UNIFEOB
ESCOLA DE NEGÓCIOS

2023

PROJETO DE CONSULTORIA EMPRESARIAL

UNIFEOB

CENTRO UNIVERSITÁRIO DA FUNDAÇÃO DE ENSINO OCTÁVIO BASTOS

ESCOLA DE NEGÓCIOS

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

PROJETO INTEGRADO

PHISHING DETECTIVE

SÃO JOÃO DA BOA VISTA, SP

NOVEMBRO 2023

UNIFEOB

CENTRO UNIVERSITÁRIO DA FUNDAÇÃO DE ENSINO OCTÁVIO BASTOS

ESCOLA DE NEGÓCIOS

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

PROJETO INTEGRADO

PHISHING DETECTIVE

MÓDULO - Inteligência Artificial

Inteligência Artificial – Prof. Rodrigo Marudi de Oliveira
Segurança em Sistema Computacionais - Prof. Nivaldo de Andrade

Estudantes:
Mara Vicentina Pinto, RA 1012023100321

SÃO JOÃO DA BOA VISTA, SP
NOVEMBRO , 2023

SUMÁRIO

1 INTRODUÇÃO **4**

2 DESCRIÇÃO DA EMPRESA **5**

3 PROJETO DE CONSULTORIA EMPRESARIAL **6**

3.1 INTELIGÊNCIA ARTIFICIAL 6

3.1.1 INTRODUÇÃO À APLICAÇÃO DA IA 7

3.1.2 IMPLEMENTAÇÃO E TÉCNICAS UTILIZADAS 7

3.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS 15

3.2.1 CONCEITOS E IMPLEMENTAÇÃO DE SEGURANÇA 15

3.2.2 DETECÇÃO E PREVENÇÃO DE ATAQUES 16

4 CONCLUSÃO **17**

4.1 ESTUDANTE NA PRÁTICA – LINK DO VÍDEO 17

5 REFERÊNCIAS **18**

1 INTRODUÇÃO

No cenário digital contemporâneo, o fenômeno do phishing emergiu como uma ameaça significativa para a segurança cibernética. Este tipo de ataque tem se tornado uma ferramenta de criminosos cibernéticos que visam roubar informações sensíveis, como senhas, números de cartão de crédito e dados pessoais.

Esse fenômeno tem sido uma fonte crescente de preocupação tanto para indivíduos quanto para organizações, à medida que cibercriminosos aprimoram constantemente suas táticas para explorar a ingenuidade e a confiança das vítimas. O phishing se baseia na manipulação psicológica e na engenharia social para persuadir as pessoas a divulgar informações confidenciais, muitas vezes se disfarçando de entidades confiáveis, como bancos, redes sociais ou empresas de comércio eletrônico.

O intuito deste projeto é desenvolver uma ferramenta que analisa o conteúdo de e-mails, verifica se eles contêm possíveis tentativas de phishing e fornece feedback ao usuário sobre a suspeita de phishing nos e-mails.

Com essa solução, busca-se automatizar a detecção de phishing, para possibilitar uma maior segurança e conscientização em relação aos usuários e seus e-mails.

2 DESCRIÇÃO DA EMPRESA

A empresa contatada tem como nome social “ALEXANDRE BENEVIDES DE CARVALHO CORDEIRO” CNPJ 40.859.695/0001-86 que está localizada na cidade de São João da Boa Vista, na rua Hélio Correa da Fonseca, n200, Sala 03 e bairro Jardim Santa Rita.

Nos encontros realizados com o cliente em questão, foi nos relatado que gostaria de realizar um sistema mais eficaz para a detecção e segurança de e-mails contra phishing.

Após análise detalhada do caso, contatou-se o cliente buscando apresentar uma proposta de uma plataforma de fácil acesso e usabilidade, que faria a detecção de phishing através do acesso ao e-mail informado. Com essa solução, buscamos resolver o problema enfrentado por ele anteriormente.

3 PROJETO DE CONSULTORIA EMPRESARIAL

A empresa contatada atua na área de reparação e manutenção de computadores e de equipamentos periféricos, desde 2021 quando foi fundada. Tendo como missão e valor o oferecimento de serviços de reparação e manutenção de computadores e equipamentos periféricos de alta qualidade, com rapidez e eficiência, a fim de garantir a satisfação dos seus clientes.

