



**TRIBUNAL REGIONAL ELEITORAL DO PARANÁ**  
**Secretaria de Administração**  
Coordenadoria de Licitações e Contratos  
Seção de Atendimento aos Sistemas Administrativos e Contratações Diretas  
SASAC

**TERMO DE INEXIGIBILIDADE DE LICITAÇÃO Nº 011/2022**  
**PAD Nº 6964/2022**

O **TRIBUNAL REGIONAL ELEITORAL DO PARANÁ**, com sede em Curitiba-PR, na Rua João Parolin, 224, inscrito no CNPJ/MF sob nº 03.985.113/0001-81, neste ato representado por seu Diretor-Geral, Dr. Valcir Mombach, pelo presente instrumento, regido pela Lei 8.666, de 21.06.93 e legislações pertinentes, contrata a empresa **SBC PERFORMANCE E EMPRESARIAIS EIRELI (Strong Business Consulting)**, CNPJ nº **26.306.940/0001-05**, com sede na cidade de São Bernardo do Campo - SP, na Avenida Francisco Preste Maia, 275, conj. 122, bairro Centro, CEP 09.770-000, telefones (11) 3939 -0988 e (11) 9 8027-6399, e-mail [info@strongsecurity.com.br](mailto:info@strongsecurity.com.br) e [caio@strongsecurity.com.br](mailto:caio@strongsecurity.com.br) para participação de 1 (um) servidor no seminário online “CISSP OFFICIAL – Certified Information Systems Security Professional.”, com fulcro no **Artigo 25, inc. II, c/c art. 13, inc. VI**, da Lei nº 8.666/93, inexigibilidade de licitação:

**Art. 25.** *É inexigível a licitação quando houver inviabilidade de competição, em especial:*

...

**II** - *para a contratação de serviços técnicos enumerados no art. 13 desta Lei, de natureza singular, com profissionais ou empresas de notória especialização, vedada a inexigibilidade para serviços de publicidade e divulgação;*

**Art. 13.** *Para os fins desta Lei, consideram-se serviços técnicos profissionais especializados os trabalhos relativos a:*

...

**VI** - *treinamento e aperfeiçoamento de pessoal;*

Observa-se, deste modo, a inexigibilidade de licitação, pois a contratação fundamenta-se na prestação de serviço técnico, de natureza singular e de notória especialização, do profissional que ministrará o curso, comprovada através das informações prestadas a seguir:

**Currículo do Professor Ricardo Giorgi**

Auditor, assessor e consultor de Projetos de Infraestrutura de Segurança da Informação, Gestão de Riscos, Ethical Hacking, Forense Digital, Gestão de Fraudes e Infraestrutura. LGPD, Consultor GDPR.

Professor de MBA da FIAP, Mackenzie, FIA, FIT, Febracorp, EPD e Universidades IBTA. Possui como principais certificações: CISA, CISSP-ISSAP, CISM, CRISC, CGEIT, ISO 27001 LA, VCP, CCSI, SSCP,

GREM, CEH, ECSA, Security+, Ethical Hacking, Secure Programming, RHCE, LPI, MCSO, CCNA, Network+, ITIL v2. Instrutor para (ISC)2 CISSP e SSCP Seminários de Revisão CBK. Mentor e Produtor de cursos do SANS Institute. Membro da ACFE (Certified Fraud Examiners) Ricardo é Msc. em Engenharia de Computação pelo IPT – USP, pós-graduado pela FASP em Consultoria em Internet, vice-presidente do (ISC)2 Brazil Chapter e Membro-Fundador do ISSA BrazilChapter

Suas maiores especialidades são: Segurança da Informação, Gestão de Riscos, Infraestrutura, Ethical Hacking, Análise de Vulnerabilidades, Criptografia, Segurança, Auditoria, Políticas de Segurança, Conscientização sobre Segurança, Operações de Segurança, Computação em Nuvem, Gestão de Fraudes, Gestão de Identidade, ITIL e Internet das Coisas.

O valor total desta contratação é de **R\$ 11.040,00** (onze mil e quarenta reais), estando inclusos todos os tributos, encargos sociais, ônus trabalhistas e previdenciários, ou outros de quaisquer naturezas para a prestação do serviço.

