Edital nº 02/2025 – Capacitação em Cibersegurança e Monitoramento de dispositivos IoT

O(A) Diretor(a)-geral do INDT, Manaus - Amazonas, no uso de suas atribuições legais, por meio da Área de Capacitação INDT Educacional, torna público o Edital nº 02/2025 – Seleção de participantes para o **Capacitação em Cibersegurança e Monitoramento de dispositivos IoT**

1. DA FINALIDADE

1.1 Este programa tem como finalidade capacitar profissionais e membros da comunidade em tecnologias disruptivas com foco em cibersegurança e Internet das Coisas (IoT), visando a formação técnica de excelência e o fortalecimento da segurança digital em ambientes industriais.

1.2 O projeto promove a integração entre teoria e prática, por meio de aulas em laboratório, atividades imersivas no ambiente fabril para desenvolvimento de projetos aplicados, contribuindo para a transformação digital e a inovação tecnológica no ecossistema regional. O projeto conta com a parceria da empresa **Compal Eletrônica da Amazônia Ltda.**

2. DOS OBJETIVOS

2.1 Capacitar 60 participantes comunidade em fundamentos técnicos de segurança da informação e práticas avançadas de cibersegurança aplicadas a ambientes industriais e dispositivos IoT.

2.2 Desenvolver competências para elaboração de políticas de segurança, monitoramento de rede, análise de vulnerabilidades e execução de testes de intrusão (pentests) em ambientes simulados e reais.

2.3 Promover experiências práticas por meio de acesso ao laboratório de cibersegurança do INDT e de uma residência tecnológica com foco em desafios reais da indústria 4.0.

3. DAS AULAS E DA CARGA HORÁRIA

A capacitação será realizada em formato híbrido, combinando encontros presenciais e atividades online, organizados em duas turmas com **30 alunos cada**, totalizando **60 participantes**. A divisão das turmas visa otimizar o uso dos laboratórios do INDT e garantir a qualidade do acompanhamento pedagógico.

- **Turma 1**: Aulas presenciais às **segundas e quartas-feiras**, e aulas online às **sextas-feiras**.
- **Turma 2**: Aulas presenciais às **terças e quintas-feiras**, e aulas online às **sextas-feiras**.

A estrutura híbrida permite flexibilidade no aprendizado, favorecendo a participação ativa dos alunos, sem comprometer a qualidade e a profundidade dos temas abordados, especialmente nas práticas em laboratório e nos momentos de interação com profissionais da indústria.

O programa é dividido em **08 módulos** (conforme Item 3.2 deste edital) e estruturado em três etapas principais: **capacitação teórica e prática**, **mentoria especializada** e **residência tecnológica**. Ao longo do curso, os alunos estarão imersos em atividades que combinam o aprendizado conceitual com a aplicação prática, permitindo o desenvolvimento de competências técnicas em cibersegurança e monitoramento de dispositivos IoT. A carga horária total da formação é de **282 horas**.

Tendo seu início programado para ocorrer em 23 de Junho de 2025 e o término previsto para 26 de Novembro de 2025, no horário de 18:00h às 22:00h na sede do INDT.

Endereço	Av. José Moacir Teberga de Toledo, 1520, CEP: 69044-235 - Planalto, Manaus. Localizado no Parque Mosaico.
Localização	https://maps.app.goo.gl/WXxq1HKyjb92kJxP8
Imagem da Fachada	

3.1. Os treinamentos ocorrerão nas modalidades **teórica e prática**, estruturados em três principais etapas complementares:

- **Capacitação Técnica:** Nesta etapa, os alunos terão acesso a conteúdos teóricos e práticos por meio de 8 módulos, abordando temas como LGPD aplicada à indústria, segurança da informação, backup e recuperação de dados, monitoramento de infraestrutura de TI, segurança em aplicações IoT, técnicas de ataque (Red Team) e defesa (Blue Team). As aulas acontecerão em laboratórios equipados do INDT e em ambiente virtual, com atividades aplicadas ao contexto da Indústria 4.0.

- **Mentoria Especializada:** Os participantes contarão com sessões de mentoria conduzidas por especialistas da **UFAM** e **PUC Campinas**, com foco na aplicação dos conhecimentos adquiridos, resolução de dúvidas e orientação no desenvolvimento de soluções de segurança cibernética.

