ERICA CRISTINA DOREA ROSSITER TAVARES
01/02/2024 08:41

TERMO DE REFERÊNCIA - INEXIGIBILIDADE DE LICITAÇÃO

CONTRATAÇÃO DE VAGAS EM EVENTO EXTERNO DE CAPACITAÇÃO

LEI Nº 14.133/2021

1. OBJETO (Art. 6º, Inciso XXIII, alíneas “a” e “c”)
1.1 Contratação de inscrições em curso, conforme dados a seguir:

Nome do curso:	Foundations of Incident Management – FIM (Fundamentos em Segurança da Informação)
Unidade Promotora do evento:	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)
Contratado(a):	NIC.br - Núcleo de Informação e Coordenação do Ponto BR
Unidade demandante:	Secretaria de Tecnologia da Informação e Comunicações - SETIC
Nº de vagas a serem contratadas:	05(cinco) vagas
CATSER	25232 - Pagamento Inscrição Eventos

2. PÚBLICO ALVO

Servidores lotados na **Coordenadoria de Segurança da Informação - COSI e do Núcleo de Segurança Cibernética – NSECI** do Tribunal Regional do Trabalho da 5ª Região.

3. PREVISÃO NO PLANO ANUAL DE CAPACITAÇÃO

A demanda está prevista no Plano Anual de Capacitação da unidade?
(x)Sim ( ) Não ( ) A unidade não possui Plano de Capacitação específico

4. JUSTIFICATIVA DA CONTRATAÇÃO (Art. 6°, Inciso XXIII, alínea “b”)

Considerando a recente modificação na estrutura organizacional deste TRT com a criação das áreas de Coordenação de Segurança da Informação - COSI e respectivas Divisão de Privacidade e Proteção de Dados Pessoais e Divisão de Especialização em Segurança Cibernética ***(RA TRT nº 0029/2022 e Ato TRT5 GP nº 0737/2023);***

A capacitação se faz necessária em face dos servidores participantes do treinamento estarem lotados nestas áreas e desempenhando atividades de segurança da informação, privacidade e proteção de dados, que exigem atualizações constantes de conhecimento.

5. REQUISITOS DA CONTRATAÇÃO (Art. 6°, Inciso XXIII, alínea “d”)

5.1 Modalidade: (x) Presencial ( ) Telepresencial (ao vivo) ( ) À distância

5.2 Certificado: (x) Ao final do treinamento a contratada deverá emitir certificado para cada participante com no mínimo os seguintes dados: nome do treinamento, modalidade, nome do aluno, carga horária, data de início e término.

5.3 Critérios para o Aceite de inscrição, doc. 05 e 09: O preenchimento do formulário de inscrição não é garantia de vaga no curso. As inscrições nos cursos serão aceitas conforme a disponibilidade de vagas e adequação dos candidatos aos pré-requisitos exigidos e aos critérios de aceite.

Os cursos do CERT.br, que são subsidiados pelo NIC.br, são oferecidos com o objetivo de contribuir para que o País conte com o maior número possível de CSIRTs bem estruturados e com seus profissionais capacitados.

Como a demanda por treinamento é maior que a capacidade de oferta, para atingir o objetivo acima o CERT.br estabeleceu critérios para balizar a decisão de quais inscrições serão aceitas e quais serão colocadas em lista de espera.

O CERT.br leva em consideração os seguintes fatores como composição do critério para aceitar as solicitações de inscrição nos cursos:

- Usar um e-mail institucional, associado à organização (i.e. fulano@domínio_da_organização);
- Trabalhar no CSIRT/SOC da organização;
- Desempenhar as funções de CSIRT/SOC mesmo que a organização não tenha estes times formalizados;
- Atuar em função técnica relacionada com segurança cibernética;
- Estar implantando um CSIRT/SOC;
- Atuar em função técnica relacionada com redes ou infraestrutura de TI;

Observações:

1. Em todos os casos serão aceitas inscrições de no máximo 2 participantes de uma mesma instituição por turma, seguindo a ordem de solicitação de inscrição;

2. Serão priorizadas as inscrições de profissionais atuantes em setores ou serviços críticos na Internet no Brasil;
3. Inscrições que utilizarem como e-mail principal de contato endereços não associados a uma instituição (seja empresa, órgão de governo, universidade, organização sem fins lucrativos, etc), serão automaticamente colocadas em espera.

