SEGURANÇA DA *informação*

GRUPO 12
BRUNO ROGACHESKI
GIOVANNA MONTEFUSCO
THIAGO SAMPAIO

O QUE É? *Segurança da Informação*

Um mecanismo de segurança é qualquer processo projetado para detectar, impedir ou permitir a recuperação de um ataque a segurança. Alguns mecanismos são, por exemplo: algoritmos de criptografia, assinaturas digitais e protocolos de segurança

PRINCÍPIOS - *Segurança da Informação*

- **Autenticação** - garante origem dos dados
- **Controle de acesso** - impede o uso não autorizado dos recursos
- **Confidencialidade dos dados** - garante a proteção dos dados
- **Integridade de dados** - dados enviados são iguais aos recebidos
- **Irretratabilidade** - prova que a mensagem foi enviada e recebida pelas partes especificadas

Breve

Histórico

1918- máquina Enigma para uso militar

Anos 80 - Popularização do uso de computadores

Início de 2000 - Grande número de ataques relacionados a segurança

- Algoritmo RSA
- Blockchain

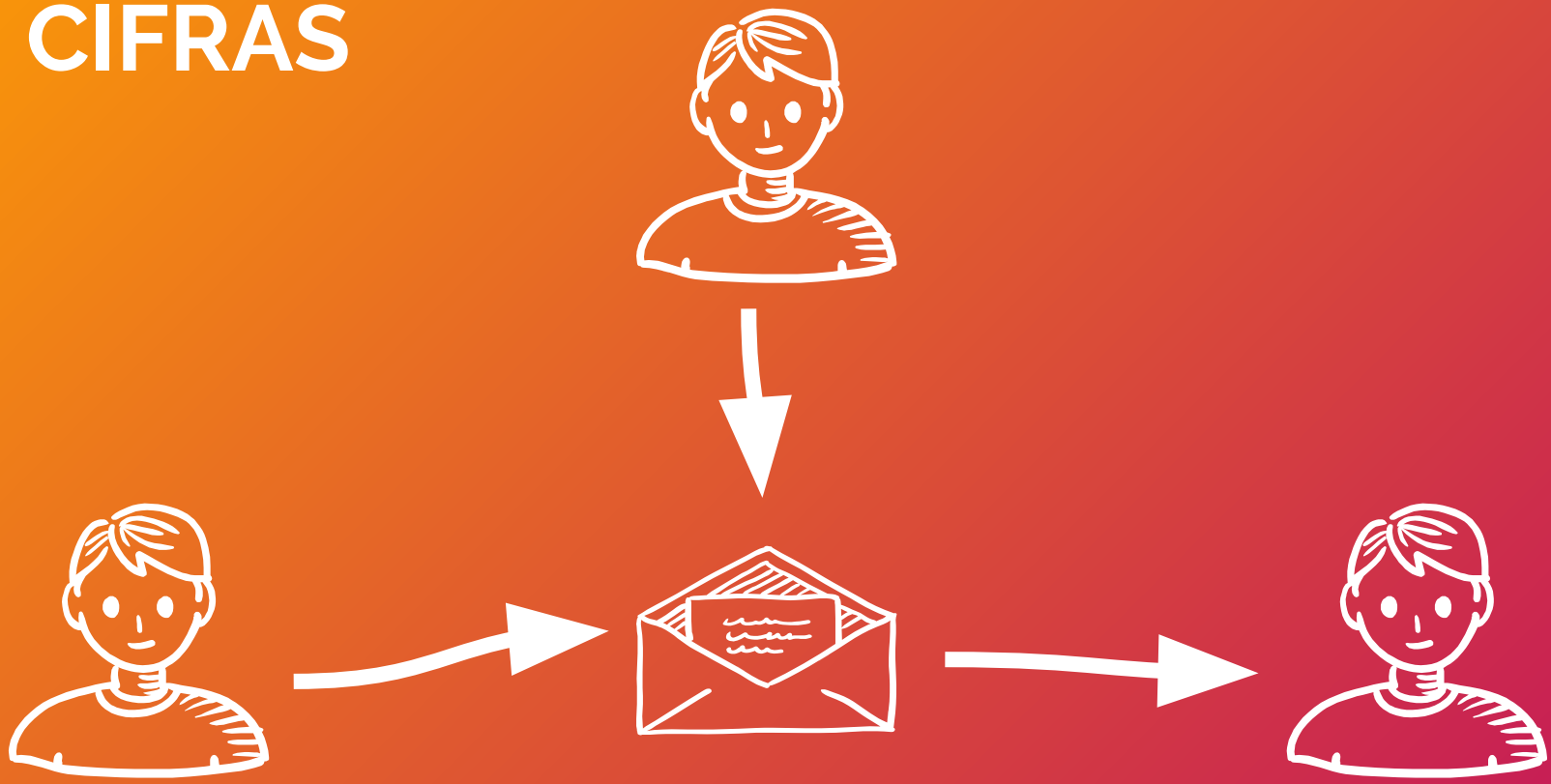
Fonte: CERT

Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores - atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes em contato

