



***SEUS DADOS  
ESTÃO SEGUROS?***



# ***APRESENTAÇÃO***





Os crimes cibernéticos custam bilhões de dólares por ano à economia global. O estudo feito pelo *Center for Strategic and International Studies* (CSIS) aponta que empresas registram uma perda de pelo menos 100 bilhões de dólares anuais por ciberespionagem e por crimes cibernéticos, incluindo a perda de propriedade intelectual.

Para combater esse tipo de atividade existe a Estuário TI.





A Estuário TI é uma empresa pernambucana, que atua na área de Segurança da Informação. O nosso trabalho é fornecer tecnologia para a proteção contínua de dados dos nossos clientes.





***EXPERIÊNCIA***





EXPERIÊNCIA



Contamos com uma grande experiência em projetos corporativos, nas esferas pública e privada, provendo a segurança de empresas das áreas de saúde, educação, direito e construção civil. A Estuário TI posiciona-se no mercado como um serviço personalizado e de custo-benefício sob medida.





# ***HISTÓRIA***





Fundada em 2012 no ambiente do Porto Digital, com a intenção de suprir as necessidades do mercado de segurança da informação. A Estuário TI faz parte do cenário da Cultura Digital pernambucana, que é reconhecido como o maior parque tecnológico do Brasil em faturamento e número de empresas. Nossa empresa fica localizada no bairro da Madalena em Recife, e com filiais em São Paulo e Rio de Janeiro.







# *SERVIÇOS*





Nosso trabalho é feito com base em pesquisa pesquisa voltada para buscar e identificar vulnerabilidades desconhecidas, e inovação tecnológica, de acordo com a expertise diversificada da nossa equipe.

A Estuário TI oferece os seguintes serviços e soluções:



## 4.1 // ANÁLISE DE APLICAÇÕES WEB



Identifique e elimine ameaças no desenvolvimento de suas aplicações. Busca e identifica vulnerabilidades capazes de impactar nas aplicações, bem como no modelo de negócio da empresa. A análise ajuda a reduzir custos no ciclo de desenvolvimento ao minimizar os riscos relacionados à segurança da informação.

- **Gerencie as vulnerabilidades com o Wing** > Ao final da análise, as falhas encontradas são documentadas no Wing, nosso software online de gestão de vulnerabilidade. Através de um dashboard inteligente é possível ter uma visão ampla e detalhada dos resultados, atribuir quem deve fazer as correções e acompanhar o status das tarefas.

- **Mantenha a base de conhecimento** > O Wing estabelece uma base de conhecimento sobre o estado das suas aplicações no momento do teste, que pode ser facilmente compartilhada com futuros colaboradores da empresa. Um sistema controlado, acessível a qualquer hora e de qualquer lugar.

- **Estuário LAB** > Contamos com uma equipe de pesquisa voltada para buscar e identificar vulnerabilidades desconhecidas, nunca antes publicadas, mais conhecidas como ODay. Saber da existência dessas falhas e como explorá-las garantem que você esteja sempre a frente do invasor.



## 4.2 // PENTEST ou Teste de Intrusão



- Fique ao menos um passo à frente do invasor > Focado na infraestrutura de networking, o teste age como um invasor interno ou externo interessado em encontrar e explorar as vulnerabilidades. Mas não qualquer atacante. Nossos especialistas procuram falhas manualmente, num processo meticuloso de busca, garantindo resultados mais eficientes e precisos, que só um humano com expertise é capaz de alcançar.
- Gerencie as vulnerabilidades com o Wing > Ao final do teste, as falhas encontradas são documentadas no Wing, nosso software online de gestão de vulnerabilidade. Através de um dashboard inteligente é possível ter uma visão ampla e detalhada dos resultados, atribuir quem deve fazer as correções e acompanhar o status das tarefas.
- Mantenha a base de conhecimento > O Wing estabelece uma base de conhecimento sobre o estado da sua rede no momento do teste, que pode ser facilmente compartilhada com futuros colaboradores da empresa. Um sistema controlado, acessível a qualquer hora e de qualquer lugar.
- Estuário LAB > Contamos com uma equipe de pesquisa voltada para buscar e identificar vulnerabilidades desconhecidas, nunca antes publicadas, mais conhecidas como ODay. Saber da existência dessas falhas e como explorá-las garante que você esteja sempre a frente do invasor. Para testes de intrusão contínuos e diários, temos a Gestão de Vulnerabilidades em infraestrutura.