6. MODELO DE EXECUÇÃO DO OBJETO (Art. 6°, Inciso XXIII, alínea “e”)

6.1 Detalhamento do evento

Período de realização*:	• Turma 2 - 15/04 a 19/04/2024 (05 dias); • Turma 3 - 20/05 a 24/05/2024 (05 dias); • Turma 4 - 22/07 a 26/07/2024 (05 dias).
Carga horária:	**40 horas**
Local de realização:	Os cursos são todos ministrados em São Paulo–SP, na sede do NIC.br, no bairro Brooklin Novo.
Plataforma para acesso (quando couber)	Não se aplica.
Há necessidade de pagamento de diárias aos participantes?	(x) Sim ( ) Não Obs: caso exista necessidade, proceder conforme norma de pagamento de diárias, Ato TRT5 n. 299/2013
Há necessidade de compra de passagens para os participantes?	(x) Sim ( ) Não obs: caso exista necessidade, proceder conforme norma de pagamento de diárias, Ato TRT5 n. 299/2013

*** Política de inscrição - Limite por Instituição**

No curso Foundations of Incident Management (FIM) serão aceitas inscrições de no máximo 2 participantes de uma mesma instituição por turma, seguindo a ordem de solicitação de inscrição e os critérios de aceite, doc. 08.

DESCRIÇÃO

Este curso de 5 dias é destinado ao pessoal técnico de Grupos de Segurança e Resposta a Incidentes (CSIRTs), SOCs e outras áreas relacionadas com atividades de Gestão de Incidentes de Segurança Cibernética.
Este curso fornece conhecimentos fundamentais para profissionais que precisam entender as funções de um serviço de Gestão de Incidentes Cibernéticos e como prover este serviço com resiliência. Ele apresenta uma visão geral dos conceitos relacionados com gestão de incidentes, onde estas atividades se encaixam no ecossistema de segurança cibernética e gestão de risco, bem como aborda tópicos como ameaças atuais mais relevantes e a natureza das atividades de resposta a incidentes.

Durante o curso os alunos irão:

1. Aprender como obter as informações necessárias para tratar um incidente;
2. Compreender a importância de possuir e seguir políticas e procedimentos pré-definidos;
3. Entender os aspectos técnicos relacionados com tipos de ataques comumente reportados;
4. Realizar tarefas de análise e resposta em diversos cenários de incidentes;
5. Aplicar habilidades de pensamento crítico na resposta a incidentes;
6. Identificar potenciais problemas a serem evitados durante o trabalho de gestão de incidentes.

O curso incorpora atividades interativas, discussões em grupo e exercícios práticos. Os participantes terão a oportunidade de participar em cenários de resposta a incidentes que poderão encontrar no dia a dia do seu trabalho, em exercícios em formato *table top.*

Objetivos

Este curso ajudará os participantes a:

1. Identificar o que deve ser implementado previamente para facilitar o tratamento de incidentes;
2. Definir consciência situacional e os tipos de fontes dedados para coletar informações de interesse;
3. Comparar os tipos de análise que podem ser realizadas, como eles diferem e quando usá-los;
4. Explorar os desafios no compartilhamento de informações e algumas iniciativas que procuram lidar com esses desafios;
5. Reconhecer ameaças e alvos atuais;
6. Reconhecer a importância de seguir processos, políticas e procedimentos bem definidos

7. Identificar as questões técnicas, de comunicação e coordenação envolvidas na execução bem-sucedida do tratamento de incidentes;
8. Analisar criticamente e avaliar o impacto dos incidentes de segurança da informação
9. Construir e coordenar estratégias efetivas de resposta para vários tipos de incidentes de segurança da informação.

Tópicos Abordados

1. Compreensão do ambiente de ameaças atual e dos processos de gestão incidentes;
2. Código de ética de um CSIRT;
3. Ferramentas e tecnologias de segurança usadas porum CSIRT;
4. Identificação de informações críticas;
5. Detecção e análise de incidentes;
6. Processo de triagem;
7. Identificação dos passos básicos da resposta;
8. Ataques envolvendo DNS e uso de DNS no processo de tratamento de incidentes;
9. Busca de informações de contato;
10. Coordenação da resposta a incidentes e disseminação de informações;
11. Tratamento de ataques comuns envolvendo e-mails e códigos maliciosos;
12. Cooperação com as polícias e os operadores da justiça

