparta-Precatório, Folha de Pagamento e o site institucional do TRF5.</p> <p>Esta oficina contempla a identificação das ações de comunicação que devem ser realizadas pela instituição durante o tratamento dos incidentes.</p>	12 horas
SUGESTÃO DE OFICINAS PARA 2026	
<p>OFICINA 4 - TRATAMENTO RISCOS PARA OS DEMAIS CENÁRIOS</p> <p>Desastres naturais, sabotagem, greve e/ou falência de fornecedores, paralisação de transportes, falhas no fornecimento de energia, água e comunicação em nuvem.</p> <p>ELABORAÇÃO DE PLANOS PARA OS SERVIÇOS DE TIC: SEI, PJe 2.0, Esparta-Precatório, Folha de Pagamento e o site institucional do TRF5.</p> <ul style="list-style-type: none"> • Estabelecimento do contexto específico. • Análise das causas e consequências dos eventos de riscos relacionados com continuidade de negócios (cenários). • Avaliação dos riscos (classificação). • Levantamento dos controles existentes e de controles a serem implementados. • Cálculo do risco residual. 	20 horas
<p>OFICINA 5 - GESTÃO DE INCIDENTE EM CASO DE OCORRÊNCIA DOS DEMAIS CENÁRIOS</p> <p>Elaboração de Plano de Gestão de Incidente para os serviços de TIC: SEI, PJe 2.0, Esparta-Precatório, Folha de Pagamento e o site institucional do TRF5, em caso de ocorrência dos seguintes cenários: desastres naturais, sabotagem, greve e/ou falência de fornecedores, paralisação de transportes, falhas no fornecimento de energia, água e comunicação em nuvem.</p>	20 horas

Gestão de Riscos e Continuidade de Serviços de TIC – Teoria & Prática

Proposta de Curso n. 2025.08.03

3. Carga Horária e Público Alvo

A carga horária total desta capacitação, prevista para ser realizada em 2025 e 2026 contemplando o módulo teórico e oficinas totaliza 78 (setenta e oito) horas, conforme detalhado na tabela a seguir.

ITEM	QTD	DESCRIÇÃO	PÚBLICO ALVO	CARGA HORÁRIA
01	01	MÓDULO TEÓRICO: Gestão de Riscos e Continuidade dos Serviços de TIC.	Servidores da DTIC, DEGEST e das unidades de negócio dos serviços: SEI, Pje 2.0, Esparta-Precatório, Folha de Pagamento e o site institucional do TRF5.	10 horas
02	01	OFICINA 1 - Elaboração da minuta da declaração de escopo do SGC no âmbito dos serviços de TIC.	Servidores da DTIC, DEGEST e das unidades de negócio dos serviços: SEI, Pje 2.0, Esparta-Precatório, Folha de Pagamento e o site institucional do TRF5	4 horas
03	01	OFICINA 2 - Elaboração de minuta do Plano de Tratamento de Risco de ataque cibernético.	Servidores da DTIC.	12 horas
04	01	OFICINA 3 - Elaboração de minuta do Plano de Gestão de Incidente referente à ataque cibernético.	Servidores da DTIC, DEGEST e das unidades de negócio dos serviços: SEI, Pje 2.0, Esparta-Precatório, Folha de Pagamento e o site institucional do TRF5.	12 horas
05	01	OFICINA 4 - Elaboração de minuta de Plano de Tratamento de Risco de: sabotagem, desastres naturais, greve e/ou falência de fornecedores, paralisação de transportes, falhas no fornecimento de energia, água e comunicação em nuvem.	Servidores da DTIC e servidores das demais unidades que possam atuar na mitigação dos riscos destes cenários.	20 horas
06	01	OFICINA 5 - Elaboração de minuta de Plano de Gestão de Incidente em caso de ocorrência dos cenários relacionados na OFICINA 4.	Servidores da DTIC, DEGEST e das unidades de negócio dos serviços: SEI, Pje 2.0, Esparta-Precatório, Folha de Pagamento e o site institucional do TRF5.	20 horas
CARGA HORÁRIA TOTAL				78 HORAS