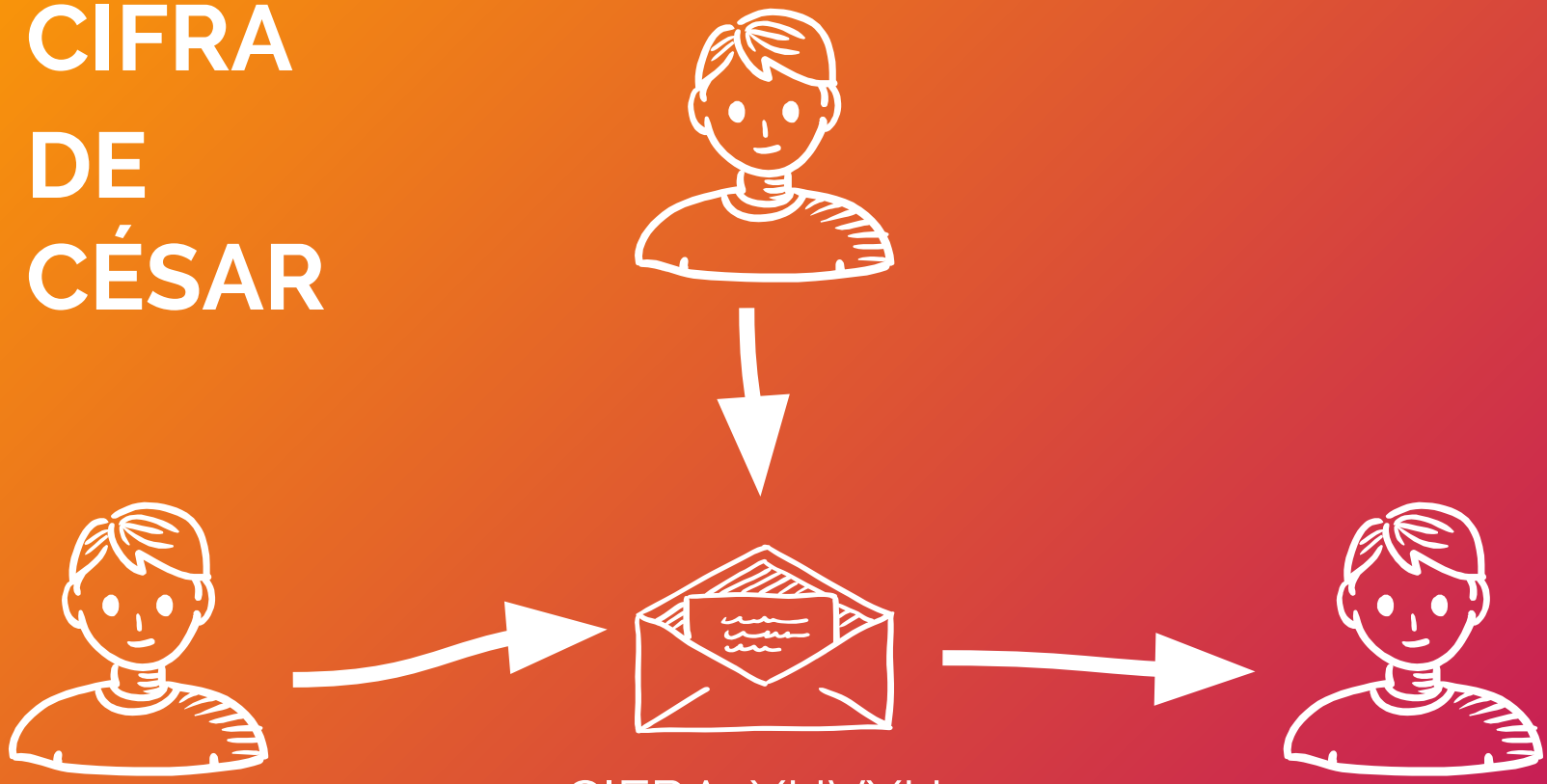
TÓPICOS DE SEGURANÇA DA INFORMAÇÃO

- Cifras clássicas
  - *Cifra de César*
  - *Cifra de deslocamento*
- Encriptação
  - *Chave pública (encriptação assimétrica)*

CIFRAS



CIFRA DE CÉSAR



MENSAGEM: TESTE

CIFRA: XHVXH

SEIS PRINCÍPIOS DAS CIFRAS

Século XIX - Auguste Kerckhoff

1.

O sistema deve ser indecifrável, se não matematicamente, pelo menos na prática.

2.

O aparato não deve requerer sigilo e não deve ser um problema se ele cair nas mãos dos inimigos.

3.

Deve ser possível memorizar uma chave sem ter que anotá-la e deve ser possível modificá-la se necessário.

4.

Deve ser possível aplicar a sistemas telegráficos.

5.

O aparato deve ser portátil e não deve necessitar de muitas pessoas para manipulá-lo e operá-lo.

6.

O sistema deve ser fácil de usar e não deve ser estressante usá-lo e não deve exigir que o usuário conheça e siga uma longa lista de regras.

CIFRA DE DESLOCAMENTO

CONHECE O MECANISMO

MENSAGEM: TESTE

CHAVE: 5

CIFRA: ZJYZJ

CRIPTOGRAFIA

- **Criptografia simétrica**: *mesma chave para encriptar e decriptar_*
- **Criptografia assimétrica**: *uma chave para encriptar e outra para decriptar_*