Público Alvo

1. Integrantes de CSIRTs e analistas de SOC que tenham pouca ou nenhuma experiência (um a três meses de experiência), e que estejam envolvidos com atividades de gestão de incidentes, incluindo atividades detecção e resposta a ataques;
2. Integrantes experientes de CSIRTs e SOCs que tenham interesse em validar seus processos ou em aumentar seus conhecimentos através de treinamento formal e boas práticas operacionais;
3. Profissionais que potencialmente venham a atuar em grupos de resposta a incidentes (CSIRTs) ou áreas ligadas à gestão de incidentes;
4. Administradores de redes e sistemas que sejam responsáveis por identificar e responder a incidentes de segurança ou outras atividades ligadas à proteção das redes.

6.2 Dados dos participantes

Turma - Período	Matrícula	Participante	Lotação
TURMA 02 - 15/04 a 19/04/2024	12450-8	Thiago da Silva Gilla	COSI
TURMA 03 - 20/05 a 24/05/2024	12583-0	Joyce Queiroz e Silva	NSECI
TURMA 03 - 20/05 a 24/05/2024	1904-8	Denilson Luis Torres dos Santos	COSI
TURMA 04 - 22/07 a 26/07/2024	7433-2	Hetug Sardeiro Porto	COSI
TURMA 04 - 22/07 a 26/07/2024	6816-2	Ruth Marques Gomes de Oliveira	NSECI

7. MODELO DE GESTÃO DO TREINAMENTO (Art. 6°, Inciso XXIII, alínea “f”)

A concepção, coordenação técnico-administrativa e fiscalização será realizada pela Escola Judicial.

7.1 A gestão e fiscalização da contratação serão regidas, no que couber, pelo ato 32/2023, que trata sobre a fiscalização dos contratos no âmbito do Tribunal Regional do Trabalho da 5ª Região –TRT5, bem como pelos arts. 115 a 123 da Lei nº 14.133/2021, devendo ainda ser observado o seguinte:

7.2 A gestão administrativa e a fiscalização do contrato caberá ao (à) Escola Judicial, a quem competirá gerenciar quaisquer alterações decorrentes da contratação, recebimento do objeto e por atestar as notas fiscais para pagamento, na condição de representante do contratante.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO (Art. 6°, Inciso XXIII, alínea “g”)

8.1. O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta-corrente indicados pela CONTRATADA, no prazo máximo de até 5 (cinco) dias úteis contados da finalização da liquidação.

a) A CONTRATADA, **no prazo de 5 (cinco) dias úteis após a assinatura do contrato**, deverá providenciar o credenciamento no Sistema de Gestão Orçamentária e Financeira da Justiça do Trabalho - (SIGEO-JT) para viabilizar os pagamentos das faturas vincendas no curso da execução do contrato.

(Para instruções deve ser acessado o seguinte link: https://docs.google.com/document/d/1l4hln6y4i2nAlXuTrkBcTYmMtiMzN_8Ebv6Bbd7Edvg/edit?usp=sharing)

b) **A CONTRATADA deverá emitir e protocolar a nota fiscal no sistema SIGEO-JT**, acompanhada da regularidade fiscal e trabalhista (CND-Federal, CRF e CNDT ou SICAF), para fins de validação/ateste pelo fiscal do contrato e posterior liquidação, que caracterizará **o recebimento definitivo**.

c) O **prazo de liquidação** será de até 5 (cinco) dias úteis, a contar do recebimento da nota fiscal **com ateste.**

d) Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como: prazo de validade, data da emissão, dados do contrato e do órgão contratante, o período respectivo de execução do contrato, o valor a pagar e eventual destaque do valor de retenções tributárias cabíveis.

e) Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que a CONTRATADA providencie as medidas saneadores, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao CONTRATANTE.

f) O CONTRATANTE deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

g) Constatando-se junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CONTRATANTE.

h) Não havendo regularização ou sendo a defesa considerada improcedente, o CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto inadimplência da CONTRATADA, bem como quanto a existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

i) Persistindo a irregularidade, o CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.

j) Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

k) Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

l) A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida LC.

m) Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

n) No caso de atraso pelo CONTRATANTE, os valores devidos à CONTRATADA serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA de correção monetária.

o) A pessoa jurídica para quem será feito o pagamento é o NIC.br:

Razão Social: NIC.br - Núcleo de Informação e Coordenação do Ponto BR
CNPJ: 05.506.560/0001-36
Insc. Estadual: Isento
Insc. Municipal: 3.198.078-3
Endereço: Av. das Nações Unidas, 11541, 7º andar, Brooklin Novo, CEP 04578-000 - São Paulo / SP
Telefone: (11) 5509 3511
Fax: 11) 5509 3512
Site: https://nic.br/

9. SELEÇÃO DO FORNECEDOR (Correlação com Art. 6°, Inciso XXIII, alínea “h”)

9.1 Enquadramento legal

Trata-se de contratação de empresa que atua na área de treinamento, sendo necessário o enquadramento na hipótese de inexigibilidade de licitação, prevista no inciso III, alínea f, do art. 74 da Lei n. 14.133.

9.1.1 Da inviabilidade de competição

A inexigibilidade de licitação decorre da impossibilidade de se estabelecer uma competição entre os possíveis interessados, seja pelo fato de que aquele prestador é o único que atende às peculiaridades do objeto contratual pretendido, seja pela impossibilidade de comparação objetiva entre as propostas, eis que se trata de serviço eminentemente intelectual, cuja produção atrela-se especificamente à técnica única de abordagem e modelagem, inerentes a cada profissional ou empresa do ramo.

9.1.2 Da notória especialização

9.1.2.1. Instrutor

Os instrutores dos cursos do CERT.br possuem sólida formação em administração e segurança de redes, além de uma ampla experiência na área de tratamento de incidentes de segurança em computadores.

Os instrutores foram aprovados e treinados pelo CERT® Division, da Carnegie Mellon® University, para ministrar estes cursos, e detém a credencial SEI-Authorized CERT Instructor.

O *CERT® Division* é um centro de excelência em Segurança Internet, localizado no *Software Engineering Institute* (SEI), um Centro de Pesquisa e Desenvolvimento mantido pelo governo dos Estados Unidos da América e operado pela Carnegie Mellon® University.

O CERT Coordination Center® (CERT®/CC) foi criado em 1988, sendo o primeiro CSIRT a ser estabelecido no mundo. Com a expansão da Internet e com a sofisticação dos atacantes surgiram novas demandas, que levaram o CERT®/CC a ser apenas um dos componentes do CERT® Division.

Cristine Hoepers, Gerente Geral do CERT.br, é formada em Ciências da Computação pela Universidade Federal de Santa Catarina (UFSC) e Doutora em Computação Aplicada pelo Instituto Nacional de Pesquisas Espaciais (INPE). Possui a credencial SEI-Authorized CERT Instructor, que a habilita a ministrar os cursos do CERT® Division licenciados pelo CERT.br. Possui também a certificação Certified SIM3 Auditor, que a habilita a auditar o nível de maturidade de CSIRTs de acordo com o Modelo de Maturidade SIM3 (Security Incident Management Maturity Model).

Trabalha com Gestão de Incidentes de Segurança no CERT.br desde 1999, onde atualmente se dedica mais à área de Transferência do Conhecimento, em especial Treinamentos e Aconselhamento Técnico e de Políticas. Participou do Conselho Diretor do FIRST e da Coordenação dos Fóruns de Boas Práticas sobre Spam e CSIRTs do Internet Governance Forum (IGF), das Nações Unidas. Em 2020 recebeu do M3AAWG, maior organização mundial de combate a abusos online, o prêmio anual Mary Litynski, por seu trabalho para aumentar a resiliência da Internet. Foi moderadora e palestrante em eventos nacionais e internacionais, incluindo fóruns da OEA, ONU, ITU, LACNIC, FIRST, APWG e M3AAWG, abordando os temas de Gestão de Incidentes, Privacidade, Implantação de CSIRTs, Fraudes na Internet, Spam e Honeypots.

Klaus Steding-Jessen, Gerente Técnico do CERT.br, é formado em Engenharia da Computação pela Universidade Estadual de Campinas (Unicamp) e Doutor em Computação Aplicada pelo Instituto Nacional de Pesquisas Espaciais (INPE). Possui a credencial SEI-Authorized CERT Instructor, que o habilita a ministrar os cursos do CERT® Division licenciados pelo CERT.br. Possui também a certificação Certified SIM3 Auditor, que o habilita a auditar o nível de maturidade de CSIRTs de acordo com o Modelo de Maturidade SIM3 (Security Incident Management Maturity Model).