A despesa correrá à conta do Programa de Trabalho 02.122.0033.20GP.0041 – Capacitação da Escola Judiciária Eleitoral – TRE-PR, Elemento de Despesa 33.90.40.20.

O código para lançamento no Sistema Integrado de Administração de Serviços Gerais – SIASG será: 21172 – treinamento qualificação profissional; unidade de fornecimento: unidade.

Curitiba, 08 de abril de 2022.

Anete Diesel  
Chefe da Seção de Atendimento aos Sistemas Administrativos e Contratações Diretas e.e.  
**SASAC**

## **TERMO DE REFERÊNCIA**

### **1. OBJETO**

Participação do servidor Lucas Barke Bruzonb, chefe da Seção de Segurança Cibernética, SSC, no seminário on-line CISSP OFFICIAL – Certified Information Systems Security Professional.

**1.1.** O seminário será realizado na modalidade à distância on-line ao vivo

### **2. OBJETIVO DO CURSO**

Capacitar o Chefe da recém-criada Seção de Segurança Cibernética (SSC), de acordo com a Estratégia Nacional de capacitação em Cibersegurança, PAD 3507/2022, nos conhecimentos tecnológicos e gerenciais necessários para implantação da governança de Segurança da Informação, gerenciamento de risco, implantação de políticas, avaliação e teste de segurança e operações de segurança.

### **3. CONTEÚDO PROGRAMÁTICO**

#### **3.1.DOMÍNIO 1: PESO DO EXAME 15%**

##### **Security and Risk Management (Gestão de Segurança e Risco)**

**3.1.1.** Compreender, cumprir e promover a ética profissional;

**3.1.2.** Compreender e aplicar os conceitos de segurança;

**3.1.3.** Avaliar e aplicar os princípios de governança de segurança;

**3.1.4.** Determinar conformidade e outros requisitos;

**3.1.5.** Compreender as questões legais e regulamentares que dizem respeito à segurança da informação em um contexto holístico;

**3.1.6.** Compreender os requisitos para os tipos de investigação (ou seja, administrativos, criminais, civis, regulamentares, padrões da indústria);

**3.1.7.** Desenvolver, documentar e implementar políticas, padrões, procedimentos e diretrizes de segurança;

**3.1.8.** Identificar, analisar e priorizar os requisitos de Continuidade de Negócios (BC);

**3.1.9.** Contribuir e fazer cumprir as políticas e procedimentos de segurança pessoal;

**3.1.10.** Compreender e aplicar os conceitos de gestão de risco;

**3.1.11.** Compreender e aplicar conceitos e metodologias de modelagem de ameaças;

**3.1.12.** Aplicar conceitos de Supply Chain Risk Management (SCRM);

**3.1.13.** Estabelecer e manter um programa de conscientização, educação e treinamento de segurança.

## **3.2. DOMÍNIO 2: PESO DO EXAME 10%**

### **Asset Security (Segurança de ativos)**

- 3.2.1. Identificar e classificar informações e ativos;
- 3.2.2. Estabelecer informações e requisitos de manuseio de ativos;
- 3.2.3. Provisionar recursos com segurança;
- 3.2.4. Gerenciar o ciclo de vida dos dados;
- 3.2.5. Garantir a retenção de ativos adequada (por exemplo, Eng-of-Life (EOL), End-of-Support (EOS))
- 3.2.6. Determinar controles de segurança de dados e requisitos de conformidade.

## **3.3. DOMÍNIO 3: PESO DO EXAME 13%**

### **Security Architecture and Engineering (Arquitetura e Engenharia de Segurança)**

- 3.3.1. Pesquisar, implementar e gerenciar processos de engenharia usando princípios de design seguros;
- 3.3.2. Compreender os conceitos fundamentais dos modelos de segurança (por exemplo, Biba, Star Model, Bell-LaPadula);
- 3.3.3. Selecione os controles com base nos requisitos de segurança dos sistemas;
- 3.3.4. Compreender os recursos de segurança dos Sistemas de Informação (IS) (por exemplo, proteção de memória, Trusted Platform Module (TPM), criptografia / descryptografia);
- 3.3.5. Avaliar e mitigar as vulnerabilidades de arquiteturas de segurança, projetos e elementos de solução;
- 3.3.6. Selecionar e determinar soluções criptográficas;
- 3.3.7. Compreender métodos de ataques criptanalíticos;
- 3.3.8. Aplicar princípios de segurança ao projeto do local e da instalação
- 3.3.9. Projetar controles de segurança do local e das instalações