Gestão de Riscos e Continuidade de Serviços de TIC – Teoria & Prática

Proposta de Curso n. 2025.08.03

4. Cronograma

O cronograma e a duração dos encontros serão definidos em comum acordo com o TRF5, objetivando a escolha de horários e periodicidade que melhor viabilizem a participação dos servidores envolvidos nesta temática. A título de sugestão, segue a proposição de datas e horários:

ATIVIDADE	C. H	PERÍODO	HORÁRIO
MÓDULO TEÓRICO	10h	06 a 10/out/2025	14h às 16h
OFICINA 1	4h	14 e 16/out/2025	14h às 16h
OFICINA 2	12h	21, 23,28 e 30/out/2025	14h às 17h
OFICINA 3	12h	04, 06, 11, 13/nov/2025	14h às 17h
OFICINA 4	20h	27, 28, 29/jan, 03, 04, 05, 10, 11, 12 e 24/fev/2026	14h às 16h
OFICINA 5	20h	03, 04, 05, 10, 11, 12, 17, 18, 19, 24/mar/2026	14h às 16h

5. Recursos Metodológicos

O conteúdo programático será desenvolvido por meio aulas expositivas e atividades práticas para a obtenção dos produtos propostos na ementa deste curso.

6. Ambiente Operacional

As aulas e as oficinas serão realizadas por meio de encontros presenciais, nas instalações desse Tribunal, ou por meio de aulas on-line síncronas.

7. Investimento e validade da proposta

O valor total da proposta, considerando a realização do módulo teórico e das cinco oficinas é de R\$ 29.172,00 (vinte e nove mil, cento e setenta e dois reais), **sem limitação de quantidade de participantes.**

Gestão de Riscos e Continuidade de Serviços de TIC – Teoria & Prática

Proposta de Curso n. 2025.08.03

Forma de pagamento

O pagamento deve ser feito ao final da execução de cada um dos módulos indicados no item 3 desta proposta (empenho global).

Esta proposta é válida por 90 (noventa) dias.

Dados bancários:

MEI MONICA MARIA DE SOUZA MONTEIRO 27655776415.

CNPJ 37.051.549/0001-15

Banco 0260 - Nu Pagamentos S.A. - Instituição de Pagamento

Agência 0001 - Conta: 53201283-0

FACILITADORA

Mônica Monteiro é mestre em Gestão Pública pela Universidade Federal de Pernambuco (UFPE), bacharela em Ciência da Computação pela Universidade São Paulo (USP). Participou da elaboração da política e da metodologia de Gestão de Riscos do Tribunal Regional do Trabalho da 6ª. Região (TRT6), foi a gerente do projeto de implantação da Gestão de Riscos naquele Tribunal. Ao longo de mais de 8 anos de experiência, elaborou os Planos de Tratamento de Riscos para processos de contratação de diversos órgãos públicos, dentre eles o TRT6, Tribunal Regional Federal da 5ª. Região (TRF5) e Seções Judiciárias de Alagoas, Ceará, Pernambuco, Rio Grande do Norte e Sergipe. Além disso, elaborou Planos de Tratamento de Riscos para processos organizacionais das mais diversas áreas, sejam eles da área finalística como Balcão Virtual, Agravo de Instrumento, Procedimento Ordinário quanto processos de suporte como Folha de Pagamento, Gestão de Infraestrutura de TIC, Aposentadoria de Servidores, Eliminação de Autos Findos, Pagamento de Peritos, dentre outros. Realizou diversas capacitações em Gestão de Riscos e Gestão de Processos, Sistema de Continuidade de Negócios, Governança Corporativa entre outros temas. Atua, também, na área de governança de tecnologia da informação e comunicação.

É palestrante, mentora e professora universitária. Iniciou sua carreira profissional na iniciativa privada em 1982, trabalhando na Itautec Informática. Em 1996, ingressou por meio de concurso público no Tribunal Eleitoral de Pernambuco, onde permaneceu por 18 anos, ocupando diversos cargos técnicos e de gestão.

e-mail: monica.monteiro@mm360.com.br

profa.monicamonteiro@gmail.com

CV Lattes: <http://lattes.cnpq.br/7207712079724953>

<https://www.linkedin.com/in/monica-monteiroconsultoria>

Recife, 03 de setembro de 2025.