Como a empresa em questão lida com informações confidenciais de clientes e parceiros. Tiveram a necessidade de um sistema de detecção de phishing para seus e-mails que é crucial para proteger contra ataques cibernéticos que visam roubar dados sensíveis ou instalar malware. Isso ajudaria a manter a integridade dos sistemas e evitar prejuízos financeiros e de reputação, garantindo a segurança dos clientes e parceiros.

Nesta etapa do PI serão apresentados os conteúdos que cada unidade de estudo utilizou para realizar o projeto, assim como a forma que foram aplicados na empresa escolhida para a realização do projeto.

3.1 INTELIGÊNCIA ARTIFICIAL

A Inteligência Artificial (IA) é a área da ciência da computação que se concentra em criar sistemas capazes de realizar tarefas que normalmente requerem inteligência humana, como aprendizado, raciocínio e resolução de problemas. Isso é alcançado por meio do uso de algoritmos avançados e técnicas como redes neurais artificiais.

A relevância da Inteligência Artificial na atualidade é ampla e profunda. A IA tem impacto em várias indústrias, automatizando tarefas rotineiras, aprimorando a tomada de decisões, melhorando a medicina, habilitando assistentes virtuais e impulsionando inovações em áreas como veículos autônomos e segurança cibernética. A capacidade da IA de analisar grandes volumes de dados e fornecer insights valiosos está transformando a maneira como as empresas operam e como as pessoas interagem com a tecnologia no dia a dia.

A IA está moldando o presente e o futuro, com implicações abrangentes em inovação, economia e sociedade. Sua influência só tende a crescer à medida que continuamos a explorar seu potencial em diferentes campos e a incorporá-la cada vez mais em nossa vida cotidiana.

A integração da inteligência artificial nesse projeto de detecção de phishing é essencial para aprimorar a precisão na identificação de ameaças cibernéticas. A IA pode

analisar o comportamento de e-mails e identificar indicadores de phishing, reduzindo falsos positivos e melhorando a detecção.

3.1.1 INTRODUÇÃO À APLICAÇÃO DA IA

Um usuário recebe um e-mail supostamente da sua instituição bancária, solicitando a atualização imediata de suas informações de conta devido a uma suposta atividade suspeita. O e-mail contém um link que direciona para uma página falsa, onde o usuário é induzido a inserir suas credenciais bancárias.

Uma aplicação de IA especializada em detecção de phishing pode identificar vários indicadores de que esse e-mail é uma tentativa fraudulenta. A análise do conteúdo revelaria discrepâncias na linguagem, como erros gramaticais, incoerências com a comunicação padrão do banco e a presença de solicitações urgentes e atípicas.

Caso a aplicação identifique esses indicadores como potenciais ameaças de phishing, ela pode automaticamente marcar o e-mail como suspeito, alertando o usuário. Isso evita que o usuário inadvertidamente compartilhe informações sensíveis e se proteja contra possíveis ataques.

Dessa forma, a aplicação de IA age como uma camada proativa de defesa, identificando e-mails de phishing, mitigando efetivamente o risco de comprometimento de informações confidenciais e protegendo contra ataques cibernéticos.

3.1.2 IMPLEMENTAÇÃO E TÉCNICAS UTILIZADAS

O projeto realizado se chama Phishing Detective, em seu desenvolvimento utilizou-se a Linguagem de Marcação de Hipertexto HTML 5, Folhas de Estilo em Cascata CSS, JavaScript, PHP. Além disso, também utilizou-se o framework Bootstrap.

No contexto deste projeto específico, o PHP é usado para criar um script que se conecta a servidores de e-mail, verifica o conteúdo dos e-mails em busca de tentativas de phishing e exibe os resultados em uma página da web. Buscando lidar com solicitações de servidor e interações com serviços de e-mail por meio da extensão IMAP do PHP.

No projeto desenvolvido, Phishing Detective as técnicas de IA específicas, não foram incorporadas diretamente no código. Em vez disso, o script em PHP concentra-se principalmente na análise de e-mails em busca de possíveis tentativas de phishing usando regras personalizadas, bem como na decodificação de assuntos de e-mail.

As técnicas específicas de IA, como redes neurais convolucionais, redes multicamada e perceptrons, são geralmente usadas em casos de detecção de ameaças mais complexas, como reconhecimento de imagens, processamento de linguagem natural avançado e análise de padrões profundos de dados. A detecção de phishing tradicional pode ser tratada com eficácia usando regras específicas que não requerem o uso de redes neurais.