CIFRA DE DESLOCAMENTO

CONHECE O MECANISMO

MENSAGEM: TESTE

CHAVE: 5

CIFRA: ZJYZJ

CHAVE PÚBLICA - ENCRIPTAÇÃO ASSIMÉTRICA

CHAVE PÚBLICA

MENSAGEM ENCRIPTADA

CHAVE PRIVADA

EXEMPLO: CHAVE PÚBLICA

segurança da informação

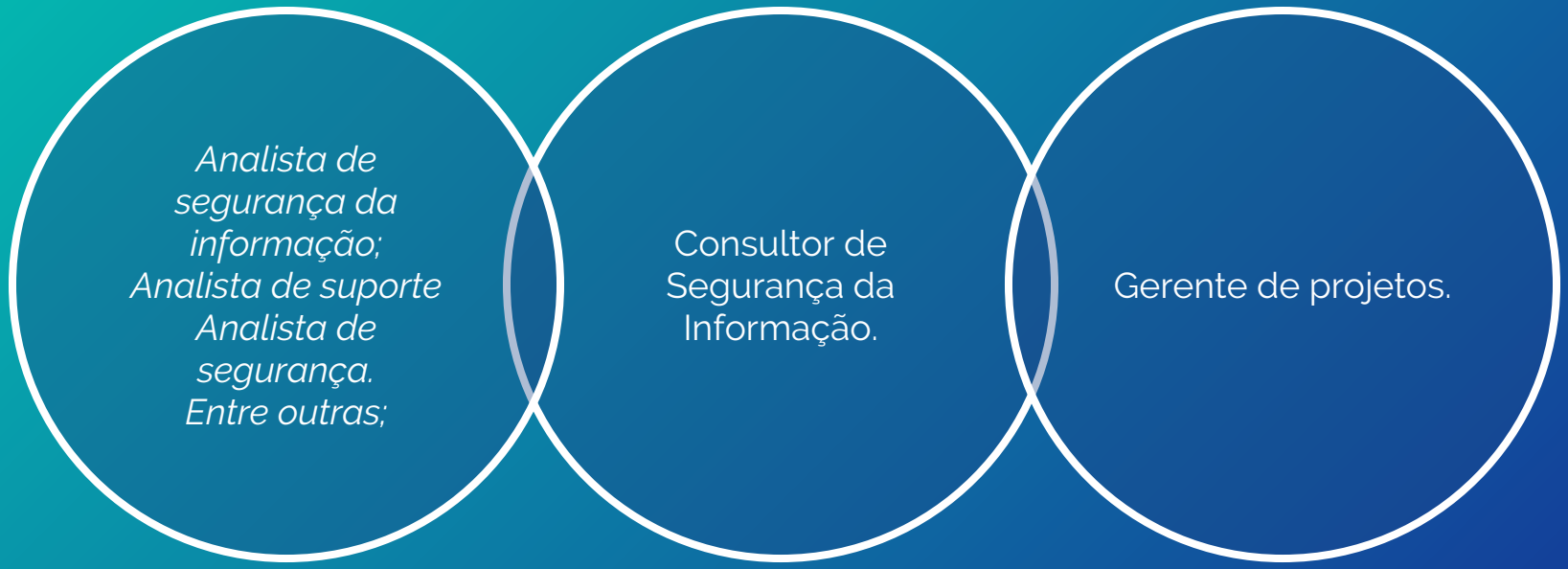
Chave pública

(7, 55)
Mensagem: 2
2^7 *mod* 55
128 *mod* 55
Mensagem encriptada: 18

Chave privada

(23, 55)
Mensagem encriptada: 18
18^23 *mod* 55
743477...832 *mod* 55
Mensagem: 2

