Proposta ESR/RNP nº6416/2021

Ao
Sr. Eduardo França de Aguiar
Tribunal de Justiça do Estado do Piauí - TJPI

I - Apresentação da Escola Superior de Redes RNP

Excelência em ensino na área de Tecnologia da Informação e Comunicação. Esta é a proposta da Escola Superior de Redes (ESR). Há mais de 25 anos gerenciando a Internet acadêmica nacional, a Rede Nacional de Ensino e Pesquisa (RNP) criou a Escola Superior de Redes com o objetivo de disseminar o conhecimento em tecnologias da informação e comunicação. A formação é prática com atividades em laboratório de informática que são desenvolvidas para refletir as situações, problemas e desafios encontrados no dia a dia do profissional de redes.

A Rede Nacional de Ensino e Pesquisa (RNP), através da rede Ipê, provê serviço Internet com facilidades de trânsito nacional e internacional em uma infraestrutura com alta largura de banda e suporte a aplicações avançadas.

Os cursos da Escola Superior de Redes foram elaborados para que sua empresa aumente a eficiência no uso de redes digitais e no conjunto de aplicações de comunicação e colaboração, que permitem reduzir custos operacionais, para trazer mais agilidade para os negócios e garantir maior segurança das informações.

II - Áreas temáticas

Governança de TI

A Governança de TI está relacionada ao desenvolvimento de um conjunto estruturado de competências e habilidades estratégicas para profissionais de TI, responsáveis pelo planejamento, implantação, controle e monitoramento de programas e projetos de governança, requisitos fundamentais para as organizações, do ponto de vista de aspectos operacionais e de implicações legais.

A área de Governança de TI da ESR/RNP oferece cursos aos profissionais que atuam ou desejam atuar como gestores de tecnologia da informação em organizações de diversos setores e que buscam uma formação baseada em

esr.rnp.br
(61) 3243-4337
(61) 3243-4340
(61) 3243-4341 fax

modelos de melhores práticas gerenciais e ferramentas aplicáveis ao mundo de negócios em TI. Os cursos buscam atender à necessidade crescente das organizações de otimizar a aplicação de recursos, reduzir os custos e alinhar o setor de TI às suas estratégias de negócio.

Segurança

As notáveis vantagens trazidas pela Internet, como o comércio eletrônico e as transações bancárias on-line, facilitam a nossa vida, mas ao mesmo tempo atraem riscos que tem forte impacto na área de segurança da informação. A metodologia da ESR é capacitar o aluno para pensar preventivamente e tratar os incidentes quando não for possível evitá-los. As atividades práticas refletem a realidade do analista de segurança ao lidar com incidentes de segurança e investigações forenses, tornando-o um profissional valorizado nas corporações.

III - Cursos oferecidos

Curso	Local	Data prevista
Planejamento e Gestão Estratégica de TI (EaD) (GTI28)	ESR EaD	*A definir*
Fundamentos do COBIT 2019 (EaD) (GTI32)	ESR EaD	*A definir*
Gerenciamento Ágil de Projetos de TI (EaD) (GTI33)	ESR EaD	*A definir*
Elaboração de PDTI (EaD) (GTI39)	ESR EaD	*A definir*
Planejamento de Contratações de TI no Judiciário (EaD) (GTI43)	ESR EaD	*A definir*
Plano de Contratações Públicas de Bens e Serviços com base na IN 01/2019 – SGD/ME (EaD) (GTI44)	ESR EaD	*A definir*
Fundamentos de Gerenciamento de Serviços com ITIL4 (EaD) (GTI47)	ESR EaD	*A definir*
Sistema de Gestão da Integridade – Compliance & Antissuborno (GTI54)	ESR EaD	*A definir*

Escola Superior de Redes RNP
esr.rnp.br

RNP

Curso	Local	Data prevista
Segurança de Redes e Sistemas (EaD) (SEG18)	ESR EaD	*A definir*
Tratamento de Incidentes de Segurança (EaD) (SEG19)	ESR EaD	*A definir*
Teste de Invasão de Aplicações Web (EaD) (SEG21)	ESR EaD	*A definir*
Hardening em Linux (EaD) (SEG22)	ESR EaD	*A definir*
PenTest + EaD (parceria oficial CompTIA) (SEG23)	ESR EaD	*A definir*
CySA+ EaD (parceria oficial CompTIA) (SEG24)	ESR EaD	*A definir*
Security+ EaD (parceria Oficial CompTIA) (SEG25)	ESR EaD	*A definir*
CASP+ (CAS-003) EaD (parceria Oficial CompTIA) (SEG31)	ESR EaD	*A definir*
Cibersegurança EaD (parceria oficial Ascend) (SEG34)	ESR EaD	*A definir*
Correlacionamento de eventos com Graylog (SEG35)	ESR EaD	*A definir*

IV - Público alvo

Colaboradores daSecretaria de Tecnologia da Informação e Comunicação - STIC do Tribunal de Justiça do Estado do Piauí - TJPI.

V - Material didático

- Todo o material oficial CompTIA disponibilizado nos cursos da proposta estão em inglês;
- A ESR oferece ainda o acesso ao laboratório virtual da CompTIA para execução de exercícios práticos, em inglês.
- No material dos cursos dos parceiros CompTIA e EXIN estão inclusos os vouchers para realização da prova de certificação pelos alunos, considerando o número de vagas contratados nas turma (1 por aluno/aquisição);
- Ressaltamos que os vouchers terão validade de 1 (hum) ano para a realização das provas, contando a partir do início dos cursos.
- O material de apoio de todos os treinamentos serão disponibilizados somente no Ambiente Virtual de Aprendizagem (AVA), e inclui: conteúdo do curso, agenda do curso, tarefas, questionários, simulado, materiais extras e vídeo do encontro

Escola Superior de Redes RNP
esr.rnp.br

RNP

online.

VI - Número de vagas

Serão oferecidas 113 (cento e treze) vagas, conforme cronograma proposto.

VII - Carga horária

- O nível de cada treinamento é conforme descrito nas ementas dos cursos;
- Os cursos Segurança de Redes e Sistemas (EaD), Tratamento de Incidentes de Segurança (EaD), Teste de Invasão de Aplicações Web (EaD), Hardening em Linux (EaD), PenTest + EaD (parceria oficial CompTIA), CySA+ EaD (parceria oficial CompTIA), Security+ EaD (parceria Oficial CompTIA), CASP+ (CAS-003) EaD (parceria Oficial CompTIA, Cibersegurança EaD (parceria oficial Ascend), Planejamento de Contratações de TI no Judiciário (EaD), Correlacionamento de eventos com Graylog e Plano de Contratações Públicas de Bens e Serviços com base na IN 01/2019 – SGD/ME (EaD), são divididos em 10 sessões de aprendizagem, totalizando 40 horas.
- Os cursos Planejamento e Gestão Estratégica de TI (EaD), Fundamentos do COBIT 2019 (EaD), Gerenciamento Ágil de Projetos de TI (EaD), Elaboração de PDTI (EaD, Fundamentos de Gerenciamento de Serviços com ITIL4 (EaD) e Sistema de Gestão da Integridade – Compliance & Antissuborn (ED, são dividido em 6 sessões de aprendizagem, totalizando 24 horas.
- A carga horária do cursos da ESR são distribuídas em 50% de aulas EaD síncrona e 50% de auto estudo, conforme ementas.

VIII - Infraestrutura

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone;
- As aulas EaD são síncronas e com interação, podendo ser por zoom, webconf ou similar;
- O conteúdo do curso é acessado diretamente no Ambiente Virtual de Aprendizagem (AVA) do curso;
- O acesso à plataforma EaD da ESR é de responsabilidade do aluno;
- A ESR não fornecerá equipamentos ou link de internet para realização do curso.

Escola Superior de Redes RNP

esr.rnp.br

RNP

IX - Pré-matricula

Após a validação desta proposta, o responsável pelo aceite deverá realizar as pré-matrículas dos colaboradores no endereço encaminhado pela Escola Superior de Redes RNP.

Somente as inscrições realizadas por este endereço serão consideradas válidas.

X - Locais e horários da realização dos cursos

Local: Plataforma EaD ESR

Turmas

- Planejamento e Gestão Estratégica de TI (EaD) - A definir
- Fundamentos do COBIT 2019 (EaD) - A definir
- Gerenciamento Ágil de Projetos de TI (EaD) - A definir
- Planejamento de Contratações de TI no Judiciário (EaD) - A definir
- Elaboração de PDTI (EaD) - A definir
- Plano de Contratações Públicas de Bens e Serviços com base na IN 01/2019 – SGD/ME (EaD) - A definir
- Fundamentos de Gerenciamento de Serviços com ITIL4 (EaD) - A definir
- Sistema de Gestão da Integridade – Compliance & Antissuborno - A definir
- Segurança de Redes e Sistemas (EaD) - A definir
- Tratamento de Incidentes de Segurança (EaD) - A definir
- Teste de Invasão de Aplicações Web (EaD) - A definir
- Hardening em Linux (EaD) (SEG22) - A definir
- PenTest + EaD (parceria oficial CompTIA) - A definir
- CySA+ EaD (parceria oficial CompTIA) - A definir
- Security+ EaD (parceria Oficial CompTIA) - A definir
- CASP+ (CAS-003) EaD (parceria Oficial CompTIA) - A definir
- Cibersegurança EaD (parceria oficial Ascend) - A definir
- Correlacionamento de eventos com Graylog- A definir

Os encontros online dos treinamentos, ocorrem em dois dias alternados durante semana, com duas horas de duração.

As aulas ficarão gravadas e serão disponibilizadas no AVA (Ambiente Virtual de Aprendizagem) após 24 horas de sua realização, disponíveis permanentemente. **Alertamos que o fato de assisti-las fora do horário do Encontro Online (ao vivo), não contará como presença no curso.**

O cronograma de execução das turmas será de acordo com as disponibilidades de vagas nas turmas do calendário de 2021 ou de 2022. A última semana dos cursos

Escola Superior de Redes RNP
esr.rnp.br

RNP

não possui agenda de aula, pois é voltada para a conclusão e entrega das atividades dos treinamentos.

XI - Instrutoria

Os tutores da Escola Superior de Redes RNP possuem sólida formação acadêmica e profissional.

XII - Certificado de participação

Para conclusão dos cursos do **portfólio ESR** e acesso ao certificado é necessário:

- Entregar no mínimo 50% das tarefas
- Ter 50% de presença no total de encontros online;
- Obter média 6,0 (seis) no Questionário de Avaliação final;

Para conclusão do curso dos **Parceiros CompTIA ESR** e acesso ao certificado é necessário:

- Obter 60% de acerto no Questionário de Avaliação final - Simulado;
- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online.