A integração da Inteligência Artificial (IA) neste projeto é fundamental para aprimorar a detecção de tentativas de phishing em e-mails. A IA pode melhorar a precisão e a eficiência da análise, identificando comportamentos suspeitos que podem passar despercebidos por métodos tradicionais. Em resumo, a IA aprimora a capacidade de identificar e combater ameaças cibernéticas em constante evolução, fortalecendo a segurança dos usuários e organizações.

O projeto também possui versionamento de código git e para mais informações sobre os códigos desenvolvidos está disponível no repositório que se encontra no link: https://github.com/mara-vicentina/phish-detective .

A arquitetura utilizada foi o MVC (Model-View-Controller, ou Modelo-Visão-Controle, em português). MVC é um padrão de arquitetura de software focado em reuso de código, no qual ocorre a divisão da estrutura lógica de um sistema em 3 camadas: a do Modelo, relacionada ao banco de dados; a de Visão, vinculada a visualização dos dados e das páginas; e a do Controle, responsável pela conexão e transmissão de informações entre as camadas Modelo e Visão.

No projeto em questão temos apenas View e Controller, uma vez que não há necessidade de interação direta com um banco de dados. A camada View cuida da apresentação dos dados e da interação com o usuário, enquanto a camada Controller gerencia a lógica da aplicação e a comunicação entre a View.

A seguir temos imagens dos códigos que foram implementados para realização do sistema Phishing Detective:

```php
<?php      You, 4 weeks ago • Criando projeto de detecção de phishing
// Inicialize a aplicação e carregue as configurações
require './config.php';

function autoloader($class) {
    if (str_contains($class, 'Controller')) {
        include './src/Controllers/' . $class . '.php';
    }

    if (str_contains($class, 'Service')) {
        include './src/Services/' . $class . '.php';
    }
}

spl_autoload_register('autoloader');

$request_uri = str_replace(BASE_PATH, '', $_SERVER['REQUEST_URI']);

require './routes.php';

$route = isset($routes[$request_uri]) ? $routes[$request_uri] : die('Rota não cadastrada.');
$route = explode('@', $route);

if (!isset($route[0]) || !isset($route[1])) {
    die('Rota configurada incorretamente: ');
}

$controller = $route[0];
$method = $route[1];

$controllerInstance = new $controller();
$controllerInstance->$method();
```

Figura 1. Código da index

Fonte: Autor (2023)

```php
<?php

class HomeController {

    //Método responsável por exibir a página inicial, que contém o formulário de entrada de dados.
    public function index() {
        include 'src/Views/form_email.php';
    }

    //Método que processa os dados do formulário, realiza a conexão com o servidor IMAP,
    //obtém a lista de e-mails na caixa de entrada, valida cada e-mail em relação a phishing
    //utilizando o serviço de validação, e exibe a lista resultante na página de visualização de e-mails.
    public function emailsList() {
        $phishingValidator = new PhishingValidatorService();
        $imapConnection = new IMAPConnectionService($_POST['email'], $_POST['senha'], $_POST['servidor']);
        $imapConnection->open();

        $emailIds = $imapConnection->getEmailInbox();
        $validatedEmails = [];

        if ($emailIds) {
            foreach ($emailIds as $emailId) {
                $header = $imapConnection->getHeaderInfo($emailId);

                $email = [
                    'subject'     => $header->subject,
                    'date'        => date("d/m/Y H:i", strtotime($header->date)),
                    'is_phishing' => $phishingValidator->isPhishing($header->subject),
                ];

                array_push($validatedEmails, $email);
            }
        }

        $imapConnection->close();

        include 'src/Views/emails_list.php';
    }
}
```

Figura 2. Código da HomeController

Fonte: Autor (2023)

```php
<!DOCTYPE html>
<html>
<?php
    require_once('src/Views/includes/head.php');
?>
<body>
<div id="particles-js"></div>

<div class="container-fluid">
    <div class="container p-5">
        <div class="row">
            <img id="img-logo" src="<?php echo BASE_URL.'/assets/img/logo-phish.png' ?>" alt="logo-connected" class="mx-auto d-block">
        </div>
        <div class="row m-5">
            <div class="col-md-6 offset-md-3">
                <div class="card bg-whitee">
                    <div class="card-body">
                        <h2 class="card-title text-center main-color">Verificação de E-mail</h2>
                        <form action="<?= BASE_PATH?>/listagem" method="POST">
                            <div class="form-group">
                                <label for="email" class="sec-color mt-2">E-mail:</label>
                                <input type="text" name="email" class="form-control" required>
                            </div>
                            <div class="form-group">
                                <label for="senha" class="sec-color mt-2">Senha:</label>
                                <input type="password" name="senha" class="form-control" required>
                            </div>
                            <div class="form-group">
                                <label for="servidor" class="sec-color mt-2">Servidor:</label>
                                <select name="servidor" class="form-select">
                                    <option value="gmail">Gmail</option>
                                    <option value="outlook">Outlook</option>
                                </select>
                            </div>
                            <button type="submit" class="btn btn-primary mt-4 btn-custom">Verificar E-mails</button>
                        </form>
                    </div>
                </div>
            </div>
        </div>
    </div>
</div>

<?php
    require_once('src/Views/includes/js_content.php');
?>
</body>
</html>
```

