

# Desenvolvendo software ágil enquanto somos **PCI**





## PCI **DSS**

- Padrão de segurança de dados para o segmento de **meios de pagamento**.
- Compõem **12 requisitos** desde segurança física, firewall, criptografia e armazenamento de dados.





## Contexto da **Empresa**

- Empresa com forte cultura tradicional mas com **vontade de adotar o agile**.
- Nova equipe de desenvolvimento com cerca de **50 pessoas** em João Pessoa.
- Ambiente de desenvolvimento com **tecnologias Java e .Net**.



# Hello!

*Eu sou Daniela Pitta*

Estou aqui hoje porque amo falar sobre  
Segurança da Informação.

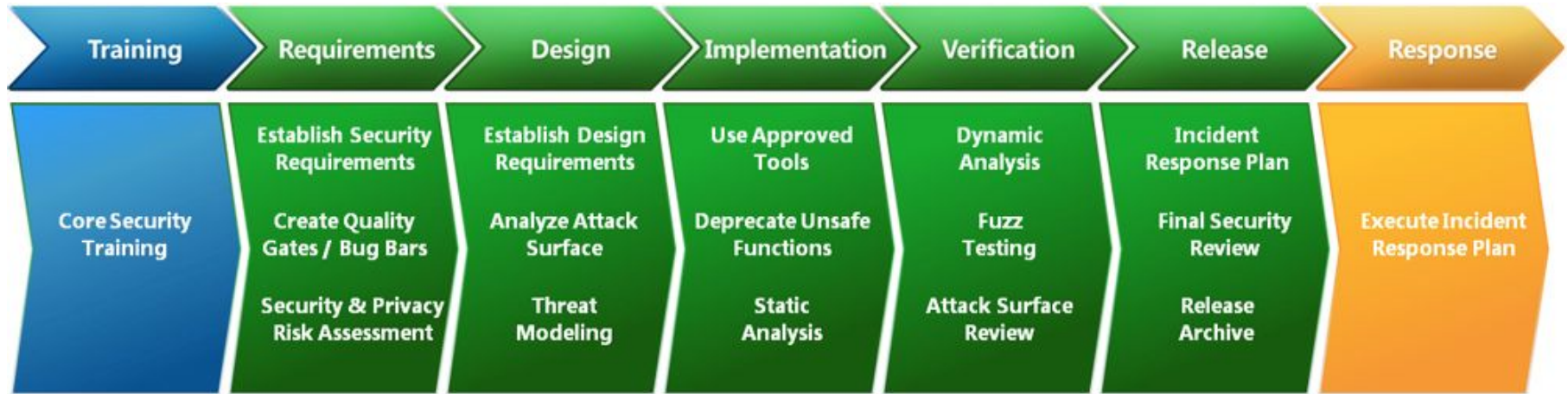
Você pode me contactar no [www.dlpitta.me](http://www.dlpitta.me)

*Como certificar os novos produtos  
de software desenvolvidos pela  
nova equipe em João Pessoa?*



“

# Microsoft Security Development Lifecycle (SDL)



Como certificar os novos produtos de software desenvolvidos pela nova equipe em João Pessoa e **atender as demandas de negócio rápido?**



“

# Mapping SDL to Agile

•**Every-Sprint practices:** Essential security practices that should be performed in every release.

•**Bucket practices:** Important security practices that must be completed on a regular basis but can be spread across multiple sprints during the project lifetime.

•**One-Time practices:** Foundational security practices that must be established once at the start of every new Agile project.





## *Requisitos Escolhidos*



“



## 6.3 Revisão de Código



- Identificação e treinamento de **revisores de código**.
- Apoio da **ferramenta TFS** para gerenciamento das revisões.

# Desenvolvedor

The screenshot shows the Visual Studio Code interface for a developer. On the left, a code editor displays CSS code with validation error messages. The right-hand side features a 'New Code Review' panel for 'Fabrikam Fiber'. The panel includes a search bar, a video link, and instructions to select reviewers. A dropdown menu shows 'Johnnie McLeod' as the selected reviewer. Below this, the review details are visible: 'Hello World border color' for 'Fabrikam Fiber' with the comment 'Changed the border color to #ddd'. At the bottom, the 'Submit Request' button is highlighted with an orange circle.

```
or validation helpers */
ation-error {
#b94a48;

ation-valid {
: none;

-validation-error {
1px solid #ddd;

"checkbox"].input-validation-error {
0 none;

-summary-errors {
#b94a48;

-summary-valid {
: none;
```