Não é possível a postergar a data final de entrega de atividades: os alunos que não finalizarem as tarefas obrigatórias serão reprovados.

A aquisição do curso já garante acesso a prova de certificação dos treinamentos com voucher, independe da aprovação no treinamento da ESR, conforme regras acima.

XIII - Investimento

Curso	Valor unit. (R$)	Desconto (%)	Qtde.	Valor total (R$)
Planejamento e Gestão Estratégica de TI (EaD) (GTI28)	750,00	0,00000	8	6.000,00
Fundamentos do COBIT 2019 (EaD) (GTI32)	750,00	0,00000	8	6.000,00
Gerenciamento Ágil de Projetos de TI (EaD) (GTI33)	750,00	0,00000	19	14.250,00

Escola Superior de Redes RNP
esr.rnp.br

RNP

Curso	Valor unit. (R$)	Desconto (%)	Qtde.	Valor total (R$)
Elaboração de PDTI (EaD) (GTI39)	960,00	0,00000	8	7.680,00
Planejamento de Contratações de TI no Judiciário (EaD) (GTI43)	1.440,00	0,00000	6	8.640,00
Plano de Contratações Públicas de Bens e Serviços com base na IN 01/2019 – SGD/ME (EaD) (GTI44)	1.280,00	0,00000	6	7.680,00
Fundamentos de Gerenciamento de Serviços com ITIL4 (EaD) (GTI47)	512,00	0,00000	10	5.120,00
Sistema de Gestão da Integridade – Compliance & Antissuborno (GTI54)	720,00	0,00000	6	4.320,00
Segurança de Redes e Sistemas (EaD) (SEG18)	960,00	0,00000	4	3.840,00
Tratamento de Incidentes de Segurança (EaD) (SEG19)	960,00	0,00000	4	3.840,00
Teste de Invasão de Aplicações Web (EaD) (SEG21)	1.440,00	0,00000	4	5.760,00
Hardening em Linux (EaD) (SEG22)	960,00	0,00000	4	3.840,00
PenTest + EaD (parceria oficial CompTIA) (SEG23)	4.500,00	0,00000	5	22.500,00
CySA+ EaD (parceria oficial CompTIA) (SEG24)	4.500,00	0,00000	4	18.000,00
Security+ EaD (parceria Oficial CompTIA) (SEG25)	4.500,00	0,00000	4	18.000,00

Escola Superior de Redes RNP

esr.rnp.br

RNP

Curso	Valor unit. (R$)	Desconto (%)	Qtde.	Valor total (R$)
CASP+ (CAS-003) EaD (parceria Oficial CompTIA) (SEG31)	4.500,00	0,00000	4	18.000,00
Cibersegurança EaD (parceria oficial Ascend) (SEG34)	2.000,00	0,00000	5	10.000,00
Correlacionamento de eventos com Graylog (SEG35)	2.000,00	0,00000	4	8.000,00
Total geral de vagas e investimento			113	171.470,00

O investimento total para 113 (cento e treze) pessoas é de R$ 171.470,00 (cento e setenta e um mil e quatrocentos e setenta Reais), inclusos os impostos: COFINS 7,60% e ISS 5%.

XIV - Forma de pagamento

O pagamento deverá ser efetuado da seguinte forma:

- Nota de empenho emitida pela instituição contratante e encaminhada a Escola Superior de Redes RNP.

Após o término do curso o setor financeiro da Rede Nacional de Ensino e Pesquisa encaminhará a nota fiscal emitida em 02 (duas) vias, com o valor total do curso.

Dados da RNP

Rede Nacional de Ensino e Pesquisa - RNP
CNPJ: 03.508.097/0001-36
Inscrição Municipal: 283810-9
Endereço: Rua Lauro Müller, 116 - sala 1103
Botafogo - Rio de Janeiro - RJ
22290-906

Dados bancários

Banco do Brasil
Agência: 1769-8
Conta Corrente: 127000-1

Escola Superior de Redes RNP
esr.rnp.br

RNP

Ressaltamos que pelo fato da RNP ser uma Organização Social vinculada ao Ministério da Ciência, Tecnologia e Inovação (MCTI) e ao Ministério da Educação (MEC) a mesma é dispensada de licitação, conforme a Lei 8.666, Artigo 24, Inciso XXIV. A RNP possui inscrição no SICAF.

XV - Condições gerais da proposta

Aceitação

A aceitação da proposta poderá ser inicialmente enviada via e-mail para atendimento@esr.rnp.br, aos cuidados de *Leandro Marcos de Oliveira Guimarães*. No ato da aceitação da proposta a Empresa Contratante deverá fornecer a Escola os seguintes dados: Razão Social, CNPJ, Inscrição Estadual e/ou Municipal ou se isento, nome e cargo da pessoa responsável, endereço completo, e-mail, telefones, lista dos participantes, nome e endereço do contato para envio da nota fiscal.

Validade

A proposta é válida até dia 17/12/2021.

Início da turma

Quórum: ocupação mínima 15 alunos. Caso não seja atendido o quórum, a ESR deverá comunicar, com 20 (vinte) dias de antecedência do início do curso, o cancelamento da turma.

Não comparecimento

O aluno que não comparecer ao curso na data de início sem prévia comunicação ou não atingir a frequência mínima exigida no item XII desta proposta, será contabilizado e cobrado, não fazendo jus à restituição de valores ou ao crédito de valores já pagos, sendo devido pelo **Contratante** o pagamento da referida vaga.

Material de cursos de Parceiros

Caso haja desistência de participação em curso de parceiros (CompTIA, EXIN e Ascend) e a ESR já tenha adquirido o material referente ao treinamento, o valor deste será cobrado do Contratante.

Escola Superior de Redes RNP
esr.rnp.br

RNP

Brasília, 07 de Outubro de 2021

Atenciosamente,

Leandro Marcos de Oliveira Guimarães
Diretor Adjunto da Escola Superior de Redes

Escola Superior de Redes RNP
atendimento@esr.rnp.br
(61) 3243-4337 / 4355
(61) 3243-4341 fax

Nome e assinatura do responsável

_____

Sr. Eduardo França de Aguiar

Data do aceite
____/____/____

A experiência de quem trouxe a internet para o Brasil agora mais perto de você

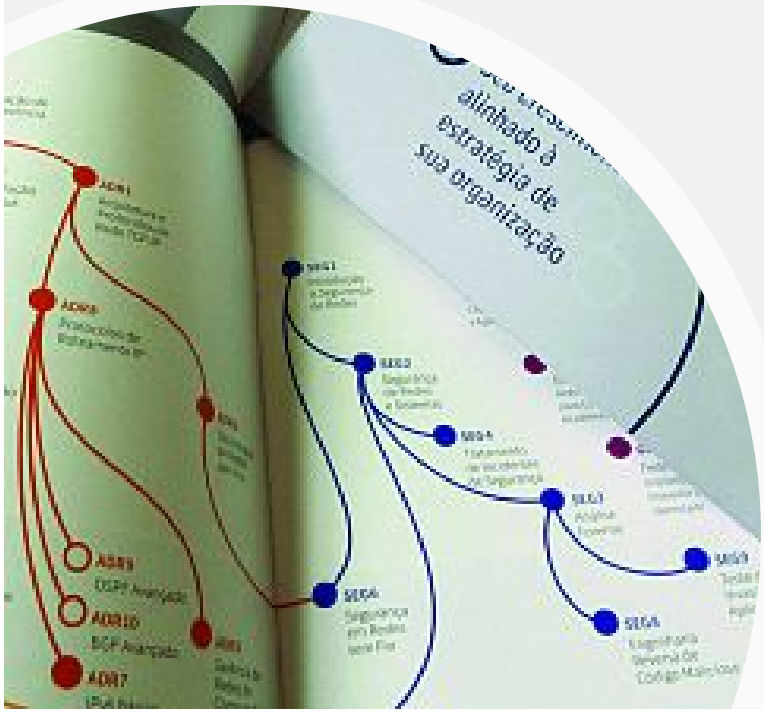
A Escola

A Escola Superior de Redes da RNP privilegia um ensino totalmente prático. Os laboratórios são montados de forma a proporcionar ao aluno um ambiente com os mesmos recursos e ferramentas que ele encontra no mercado de trabalho, bem como as atividades propostas espelham o dia-a-dia do profissional de Tecnologia da Informação e Comunicação. Os laboratórios estão conectados à Internet por meio do backbone de alta velocidade da Rede Nacional de Ensino e Pesquisa (RNP).

Cursos práticos voltados para o crescimento do profissional de TI

Cursos práticos intensivos em Tecnologias da Informação e Comunicação (TIC) nas seguintes áreas:

- Governança de TI
- Segurança



Escola Superior de Redes RNP

esr.rnp.br

RNP

A qualificação em Governança de TI é o diferencial competitivo no mercado de tecnologia da informação.

Governança de TI

A Governança de TI está relacionada ao desenvolvimento de um conjunto estruturado de competências e habilidades estratégicas para profissionais de TI, responsáveis pelo planejamento, implantação, controle e monitoramento de programas e projetos de governança, requisitos fundamentais para as organizações, do ponto de vista de aspectos operacionais e de implicações legais.

A área de Governança de TI da ESR/RNP oferece cursos aos profissionais que atuam ou desejam atuar como gestores de tecnologia da informação em organizações de diversos setores e que buscam uma formação baseada em modelos de melhores práticas gerenciais e ferramentas aplicáveis ao mundo de negócios em TI. Os cursos buscam atender à necessidade crescente das organizações de otimizar a aplicação de recursos, reduzir os custos e alinhar o setor de TI às suas estratégias de negócio

Elaboração de PDTI (EaD)

Elabore o PDTI de sua organização de acordo com as melhores práticas.
Duração: 24h

Fundamentos de Gerenciamento de Serviços com ITIL4 (EaD)

Venha conhecer como a ITIL4 apoia o gerenciamento de serviços e não só de TI.
Duração: 24h

Fundamentos do COBIT 2019 (EaD)

Aprenda a implementar a governança de TI através da metodologia do CobiT®.
Duração: 24h

Escola Superior de Redes RNP
esr.rnp.br

RNP

Gerenciamento Ágil de Projetos de TI (EaD)

Aprenda a elaborar um plano de projeto, utilizando técnicas de Gestão Ágil de Projetos, Manifesto Ágil e SCRUM.