Atua com tratamento de incidentes no CERT.br desde 1999, e atualmente se dedica às áreas de Consciência Situacional e de Transferência de Conhecimento, em especial Treinamentos. Na área de Consciência Situacional trabalha com o desenvolvimento de ferramentas que permitam, através de honeypots, entender melhor os ataques atuais e correlacionar estes dados com aqueles dos incidentes de segurança reportados ao CERT.br. Tem trabalhado no apoio à implantação de novos CSIRTs no Brasil e tem sido palestrante em diversos eventos, no Brasil e no exterior, sobre os temas de seguranca da informação, boas práticas de operação de redes e prevenção de spam e phishing.

9.1.2.2 Empresa Contratada

Sobre o NIC.br

O Núcleo de Informação e Coordenação do Ponto BR - NIC.br foi criado para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil - CGI.br, que é o responsável por coordenar e integrar as iniciativas e serviços da Internet no País.

O NIC.br, além de braço executivo do CGI.br, tem entre suas atribuições:

- o registro e manutenção dos nomes de domínios que usam o <.br> , e a distribuição de números de Sistema Autônomo (ASN) e endereços IPv4 e IPv6 no País, por meio do Registro.br;
- o tratamento e resposta a incidentes de segurança em computadores envolvendo redes conectadas à Internet no Brasil, atividades do CERT.br;
- projetos que apoiem ou aperfeiçoem a infraestrutura de redes no País, como a interconexão direta entre redes (IX.br) e a distribuição da Hora Legal brasileira (NTP.br). Esses projetos estão a cargo do Ceptro.br;
- a produção e divulgação de indicadores, estatísticas e informações estratégicas sobre o desenvolvimento da Internet no Brasil, sob responsabilidade do CETIC.br;
- promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade;

- viabilizar a participação da comunidade brasileira no desenvolvimento global da Web, atividade desenvolvida pelo Ceweb.br;
- o suporte técnico e operacional ao LACNIC, Registro de Endereços da Internet para a América Latina e Caribe;
- hospedar o W3C Chapter São Paulo, que tem como principal atribuição desenvolver padrões para Web.

Organograma do NIC.br

Devido a sua constituição, o NIC.br não pode ser dissociado do CGI.br. Sendo assim, sua estrutura apresenta-se da seguinte maneira:

1. Registro.br - Registro de domínios ".br"
2. **CERT.br - Centro de Estudos, Resposta e Tratamento de Incidente de Segurança no Brasil**
3. Cetic.br - Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
4. Ceptro.br - Centro de Estudos e e Pesquisas em Tecnologia de Redes e Operações
5. Ceweb.br - Centro de Estudos sobre Tecnologias Web
6. IX.br - Brasil Internet Exchange (PTT.br)
7. W3C Chapter São Paulo - ações para o desenvolvimento e fortalecimento dos padrões web

Sobre o CERT.br

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de Responsabilidade Nacional de último recurso, mantido pelo NIC.br.

O NIC.br é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no País. Conduz ações e projetos que trazem benefícios à infraestrutura da Internet no Brasil e implementa as decisões e os projetos do CGI.br, que é responsável por coordenar e integrar as iniciativas e serviços da Internet no país.

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Público-Alvo

O CERT.br presta serviços para qualquer rede que utilize recursos administrados pelo NIC.br, mais especificamente endereços IP ou ASNs (Números de Sistemas Autônomos) alocados ao Brasil e domínios sob o ccTLD .br.

Integração com a Comunidade

O CERT.br possui uma forte integração com as comunidades nacional e internacional de CSIRTs. Esta integração permite a formação de relações de confiança e de uma rede de contatos com atores chave para o tratamento de incidentes relevantes.

Além do processo de tratamento a incidentes em si, para atingir sua missão, o CERT.br também desenvolve outras atividades que incluem a conscientização sobre os problemas de segurança, a análise de tendências e correlação entre eventos na Internet brasileira e o auxílio ao estabelecimento de novos CSIRTs no Brasil.

Estas atividades são descritas de acordo com o padrão "FIRST CSIRT Services Framework", descrito detalhadamente no documento "Computer Security Incident Response Team (CSIRT) Services Framework".