Team Explorer - New Code Review

New Code Review | Fabrikam Fiber

Streaming Video: Using Code Review to improve qual

1 edit(s) | [View Changes](#)

Select one or more reviewers to review your changes and enter a comment for them if appropriate

Johnnie McLeod

Add Reviewer | Press Enter to add this reviewer

Hello World border color

Fabrikam Fiber

Changed the border color to #ddd

**Submit Request** [Cancel](#)

Related Work Items

# Revisor de Código

The screenshot shows the Visual Studio Code interface for a reviewer. The right-hand side features a 'Code Review' panel for 'Fabrikam Fiber'. The panel displays the review details: 'Hello World border color' requested by 'Jamal Hartnett'. A 'Send Comments' button is visible. Below, the reviewer can 'Send & Finish' the review, with options to 'View Shelveset' or 'Actions'. A note states: 'You can **Accept** or Decline to let the requestor know whether you will do the code review.' The 'Accept' button is highlighted with an orange circle. The 'Reviewers (2)' section shows 'Johnnie McLeod - Requested' and 'Raisa Pokrovskaya - Accepted'. The 'Related Work Items' section is also visible.

Team Explorer - Code Review

Code Review | Fabrikam Fiber

Hello World border color

Requested by Jamal Hartnett.

[Send Comments](#)

[Send & Finish](#) | [View Shelveset](#) | [Actions](#)

You can **Accept** or Decline to let the requestor know whether you will do the code review.

Reviewers (2)

[Add Reviewer](#)

Johnnie McLeod - Requested

Raisa Pokrovskaya - Accepted

Related Work Items



## 6.5 Tratamento de Vulnerabilidades 🔥

- Utilização da ferramenta **SonarLint** para apoio do processo de **análise estática**.
- E utilização da ferramenta **SonarQube** para apoio do processo de **análise dinâmica**.
- **Priorização** da correção das vulnerabilidades.



D

Reliability Rating on New Code is worse than A

Bugs & Vulnerabilities

Leak Period: since previous version started 8 days ago

58 D

Bugs

8 C

Vulnerabilities

25 D

New Bugs

0 A

New Vulnerabilities

Code Smells

27d A

Debt

started 8 days ago

2.4k

Code Smells

10d A

New Debt

918

New Code Smells

Duplications



8.6%

Duplications

227

Duplicated Blocks

0.0%

Duplications on 115 New Lines

# BotBuilder

24 октября 2016 г., 17:20 Version 1.2

Issues Measures Code Administration ▾

Issues

Effort

## Type

Bug	63
Vulnerability	0
Code Smell	0

## Resolution

Unresolved	63	Fixed	1
False Positive	0	Won't fix	0
Removed	63		

## Severity

## Status

## New Issues

## Rule

## Tag

cert	310
cwe	298
unused	256
pitfall	79
pvs-studio	63
pvs-studio#ga	63
misra	31
owasp-a1	11
owasp-a2	11

▲ 1 / 63 ▾

Reload

New Search

Bulk Change

BotBuilder Library/Dialogs/BotData.cs

V3072: The 'ConnectorStore' class containing IDisposable members does not itself implement IDisposable.

3 минуты назад ▾ L178 ⚙️ 🔍 ▾

Inspect: stateClient. ...

Bug ▾ Major ▾ Open ▾ Not assigned ▾ 15min effort Comment

pvs-studio, pvs-studio#ga ▾

BotBuilder Library/Dialogs/BotToUser.cs

V3072: The 'AlwaysSendDirect\_BotToUser' class containing IDisposable members does not itself implement

3 минуты назад ▾ L45 ⚙️ 🔍 ▾

IDisposable. Inspect: client. ...

Bug ▾ Major ▾ Open ▾ Not assigned ▾ 15min effort Comment

pvs-studio, pvs-studio#ga ▾

V3072: The 'BotToUserTextWriter' class containing IDisposable members does not itself implement IDisposable.

3 минуты назад ▾ L89 ⚙️ 🔍 ▾

Inspect: writer. ...

Bug ▾ Major ▾ Open ▾ Not assigned ▾ 15min effort Comment

pvs-studio, pvs-studio#ga ▾

BotBuilder Library/Dialogs/DialogTask.cs

V3072: The 'PersistentDialogTask' class containing IDisposable members does not itself implement

3 минуты назад ▾ L388 ⚙️ 🔍 ▾

IDisposable. Inspect: client. ...