Duração: 24h

Planejamento de Contratações de TI no Judiciário (EaD)

Aprenda a contratar bens e serviços de TI segundo a Resolução 182/2013 e Instrução Normativa nº 01.

Duração: 40h

Planejamento e Gestão Estratégica de TI (EaD)

Passos iniciais para as ferramentas utilizadas na Gestão de TI.

Duração: 24h

Plano de Contratações Públicas de Bens e Serviços com base na IN 01/2019 – SGD/ME (EaD)

Aprenda as novas formas de contratação de bens e serviços apresentadas na IN 01 de 04/04/2019.

Duração: 40h

Sistema de Gestão da Integridade – Compliance & Antissuborno

Você sabe o que é compliance? Suborno e corrupção são sinônimos? Você sabe como enfrentar o risco do suborno? Sua organização respeita a Lei Estadual nº 7753/2017 (Rio de Janeiro)?

Duração: 24h

Escola Superior de Redes RNP

esr.rnp.br

RNP

Elabore o PDTI de sua organização de acordo com as melhores práticas.

Elaboração de PDTI (EaD)

O curso apresenta conhecimentos essenciais para o desenvolvimento de forma prática de um plano diretor de tecnologia da informação (PDTI), a partir das informações do planejamento e a gestão estratégica de TI nas organizações. Durante o desenvolvimento aborda-se a metodologia necessária para que haja um alinhamento entre as estratégias e ações da TI e as estratégias organizacionais. O PDTI é o instrumento que permite nortear e acompanhar a atuação da área de TI, definindo estratégias e o plano de ação para implantá-las. O foco do curso está no desenvolvimento de competências práticas, a partir do alinhamento teórico de boas práticas para o desenvolvimento do PDTI com as diretrizes da estratégia de TI.

Características

DURAÇÃO:

- 3 (três) semanas de duração e mais uma semana de encerramento (total de 04 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 06 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração.

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online;
- Obter média 6,0 (seis) no Questionário de Avaliação Final.

MATERIAL:

O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários, materiais extras e vídeo do encontro online.

TÉCNICA:

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

Escola Superior de Redes RNP
esr.rnp.br

RNP

Ao final do curso, o aluno será capaz de:

- Desenvolver o plano diretor de TI (PDTI) para sua organização;
- Compreender os aspectos e processos básicos de implementação do PDTI em organizações públicas e privadas.

Conhecimentos prévios

- Recomenda-se ao aluno ter feito o curso Planejamento e Gestão Estratégica de TI, oferecido pela Escola Superior de Redes.
- Conhecimentos básicos dos processos de gestão de TI.

Investimento

- R$ 960,00

Programa do curso

- Plano Diretor de Tecnologia da Informação;
- Fase de Preparação;
- Fase de Diagnóstico: Conhecendo a Realidade da TI;
- Fase de Diagnóstico: Avaliando os Recusos de TI;
- Fase de Planejamento: Definindo Metas e Ações;
- Fase de Planejamento: Terminando o PDTI.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Venha conhecer como a ITIL4 apoia o gerenciamento de serviços e não só de TI.

Fundamentos de Gerenciamento de Serviços com ITIL4 (EaD)

O curso capacita gestores, coordenadores, gerentes e pessoal da equipe de serviços de TIC, além de demais áreas da organização, ao framework de melhores práticas de GS. Diferenciando-se da sua versão anterior, a ITIL4 não foca apenas em TI, mas oferece um conjunto de práticas voltadas para a geração de valor agregado ao cliente, considerando tanto nível técnico quanto de negócios.

Características

DURAÇÃO:

- 3 (três) semanas de duração e mais uma semana de encerramento (total de 04 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 06 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração.

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online;
- Obter média 6,0 (seis) no Questionário de Avaliação Final.

MATERIAL:

O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários, materiais extras e vídeo do encontro online.

TÉCNICA:

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Competências desenvolvidas

Ao final do curso, o aluno será capaz de:

- Dominar os conceitos, princípios-chave e modelos de processos necessários;
- Conhecer como a ITIL4 apoia as práticas de Gerenciamento de Serviços;
- Estudar o conteúdo equivalente ao exigido para o exame da ITIL 4 Foundation;
- Entender como os princípios da ITIL podem ajudar um indivíduo a entender e aplicar o gerenciamento de serviços em sua organização;
- Aplicar Gerenciamento de Serviços em toda a organização.
- Entender como melhorar a experiência do cliente e a eficiência do ITSM com a ajuda das ferramentas e técnicas da ITIL;
- Dominar os propósitos e termos-chave de 15 práticas ITIL;
- Conhecer as práticas recomendadas do setor para a implantação de serviços de TI.

Conhecimentos prévios

Não há conhecimentos prévios.

Investimento

- R$ 512,00

Programa do curso

- Introdução ao Gerenciamento de Serviços e ao ITIL;
- Gerenciamento de Serviços no mundo moderno;
- Sobre o ITIL 4;
- A estrutura e os benefícios do ITIL 4;
- O Programa de certificação ITIL;
- Conceitos chaves para o Gerenciamento de Serviços;
- Valor e co-criação de valor;
- Organização, Provedores de Serviço e Consumo de Serviço;
- Produtos e Serviços;
- Relacionamentos de Serviços;
- Valor: Entradas, custos e riscos;
- As quatro Dimensões do Gerenciamento de Serviços;
- Organizações e Pessoas;
- Informação e Tecnologia;
- Parceiros e Fornecedores;
- Fluxos de valor e Processos;
- Fatores externos;
- O Sistema de Valor do ITIL;
- Overview no sistema de valor;
- Governança;

Escola Superior de Redes RNP

esr.rnp.br

RNP

- Cadeia de valor de serviço;
- Melhoria contínua;
- Práticas;
- Práticas de Gestão do ITIL;
- Práticas gerais de Gestão;
- Práticas de gerenciamento de serviços;
- Práticas de gerenciamento técnico.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Aprenda a implementar a governança de TI através da metodologia do CobiT®.

Fundamentos do COBIT 2019 (EaD)

O curso ensina a tecnologia e os fundamentos necessários para a implantação da governança de TI através da metodologia do CobiT®, auxiliando o aluno na preparação para a realização do exame de certificação da CobiT® Foundation.

Características

DURAÇÃO:

- 3 (três) semanas de duração e mais uma semana de encerramento (total de 04 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 06 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração.

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online;
- Obter média 6,0 (seis) no Questionário de Avaliação Final.

MATERIAL:

O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários, materiais extras e vídeo do encontro online.

TÉCNICA:

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

Escola Superior de Redes RNP

esr.rnp.br

RNP

Ao final do curso, o aluno será capaz de:

- Reconhecer o público-alvo do COBIT 2019®.
- Reconhecer o contexto, os benefícios e as principais razões pelas quais o COBIT 2019® é usado como um framework de governança de informações e tecnologia.
- Reconhecer as descrições e finalidades da arquitetura de produtos do COBIT 2019® .
- Entender o alinhamento do COBIT 2019® com outros frameworks, normas e corpos de conhecimento aplicáveis.
- Compreender e descrever os princípios do “sistema” de governança e “framework” de governança.
- Descrever os componentes de um sistema de governança.
- Entender a estrutura geral e o conteúdo da Cascata de Objetivos.
- Ter uma visão geral dos 40 Objetivos de Governança e Gestão e suas declarações de propósito.
- Compreender a relação entre os objetivos de governança e gestão e os componentes de governança.
- Diferenciar o gerenciamento de desempenho baseado em COBIT 2019® usando perspectivas de maturidade e capacidade.
- Descobrir como desenhar um sistema de governança sob medida usando o COBIT 2019® .
- Explicar os pontos-chave do caso de negócios do COBIT 2019® .
- Compreender e relembrar as fases da abordagem de implementação do COBIT 2019® .
- Descrever as relações entre os Guias de Design e Implementação do COBIT 2019® .

Conhecimentos prévios

Conhecimento básico em TI.

Investimento

- R$ 750,00

Programa do curso

- Estrutura do COBIT;
- Objetivos de controle;
- Práticas de controle;
- Diretrizes de gerenciamento;
- Diretrizes de auditoria;
- Visão sistêmica das áreas e processos do COBIT;
- Componentes do framework do COBIT.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Aprenda a elaborar um plano de projeto, utilizando técnicas de Gestão Ágil de Projetos, Manifesto Ágil e SCRUM.

Gerenciamento Ágil de Projetos de TI (EaD)

O curso capacita na utilização da tecnologia e das ferramentas necessárias para o planejamento, gestão e controle de projetos , atendendo aos requisitos de uma formação sólida e consistente, contemplada no conjunto de boas práticas contido no Project Management Body of Knowledge (PMBok) do Project Management Institute (PMI), no SCRUM e no Manifesto Ágil. O curso prepara o aluno na elaboração de um plano de projeto, considerando o alinhamento às necessidades de TI de sua organização; a gerir um portfólio de projetos de TI inseridos no planejamento estratégico organizacional, utilizando técnicas ágeis.

Características

DURAÇÃO:

- 3 (três) semanas de duração e mais uma semana de encerramento (total de 04 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 06 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração.

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online;
- Obter média 6,0 (seis) no Questionário de Avaliação final;

MATERIAL:

O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários, materiais extras e vídeo do encontro online;

TÉCNICA:

Escola Superior de Redes RNP

esr.rnp.br

RNP

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

Ao final do curso, o aluno será capaz de:

- Gerenciar projetos de TI por meio da utilização de boas práticas de gestão de projetos contidas no PMBok, Guia do SCRUM e Manifesto Ágil e em outros guias de referência;
- Promover o melhor alinhamento dos projetos de TI aos objetivos inseridos no planejamento estratégico de sua organização;
- Desempenhar as suas atividades profissionais com base em processos de gestão mais estruturados, viabilizando maior eficiência operacional e melhor desempenho.

Conhecimentos prévios

- Conhecimentos básicos dos processos e atividades inerentes à área de TI.
- Uso dos aplicativos da internet.

Investimento

- R$ 750,00

Programa do curso

- Gerenciamento de Projetos de TI com base nas boas práticas do PMBOK, Manifesto Ágil e Guia do Scrum e em outros guias de referência;
- Definição de Projeto;
- As áreas de conhecimento do Gerenciamento de Projetos;
- Processos de Gerenciamento de Projetos;
- Fases e ciclo de vida do Gerenciamento de Projetos;
- Técnicas Ágeis;
- Melhoria de processos organizacionais em TI.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Aprenda a contratar bens e serviços de TI segundo a Resolução 182/2013 e Instrução Normativa n 01.