Este padrão agrupa os serviços prestados por um CSIRT em 5 grandes áreas, sendo que o CERT.br presta serviços que são parte de apenas 3 destas áreas, a saber: Gestão de Incidentes (Information Security Incident Management), Consciênca Situacional (Situational Awareness) e Transferência de Conhecimento (Knowledge Transfer).

A seguir são descritos os principais serviços e funções realizadas pelo CERT.br em cada uma destas grandes áreas de serviço.

Gestão de Incidentes

O CERT.br presta serviços da área de Gestão de Incidentes de Segurança da Informação para qualquer rede que utilize recursos administrados pelo NIC.br.

O CERT.br é um CSIRT Nacional de Último Recurso (National CSIRT of Last Resort), ou seja, um CSIRT de responsabilidade nacional que:

- Atua como ponto de contato nacional para notificação de incidentes de segurança, principalmente quando um contato mais específico não é conhecido;
- Facilita a comunicação entre profissionais, especialistas e outras equipes, no país e no exterior, que possam auxiliar em alguma fase do processo de tratamento de um incidente.

O CERT.br sempre vai procurar localizar e coordenar as atividades com CSIRTs e Grupos de Segurança das organizações envolvidas. Se nenhum grupo for localizado, será feito o melhor esforço para localizar o responsável pelo Sistema Autônomo envolvido.

A atuação depende da solicitação de uma das partes envolvidas para apoio na análise ou resposta ao incidente. Mediante solicitação de apoio, o CERT.br pode desempenhar uma das seguintes funções:

- **Coordenação:** auxiliar a comunicação e resolução do incidente através de um trabalho colaborativo com outras entidades como CSIRTs, empresas, universidades, provedores de acesso e serviços Internet, sistemas autônomos e operadores da justiça;
- **Análise Técnica:** dar suporte ao processo de análise de atividades maliciosas e de sistemas comprometidos;
- **Suporte à Mitigação e Recuperação:** dar suporte ao processo de mitigação de danos causados por um incidente e de recuperação de sistemas comprometidos.

Cabe ressaltar que o CERT.br não possui acesso às instalações ou sistemas de terceiros e sua atuação é focada em habilitar outros times a responder os incidentes da maneira mais efetiva possível.

Classificação e Divulgação das Informações: a princípio o CERT.br trata as informações recebidas como confidenciais, mas elas podem ter que ser compartilhadas com outros times ou organizações que precisem ser envolvidos para resolver um incidente. As informações serão anonimizadas sempre que possível. O CERT.br não comenta nem emite opiniões sobre incidentes específicos, independentemente de quem esteja envolvido, cabendo somente às partes envolvidas se pronunciar sobre um incidente em andamento.

Consciência Situacional

O CERT.br trabalha proativamente para aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço Internet brasileiro.

Dentre estas atividades estão a coleta e o compartilhamento de informações que possam ser usadas pela comunidade para auxiliar nos seus esforços de prevenção e recuperação de incidentes. As funções a seguir contribuem para atingir estes objetivos.

Aquisição de Dados: coletar e processar informações das mais diversas fontes, que possibilitem aumentar a visibilidade dos ataques que possam afetar redes conectadas à Internet no Brasil. As principais fontes de dados do CERT.br são:

- **Projeto Honeypots Distribuídos:** rede de honeypots desenvolvida e mantida pelo CERT.br, com sensores distribuídos em diversas redes do país, para obter dados sobre ataques a redes alocadas ao Brasil.
- **Projeto SpamPots:** rede de honeypots desenvolvida e mantida pelo CERT.br, com sensores distribuídos em diversos países, para obter dados sobre o abuso da infra-estrutura de redes conectadas à Internet para envio de spam.
- **Threat Feeds:** através de parceiros globais o CERT.br possui acesso a dados de ameaças relacionadas aos ASNs alocados ao Brasil coletados por diversas organizações. São exemplos de parceiros globais do CERT.br nessa área: Team Cymru, ShadowServer Foundation, SpamHaus e Shodan.
- **Notificações de Incidentes:** alguns dos incidentes notificados ao CERT.br geram Indicadores de Comprometimento (IoCs) que são compilados para compartilhamento com os ASNs ou com comunidades específicas, dependendo do tipo de informação e de sua classificação ou TLP.