Figura 3. Código da View form_email

Fonte: Autor (2023)

```php
<!DOCTYPE html>
<html>
<?php
    require_once('src/Views/includes/head.php');
?>
<body>
<div id="particles-js"></div>

<div class="container-fluid">
    <div class="container p-5">
        <div class="row">
            <img id="img-logo" src="<?php echo BASE_URL.'/assets/img/logo-phish.png' ?>" alt="logo-connected" class="mx-auto d-block">
        </div>
        <div class="row m-5">
            <div class="col-md-10 offset-md-1">
                <div class="card custom-card overflow-auto p-2 bg-whitee">
                    <div class="card-body">
                        <h2 class="text-center main-color">Resultados da Verificação de E-mail</h2>
                        <p class="sec-color mt-2">E-mail: <?php echo $_POST['email']; ?></p>
                        <p class="sec-color mt-2">Servidor: <?php echo $_POST['servidor']; ?></p>
                        <div class="table-responsive">
                            <table class="table table-bordered table-hover">
                                <thead>
                                    <tr>
                                        <th class="main-color text-left">Assunto</th>
                                        <th class="main-color text-left">Data</th>
                                        <th class="main-color text-left">Phishing Safe</th>
                                    </tr>
                                </thead>
```

Figura 4. Código da View emails_list

Fonte: Autor (2023)

```
                        <tbody>
                            <?php foreach ($validatedEmails as $email): ?>
                                <tr>
                                    <td class="text-left"><?php echo imap_utf8($email['subject']); ?></td>
                                    <td class="text-center"><?php echo htmlspecialchars($email['date']); ?></td>
                                    <td class="text-center">
                                        <?php echo $email['is_phishing'] ? '<span class="text-danger"><i class="bi-patch-exclamation-fill icon-size"></i></span>' :
                                        '<span class="text-success"><i class="bi-patch-check-fill icon-size"></i></span>'; ?>
                                    </td>
                                </tr>
                            <?php endforeach; ?>
                        </tbody>
                    </table>
                </div>
            </div>
        </div>
    </div>
</div>

    <?php
        require_once('src/Views/includes/js_content.php');
    ?>
</body>
</html>
```

Figura 5. Código da View emails_list - continuação

Fonte: Autor (2023)

```php
<?php

class IMAPConnectionService {
    private $email;
    private $password;
    private $serverUrl;
    private $imapStream;

    public function __construct($email, $password, $serverName) {
        $this->email     = $email;
        $this->password  = $password;
        $this->serverUrl = $this->getServerUrlByName($serverName);
    }

    //Abre a conexão IMAP com o servidor usando as credenciais fornecidas.
    public function open() {
        $this->imapStream = imap_open($this->serverUrl, $this->email, $this->password);

        if (!$this->imapStream) {
            die('Não foi possível abrir a conexão IMAP: ' . imap_last_error());
        }
    }

    //Fecha a conexão IMAP previamente aberta, se existir.
    public function close() {
        if ($this->imapStream) {
            imap_close($this->imapStream);
        }
    }

    //Retorna o stream IMAP atualmente aberto.
    public function getImapStream() {
        return $imapStream;
    }

    //Obtém a URL do servidor IMAP com base no nome do servidor fornecido.
    private function getServerUrlByName($serverName) {
        $servers = [
            'gmail'   => '{imap.gmail.com:993/imap/ssl/novalidate-cert}INBOX',
            'outlook' => '{outlook.office365.com:993/imap/ssl/novalidate-cert}INBOX',
        ];

        return $servers[$serverName];
    }

    //Obtém uma lista de IDs de e-mails na caixa de entrada.
    public function getEmailInbox() {
        return imap_search($this->imapStream, 'ALL');
    }

    //Obtém informações do cabeçalho de um e-mail específico com base no ID fornecido.
    public function getHeaderInfo($emailId) {
        return imap_headerinfo($this->imapStream, $emailId);
    }
}
```