TRAJETÓRIAS PROFISSIONAIS

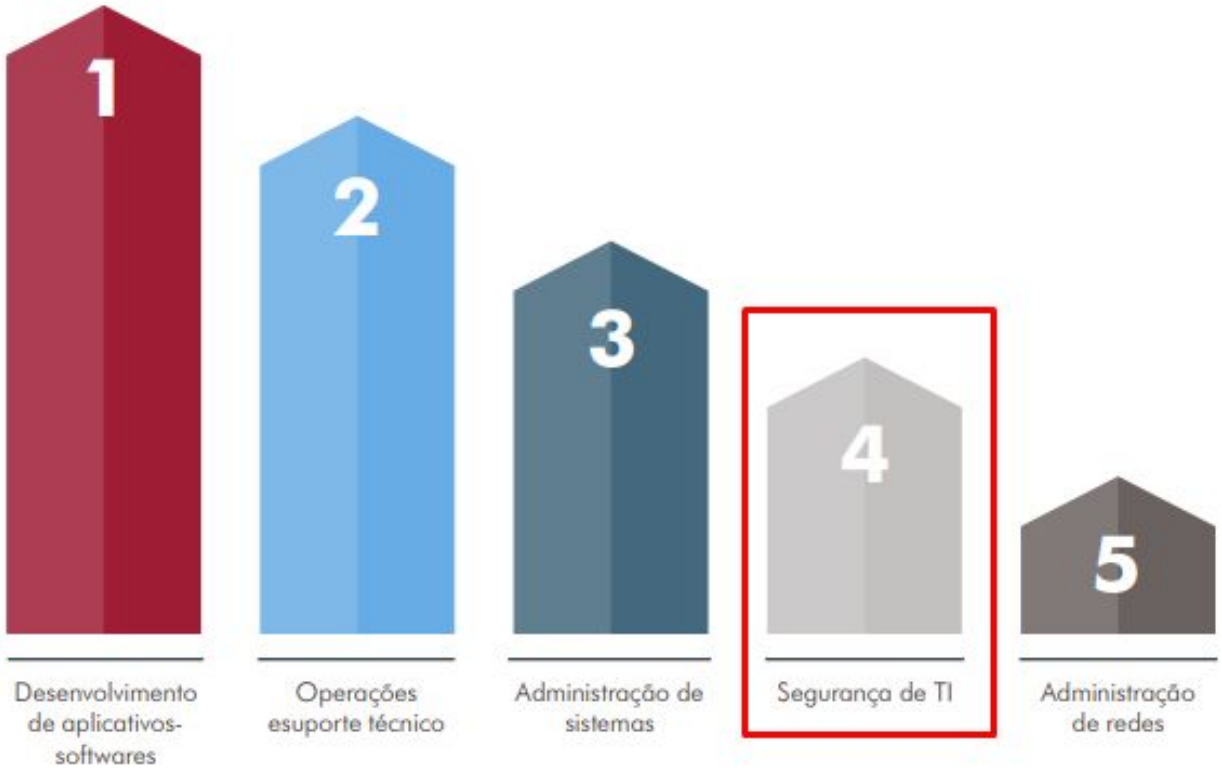


Quanto ganha um consultor de segurança da informação?