Compartilhamento de Informações: as informações coletadas e processadas pelo CERT.br são compartilhadas com a comunidade de diversas formas e sempre respeitando os níveis de confidencialidade ou a classificação TLP, dependendo da natureza da informação:

- **Estatísticas Públicas:** o CERT.br mantém um conjunto de métricas públicas derivadas dos dados de notificações voluntárias de incidentes de segurança, dos dados capturados nos honeypots e de dados recebidos através de parceiros. Estes dados podem ser acessados nas seguintes páginas: https://cert.br/stats/ https://honeytarg.cert.br/honeypots/stats/flows/current/
- **Notificações para Sistemas Autônomos:** o CERT.br analisa os dados recebidos dos diversos parceiros de forma a identificar sistemas mal configurados que possam ser abusados por terceiros, bem como para identificar possíveis sistemas vulneráveis a comprometimento. Estes dados são agrupados por ASN e são enviadas semanalmente notificações para os responsáveis contendo estas informações e, também, com dicas sobre como identificar e resolver os problemas.
- **Compartilhamento via MISP:** O CERT.br tem incentivado o uso de MISP para compartilhamento de informações de ameaças na comunidade de CSIRTs brasileiros como uma forma de automatizar este processo, utilizando uma plataforma aberta, gratuita e amplamente utilizada pela comunidade internacional. Atualmente o CERT.br compartilha algumas categorias de dados via MISP com CSIRTs e com algumas comunidades de cooperação setorial. Informações sobre o MISP do CERT.br e sobre a comunidade nacional de MISP podem ser encontradas em: https://cert.br/misp/

Transferência de Conhecimento

Para melhor cumprir sua missão, o CERT.br investe em serviços que permitam transferir para a comunidade o conhecimento adquirido na análise de ameaças e vulnerabilidades observadas no dia a dia. Estes serviços incluem o incentivo para a formação de uma

comunidade de CSIRTs no país e a disseminação de boas práticas e materiais de conscientização, para melhor prevenir e tratar incidentes de segurança. Os serviços listados a seguir fazem parte dos esforços para Transferência de Conhecimento.

Conscientização

- Desenvolver materiais de boas práticas para administradores de redes Internet e usuários finais;
- Realizar reuniões com setores diversos da Internet no Brasil, de modo a articular a cooperação e implantação de boas práticas de segurança;
- Fomentar a cooperação entre CSIRTs através da organização do Fórum Brasileiro de CSIRTs, da manutenção de listas de discussão e da lista de CSIRTs Brasileiros;
- Ministrar palestras e workshops, de forma a disseminar boas práticas de segurança nos mais diversos setores.

Treinamento

- Oferecer treinamentos na área de tratamento de incidentes de segurança, especialmente para membros de CSIRTs e para instituições que estejam criando seu próprio grupo;
- Ministrar módulos relativos à segurança e tratamento de incidentes em treinamentos organizados por organizações parceiras.

Aconselhamento Técnico e de Políticas

- Participar das discussões nacionais e internacionais de Governança da Internet, com intuito de esclarecer questões técnicas e levar a estes fórums a visão de grupos de tratamento de incidentes, incluindo possíveis impactos de decisões políticas na segurança das redes;
- Participar de grupos de trabalho e discussões governamentais e setoriais, de forma a compartilhar o conhecimento e incentivar a adoção de boas práticas.

História e Governança

O CERT.br (antigo NBSO) foi criado em junho de 1997 por iniciativa do Comitê Gestor da Internet no Brasil (CGI.br), seguindo as recomendações do relatório ***"Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil"***, publicado em agosto de 1996. Este relatório foi desenvolvido pelo subgrupo de trabalho de segurança do GTER por solicitação do CGI.br.

Parte da história do CERT.br foi documentada no Capítulo ***"Wisdom from the Field"***, do Guia Getting started with a National CSIRT guide, que contou com os Gerentes do CERT.br como especialistas entrevistados. Este Guia, além de ilustrar boas práticas

com o exemplo do Brasil, também aborda o papel do NIC.br e do CGI.br para o desenvolvimento da Internet no país, bem como o modelo multissetorial de Governança.

As atividades conduzidas pelo CERT.br contribuem para o cumprimento das seguintes atribuições do CGI.br:

> I - estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil;
> IV - promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade;
> VI - ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;

De maneira complementar, as atividades do CERT.br são prestadas de acordo com o Estatuto do NIC.br, em especial para atingir os seguintes objetivos da entidade:

> IV - atender aos requisitos de segurança e emergências na Internet Brasileira em articulação e cooperação com as entidades e os órgãos responsáveis;
> VII - promover ou colaborar na realização de cursos, simpósios, seminários, conferências, feiras e congressos, visando contribuir para o desenvolvimento e aperfeiçoamento do ensino e dos conhecimentos nas áreas de suas especialidades.