Figura 6. Código da Classe IMAPConnectionService

Fonte: Autor (2023)

```php
<?php

class PhishingValidatorService {

    private $keywords;

    public function __construct() {
        $this->keywords = ["senha", "confirme", "urgente", "clique", "phishing", "ganhou", "ação necessária", "fatura"];
    }

    //Verifica se o texto fornecido contém palavras-chave associadas a e-mails de phishing.
    //Converte o texto para minúsculas antes da comparação para garantir que não seja sensível a maiúsculas.
    //Retorna verdadeiro se o texto contiver uma palavra-chave de phishing, caso contrário, retorna falso.
    public function isPhishing($text) {
        $text = strtolower($text);

        foreach ($this->keywords as $keyword) {
            if (strpos($text, $keyword) !== false) {
                return true;
            }
        }

        return false;
    }

}
```

Figura 7. Código da Classe PhishingValidatorService

Fonte: Autor (2023)

Os procedimento realizados no desenvolvimento foram:

1. Criação de uma página contendo um formulário com inserção dos dados de e-mail e senha, escolha do servidor de e-mail e botão para verificar os e-mails.

Para fins de teste deixou-se disponível os seguintes dados:

e-mail: phishdetective7@outlook.com e senha: Ab@123456789 .

Figura 8. Página Inicial com Formulário de Verificação de E-mail

Fonte: Autor (2023)

2. Criação de uma página contendo uma listagem com os resultados da verificação do e-mail, caso ele seja considerado phishing haverá um ícone de exclamação.

Figura 9. Página de Listagem Após a Verificação dos E-mails

Fonte: Autor (2023)

3.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS

A segurança em sistemas computacionais é de suma importância devido à necessidade de proteger dados sensíveis, prevenir ameaças cibernéticas, garantir a continuidade dos negócios e preservar a reputação das organizações.

Além disso, a privacidade do usuário e a conformidade com regulamentações são fatores cruciais. A confiabilidade da segurança também fomenta a inovação e a confiança dos usuários nas tecnologias digitais. Em um cenário em constante evolução, a segurança em sistemas computacionais desempenha um papel central na proteção da integridade e da confiabilidade das operações empresariais e da sociedade como um todo.

3.2.1 CONCEITOS E IMPLEMENTAÇÃO DE SEGURANÇA

O conceito de segurança lógica refere-se à proteção de sistemas e dados por meio de medidas como firewalls, criptografia e políticas de acesso. Já a segurança física envolve proteção contra ameaças físicas, como acesso não autorizado a instalações e equipamentos, através de barreiras físicas, câmeras e controle de acesso.

Já o conceito de valor da informação está relacionado à importância e utilidade que os dados têm para uma organização. Esse valor pode ser categorizado em critérios como confidencialidade, integridade e disponibilidade. A avaliação do valor da informação é crucial para determinar o nível apropriado de segurança a ser aplicado, garantindo que os recursos sejam direcionados eficientemente para proteger dados críticos e sensíveis. Isso inclui a compreensão de como a perda, corrupção ou indisponibilidade dessas informações pode afetar a operação e a reputação da empresa. O gerenciamento eficaz do valor da informação orienta as estratégias de segurança para manter um equilíbrio adequado entre proteção e acessibilidade.

Na recente interação com a empresa, implementamos com sucesso um sistema avançado de detecção de phishing para e-mails. Essa medida proativa é fundamental para fortalecer a segurança cibernética da organização, pois os ataques de phishing representam uma ameaça significativa, visando obter acesso não autorizado a informações confidenciais.

3.2.2 DETECÇÃO E PREVENÇÃO DE ATAQUES

Adotamos um sistema de detecção de phishing em emails que verifica os e-mails daquela conta e identifica quais as possíveis ameaças.

Utilizamos um sistema avançado de detecção de phishing para e-mails. A implementação desse sistema contribuiu não apenas para proteger os dados sensíveis da empresa, mas também para preservar a confiança dos clientes e parceiros ao garantir que as comunicações eletrônicas sejam seguras e livres de tentativas de fraude.

4 CONCLUSÃO

A relevância da Inteligência Artificial (IA) é incontestável no cenário atual, permeando diversos setores com avanços significativos. No contexto de segurança cibernética, a IA desempenha um papel crucial ao oferecer detecção avançada de ameaças, adaptando-se continuamente a padrões emergentes.