## **3.4. DOMÍNIO 4: PESO DO EXAME 13%**

### **Communication and Network Security (Segurança de comunicação e rede)**

- 3.4.1. Avaliar e implementar princípios de design seguro em arquiteturas de rede;
- 3.4.2. Componentes de rede seguros;
- 3.4.3. Implementar canais de comunicação seguros de acordo com o design.

## **3.5. DOMÍNIO 5: PESO DO EXAME 13%**

## **Identity and Access Management (IAM) (Gerenciamento de identidade e acesso (IAM))**

- 3.5.1.** Controle o acesso físico e lógico aos ativos;
- 3.5.2.** Gerenciar a identificação e autenticação de pessoas, dispositivos e serviços;
- 3.5.3.** Identidade federada com um serviço de terceiros;
- 3.5.4.** Implementar e gerenciar mecanismos de autorização;
- 3.5.5.** Gerenciar o ciclo de vida de provisionamento de identidade e acesso;
- 3.5.6.** Implementar sistemas de autenticação.

## **3.6. DOMÍNIO 6: PESO DO EXAME 12%**

### **Security Assessment and Testing (Avaliação e teste de segurança)**

- 3.6.1.** Projetar e validar estratégias de avaliação, teste e auditoria;
- 3.6.2.** Realizar testes de controle de segurança;
- 3.6.3.** Coletar dados do processo de segurança (por exemplo, técnico e administrativo);
- 3.6.4.** Analisar a saída do teste e gerar relatório;
- 3.6.5.** Realizar ou facilitar auditorias de segurança.

## **3.7. DOMÍNIO 7: PESO DO EXAME 13%**

### **Security Operations (Operações de Segurança)**

- 3.7.1.** Compreender e cumprir as investigações;
- 3.7.2.** Conduzir atividades de registro e monitoramento;
- 3.7.3.** Realizar gerenciamento de configuração (CM) (por exemplo, provisionamento, linha de base, automação);
- 3.7.4.** Aplicar conceitos básicos de operações de segurança;
- 3.7.5.** Aplicar proteção de recursos;
- 3.7.6.** Conduzir gerenciamento de incidentes;
- 3.7.7.** Operar e manter medidas preventivas e de detecção;
- 3.7.8.** Implementar e dar suporte ao gerenciamento de patch e vulnerabilidade;
- 3.7.9.** Compreender e participar dos processos de gestão da mudança;
- 3.7.10.** Implementar estratégias de recuperação;
- 3.7.11.** Implementar processos de recuperação de desastres (DR);
- 3.7.12.** Planos de recuperação de desastres de teste (DRP);

**3.7.13.** Participar de exercícios e planejamento de Continuidade de Negócios (BC);

**3.7.14.** Implementar e gerenciar a segurança física;

**3.7.15.** Abordar questões de segurança e proteção do pessoal.

### **3.8. DOMÍNIO 8: PESO DO EXAME 11%**

#### **Software Development Security (Segurança de desenvolvimento de software)**

**3.8.1.** Compreender e integrar segurança no Ciclo de Vida de Desenvolvimento de Software (SDLC);

**3.8.2.** Identificar e aplicar controles de segurança em ambientes de desenvolvimento;

**3.8.3.** Avalie a eficácia da segurança de software;

**3.8.4.** Avaliar o impacto de segurança do software adquirido;

**3.8.5.** Definir e aplicar diretrizes e padrões de codificação seguros.

### **4. LOCAL E DATA**

O curso será realizado em ambiente virtual, ao vivo, pela plataforma On-line Strong Security Brasil, no período de 18 a 29/04/2022, das 19h às 23h de segunda à sexta-feira, cada aula de 4 (quatro) horas de duração totalizando uma carga horária de 40 (quarenta) horas aula.