### 4.3 // ASA Administração Segura Assistida



• **Administre a proteção da sua infraestrutura de rede com o nosso time** > Com a Administração Segura Assistida a infraestrutura de servidores da sua empresa passa a ser administrada pelo nosso time de experts em segurança da informação. Voltado especialmente para companhias que não possuem equipes de administração de sistemas, o serviço conta com SLA ágil, variável de acordo com a necessidade da sua empresa.

• **SAS Estuário** > Através do nosso software de abertura de serviço você pode fazer chamados e priorizá-los como baixo, médio ou crítico. Cada criticidade tem uma SLA específica de acordo com a necessidade do cliente.

• **Gerencie as vulnerabilidades com o Wing** > Ao final da análise, as falhas encontradas são documentadas no Wing, nosso software online de gestão de vulnerabilidade. Através de um dashboard inteligente é possível ter uma visão ampla e detalhada dos resultados, atribuir quem deve fazer as correções e acompanhar o status das tarefas.

• **Mantenha a base de conhecimento** > O Wing estabelece uma base de conhecimento sobre o estado da suas aplicações no momento do teste, que pode ser facilmente compartilhada com futuros colaboradores da empresa. Um sistema controlado, acessível a qualquer hora e de qualquer lugar.



## 4.4 // TREINAMENTOS EM SEGURANÇA DA INFORMAÇÃO



Realizamos treinamentos de Análise de aplicações Web e Testes de Intrusão *in company* ou em nossas dependências. O treinamento de análise de aplicações web é voltado para o público que desenvolve aplicações web. Já o de teste de intrusão é focado em quem administra a rede da empresa (administradores de sistemas).

- Treinamento em Análise de Aplicações Web > *Ensina como identificar, explorar e corrigir as principais vulnerabilidades de uma aplicação web. O curso é focado na descoberta de novas vulnerabilidades, através de ferramentas automatizadas, e também de análise manual.*

- Treinamento em Testes de Intrusão > *Ensina as principais técnicas para a condução de um Teste de Intrusão externo.. O curso é 100% prático e aborda novos e antigos métodos, técnicas e ferramentas. Para isso, serão utilizados laboratórios reais (on-line), sem as famosas máquinas virtuais cheias de vulnerabilidades viciadas.*



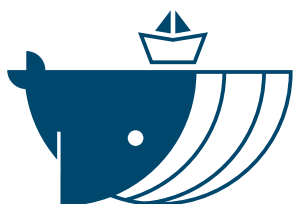


# ***PRODUTOS***





EL PESCADOR



A primeira plataforma para envio de phishing educativo do Brasil. Ela capacita o seu time contra ataques através de emails maliciosos por meio da nossa ferramenta de educação virtual.

## COMO SE PROTEGER?

### 01 Criação de Campanha

#### Click-only



Campanha que sugere ao usuário clicar em um conteúdo de email fraudulento.

#### Coleta de informação



Campanha que visa a coleta de informações sensíveis como senhas, documentos, etc.

#### Anexo



Campanha que sugere a abertura de anexo, simulando uma possível infecção da estação de trabalho do colaborador.

#### Personalizado



Campanha para um usuário ou grupo específico com base no tipo de informação consumida.

### 02 Cadastro e envio



Pelo nosso sistema você pode montar uma lista das pessoas que receberão o phishing, além de programar datas de envio, receber avaliação, entre outros.

### 03 Acompanhamento



Acompanhe em tempo real quais os usuários fisgados, quais deles assistiram os vídeos e responderam ao questionário de reciclagem. Por meio do nosso Dashboard, você ainda poderá reenviar os treinamentos para aqueles que não concluíram o processo.







O Avisa.lá monitora a disponibilidade e segurança de seu site, afinal, ninguém quer vê-lo fora do ar. A melhor parte disso é que você recebe alertas de qualquer problema através de aplicação mobile, SMS, email ou ligação telefônica. Você pode ficar um pouco mais por dentro:

#### Monitoramento de Disponibilidade

Aqui você acompanha a disponibilidade do seu site, desde a página inicial até pontos específicos, como carrinho de compra, área de cliente, blog, formulários de login, etc.