- **Residência Tecnológica:** Nesta etapa imersiva, os alunos poderão aplicar seus conhecimentos em ambientes reais. As atividades incluem o diagnóstico de segurança, execução de testes de intrusão (pentests), criação de relatórios técnicos e desenvolvimento de políticas e rotinas de segurança para sistemas industriais.

A carga horária total da formação é de **282 horas**, garantindo uma experiência completa que une conhecimento técnico, aplicação prática e integração com o mercado.

3.2. O Conteúdo programático será disposto de acordo com o modelo abaixo:

Módulos	Conteúdo Programático	Etapa	Carga Horária
1	LGPD aplicada à indústria • Introdução à LGPD e Contextualização na Indústria • Estrutura e Requisitos da LGPD • Gestão de Incidentes e Resposta a Incidentes de Segurança • Boas Práticas e Políticas de Conformidade na Indústria	Capacitação	12
2	Segurança da Informação aplicada a à Indústria • Fundamentos da segurança da informação • Criptografia e envio de dados seguros	Capacitação	40

	• Sistemas de arquivos criptografados • Configuração de Firewall • Identificação de vulnerabilidades • Estratégias de proteção em ambientes industriais		
3	Estratégias de Backup e Recuperação de Dados em Situações Críticas em ambientes industriais • Fundamentos de Backup e Recuperação de Dados • Planejamento e Estratégias de Backup • Implementação de Rotinas de Backup • Recuperação de Dados e Continuidade de Negócios • Desafios e Soluções em Situações Críticas • Instalação e configuração do FreeNAS	Mentoria e Imersão	40
4	Sistemas de Monitoramento de Infraestrutura de TI em ambientes industriais • Introdução aos Sistemas de Monitoramento • Monitoramento Proativo da Infraestrutura de TI • Análise de Dados e Geração de Alertas • Otimização de Sistemas de Armazenamento • Wazuh + Zabbix + Grafana	Capacitação	40
5	Segurança em aplicações IoT • Autenticação e aplicações legadas • Desafios: padrões inconsistentes, falta de criptografia, acesso compartilhado à rede, vulnerabilidades físicas, dentre outros • Soluções: segurança física, segurança de acesso remoto, redes privadas, detecção de anormalidades, dentre outros	Capacitação	40
6	Topicos avançados: Técnicas Avançadas de Ataque (Red Team) • Fundamentos de Red Team • PenTest em Redes Estruturadas • Redes Wireless, Dispositivos IoT	Capacitação	20

	• Aplicações Web e Cloud em IoT		

7	Topicos avançados: Técnicas Avançadas de Defesa (Blue Team)
	• Ambiente Blue Team
	  ○ Virtualização
	  ○ Redes de computadores
	  ○ Serviços em rede
	• Inteligência de ameaças
	  ○ Gerenciamento de logs
	  ○ SIEM (Security Information and Event Management)
	  ○ Técnicas avançadas de Engenharia social
	• Computação forense
	  ○ Perícia computacional
	  ○ Metodologias e processos de investigação
	  ○ Análise forense de redes
	• Respostas a incidentes
	  ○ Tipos de incidentes
	  ○ Gerenciamento de Vulnerabilidades
	  ○ Implementação de CSIRT (Computer Security Incident Response Team)
		Capacitação	20

8	Projeto Final + Laboratório voltado para monitoramento de dispositivo IoT • Processo de inovação tecnológica; • Laboratório englobando práticas na construção de políticas de segurança, rotinas de backup, monitoramento de rede e tratamento de vulnerabilidades • Residência Tecnológica: Imersão na indústria parceira para diagnóstico ou execução de pentests e envio de relatório de segurança	Imersão e Mentoria	70
Carga Horária Total		**282**	

4. DO PÚBLICO-ALVO E REQUISITOS MÍNIMOS

4.1. **Público Alvo:** O público-alvo deste projeto será composto por alunos, profissionais que possuam interesse ou atuem em áreas relacionadas à tecnologia da informação, segurança digital, automação industrial, redes de computadores e Internet das Coisas (IoT).

4.2 Requisito mínimo de formação: O curso é aberto a estudantes e profissionais que tenham o ensino médio completo. Será priorizado o ingresso de candidatos com formação técnica ou superior (em andamento ou concluída) em áreas como Tecnologia da Informação, Redes, Engenharia, Sistemas, Computação, Automação Industrial ou afins. É desejável que o candidato tenha familiaridade com informática, raciocínio lógico e interesse em atuar com segurança cibernética.