### **5. OBRIGAÇÕES DA CONTRATADA**

A empresa contratada deverá:

**5.1.** Manifestar o aceite da Nota de Empenho no prazo máximo de **24 (vinte e quatro) horas**, contados do comunicado feito pelo TRE. Não ocorrendo o aceite da Nota de Empenho no prazo determinado, a contratada estará sujeita às penalidades cabíveis.

**5.2.** Considerando a Resolução n. 879/2021, art. 13, § 2º, a empresa deverá atender às necessidades específicas a seguir:

**5.2.1.** Envio do certificado;

**5.2.2.** Lista de presença diária do aluno.

**5.2.3.** Avaliação de Reação.

### **6. PROTEÇÃO DE DADOS**

**6.1.** É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução do objeto para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

**6.2.** As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução do objeto, em consonância com o disposto na Lei nº 13.709/2018, sendo vedado o repasse das informações a outras

empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do contido neste termo.

**6.3.** As partes responderão administrativa e judicialmente, em caso de causarem danos patrimoniais, morais, individual ou coletivo, aos titulares de dados pessoais, repassados em decorrência da execução do objeto, por inobservância à LGPD.

**6.4.** Em atendimento ao disposto na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), o contratante, para a execução do objeto deste termo, poderá ter acesso aos dados pessoais dos representantes da contratada, tais como: número do CPF e do RG, endereço eletrônico, cópia do documento de identificação.

**6.5.** A contratada declara que tem ciência da existência da Lei Geral de Proteção de Dados (LGPD) e se compromete a adequar todos os procedimentos internos ao disposto na legislação, com intuito de proteção dos dados pessoais repassados pelo contratante.

**6.6.** A contratada fica obrigada a comunicar ao contratante, em até 24 (vinte e quatro) horas, qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da LGPD.

## **7. GESTÃO E FISCALIZAÇÃO**

**7.1.** Nos termos da Lei 8.666/93, art. 67, parágrafos 1.º e 2.º, o acompanhamento desta contratação se dará pelo gestor e, na sua ausência, impedimentos ou afastamentos, pelo substituto oficialmente designado.

**7.2.** Caberá ao gestor:

a) Acompanhar a contratação de acordo com as cláusulas deste termo, determinando o que for necessário para regularização das faltas ou defeitos observados, sob pena de responsabilização administrativa;

b) Comunicar à contratada via e-mail, carta ou ofício, os problemas relacionados à execução do objeto ou irregularidades encontradas;

c) Nos casos de irregularidades passíveis de sanções, abrir processo administrativo, na modalidade eletrônica (PAD), instruí-lo devidamente, com todas as informações pertinentes, em formulário específico, anexando cópia do e-mail enviado para o fornecedor referente à intenção de abertura de processo administrativo e com o respectivo comprovante de recebimento pela contratada, e encaminhá-lo para apreciação superior;

d) Receber e atestar o documento fiscal referente à execução do objeto, encaminhando-o ao setor responsável da Secretaria de Orçamento, Finanças e Contabilidade do TRE-PR para pagamento.

**7.3.** Se houver desacordo nas especificações do objeto, contidas nesse termo, não ocorrerá o atestado do documento fiscal.

## **8. PAGAMENTO**

**8.1.** O documento fiscal poderá ser emitido na forma eletrônica - NOTA FISCAL ELETRÔNICA, nos termos da legislação vigente, devendo ser encaminhado ao responsável pela fiscalização da contratação do TRE-PR por e-mail, em formato “.pdf”, ou poderá ser apresentado na forma física.

**8.2.** O documento fiscal deverá ser emitido pela contratada no prazo de até 05 (cinco) dias úteis do aceite do objeto deste termo e deverá conter o nome e número do banco, agência e conta corrente para depósito. A conta corrente obrigatoriamente deverá ser da própria contratada.

**8.3.** Outras especificações necessárias ao documento fiscal, as quais são requisitos indispensáveis para que possa ser atestado e encaminhado para pagamento:

- CNPJ do TRE: 03.985.113/0001-81
- Data de emissão do documento fiscal
- Descritivo dos valores unitário e total;

**8.4.** Caso a empresa contratada seja optante do SIMPLES, deverá a NF estar acompanhada de Declaração, conforme anexo IV da IN 1234/12 da SRF, nos termos do Inciso XI do artigo 6º.