**01**

#### Monitoramento de Segurança

O Avisa.lá monitora também a segurança do seu site. As checagens identificam distribuição de malwares, pichação virtual (deface), sequestro de DNS e gerenciadores de conteúdo.

**02**

#### Alertas // 03



Se um problema for detectado, alertas serão emitidos por diversos canais de notificações, como chamada por voz, email, SMS e push notification.

**avisa.lá**

#### 04 // Aplicativo Mobile

Com a aplicação mobile Avisa.lá, você observa o status de disponibilidade e segurança do seu site 24 horas.

**05**

#### Time Conectado

Você não é o único a receber os alertas do sistema. Basta cadastrar os contatos do seu grupo e todos receberão as notificações do Avisa.lá.



#### Dashboard Descomplicado

Nosso dashboard apresenta os pontos mais importantes sobre a disponibilidade e da segurança do seu site. As informações são exibidas de forma simples e intuitiva.

**06**



# ***NÚMEROS***



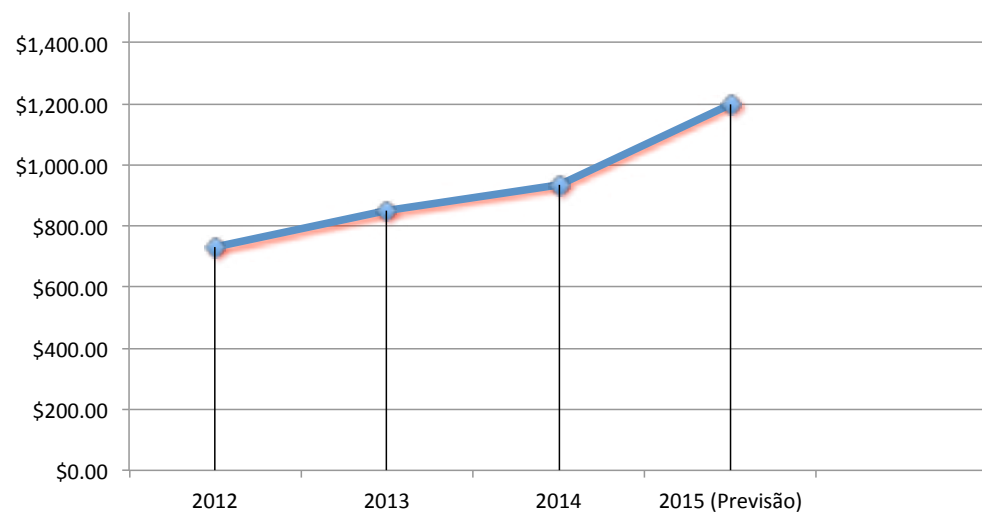


Gráfico referente ao Faturamento Anual

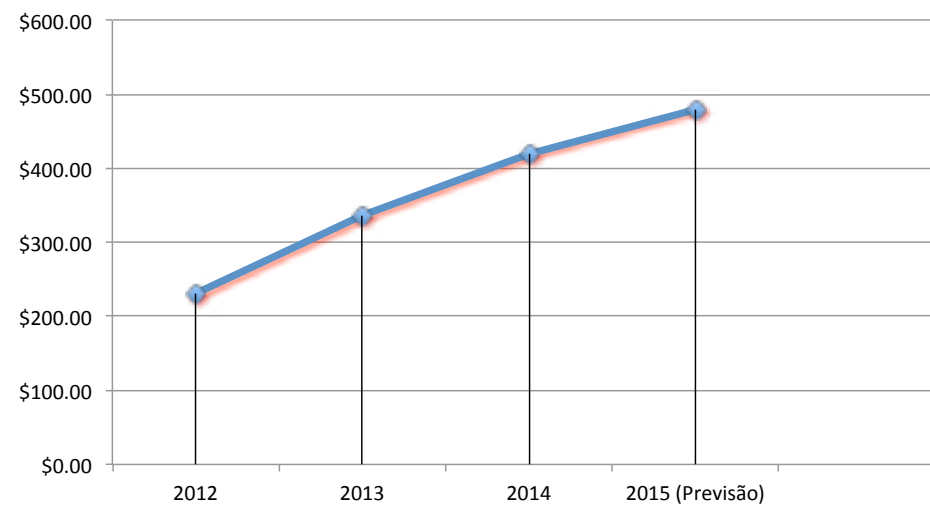


Gráfico referente ao Custo Operacional Anual

\*Nosso Fluxo de Caixa é igual ao Custo Operacional Mensal.