Planejamento de Contratações de TI no Judiciário (EaD)

Enquanto os gestores de TI das organizações públicas do Executivo devem realizar a contratação de serviços de TI segundo a Instrução Normativa nº1 (IN01), o Judiciário deve seguir a Resolução 182 do Conselho Nacional de Justiça (CNJ). Este cenário exige dos profissionais o conhecimento de modelos de referência e práticas adotadas com sucesso por organizações públicas dos dois poderes, além da legislação e jurisprudência específicas de cada área.

Seguindo as principais do orientações do CNJ, o curso Planejamento de Contratações de TI no Judiciário, permite aos gestores o amplo entendimento da Resolução 182, com o desenvolvimento de competências para a adequada condução do processo de contratação de serviços de TI nas organizações que respondem às regras do Judiciário.

Características

DURAÇÃO:

- 5 (cinco) semanas de duração e mais uma semana de encerramento (total de 06 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 10 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração;

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online;
- Obter média 6,0 (seis) no Questionário de Avaliação Final.

MATERIAL:

O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários, materiais extras e vídeo do encontro online.

Escola Superior de Redes RNP

esr.rnp.br

RNP

TÉCNICA:

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

Ao final do curso, o aluno será capaz de:

- Executar e gerenciar a aplicação de recursos públicos nos processos de compras e contratação de serviços de TI necessários aos objetivos dos projetos e atividades públicas, de acordo com os marcos legais e a jurisprudência do Tribunal de Contas da União;
- Entender os aspectos e processos básicos para uma adequada contratação de serviços de TI para órgãos submetidos ao controle administrativo e financeiro do CNJ;
- Entender os aspectos e processos básicos para uma adequada contratação de serviços de TI para organizações da administração pública federal;
- Compreender a aplicação da IN01 nas organizações públicas, resoluções e demais normas e leis.

Conhecimentos prévios

Recomenda-se a realização do curso: Elaboração de PDTI, oferecido pela Escola Superior de Redes.

Investimento

- R$ 1.440,00

Programa do curso

- Sistemas Orçamentários da União
- Sistemas Orçamentários do Judiciário
- Planejamento Estratégico do Judiciário
- Planejamento Estratégico de Tecnologia da Informação e Comunicação – PETIC
- Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC
- A Resoluções do CNJ
- A Resolução 182/2013
- Acórdãos 1603/2008, 145/2011, 54/2012 e 1233/2012
- Outros modelos de Contratação de TIC
- Origem
- Modelo SISP
- Modelo CFJ
- Compreensão da resolução 182
- Discussão da Resolução
- Esquema de processo
- Glossário

Escola Superior de Redes RNP

esr.rnp.br

RNP

- Impedimentos de contratações
- Atribuições dos atores envolvidos
- Plano de Contratações
- Fases de Elaboração
- Estudos Preliminares
- Elaboração do DOD
- Análise de Viabilidade da Contratação
- Sustentação do Contrato
- Estratégia da Contratação
- Análise de Riscos
- Conceituação de Riscos
- Riscos do Planejamento da Contratação
- Riscos da Contratação
- Riscos da Execução Contratual
- Projeto Básico ou Termos de Referência
- Checklist de TR
- Auditoria
- Ordens de Serviços
- Elaboração de OS
- Termos de Recebimento
- Elaboração de TR provisório
- Elaboração de TR definitivo
- Gestão da Execução do Contrato
- Recomendações e formulários

Escola Superior de Redes RNP

esr.rnp.br

RNP

Passos iniciais para as ferramentas utilizadas na Gestão de TI.

Planejamento e Gestão Estratégica de TI (EaD)

O curso fornece conhecimentos essenciais para o planejamento e a gestão estratégica de TI nas organizações. O foco está no alinhamento da estratégia de TI com o alcance das metas do negócio da organização, na busca pela vantagem competitiva através do constante refinamento dos processos organizacionais. Ao final do curso o aluno estará capacitado a elaborar uma política gerencial alinhada aos interesses da sua organização, com base em uma visão sistêmica e estratégica da Governança de TI e seu impacto nos negócios.

Características

DURAÇÃO:

- 3 (três) semanas de duração e mais uma semana de encerramento (total de 04 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 06 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração.

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online;
- Obter média 6,0 (seis) no Questionário de Avaliação Final.

MATERIAL:

O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários, materiais extras e vídeo do encontro online;

TÉCNICA:

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Competências desenvolvidas

Ao final do curso, o aluno será capaz de:

- Analisar os impactos estratégicos de TI nos negócios;
- Entender os aspectos e processos básicos de planejamento e gestão estratégica de TI nas organizações públicas e privadas.

Conhecimentos prévios

- Conhecimentos básicos dos processos de gestão de TI;
- Uso dos aplicativos da internet.

Investimento

- R$ 750,00

Programa do curso

- Relações entre a gestão, as estratégias de negócio e as estratégias de TI;
- Mudança organizacional e diagnóstico de maturidade do planejamento;
- Conceitos relacionados à ferramenta Balanced ScoreCard (BSC);
- Habilidades e conhecimentos específicos de profissionais da área de TI na organização para a realização de metas estratégicas da área de TI;
- Alinhamento da área de TI com as metas estratégicas de longo prazo das organizações e seu controle através da criação de indicadores;
- Análise da relação entre PEE, PETI, PDTI.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Aprenda as novas formas de contratação de bens e serviços apresentadas na IN 01 de 04/04/2019.

Plano de Contratações Públicas de Bens e Serviços com base na IN 01/2019 – SGD/ME (EaD)

Um novo desafio se apresenta aos gestores e profissionais de TI das organizações públicas. A Instrução Normativa – IN 04/2014, sofreu alterações significativas e as normas e processos de Contratação de Bens e Serviços de TI foram revistos a partir de abril de 2019. A IN 01 de 04/04/2019 passa a englobar outras normas e várias recomendações em aquisições específicas como fábrica de software, sala-segura ou sala cofre, além contratação em nuvem. Esta nova instrução se aplica a todos os órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP.

Características

DURAÇÃO:

- 5 (cinco) semanas de duração e mais uma semana de encerramento (total de 06 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 10 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração.

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online;
- Obter média 6,0 (seis) no Questionário de Avaliação Final.

MATERIAL:

O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários, materiais extras e vídeo do encontro online.

TÉCNICA:

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;

Escola Superior de Redes RNP
esr.rnp.br

RNP

- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

Ao final do curso, o aluno será capaz de:

- Executar e gerenciar a aplicação de recursos públicos nos processos de compras e contratação de serviços de TI necessários aos objetivos dos projetos e atividades públicas, de acordo com os marcos legais e a jurisprudência do Tribunal de Contas da União;
- Entender os aspectos e processos básicos para uma adequada contratação de serviços de TI para organizações públicas;
- Compreender e aplicar a IN01 nas organizações públicas;
- Implementar as instruções da IN01, baseado em templates elaborados em sala, para aplicação direta em seu órgão.

Conhecimentos prévios

Recomenda-se a realização do curso Fundamentos de Governança de TI, oferecido pela Escola Superior de Redes.

Investimento

- R$ 1.280,00

Programa do curso

- Principais diferenças da IN 04/2014 e a IN 01/2019;
- Ministério da Economia – Nova organização;
- Secretaria de Governo Digital;
- SISP;
- Plano Anual de Contratações Corporativas - PAC;
- Programação Estratégica de Contratações;
- Contratações;
- PDTI;
- Restrições de contratações;
- Vedações;
- Critérios;
- Planejamento da Contratação;
- Seleção de Fornecedores;
- Gestão do Contrato;
- Gestão de Riscos;
- Diretrizes Específicas;
- Base legal e legislação vigente.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Você sabe o que é compliance? Suborno e corrupção são sinônimos? Você sabe como enfrentar o risco do suborno? Sua organização respeita a Lei Estadual n 7753/2017 (Rio de Janeiro)?

Sistema de Gestão da Integridade – Compliance & Antissuborno

O curso promove a compreensão dos relacionamentos de uma organização, identificando os riscos presentes e os seus potenciais impactos, e como estabelecer um sistema de gestão compatível com as exigências do século XXI, atendendo aos principais marcos legais e normativos, com destaque para:

ISO 19600 (Sistema de gestão de compliance – Diretrizes)

ISO 37001 (Sistemas de gestão antissuborno – Requisitos)

Lei Federal nº 12846/2013 (Lei Anticorrupção – LAC)

Decreto Lei nº 8420/2015 (Programa de Integridade – Compliance)

Lei Estadual nº 7753/2017 (Programa de Integridade do Rio de Janeiro)

Características

DURAÇÃO:

- 3 (três) semanas de duração e mais uma semana de encerramento (total de 4 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 6 encontros). Os encontros serão

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online;

Escola Superior de Redes RNP

esr.rnp.br

RNP

- Obter média 6,0 (seis) no Questionário de Avaliação final;

MATERIAL:

- O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteú
  questionários, materiais extras e vídeo do encontro online.

TÉCNICA:

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador F
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

- Desenvolver e manter as informações documentadas do sistema de gestão;
- Compreender o contexto organizacional (interno e externo);
- Cumprir com seu papel no enfrentamento da corrupção;
- Identificar e tratar os riscos associados com a integridade/compliance;
- Planejar os processos e controles, conforme os objetivos da organização;
- Assessorar na elaboração de um código de conduta adequado;
- Orientar outras partes interessadas para a manutenção da integridade;
- Desenvolver métricas, indicadores e processos de monitoramento e controle;
- Conhecer os princípios da governança corporativa;
- Assegurar a melhoria contínua do sistema de gestão;
- Auxiliar no processo de certificação da ISO 37001;
- Conduzir a aplicação do método PDCA;
- Colaborar de forma assertiva no cumprimento da legislação;
- Avaliar o desempenho de parceiros de negócio;
- Analisar o atendimento dos requisitos normativos;
- Participar de auditoria do sistema de gestão;
- Coordenar treinamentos e ações de conscientização sobre o tema;

Conhecimentos prévios

Não há.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Investimento

- R$ 720,00

Programa do curso

- Gênesis
- O que é corrupção? Uma breve história da corrupção
- O contexto organizacional

- O que é uma organização? O contexto interno da organização. O contexto externo da organização
- As partes interessadas, quem são e o que querem?
- Conflito de interesse e Conflito de agenda
- Gerenciamento de riscos
- O que é risco? Identificação de riscos. Análise Qualitativa dos riscos.
- Análise Quantitativa dos riscos. Tratamento dos riscos
- O papel da liderança
- O que é a política de gestão?
- Escopo do sistema de gestão
- Atribuições e responsabilidades
- Objetivos do Sistema de gestão
- O que é uma métrica?
- Indicadores – BSC, KPI e KRO
- Desempenho do sistema de gestão
- Planejamento dos processos
- O que é um processo? Mapeamento de um processo. Medição do processo
- Conscientização
- O que é competência?
- A importância da comunicação
- Treinamento, formas de realização
- Parceiro de negócio
- O que é um parceiro de negócio?
- Cadeia de suprimento
- Critérios para escolha e manutenção de seu parceiro
- Monitoramento e controle
- O que é um canal de preocupação?
- Due diligence – escopo, profundidade e limitação
- Auditorias de primeira parte, segunda parte e terceira parte
- Gestão da informação documentada
- Em busca da excelência
- O que é benchmarking?
- Ação corretiva
- Melhoria contínua
- Normas e Certificação
- O que certificação?
- ISO 19600
- ISO 37001
- Compliance e Antissuborno
- Como implantar um sistema de gestão
- O que é um sistema de gestão?
- O método PDCA
- Um mapa para sua jornada

Escola Superior de Redes RNP

esr.rnp.br

RNP

Conheça as ferramentas de segurança e aprenda como evitar e tratar incidentes de segurança.