Os serviços do CERT.br, com exceção dos cursos licenciados da Universidade Carnegie Mellon, são prestados gratuitamente a todas as redes que utilizam recursos administrados pelo NIC.br (endereços IP ou ASNs alocados ao Brasil e domínios sob o ccTLD .br). Os recursos financeiros para a prestação destes serviços vem do registro de domínios sob o ccTLD .br.

9.1.3. Razão da Escolha

O Núcleo de Informação e Coordenação do Ponto BR – NIC.br, através da CERT.br, é a fonte de todo o conhecimento nacional na área de proteção de dados.

A escolha de uma empresa com tamanha representatividade no mercado nacional e detentora de uma base sólida de conhecimento e de profissionais altamente qualificados se apresenta como algo natural, tendo em vista a busca deste E. Tribunal pela excelência na prestação dos serviços de Tecnologia da Informação e Comunicações, TIC, que se refletirá na excelência da prestação jurisdicional, missão da Justiça do Trabalho.

Neste PROAD, segue cópia da tela de apresentação do curso aberto ao público em geral (https://cursos.cert.br/fim/).

10. JUSTIFICATIVA DO PREÇO (Art. 6°, Inciso XXIII, alínea “i”)

10.1. O valor total da contratação é de R$ 16.500,00(dezesseis mil e quinhentos reais) para 05(cinco) vagas de treinamento a um custo unitário de R$ 3.300,00(Três mil e trezentos reais).

Neste PROAD, segue cópia da tela de apresentação do curso aberto ao público em geral com os valores (https://cursos.cert.br/fim/).

O preço proposto para o curso revela-se compatível com o mercado de TIC, estando em sintonia com os valores oferecidos para outras empresas, conforme pesquisa realizada, doc. 06.

Segundo a instituição:

Não há nenhum tipo de isenção, bolsa ou descontos para inscrições de vários profissionais de uma mesma instituição.

O valor cobrado pelos cursos apenas recupera os valores referentes aos royalties anuais e às licenças por certificado emitido, que são pagos ao SEI/CMU, e os valores do material.

Para manter o valor acessível ao maior número de organizações possível, o curso conta com uma contrapartida do NIC.br para os gastos com instrutores, local e alimentação.

Esta contrapartida permite cobrar um valor reduzido se comparado com valores de mercado, *mas, ainda assim, propiciando a todos um treinamento de qualidade, focado em transmitir a experiência do CERT.br em tratamento de incidentes, bem como facilitar a cooperação entre os profissionais que atuam nessa área.*

O CERT.br acredita que para atingir sua missão de "aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil" é essencial que possamos contribuir com cursos de qualidade, com valor acessível, para que o País conte com o maior número possível de CSIRTs bem estruturados e com seus profissionais capacitados.

SISTEMA DE AVALIAÇÃO

Os certificados dos Cursos Oficiais do CERT® Division ministrados pelo CERT.br têm a mesma validade daqueles emitidos diretamente pela Carnegie Mellon® University.

Serão emitidos certificados para os alunos que obtiverem 90% de presença.

O certificado de conclusão do curso é equivalente a 2.5 CEUs (Continuing Education Units), emitidos pela Carnegie Mellon® University.

INCLUÍDO NA INSCRIÇÃO

Estão incluídos no valor da inscrição:

- Apostila em formato impresso e PDF;
- Cópias impressas dos exercícios práticos e de documentos de apoio;
- **Almoço e coffee-breaks pela manhã e à tarde.**

11. ADEQUAÇÃO ORÇAMENTÁRIA (Art. 6°, Inciso XXIII, alínea "j")

11.1 As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

11.2 A contratação será atendida pela dotação a ser informada oportunamente pela Escola Judicial.

12. CRITÉRIO DE SUSTENTABILIDADE AMBIENTAL:

A contratação possui critérios de sustentabilidade e/ou observou as práticas sustentáveis do Guia de Contratações?

(x) Não

( ) Sim - discrimine a seguir:

Salvador, 31 de janeiro 2024

Érica Rossiter
Diretora da Secretaria de Tecnologia da Informação e Comunicações – SETIC
Integrante Requisitante