5. DAS VAGAS

5.1. Serão ofertadas um total de **60 (sessenta) vagas**, levando em consideração o disposto na seção **4. DO PÚBLICO-ALVO E REQUISITOS MÍNIMOS**.

6. DAS INSCRIÇÕES

6.1. A inscrição do candidato implicará o conhecimento e será subentendido aceitação das normas legais pertinentes e condições estabelecidas neste Edital, em relação às quais não poderá alegar desconhecimento;

6.2 Formas de Inscrição: Serão aceitas inscrições via internet, no endereço eletrônico Formulário de Inscrição entre **09 de junho de 2025 a 15 de junho de 2025. Os dados a serem preenchidos são:**

a) Nome do candidato: *(preencher o nome completo sem abreviações);*
b) Digite o seu CPF: *(preencher o CPF sem traços ou pontos);*
c) Selecione o seu grau de escolaridade: *(selecionar entre as opções apresentadas no formulário sobre em qual escolaridade se encontra no momento da inscrição);*
d) E-mail: *(preencher com seu e-mail mais utilizado, pois toda comunicação do processo seletivo será realizada por e-mail);*
e) Selecionar a confirmação que enviou os documentos para o e-mail informado: *(marcar essa opção no formulário);*
f) Selecionar a confirmação que leu e está de acordo com a Política de Privacidade: *(marcar essa opção no formulário);*
g) Selecionar que atesta que as informações preenchidas no formulário são verdadeiras: *(marcar essa opção no formulário).*
h) Anexar, em formato PDF ou imagem (JPG/PNG), os seguintes documentos:

- ***Documento de Identidade com foto*** *(RG, CNH ou equivalente);*
- ***CPF*** *(caso não conste no documento de identidade);*
- ***Comprovante de Escolaridade****: certificado ou declaração de conclusão do ensino médio, técnico, graduação ou pós-graduação, conforme o caso;*
- ***Currículo atualizado*** *(preferencialmente em PDF, contendo experiências profissionais, cursos e certificações relacionados à área de tecnologia);*
- ***Comprovante de experiência profissional ou declaração de atividades na área de tecnologia da informação, cibersegurança, redes ou inovação tecnológica*** *(opcional, mas pode contribuir para a pontuação na seleção).*

6.3 Os aprovados no processo seletivo serão contemplados com uma bolsa integral para cursar a capacitação, ou seja, não custearão a mensalidade;

6.4 É de exclusiva responsabilidade do candidato ou responsável legal as informações dos dados cadastrais no ato de inscrição;

6.5 O INDT não se responsabiliza por solicitações de inscrição não recebidas por motivo de ordem técnica dos computadores, falhas de comunicação, congestionamento das linhas de comunicação, bem como outros fatores de ordem técnica que impossibilitem a transferência de dados. Caso o candidato não receba um e-mail de confirmação que seu cadastro está sendo analisado, este deverá enviar um e-mail para treinamento@indt.org.br reportando o ocorrido;

6.6 O candidato poderá acompanhar a sua inscrição pela internet, por meio de notificação no seu e-mail após cadastro de inscrição preenchido no site Formulário de Inscrição.

6.7 Após o período de inscrição, o(a) candidato(a) ou seu representante não poderão alterar dados pessoais.

7. DO CRONOGRAMA

7.1. As fases e prazos deste edital ficam assim definidos:

Fases	Prazos
1. Publicação do edital	**09/06/2025**
2. Período de inscrição	**09/06/2025 a 15/06/2025**
3. Divulgação do resultado	**19/06/2025**
4. Período de realização do curso	**23/06/2025 a 26/11/2025**

8. DA HOMOLOGAÇÃO

8.1. Somente serão homologadas as inscrições que atenderem às normas e requisitos do presente edital.

8.2 O candidato que não cumprir os prazos estabelecidos em qualquer uma das fases da seleção, estará automaticamente **DESCLASSIFICADO**.

9. DA SELEÇÃO E DIVULGAÇÃO DOS RESULTADOS

9.1. Serão selecionados os participantes que tiverem o nível mínimo de formação exigida neste edital conforme seção **4. DO PÚBLICO-ALVO E REQUISITOS MÍNIMOS**.