Segurança

As notáveis vantagens trazidas pela Internet, como o comércio eletrônico e as transações bancárias on-line, facilitam a nossa vida, mas ao mesmo tempo atraem riscos que tem forte impacto na área de segurança da informação. A metodologia da ESR é capacitar o aluno para pensar preventivamente e tratar os incidentes quando não for possível evitá-los. As atividades práticas refletem a realidade do analista de segurança ao lidar com incidentes de segurança e investigações forenses, tornando-o um profissional valorizado nas corporações.

CASP+ (CAS-003) EaD (parceria Oficial CompTIA)

A CompTIA Advanced Security Practitioner (CASP) é a certificação ideal para profissionais técnicos que desejam permanecer imersos em tecnologia e não apenas gerenciar.
Duração: 40h

Correlacionamento de eventos com Graylog

Aprenda a coletar, correlacionar e extrair informações relevantes a partir dos logs gerados por seus servidores e aplicações dentro do datacenter.
Duração: 40h

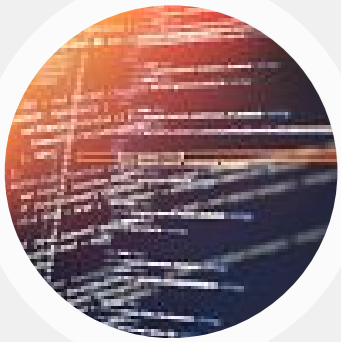
CySA+ EaD (parceria oficial CompTIA)

Aprenda a como aplicar análise comportamental a redes e dispositivos para prevenir, detectar e combater ameaças de segurança cibernética.
Duração: 40h

Escola Superior de Redes RNP

esr.rnp.br

RNP



Hardening em Linux (EaD)

Aprenda a mitigar risco e executar atividades corretivas na sua infraestrutura baseada no sistema operacional Linux, com objetivo de torná-la preparada para enfrentar tentativas de ataques internos e externos.
Duração: 40h

PenTest + EaD (parceria oficial CompTIA)

O curso PenTest+ foi desenvolvido para profissionais de cibersegurança encarregados pelos testes de penetração e gestão de vulnerabilidades dentro de uma organização.
Duração: 40h

Security+ EaD (parceria Oficial CompTIA)

O CompTIA Security+ é uma certificação global que valida as habilidades básicas que são requeridas para desempenhar papéis de segurança da informação e avançar na carreira de TI.
Duração: 40h

Segurança de Redes e Sistemas (EaD)

Conheça as melhores ferramentas de segurança e aprenda a instalar e configurar sistemas Windows e Unix de forma segura.
Duração: 40h

Teste de Invasão de Aplicações Web (EaD)

Defenda as suas aplicações web e seja um especialista em Pentest.
Duração: 40h

Tratamento de Incidentes de Segurança (EaD)

Aprenda a tratar incidentes de segurança e obtenha o conhecimento necessário para estruturar um CSIRT (Computer Security Incident Response Team) para sua organização.
Duração: 40h

Escola Superior de Redes RNP
esr.rnp.br

RNP

Cibersegurança EaD (parceria oficial Ascend)

Este treinamento tem como objetivo melhorar seu conhecimento sobre análise e interpretação de dados, detecção de ameaças, gerenciamento de vulnerabilidades, resposta a incidentes e arquitetura de segurança.

Duração: 40h

Escola Superior de Redes RNP

esr.rnp.br

RNP

A CompTIA Advanced Security Practitioner (CASP) é a certificação ideal para profissionais técnicos que desejam permanecer imersos em tecnologia e não apenas gerenciar.

CASP+ (CAS-003) EaD (parceria Oficial CompTIA)

A certificação CompTIA Advanced Security Practitioner (CASP) tem como objetivo formar profissionais técnicos que desejam permanecer imersos em tecnologia, e não apenas gerenciar. Enquanto os gerentes de cibersegurança ajudam a identificar quais políticas e estruturas podem ser implementadas, os profissionais com certificação CASP apontam como implementar soluções dentro dessas políticas e estruturas.

Este é um curso de nível avançado em gerenciamento de riscos; operações e arquitetura de segurança corporativa; pesquisa e colaboração e integração da segurança corporativa.

A CASP está em conformidade com os padrões ISO 17024 e é aprovada pelo Departamento de Defesa dos EUA, atendendo aos requisitos da diretiva 8140/8570.01-M.

Características

DURAÇÃO:

- 5 (cinco) semanas de duração e mais uma semana de encerramento (total de 06 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 10 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração.

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Obter 60% de acerto no Questionário de Avaliação final - Simulado;
- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online.

MATERIAL:

- Todo o material oficial CompTIA disponibilizado neste curso está em inglês;

Escola Superior de Redes RNP

esr.rnp.br

RNP

- O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários, simulado, materiais extras e vídeo do encontro online.

TÉCNICA:

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

Ao final do curso, o aluno será capaz de:

- Entender o que é segurança corporativa, incluindo técnicas, requisitos e conceitos de arquitetura e operações;
- Utilizar a análise de riscos por meio da interpretação de dados de tendência e antecipação de necessidades de ciberdefesa associadas as necessidades do negócio;
- Compreender tópicos de segurança avançados, incluindo dispositivos móveis e SFF, além de vulnerabilidade de softwares;
- Entender, de forma mais ampla, a integração de tecnologias de virtualização e nuvem em uma arquitetura corporativa segura;
- Utilizar e implementar técnicas criptográficas como Blockchain-Criptomoedas e criptografia de dispositivos móveis.

Conhecimentos prévios

- Conhecimento intermediário em conceitos de segurança da informação, incluindo, mas não limitado a IAM (Gestão de Acesso e Identidade), conceito e implementação de criptografia, conceitos e implementação de redes e segurança da informação;
- Experiência prática em implementação de segurança em vários ambientes de segurança, incluindo pequenas e médias empresas, assim como em grandes corporações;
- Inglês básico para leitura;
- Possuir as habilidades necessárias para a certificação official CompTIA® Security+® (Exam SYO-601) ou similar e CompTIA® CySA+® (Exam CSO-002).

Investimento

- R$ 4.500,00

Programa do curso

- Apoio à governança de TI e gerenciamento de riscos;
- Aproveitando a colaboração para apoiar a segurança;
- Usando pesquisa e análise para proteger a empresa;
- Integrando Técnicas Avançadas de Autenticação e Autorização;

Escola Superior de Redes RNP
esr.rnp.br

RNP

- Implementação de técnicas criptográficas;
- Implementando controles de segurança para hosts;
- Implementando controles de segurança para dispositivos móveis;
- Implementando Segurança de Rede;
- Implementando Segurança no Ciclo de Vida de Desenvolvimento de Sistemas e Software;
- Integrando ativos em uma arquitetura corporativa segura;
- Conduzindo avaliações de segurança;
- Resposta e recuperação de incidentes.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Aprenda a coletar, correlacionar e extrair informações relevantes a partir dos logs gerados por seus servidores e aplicações dentro do datacenter.

Correlacionamento de eventos com Graylog

O curso ensina o aluno sobre os aspectos teóricos e legais sobre a gestão de logs e retenção de dados, e como operacionalizar esses procedimentos com o SIEM open source Graylog. Além da instalação, configuração e manutenção da ferramenta, também são tratados tópicos como a criação de filtros e pipelines de processamento de eventos, construção de dashboards amigáveis e alertas administrativos.

Características

DURAÇÃO:

- 5 semanas de duração e mais uma semana de encerramento (total de 6 semanas);
- 2 encontros online por semana com o tutor (total de 10 encontros). Os encontros serão ao vivo e terão 2 horas de duração;

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Obter média 6,0 (seis) no Questionário de Avaliação final;
- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online.

MATERIAL:

- O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários ou simulados materiais extras e vídeo do encontro online.

TÉCNICA:

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

- Compreender a importância da coleta e correlacionamento de eventos em larga escala, do ponto de vista da segurança da informação, para organizações de todos os portes.

Escola Superior de Redes RNP

esr.rnp.br

RNP

- Instalar, configurar, integrar e realizar procedimentos de manutenção em um cluster SIEM Graylog.
- Configurar sistemas diversos para envio de registros para processamento pelo SIEM Graylog.
- Criação de filtros, pipelines de processamento e lookup tables para viabilizar indexação de informações complexas.
- Pesquisar, correlacionar, criar alertas e dashboards para eventos coletados.

Conhecimentos prévios

- Recomenda-se que o aluno possua conhecimentos avançados em operação de servidores Linux em linha de comando, bem como servidores Windows.
- Conhecimentos básicos em segurança da informação.
- Noções básicas de processamento de arquivos-texto, expressões regulares e programação.

Investimento

- R$ 2.000,00

Programa do curso

- Introdução à gestão de logs
- Arquitetura e instalação do Graylog
- Usuários, papéis e integração com sistemas externos
- Coleta e ingestão de logs
- Expressões regulares, padrões GROK e filtros
- Pipelines de processamento e lookup tables
- Plugins, Content Packs e geolocalização de informações
- Pesquisando registros
- Configuração de alertas e dashboards
- Procedimentos de manutenção, backup e atualização

Escola Superior de Redes RNP

esr.rnp.br

RNP

Aprenda a como aplicar análise comportamental a redes e dispositivos para prevenir, detectar e combater ameaças de segurança cibernética.