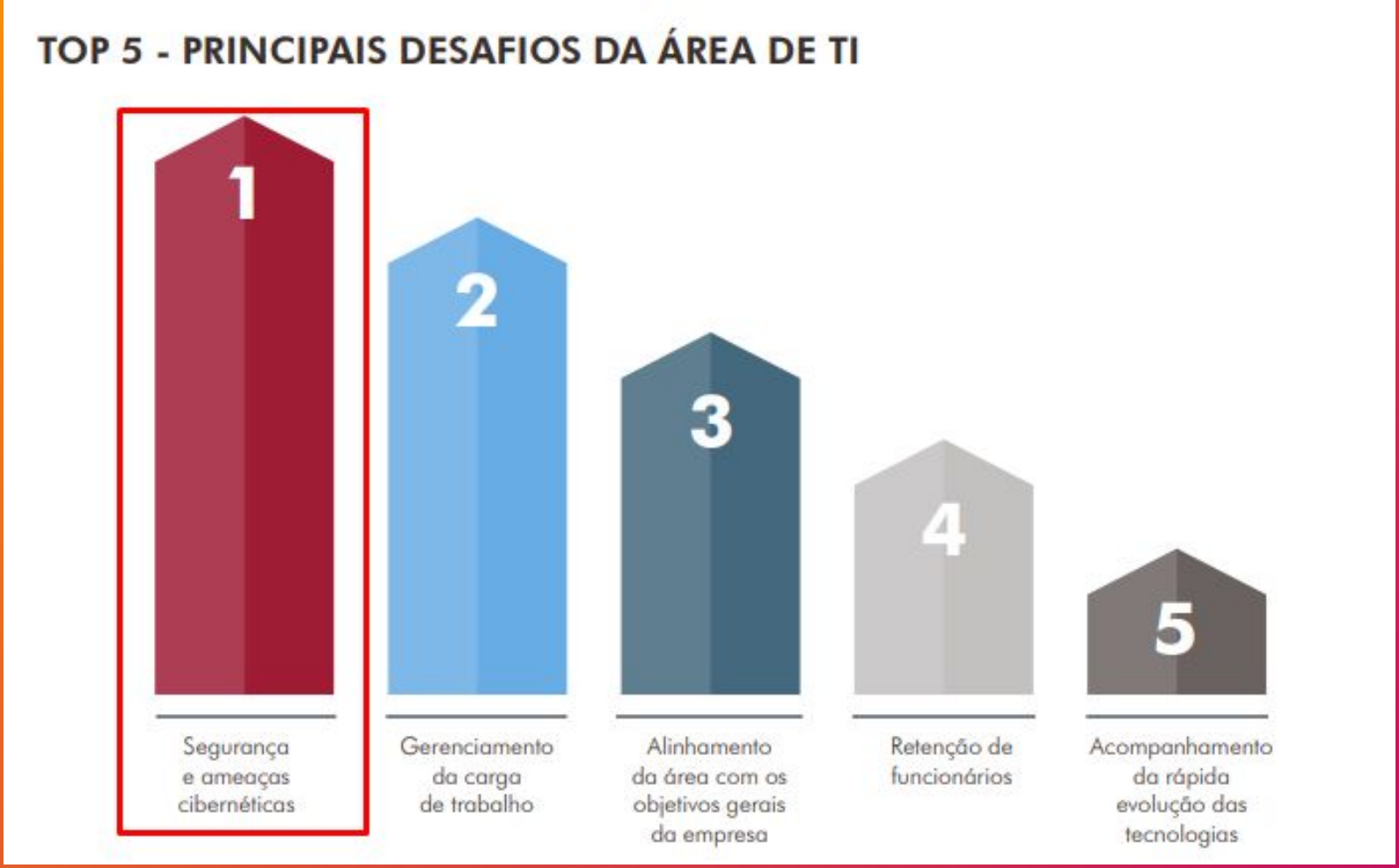
Os salários foram calculados com base nos valores informados pelos candidatos do VAGAS.com.