**8.5.** O atesto do documento fiscal deverá ser feito até 05 (cinco) dias úteis, após comprovação do cumprimento de todas as exigências desta contratação.

**8.6.** O documento fiscal, acompanhado das certidões regularizadas da empresa, após o atestado da contratação, deverá ser encaminhado à Secretaria de Orçamento, Finanças e Contabilidade, para que se providencie o pagamento.

**8.7.** O pagamento será feito em parcela única, por meio de ordem bancária, creditada na conta corrente da contratada, no valor do documento fiscal, em até 05 (cinco) dias úteis, sempre contados após o atestado do documento fiscal.

**8.8.** Caso a contratada esteja inadimplente quanto à documentação habilitatória, conferida pela contratante para pagamento, estará sujeita à abertura de processo administrativo, visando regularizar a documentação sob pena de ser aplicada a sanção de advertência.

**8.9.** A atualização monetária e a multa, provenientes do atraso no recolhimento das obrigações tributárias e/ou previdenciárias serão descontadas do valor do documento fiscal correspondente, quando a contratada lhe der causa.

**8.10.** O não atendimento às especificações do documento fiscal, bem como a não comprovação da regularidade fiscal, darão causa às penalidades cabíveis.

**8.11.** Havendo erro na apresentação do documento fiscal ou dos documentos pertinentes à contratação, ou ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará pendente até que a contratada providencie as medidas saneadoras. Nessa hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação, não acarretando qualquer ônus para a contratante.

**8.12.** Nos casos de eventuais atrasos de pagamento, desde que a contratada não tenha concorrido para tanto e mediante solicitação formal da interessada, fica estabelecido que os encargos moratórios (juros e correção monetária) devidos pelo TRE-PR entre a data prevista para o pagamento e a do efetivo pagamento, serão calculados por meio da aplicação da fórmula  $EM = I \times N \times VP$ , onde:

EM = Encargos Moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso;



$I = \text{Índice de compensação financeira} = 0,00016438$ , assim apurado:

$I = i/365$  (onde  $i$  = taxa percentual anual no valor de 6%)

$I = (6/100)/365$ .

## **9. SANÇÕES**

**9.1.** O descumprimento a quaisquer das obrigações descritas no presente instrumento poderá ensejar abertura de processo administrativo, garantido o contraditório e a ampla defesa, com aplicação das seguintes sanções, de acordo com o capítulo IV da Lei nº 8666/93:

a) Advertência;

b) Multa:

1. Multa de 15% (quinze por cento) sobre o valor total da contratação, pelo atraso no início do evento, ou pelo não cumprimento do cronograma proposto;

2. Multa de 20% (vinte por cento) sobre o valor total contratado, em caso de recusa em prestar os serviços;

3. Multa de 5% (cinco por cento), sobre o valor total da contratação, pelo inadimplemento de obrigações acessórias.

c) Declaração de inidoneidade para licitar e contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição, ou até que seja promovida a reabilitação, na forma da lei, perante a própria autoridade que aplicou a penalidade;

d) Suspensão temporária de participação em licitação e impedimento de contratar com a Administração por prazo não superior a 2 (dois) anos, de acordo com a natureza da falta.

**9.2.** No caso de aplicação de multa determinada em processo administrativo que garanta a ampla defesa ao contratado, esta deverá recolher à União o valor imputado por meio de GRU.

**9.3.** As multas imputadas à contratada cujo montante seja superior ao mínimo estabelecido pelo Ministério da Fazenda e não pagas no prazo concedido pela Administração, serão inscritas em Dívida Ativa da União e cobradas com base na Lei nº 6.830/80, sem prejuízo da correção monetária.

## **10. DISPOSIÇÕES FINAIS**

Dúvidas referentes a esta contratação poderão ser sanadas com a Seção de Educação à Distância do TRE-PR, pelos telefones: (41) 3330-8544, (41) 3330-8573 e (41) 3330-8885 e e-mail [sead@tre-pr.jus.br](mailto:sead@tre-pr.jus.br), no horário das 12h00 às 19h00.