CySA+ EaD (parceria oficial CompTIA)

O objetivo da certificação CompTIA CySA+ é formar profissionais que possam aplicar análises comportamentais às redes para melhorar o estado geral de segurança por meio da identificação e combate a malware e ameaças persistentes avançadas (APTs), resultando em uma visibilidade aprimorada de ameaças em uma ampla superfície de ataque.

Este curso cobre todo conhecimento exigido para a certificação CompTIA CySA+ CSO-002 sendo compatível com o padrão ISO 17024 e preparado para atender aos requisitos da diretiva 8570.01-M do DoD dos EUA .

Características

DURAÇÃO:

- 5 (cinco) semanas de duração e mais uma semana de encerramento (total de 06 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 10 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração;

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Obter 60% de acerto no Questionário de Avaliação final - Simulado;
- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online.

MATERIAL:

- Todo o material oficial CompTIA disponibilizado neste curso está em inglês;
- O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários, simulado, materiais extras e vídeo do encontro online.

Escola Superior de Redes RNP

esr.rnp.br

RNP

TÉCNICA:

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

Ao final do curso, o aluno será capaz de:

- Utilizar e aplicar inteligência proativa contra ameaças para apoiar a segurança organizacional e realizar atividades de gerenciamento de vulnerabilidade;
- Aplicar soluções de segurança para gerenciamento de infraestrutura e explicar as melhores práticas de garantia de software e hardware;
- Aplicar conceitos de segurança em apoio à mitigação de risco organizacional e compreender a importância das estruturas, políticas, procedimentos e controles;
- Analisar dados como parte das atividades de monitoramento de segurança contínuas e implementar alterações de configuração nos controles existentes para melhorar a segurança;
- Utilizar procedimento de resposta a incidentes apropriado, analisar indicadores potenciais de comprometimento e utilizar técnicas forenses digitais básicas.

Conhecimentos prévios

- Recomenda-se pelo menos dois anos de experiência em Segurança de Redes de TI.
- Habilidade de reconhecer vulnerabilidades e ameaças de segurança da informação no contexto de gestão de risco;
- Habilidades operacionais de nível básico de sistemas operacionais mais comuns;
- Conhecimento básico dos conceitos e framework de políticas de segurança da informação de redes e dispositivos;
- Entendimento básico sobre conceito de redes mais comuns;
- Conhecimento básico dos principais protocolos TCP/IP;
- Inglês básico para leitura;
- Possuir as habilidades necessárias para a certificação official CompTIA® Security+® (Exam SYO-601) ou similar.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Investimento

- R$ 4.500,00

Programa do curso

- Explicando a importância dos controles de segurança e da segurança;
- Utilizando inteligência e dados de ameaças;
- Analisando o monitoramento de segurança;
- Coleta e consulta de dados de monitoramento de segurança;
- Utilizando forense Digital e técnicas de análise de indicadores;
- Aplicando procedimentos de resposta a incidentes;
- Aplicando mitigação de risco e estruturas de segurança;
- Executando o gerenciamento de vulnerabilidades;
- Aplicação de soluções de segurança para gerenciamento de infraestrutura;
- Noções básicas sobre privacidade e proteção de dados;
- Aplicando Soluções de Segurança para Software Assurance;
- Aplicando soluções de segurança para nuvem e automação.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Aprenda a mitigar risco e executar atividades corretivas na sua infraestrutura baseada no sistema operacional Linux, com objetivo de torná-la preparada para enfrentar tentativas de ataques internos e externos.

Hardening em Linux (EaD)

O curso tem como objetivo auxiliar administradores Linux interessados em proteger suas redes, mitigar riscos e executar atividades corretivas preparando sua infraestrutura de servidores Linux para resistir a determinadas tentativas de ataques ou violação na segurança da informação.

Características

Competências desenvolvidas

Ao final do curso, o aluno será capaz de:

- Realizar aplicações de baseline de segurança, com foco em Hardening do sistema operacional linux;
- Colocar um servidor Linux em produção, utilizando boas práticas de segurança que também possibilitará conformidade com vários itens destacados na NBR ISO/IEC 27002;
- Implantar serviços de log centralizado, resolução de nomes, atualização de horário e autenticação para garantir a padronização e segurança de servidores Linux;
- Implementar um ecossistema com o objetivo de implantar, automatizar e gerir a configuração segura de máquinas Linux utilizando o Ansible.

Conhecimentos prévios

- Recomenda-se a realização dos cursos: Administração de Sistemas Linux e Segurança de Redes e Sistemas, oferecidos pela Escola Superior de Redes.

Escola Superior de Redes RNP

esr.rnp.br

RNP

- Conhecimento de administração de sistemas Linux e de segurança de redes.

Investimento

- R$ 960,00

Programa do curso

Sessão 1: Instalação e configurações iniciais

- Criação de máquina virtual no Virtualbox
- Configuração do LVM
- Clonando máquinas virtuais
- Operações avançadas com LVM
- Criptografia de partições

Sessão 2: Firewall e DNS

- Criação da VM de firewall e DNS primário
- Configuração do servidor DNS primário e Secundário
- Configuração do DNSSEC

Sessão 3: Autenticação centralizada

- Configuração do servidor LDAP
- Configurando uma autoridade certificadora (CA) para o SSH integrada ao LDAP
- Restringindo login por grupos e usuários
- Bloqueando tentativas de brute force contra o SSH

Sessão 4: Controles de segurança

- Requisitos de senha na base LDAP
- Configuração do servidor de arquivos NFS e quotas de disco
- Uso de ACLs localmente e via NFS

Sessão 5: Gestão de configuração

- Instalação e configuração inicial do Ansible
- Uso de roles no Ansible
- Versionamento de configuração com git

Sessão 6: Registro e correlacionamento de eventos

- Criação da VM de gestão de logs
- Configuração do NTP
- Registro de comandos digitados com SnoopyLog
- Instalação e configuração inicial do Graylog

Escola Superior de Redes RNP

esr.rnp.br

RNP

Sessão 7: Hardening de sistemas web

- Configuração do servidor de banco de dados
- Configuração do servidor web www1 e ww2 com balanceador de carga

Sessão 8: Isolamento de processos e conteinerização

- Criação da VM docker1 e VM docker2
- Trabalhando com containers e registry externo
- Construindo serviços com o Docker
- Operando com múltiplos membros no cluster
- Adicionando novos serviços ao cluster
- Configurando a persistência dos dados

Sessão 9: Criação de sistemas Linux customizados

- Criação da VM de build com uma distribuição mínima
- Utilizando um repositório local de pacotes

Sessão 10: Módulos de segurança do kernel, auditoria e detecção de intrusão

- Instalação do AppArmor
- Auditoria automatizada de sistemas usando o OpenSCAP
- Detecção de intrusão local utilizando o OSSEC

Escola Superior de Redes RNP

esr.rnp.br

RNP

O curso PenTest+ foi desenvolvido para profissionais de cibersegurança encarregados pelos testes de penetração e gestão de vulnerabilidades dentro de uma organização.

PenTest + EaD (parceria oficial CompTIA)

DESCRIÇÃO:

As organizações lutam para se proteger e proteger os seus clientes contra vazamentos de segurança e privacidade. A capacidade de realizar testes de penetração em ambientes computacionais é uma habilidade emergente que está se tornando cada vez mais valiosa para as organizações que procuram proteção, e ainda mais lucrativo para os profissionais que possuem essas habilidades. Nesse curso, você será apresentado às metodologias e conceitos gerais para realização de pen testing podendo aprimorar suas habilidades a partir de uma simulação de penTest+ em uma empresa fictícia.

Este curso cobre todo conhecimento exigido para a certificação CompTIA Pentest+ PT0-001 sendo compatível com o padrão ISO 17024 e preparado para atender aos requisitos da diretiva 8140 / 8570.01-M do DoD dos EUA .

Características

DURAÇÃO:

- 5 (cinco) semanas de duração e mais uma semana de encerramento (total de 06 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 10 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração;

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Obter 60% de acerto no Questionário de Avaliação final - Simulado;
- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online.

Escola Superior de Redes RNP

esr.rnp.br

RNP

MATERIAL:

- Todo o material oficial CompTIA disponibilizado neste curso está em inglês;
- O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários, simulado, materiais extras e vídeo do encontro online.

TÉCNICA:

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

Ao final do curso, o aluno será capaz de:

- Explicar a importância do planejamento e os principais aspectos das avaliações baseadas em conformidade;
- Reunir informações para se preparar para a exploração, executar uma varredura de vulnerabilidade e analisar os resultados;
- Explorar vulnerabilidades de rede, sem fio, de aplicativos e baseadas em RF, resumir ataques de segurança física e executar técnicas de pós-exploração;
- Realizar exercícios de coleta de informações com várias ferramentas e analisar a saída e uso de scripts básicos (limitados a: Bash, Python, Ruby, PowerShell);
- Utilizar as melhores práticas de redação e tratamento de relatórios, explicando as estratégias de mitigação recomendadas para vulnerabilidades descobertas.

Conhecimentos prévios

- Conhecimento intermediário em conceitos de segurança da informação, incluindo, mas não limitado a IAM (Gestão de Acesso e Identidade), conceito e implementação de criptografia, conceitos e implementação de redes e segurança da informação;
- Experiência prática em implementando segurança em vários ambientes de segurança, incluindo pequenas e médias empresas, assim como em grandes corporações;
- Inglês básico para leitura;
- Possuir as habilidades necessárias para a certificação official CompTIA® Security+® (Exam SYO-601) ou similar.

Investimento

- R$ 4.500,00

Escola Superior de Redes RNP

esr.rnp.br

RNP

Programa do curso

- Planejamento e Escopo dos Testes de Penetração;
- Conduzindo Reconhecimento Passivo;
- Realizando Testes Não-Técnicos;
- Conduzindo Reconhecimento Ativo;
- Analisando Vulnerabilidades;
- Penetrando Redes;
- Exploitando Vulnerabilidades Baseadas no Host;
- Testando Aplicações;
- Completando as Tarefas Pós-Exploit;
- Analisando e Reportando os Resultados do Pen Test.

Escola Superior de Redes RNP

esr.rnp.br

RNP

O CompTIA Security+ é uma certificação global que valida as habilidades básicas que são requeridas para desempenhar papéis de segurança da informação e avançar na carreira de TI.