9.2 A seleção será composta por critérios mínimos de escolaridade exigida neste edital e análise curricular, seguindo as seguintes pontuações:

Escolaridade	Pontuação
Pós-graduação completa em áreas afins (TI, Redes, Cibersegurança, Computação, Engenharia, e afins.)	5
Ensino Superior completo em áreas afins	4
Curso Técnico em áreas afins (Informática, Redes, e afins)	3
Ensino Médio Completo	2
Experiência profissional em áreas de tecnologia da informação ou segurança cibernética (mínimo 6 meses)	3
Experiência profissional e/ou estudos em cibersegurança, IoT ou projetos de inovação tecnológica (mínimo 6 meses)	3

Observações:
1- A pontuação por escolaridade considerará apenas a maior titulação.
2- O Tempo de atuação profissional não poderá ser somado contando apenas um deles.
3- Só poderão ser somadas as pontuações de escolaridade com tempo de atividade profissional.

9.3. O resultado da seleção dos candidatos será publicado nas redes sociais do INDT (Linkedin e Instagram), além de ser informado por e-mail, a partir do dia **19/06/2025**.

9.4 Serão considerados **CLASSIFICADOS** no processo seletivo, 80 candidatos que atenderam a todos os requisitos do processo seletivo.

9.5 Serão considerados **APROVADOS** no processo seletivo, os 60 (sessenta) primeiros colocados no processo seletivo.

9.6 Os demais candidatos classificados comporão a lista de espera, esta não gera garantia de vaga, **ficando sua aprovação condicionada à abertura de vagas em virtude de desistência de candidatos aprovados até o início do curso**.

10. DOS CRITÉRIOS DE DESEMPATE

10.1. Os critérios de desempate serão:

a) Candidato(a) elegível que enviou todos os documentos primeiro;
b) Candidato(a) maior de idade;
c) Candidato(a) que atue na área de infraestrutura e redes e segurança de redes;

11. DA MATRÍCULA

11.1. As MATRÍCULAS ocorrerão **no período de 16 de junho de 2025 a 18 de junho de 2025** de forma **online**, no horário das 9h30 às 17h30 via e-mail.

12. DA CERTIFICAÇÃO

12.1 A avaliação dos alunos será realizada por meio de atividades em sala de aula, participação nas discussões e projetos práticos.

12.2 Para aprovação no curso o aluno deve ter:

a) Frequência mínima maior ou igual a 75%. Caso isso não aconteça, o aluno será reprovado por frequência;
b) Média das notas de atividades (MR) maior ou igual a 5,0. Caso isso não aconteça, o aluno será reprovado com média final igual à média das notas das atividades;
c) Média final maior ou igual a 5,0, que seria obtida pela média aritmética das provas e atividades realizadas ao longo do curso.

12.3 Após a finalização da capacitação será emitido um certificado de participação no treinamento.

13. DA LEI GERAL DE PROTEÇÃO DE DADOS

13.1. Ao se inscrever neste processo seletivo, o candidato e seus representantes legais reconhecem e CONCORDAM E AUTORIZAM que o INDT irá coletar, armazenar e processar seus dados pessoais conforme estabelecido na Lei Geral de Proteção de Dados (Lei no 13.709/2018);

13.2. A coleta e o processamento dos dados pessoais do candidato têm como finalidade exclusiva a avaliação, divulgação de resultado, chamada e processo de admissão nos cursos técnicos oferecidos pela INDT. Consulte nossa Política de Privacidade de Dados;

13.3. Os dados pessoais coletados serão mantidos pela Instituição apenas pelo período necessário para atingir as finalidades especificadas nesta cláusula ou conforme exigido por obrigações legais ou regulatórias. Após este período, os dados serão excluídos de forma segura e irreversível;

13.4. INDT implementa medidas de segurança técnicas e organizacionais apropriadas para proteger os dados pessoais do candidato contra acesso não autorizado, perda ou destruição, levando em consideração os riscos envolvidos no processamento.

14. DAS DISPOSIÇÕES FINAIS

14.1. É responsabilidade de cada participante acompanhar as publicações referentes a este edital;

14.2. A qualquer tempo este edital poderá ser revogado, retificado ou anulado, no todo ou em parte, por motivo de interesse público, sem que isso implique direito à indenização de qualquer natureza;

14.3. Os recursos quanto aos termos deste edital somente serão apreciados se submetidos à Direção-geral do INDT, mediante manifestação formal e fundamentada, em até 3 (três) dias úteis após a sua publicação;

Manaus (AM), 09 de Junho de 2025.

INSTITUTO DE DESENVOLVIMENTO TECNOLÓGICO - INDT