■ ASA ■ Análise App Web ■ PenTest ■ El Pescador ■ Treinamentos ■ Avisa.Lá

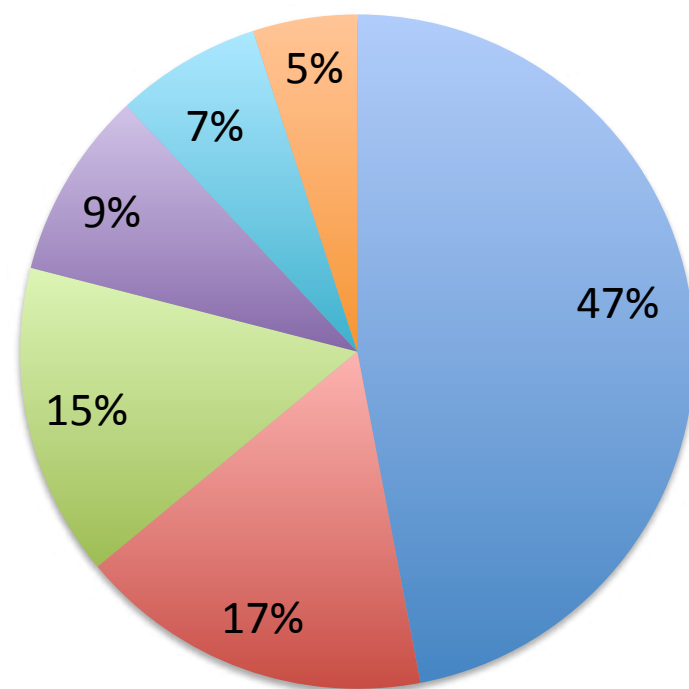
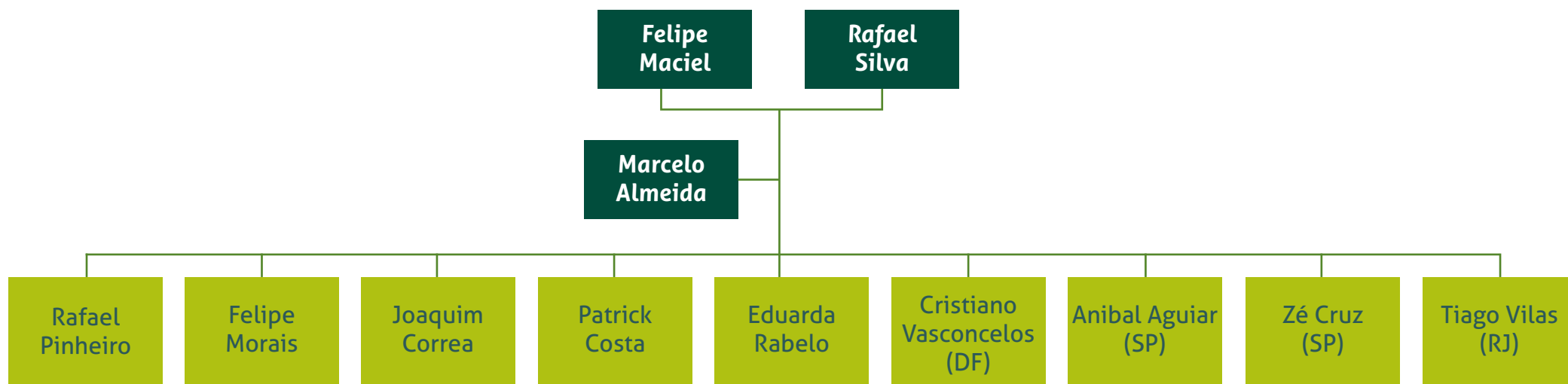


Gráfico referente ao Faturamento de cada serviço e produto do ano de 2014-2015







 / *ESTUARIOTI* • *WWW.ESTUARIOTI.COM.BR*