Sua capacidade de analisar grandes volumes de dados em tempo real, identificar comportamentos suspeitos e automatizar respostas contribui para fortalecer as defesas contra ameaças cibernéticas.

A IA não apenas aprimora a eficácia na detecção de phishing, mas também proporciona escalabilidade e aprendizado contínuo, tornando-se uma ferramenta indispensável na proteção contra ameaças em constante evolução. À medida que a cibersegurança enfrenta desafios cada vez mais complexos, a aplicação estratégica da Inteligência Artificial destaca-se como uma salvaguarda essencial para a segurança digital.

Este trabalho apresentou a aplicação prática de um sistema voltado para a detecção de phishing em e-mails, demonstrando assim, como a Inteligência Artificial pode ajudar a otimizar processos e aumentar a segurança.

4.1 ESTUDANTE NA PRÁTICA – LINK DO VÍDEO

Nesta etapa foi produzido um vídeo no formato de pitch, onde o grupo apresenta o projeto a ser utilizado pelo cliente alvo. Segue o link do vídeo:

PROJETO INTEGRADO - ADS - 2023 - Phishing Detective - https://youtu.be/nIf32WqgQGU

5 REFERÊNCIAS

CARLOS, EDER SABINO.Aspectos de Segurança dos Sistemas Computacionais: qualificações de acesso, chaves e senhas, vírus e antivírus, procedimentos de “backup”. 2017. Disponível em: https://centraldefavoritos.com.br/2017/07/02/aspectos-de-seguranca-dos-sistemas-computacionais-qualificacoes-de-acesso-chaves-e-senhas-virus-e-antivirus-procedimentos-de-backup/ . Acesso em: 10 de novembro de 2023.

CONTROLE NET.Cibersegurança: A segurança da informação em sistemas computacionais. 2023. Disponível em: https://www.controle.net/faq/ciberseguranca-a-seguranca-da-informacao-em-sistemas-computacionais . Acesso em: 13 de novembro de 2023.

COSSETTI, MELISSA CRUZ.O que é inteligência artificial. 2018. Disponível em: https://tecnoblog.net/responde/o-que-e-inteligencia-artificial/ . Acesso em: 16 de outubro de 2023.

FIA BUSINESS SCHOOL.Inteligência Artificial: o que é, como funciona e exemplos. 2023. Disponível em: https://fia.com.br/blog/inteligencia-artificial/ . Acesso em: 18 de outubro de 2023.

G. ARIANE.O Que é Phishing? Dicas para Evitar Golpes na Internet. 2023. Disponível em: https://www.hostinger.com.br/tutoriais/o-que-e-phishing-e-como-se-proteger-de-golpes-na-internet#:~:text=Phishing%20s%C3%A3o%20amea%C3%A7as%20virtuais%2C%20tamb%C3%A9m,de%20outras%20pessoas%20na%20internet . Acesso em: 19 de novembro de 2023.

HIGHER SCHOOL OF NETWORKS.09 information security risks for companies. 2021. Disponível em: https://esr.rnp.br/seguranca/riscos-de-seguranca-da-informacao-2/ . Acesso em: 08 de novembro de 2023.

HIGHER SCHOOL OF NETWORKS.What is artificial intelligence and how is it today's bet. 2022. Disponível em: https://esr.rnp.br/ciencia-de-dados/o-que-e-inteligencia-articial-esr/ . Acesso em: 19 de outubro de 2023.

PALMEIRA, GUSTAVO.A segurança computacional da sua empresa te preocupa. 2022. Disponível em: https://acao.tech/seguranca-computacional-empresa/ . Acesso em: 21 de novembro de 2023.

PEÇANHA, VITOR.Inteligência Artificial: entenda o que é e como ela funciona. 2019. Disponível em: https://rockcontent.com/br/blog/inteligencia-artificial/ . Acesso em: 29 de outubro de 2023.

RUIZ, EVANDRO EDUARDO SERON.Você confia nos sistemas computacionais? Entenda o que é a computação confidencial . 2022. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/376868/voce-confia-nos-sistemas-computacionais . Acesso em: 15 de novembro de 2023.

SERASA.O que é phishing e como se proteger de golpes virtuais. 2021. Disponível em: https://www.serasa.com.br/premium/blog/o-que-e-phishing/ . Acesso em: 20 de novembro de 2023.

SECURITY UFRJ.O que é phishing. 2023. Disponível em: https://www.security.ufrj.br/o-que-e-phishing/ . Acesso em: 21 de novembro de 2023.