Bug ▾ Major ▾ Open ▾ Not assigned ▾ 15min effort Comment

pvs-studio, pvs-studio#ga ▾

V3072: The 'PostUnhandledExceptionToUserTask' class containing IDisposable members does not itself

3 минуты назад ▾ L442 ⚙️ 🔍 ▾

implement IDisposable. Inspect: trace. ...



Bug ▾ Major ▾ Open ▾ Not assigned ▾ 15min effort Comment

pvs-studio, pvs-studio#ga ▾

BotBuilder Library/Dialogs/PromptDialog.cs

```
/* Strategy
 * 1. Replace the structure, if any, with a structure that will not be reformatted
 * 2. Remove formatting from the resulting trivia
 */
SyntaxTrivia result = trivia;
```

Remove this useless assignment to local variable 'result'. [...](#)

20 days ago ▾ L83  

 Bug ▾  Major ▾  Open ▾ Not assigned ▾ 15min effort [Comment](#)

 cert, cwe, suspicious, unused ▾

```
if (trivia.HasStructure)
{
    // GetStructure() returns SyntaxNode instead of StructuredTriviaSyntax. For C# code, this should always
    // be an actual instance of StructuredTriviaSyntax, but we handle the case where it is not by leaving
    // the structure node unaltered rather than throwing some sort of exception.
    StructuredTriviaSyntax structure = trivia.GetStructure() as StructuredTriviaSyntax;
    if (structure != null)
    {
        result = SyntaxFactory.Trivia(structure.WithoutFormatting());
    }
}
```

Remove this useless assignment to local variable 'result'. [...](#)

20 days ago ▾ L92  

 Bug ▾  Major ▾  Open ▾ Not assigned ▾ 15min effort [Comment](#)

 cert, cwe, suspicious, unused ▾

```
    }
}

return WithoutFormattingImpl(trivia);
}
```





## Considerações **Finais**

1. Construção de um processo de **desenvolvimento seguro adequado**. 🙌
2. Utilizar ferramentas para **automatização** do processo, mas cuidado com as configurações. 🛠️
3. Se você tem tempo, **comece agora e pequeno** com o que já possui. ⌚
4. Conheça as **falhas do processo** e prefira **conscientizar as pessoas** do que burocratizar. ❌
5. Invista em pessoas para atuarem como **porta-voz** do processo. 👓



## Considerações **Finais**

1. ~~Construção de um processo de desenvolvimento seguro adequado.~~ 🙅
2. Utilizar ferramentas para **automatização** do processo, mas cuidado com as configurações. 🔧
3. Se você tem tempo, **comece agora e pequeno** com o que já possui. ⌚
4. Conheça as **falhas do processo** e prefira **conscientizar as pessoas** do que burocratizar. ❌
5. Invista em pessoas para atuarem como **porta-voz** do processo. 👓



## Considerações **Finais**

1. ~~Construção de um processo de desenvolvimento seguro adequado.~~ 🖐️
2. ~~Utilizar ferramentas para automatização do processo, mas cuidado com as configurações.~~ 🛠️
3. Se você tem tempo, **comece agora e pequeno** com o que já possui. 🕒
4. Conheça as **falhas do processo** e prefira **conscientizar as pessoas** do que burocratizar. ❌
5. Invista em pessoas para atuarem como **porta-voz** do processo. 👓



## Considerações **Finais**

1. ~~Construção de um processo de desenvolvimento seguro adequado.~~ 🙌
2. ~~Utilizar ferramentas para automatização do processo, mas cuidado com as configurações.~~ 🛠️
3. ~~Se você tem tempo, comece agora e pequeno com o que já possui.~~ ⌚
4. Conheça as **falhas do processo** e prefira **conscientizar as pessoas** do que burocratizar. ❌
5. Invista em pessoas para atuarem como **porta-voz** do processo. 👓



## Considerações **Finais**

1. ~~Construção de um processo de desenvolvimento seguro adequado.~~ 🖐️
2. ~~Utilizar ferramentas para automatização do processo, mas cuidado com as configurações.~~ 🔧
3. ~~Se você tem tempo, comece agora e pequeno com o que já possui.~~ ⌚
4. ~~Conheça as falhas do processo e prefira conscientizar as pessoas do que burocratizar.~~ ❌
5. Invista em pessoas para atuarem como **porta-voz** do processo. 👓



# Obrigada!

*Alguma pergunta ?*

Você pode me encontrar no twitter como: @dlpitta