SOBRE A ÁREA

TOP 5 - ÁREAS QUE MAIS DEMANDAM PROFISSIONAIS ESPECIALIZADOS PARA PROJETOS



SOBRE A ÁREA


TOP 5 - PRINCIPAIS DESAFIOS DA ÁREA DE TI
1
Segurança e ameaças cibernéticas
2
Gerenciamento da carga de trabalho
3
Alinhamento da área com os objetivos gerais da empresa
4
Retenção de funcionários
5
Acompanhamento da rápida evolução das tecnologias

ACH2026
Redes de Computadores

matéria obrigatória oferecida pela EACH_

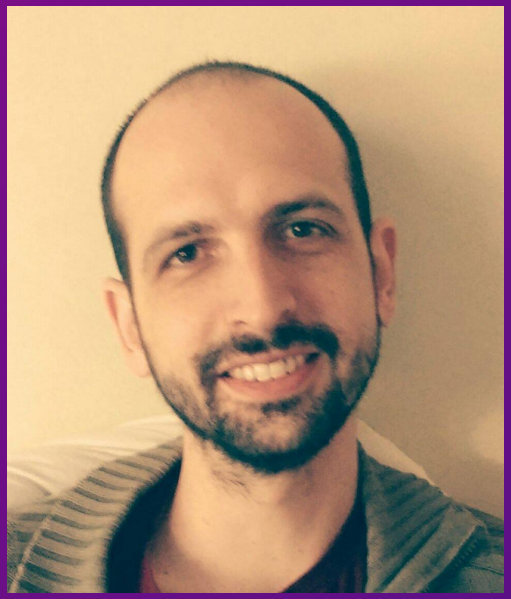
prevista para o 6º semestre_

ACH2076
Segurança da Informação

matéria optativa oferecida pela EACH_

prevista para o 7º semestre_

PROFESSORES DO CURSO DE *sistema de informação*



Prof. Dr. Marcio Moretto Ribeiro

Prof. Dr. Valdinei Freire da Silva

PROJETOS

“Privacidade e vigilância no Brasil”

Prof. Dr. Marcio Moretto Ribeiro

“Children Privacy Protection Engine for Smart Anthropomorphic Toys”

Prof. Dr. Marcelo Fantinato

Bibliografia & links uteis

- https://www.catho.com.br/profissoes/analista-de-seguranca-da-informacao/trilha-de-carreira
- https://luizfelipeferreira.com/artigo/guia-de-salarios-2018/
- Stallings, W; "Cryptography and Network Security – Principles and Practice", 3. ed. New Jersey, Prentice Hall, 2002.
- Bishop, Matt; "Computer Security – Art and Science", Addison-Wesley, 2003.
- Folha. Carreiras Análise de Segurança da Informação. Disponível em: https://www1.folha.uol.com.br/sobretudo/carreiras/2016/07/1787788-em-alta-analista-de-seguranca-de-informacao-pode-ganhar-ate-r-40-mil.shtml ;Acesso em 26 de Maio de 2018.
- Lovemondays. Cargo e Salário Analista de Segurança. Disponível em: https://www.lovemondays.com.br/salarios/cargo/salario-analista-de-seguranca-da-informacao; Acesso em 26 de Maio de 2018.
- Cert. Estatísticas de Incidentes. Disponível em: https://www.cert.br/stats/incidentes; Acesso em 26 de Maio de 2018.
- http://www.each.usp.br/si/?page_id=29
- https://www.vagas.com.br/cargo/consultor-de-seguranca-da-informacao

PERGUNTAS?