Security+ EaD (parceria Oficial CompTIA)

Este curso é focado em profissionais que possuem habilidades de Redes e Administração de Redes TCP/IP baseado em Windows e outros sistemas operacionais como MacOS, Unix ou Linux e que buscam avançar na carreira de TI adquirindo conhecimentos básicos de segurança da informação.

Este curso é desenvolvido para profissionais que estão se preparando para tirar a certificação CompTIA Security+ SY0-601.

Características

DURAÇÃO:

- 5 (cinco) semanas de duração e mais uma semana de encerramento (total de 06 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 10 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração;

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Obter 60% de acerto no Questionário de Avaliação final - Simulado;
- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online.

MATERIAL:

- Todo o material oficial CompTIA disponibilizado neste curso está em inglês;
- O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários, simulado, materiais extras e vídeo do encontro online.

Escola Superior de Redes RNP

esr.rnp.br

RNP

TÉCNICA:

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

Ao final do curso, o aluno será capaz de:

- Identificar ameaças, ataques e vulnerabilidades;
- Identificar os principais requisitos de segurança em ambientes corporativos , incluindo serviços em nuvem;
- Entender a importância da administração de identidade, gerenciamento de acesso, PKI, criptografia básica, wireless e segurança ponta a ponta;
- Realizar avaliações de segurança organizacional e propor procedimentos de resposta a incidentes, como detecção de ameaças básicas, técnicas de mitigação de riscos, controles de segurança e análise forense digital básica;
- Auxiliar no gerenciamento de risco organizacional e conformidade com regulamentações, como PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST e CCPA.

Conhecimentos prévios

- Ter pelo menos dois anos de experiência em Segurança de Redes de TI;
- Habilidade de reconhecer vulnerabilidades e ameaças de segurança da informação no contexto de gestão de risco;
- Habilidades operacionais de nível básico de sistemas operacionais mais comuns (Linux e Windows) ;
- Conhecimento básico dos conceitos e framework de políticas de segurança da informação de redes e dispositivos;
- Entendimento básico sobre conceito de redes mais comuns;
- Conhecimento básico dos principais protocolos TCP/IP.

Investimento

- R$ 4.500,00

Programa do curso

- Comparando funções de segurança e controles de segurança;
- Explicando os atores de ameaças e a inteligência sobre ameaças;
- Realizando Avaliações de Segurança;
- Identificando Engenharia Social e Malware;

Escola Superior de Redes RNP
esr.rnp.br

RNP

- Resumindo os conceitos básicos de criptografia;
- Implementando infraestrutura de chave pública;
- Implementando controles de autenticação;
- Implementando controles de gerenciamento de identidade e conta;
- Implementando uma rede segura;
- Implementando dispositivos de segurança de rede;
- Implementando protocolos de rede seguros;
- Implementando Soluções de Segurança de Host;
- Implementando Soluções Móveis Seguras;
- Resumindo os conceitos de aplicativos seguros;
- Implementando soluções de nuvem seguras;
- Explicando os conceitos de privacidade e proteção de dados;
- Executando a Resposta ao Incidente;
- Explicando a perícia digital;
- Resumindo os conceitos de gerenciamento de risco;
- Implementando Resiliência da Cibersegurança;
- Explicando a segurança física.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Conheça as melhores ferramentas de segurança e aprenda a instalar e configurar sistemas Windows e Unix de forma segura.

Segurança de Redes e Sistemas (EaD)

O aluno aprenderá sobre perímetros de segurança, através da implementação de uma solução completa de proteção de redes, utilizando técnicas como firewall, IDS, IPS e VPN. O amplo escopo de conceitos abordados permitirá a aplicação das técnicas aprendidas de autenticação e autorização segura, auditorias de segurança e os requisitos de configuração segura de servidores Linux e Windows. Após o curso, o aluno será capaz de montar um perímetro seguro, aumentar a segurança dos servidores da rede, realizar auditorias de segurança e implantar sistemas de autenticação seguros.

Características

DURAÇÃO:

- 5 (cinco) semanas de duração e mais uma semana de encerramento (total de 06 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 10 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração.

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online;
- Obter média 6,0 (seis) no Questionário de Avaliação Final.

MATERIAL:

O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários, materiais extras e vídeo do encontro online.

TÉCNICA:

Escola Superior de Redes RNP

esr.rnp.br

RNP

- Para acompanhamento do curso o aluno precisará de um computador com navegador web e o Oracle Virtual Box instalado, com memória a partir de 8GB (recomendável 16GB), com acesso direto a Internet e 200GB de espaço em disco.
- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

Ao final do curso o aluno será capaz de:

- Propor novas soluções para perímetros seguros de rede;
- Avaliar aspectos relacionados à segurança de servidores Linux e Windows;
- Empregar soluções de proteção como IDS, IPS e realizar auditorias de segurança.

Conhecimentos prévios

- Recomenda-se a realização do curso Introdução à Segurança de Redes, oferecido pela Escola Superior de Redes;
- Conceitos e ações básicas na área de segurança física e lógica de redes e sistemas, como criptografia, assinatura, certificado digital e questões de segurança da informação, edição de textos em Linux;
- Conhecimentos básicos sobre arquitetura TCP/IP;
- Conhecimentos básicos de administração de sistemas operacionais Linux e Windows Server.

Investimento

- R$ 960,00

Programa do curso

- Fundamentos de segurança
  - Da divisão de grupos
  - Topologia geral de rede
  - Configuração do Virtualbox
  - Detalhamento das configurações de rede
  - Configuração da máquinas virtuais
  - Configuração de firewall e NAT
  - Teste de conectividade das VMs
  - Instalação do Virtualbox Guest Additions nas VMs Windows
  - Instalação do Virtualbox Guest Additions nas VMs Linux
  - Exercitando os fundamentos de segurança
  - Normas e políticas de segurança
- Explorando vulnerabilidades em redes
  - Transferindo arquivos da máquina física para as VMs
  - Sniffers para captura de dados
  - Ataque SYN flood

Escola Superior de Redes RNP
esr.rnp.br

RNP

- Ataque Smurf
- Levantamento de serviços usando o nmap
- Realizando um ataque com o Metasploit em ambiente Windows
- Realizando um ataque com o Metasploit em ambiente Linux
- Realizando um ataque de dicionário com o medusa

- Firewall
  - Trabalhando com chains no iptables
  - Firewall stateful
  - Configurando o firewall FWGW1-G: tabela filter
  - Configurando o firewall FWGW1-G: tabela nat
  - Revisão final da configuração do firewall FWGW1-G
- Serviços básicos de segurança
  - Configuração do servidor de log remoto
  - Configuração do servidor de hora
  - Monitoramento de serviços
- Sistema de detecção/prevenção de intrusos
  - Instalação do Snort
  - Configuração inicial do Snort
  - Configurando atualizações de regras de forma automática com o PulledPork
  - Processando arquivos de log do Snort com o Barnyard2
  - Visualizando eventos com o Snorby
  - Integração dos serviços com o sistema
  - Gerando alertas para o IDS
  - Referências
- Autenticação, autorização e certificação digital
  - Uso de criptografia simétrica em arquivos
  - Uso de criptografia assimétrica em arquivos
  - Uso de criptografia assimétrica em e-mails
  - Criptografia de partições e volumes
  - Autenticação usando sistema OTP
- Redes privadas virtuais e inspeção de tráfego
  - Interceptação ofensiva de tráfego HTTPS com o mitmproxy
  - Inspeção corporativa de tráfego HTTPS usando o Squid
  - VPN SSL usando o OpenVPN
- Auditoria de segurança da informação
  - Instalação do Nessus
  - Realizando um scan em SO Linux
  - Realizando um scan em SO Windows
  - Efeitos do firewall em um scan
  - Auditoria de servidores web
- Configuração segura de servidores Windows
  - Uso do Microsoft Security Compliance Toolkit
  - Configuração do controlador de domínio Active Directory
  - Configuração do firewall para o Active Directory
  - Adição de clientes ao Active Directory
  - Adição de usuários ao Active Directory
  - Distribuição de configurações via GPOs
  - Instalação e configuração do WSUS
  - Configuração de clientes no WSUS
- Configuração segura de servidores Linux
  - Análise de rootkits

Escola Superior de Redes RNP

esr.rnp.br

RNP

- Inserção de senha no bootloader
- Remoção de serviços desnecessários
- Controle granular de acesso a comandos
- Controle de uso do binário su
- Controle de acesso à console do sistema
- Exigência de parâmetros mínimos de senha
- Controle de logoff automático
- Desabilitando a combinação de teclas CTRL + ALT + DEL

Escola Superior de Redes RNP

esr.rnp.br

RNP

Defenda as suas aplicações web e seja um especialista em Pentest.

Teste de Invasão de Aplicações Web (EaD)

O curso trata de testes de invasão de aplicações web, as quais, atualmente, são um dos principais alvos de ataque, devido à presença massiva nos mais diversos ambientes. Um teste de invasão, também chamado de teste de penetração ou pentest, é um método utilizado para verificar a segurança de um ambiente, plataforma ou sistema, por meio da simulação de ataques reais explorando as vulnerabilidades encontradas. Diferentemente de uma varredura de vulnerabilidades, que muitas vezes recorre ao simples uso de ferramentas automatizadas, pentest é um processo cíclico que depende principalmente do conhecimento técnico do auditor de segurança que o realiza. Este curso, então, espera introduzir as principais técnicas que podem ser empregadas.

Características

DURAÇÃO:

- 5 (cinco) semanas de duração e mais uma semana de encerramento (total de 06 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 10 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração;

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online;
- Obter média 6,0 (seis) no Questionário de Avaliação Final.

MATERIAL:

O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários, materiais extras e vídeo do encontro online.

TÉCNICA:

- Para acompanhamento do curso o aluno precisará de um computador com navegador web e o Oracle Virtual Box instalado, com memória a partir de 4GB,

Escola Superior de Redes RNP

esr.rnp.br

RNP

com acesso direto a Internet e 20GB de espaço em disco.
- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

Ao final do curso, o aluno será capaz de:

- Ter ciência sobre as vulnerabilidades de maior risco encontradas em sistemas web (OWASP Top Ten) e como elas podem ser exploradas por usuários maliciosos;
- Ensinar técnicas para a realização de Pentest em aplicações web;
- Introduzir ferramentas que podem otimizar o processo de Pentest, por meio da automatização de algumas tarefas.

Conhecimentos prévios

- Conceitos básicos de TCP/IP, HTTP;
- Conceitos básicos de Javascript;
- Conceitos básicos de bancos de dados;
- Conceitos básicos de mecanismos e protocolos criptográficos;
- Ter realizado o curso Análise Forense ou possuir conhecimento equivalente.

Investimento

- R$ 1.440,00

Programa do curso

- Arquitetura e tecnologias de aplicações web;
- Criptografia: cifras simétricas, cifras assimétricas, funções de hash criptográficas, MACs, assinaturas digitais, certificados digitais e SSL/TLS;
- Tipos de pentest e metodologia para teste de invasão;
- Injeção de SQL com acesso à plataforma subjacente, especificidades dos SGBDs e injeção de SQL às cegas;
- Injeção em LDAP, XML, SMTP e injeção de comandos;
- Transporte de credenciais por canais inseguros;
- Enumeração de usuários;
- Política de senhas fortes não implementadas pela aplicação;
- Falhas na programação ou projeto do mecanismo de autenticação;
- Mecanismos de recuperação de senhas vulneráveis;
- Condições de corrida no mecanismo de autenticação;
- Testes sobre o gerenciamento de sessões;
- Cross-Site Scripting (XSS) e CSRF;

Escola Superior de Redes RNP

esr.rnp.br

RNP

- Teste dos mecanismos de autorização;
- Testes dos mecanismos criptográficos;
- Teste completo e relatórios.
- Fundamentos e as metodologias de uma análise de risco;
- Tópicos principais para a construção de uma política de segurança;
- A navegação na Internet e as ameaças atuais;
- Navegação segura na Internet;
- Programas de segurança de um computador pessoal.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Aprenda a tratar incidentes de segurança e obtenha o conhecimento necessário para estruturar um CSIRT (Computer Security Incident Response Team) para sua organização.

Tratamento de Incidentes de Segurança (EaD)

O curso apresenta os conceitos e descreve as fases de tratamento de incidentes de segurança, com exercícios práticos e simulações de casos. Ao final do curso o aluno sai preparado para iniciar a criação de um grupo de atendimento a incidentes de segurança (Computer Security Incident Response Team CSIRT).

Características

DURAÇÃO:

- 5 (cinco) semanas de duração e mais uma semana de encerramento (total de 06 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 10 encontros). Os encontros serão ao vivo e terão 2 (duas) horas de duração;

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online;
- Obter média 6,0 (seis) no Questionário de Avaliação Final.

MATERIAL:

O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários, materiais extras e vídeo do encontro online.

TÉCNICA:

- Para acompanhamento do curso o aluno precisará de um computador com navegador web e o Oracle Virtual Box instalado, com memória a partir de 4GB, com acesso direto a Internet e 20GB de espaço em disco.

Escola Superior de Redes RNP

esr.rnp.br

RNP

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

Ao final do curso, o aluno será capaz de:

- Conhecer sobre requisitos de criação, funcionamento e atividades de um Computer Security Incident Response Team (CSIRT);
- Criar e gerenciar uma equipe de resposta a incidentes de segurança;
- Executar técnicas e ferramentas de tratamento de incidentes;
- Estudar casos e realizar simulações de incidentes.

Conhecimentos prévios

- Recomenda-se a realização do curso: Segurança de Redes e Sistemas, oferecido pela Escola Superior de Redes.
- Conceitos e ações básicas na área de segurança física e lógica de redes e sistemas, como: criptografia, assinatura, certificado digital e questões de segurança da informação.

Investimento

- R$ 960,00

Programa do curso

- Definições e fundamentos de CSIRTs;
- Gerenciamento do CSIRT;
- Riscos e ameaças;
- Processo de tratamento de incidentes;
- Aspectos operacionais da resposta a incidentes;
- Identificação de contatos;
- Análise de Logs;
- Ferramentas para análise de incidentes;
- Dinâmica de tratamento de incidentes.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Este treinamento tem como objetivo melhorar seu conhecimento sobre análise e interpretação de dados, detecção de ameaças, gerenciamento de vulnerabilidades, resposta a incidentes e arquitetura de segurança.

Cibersegurança EaD (parceria oficial Ascend)

Desenvolva habilidades para: configurar e implementar ferramentas que possam aumentar a segurança de um ambiente computacional, analisar e interpretar dados para identificar pontos fracos e ameaças, impedir ataques e executar recuperação de desastres.

Os assuntos tratados neste treinamento estão em consonância com os objetivos de aprendizagem da certificação CompTIA CYSA+ CSO-002 podendo ser utilizado como material de preparação.

Características

DURAÇÃO:

- 5 (cinco) semanas de duração e mais uma semana de encerramento (total de 6 semanas);
- 2 (dois) encontros online por semana com o tutor (total de 10 encontros). Os encontros serão ao vivo e terão 2h (duas) horas de duração;

SISTEMA DE AVALIAÇÃO:

Para conclusão do curso e acesso ao certificado é necessário:

- Obter média 6,0 (seis) no Questionário de Avaliação final;
- Entregar no mínimo 50% das tarefas;
- Ter 50% de presença no total de encontros online.

MATERIAL:

- Todo o material deste curso é disponibilizado em inglês;
- O material de apoio será disponibilizado no Ambiente Virtual de Aprendizagem (AVA): conteúdo do curso, agenda do curso, tarefas, questionários ou simulados materiais extras e vídeo do encontro online.

Escola Superior de Redes RNP

esr.rnp.br

RNP

TÉCNICA:

- Sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox ou Chrome;
- Para os encontros online recomendamos o uso de fones de ouvido com microfone.

Competências desenvolvidas

Ao final do curso, o aluno será capaz de:

- Utilizar e aplicar inteligência proativa contra ameaças para apoiar a segurança organizacional e realizar atividades de gerenciamento de vulnerabilidade;
- Aplicar soluções de segurança para gerenciamento de infraestrutura e explicar as melhores práticas de garantia de software e hardware;
- Analisar dados como parte das atividades de monitoramento de segurança contínuas e implementar alterações de configuração nos controles existentes para melhorar a segurança;
- Utilizar procedimento de resposta a incidentes apropriado, analisar indicadores potenciais de comprometimento e utilizar técnicas forenses digitais básicas.

Conhecimentos prévios

- Recomenda-se pelo menos dois anos de experiência em Segurança de Redes de TI.
- Habilidade de reconhecer vulnerabilidades e ameaças de segurança da informação no contexto de gestão de risco;
- Habilidades operacionais de nível básico de sistemas operacionais mais comuns;
- Conhecimento básico dos conceitos e framework de políticas de segurança da informação de redes e dispositivos;
- Entendimento básico sobre conceito de redes mais comuns;
- Conhecimento básico dos principais protocolos TCP/IP;
- Inglês básico para leitura;

Investimento

- R$ 2.000,00

Programa do curso

- Threat and Vulnerability Management
- Intelligence Sources
- Indicator Management
- Threats
- Attack Frameworks
- The Cyber Kill Chain
- Threat Reasearch
- Threat Modeling
- Vulnerability Identification
- Remediation and Mitigation
- Web App Scanners
- Assessment Tools and Techniques
- Attack Types

Escola Superior de Redes RNP

esr.rnp.br

RNP

- Vulnerabilities
- Threats and Vulnerabilities Associated with Specialized Technology
- More Specialized Technologies
- Cloud Service Security
- Cloud Service Weaknesses
- Software and Systems Security
- Asset Management
- Object Tracking and Containment
- Object Tracking and Containment Continued
- Identity and Access Management
- Honeypot
- Cryptography
- Encryption and Active Defense
- Software Security Platforms
- Formal Methods
- Service Oriented Architecture
- Hardware Root of Trust
- Trusted Foundry and Processors
- Trusted Technology
- Security Operations and Monitoring
- Analyses and Trends
- Endpoints
- Memory
- Network
- Logs
- Firewall Logs
- Intrusion
- Impact Analysis and SIEM
- Email Security
- Security Tools I
- Security Tools II
- Security Tools III
- Threat Hunting
- Automation Concepts
- Automation Protocols
- Incident Response
- Incident Response Process
- Response Coordination
- Data Criticality Factors
- Incident Response - Preparation
- Incident Response - Detection and Analysis
- Incident Response - Containment
- Incident Response - Post-Incident Activities
- Host-Related Indicators of Compromise
- Network-Related Indicators of Compromise
- Application-Related Indicators of Compromis
- Data Exfiltration
- Basic Digital Forensic Techniques
- Forensic Tools Continued
- Forensic Procedures

Escola Superior de Redes RNP

esr.rnp.br

RNP

- Compliance and Assessment
- Data Privacy and Protection
- Data Ownership and Retention
- Data Controls Preface
- Data Controls and Identification
- Risk Analysis and Calculation
- Risk Prioritization
- Training and Exercises
- Frameworks
- Policies and Procedures
- Data
- Audits and Assessments

Escola Superior de Redes RNP

esr.rnp.br

RNP

Governança de TI	Investimento
Elaboração de PDTI (EaD) (GTI39)	R$ 960,00
Fundamentos de Gerenciamento de Serviços com ITIL4 (EaD) (GTI47)	R$ 512,00
Fundamentos do COBIT 2019 (EaD) (GTI32)	R$ 750,00
Gerenciamento Ágil de Projetos de TI (EaD) (GTI33)	R$ 750,00
Planejamento de Contratações de TI no Judiciário (EaD) (GTI43)	R$ 1.440,00
Planejamento e Gestão Estratégica de TI (EaD) (GTI28)	R$ 750,00
Plano de Contratações Públicas de Bens e Serviços com base na IN 01/2019 – SGD/ME (EaD) (GTI44)	R$ 1.280,00
Sistema de Gestão da Integridade – Compliance & Antissuborno (GTI54)	R$ 720,00

Segurança	Investimento
CASP+ (CAS-003) EaD (parceria Oficial CompTIA) (SEG31)	R$ 4.500,00
Correlacionamento de eventos com Graylog (SEG35)	R$ 2.000,00
CySA+ EaD (parceria oficial CompTIA) (SEG24)	R$ 4.500,00
Hardening em Linux (EaD) (SEG22)	R$ 960,00
PenTest + EaD (parceria oficial CompTIA) (SEG23)	R$ 4.500,00
Security+ EaD (parceria Oficial CompTIA) (SEG25)	R$ 4.500,00
Segurança de Redes e Sistemas (EaD) (SEG18)	R$ 960,00
Teste de Invasão de Aplicações Web (EaD) (SEG21)	R$ 1.440,00
Tratamento de Incidentes de Segurança (EaD) (SEG19)	R$ 960,00
Cibersegurança EaD (parceria oficial Ascend) (SEG34)	R$ 2.000,00

Escola Superior de Redes RNP

esr.rnp.br

RNP