

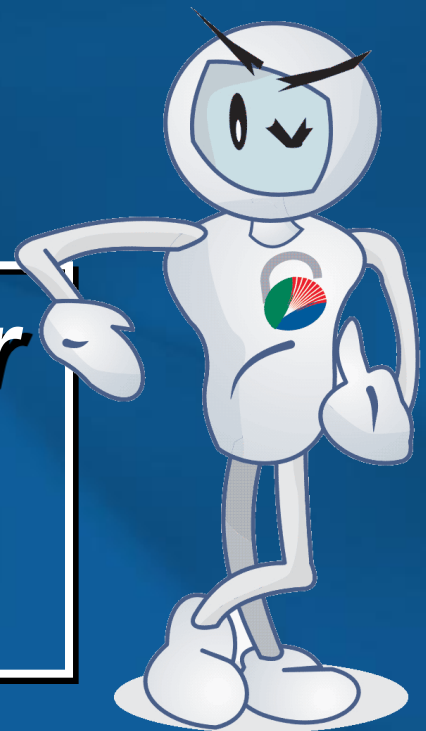
Ambiente de Segurança Corporativa

Francisco José Barreto Nunes - MSc., CISM, CSSLP



***Banco do
Nordeste***

***Institucionalizar
Segurança no
RUP-BNB***



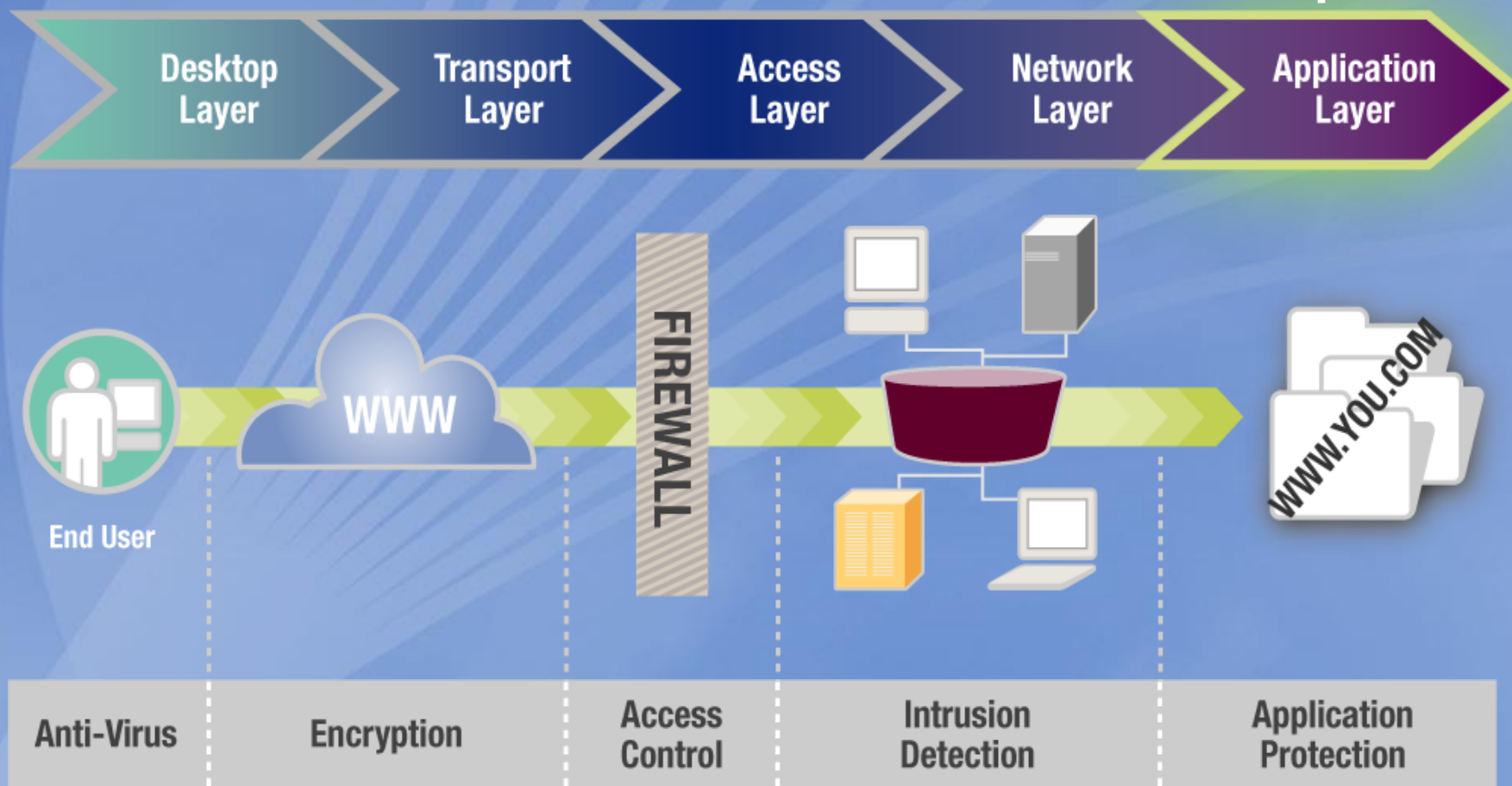
- Desafio;
- Objetivos;
- Benefícios;
- Cronograma;
- Resultados atuais;
- Dificuldades; e
- Lições aprendidas.



Banco do
Nordeste

Desafio

70% dos
ataques



Fonte: GARTNER



Banco do
Nordeste

Objetivos

- Otimizar o uso de recursos de acordo com as necessidades de segurança (análise de riscos);
- Melhorar a segurança dos aplicativos; e
- Reorganizar práticas de desenvolvimento visando atender requisitos de segurança.



**Banco do
Nordeste**

Benefícios

- **Melhoria na produtividade dos colaboradores;**
- **Elevar satisfação dos clientes; e**
- **Mitigar possíveis perdas financeiras e danos à imagem, decorrentes de incidentes de indisponibilidade, perda de confidencialidade, e perda de integridade das informações.**



Banco do
Nordeste

Cronograma

- **Etapa 1: (Concluída)**
 - Conscientização e educação.
- **Etapa 2: (Concluída e Aprovada)**
 - Adaptar artefatos do RUP-BNB;
 - Organizar ações de segurança na disciplina Requisitos.
- **Etapa 3: (Iniciada)**
 - Realizar projeto piloto;
 - Avaliar resultado, aperfeiçoar ações de segurança;
 - Identificar novas necessidades.



Banco do
Nordeste

Resultados atuais

- Inclusão de seções sobre segurança nos artefatos: Visão e Especificação Suplementar;
- Guia de orientação sobre falhas de segurança em aplicativos;
- Ações de segurança inseridas para subsidiar a disciplina Requisitos:
 - Atividade “Definir o Sistema” => Tarefa “Desenvolver Especificação Suplementar” => Etapas “Identificar Necessidades de Segurança” e “Capturar Requisitos de Segurança;”
 - Atividade “Definir uma Sugestão de Arquitetura” => Tarefa “Identificar Padrões de Segurança.”



Banco do
Nordeste

Visão

		Visão <Nome do projeto>	Página: de Data Alteração: 0/0/0000 0:00 AM Versão: <x>
CONTEÚDO			
1. Introdução			3
1.1	Finalidade		3
1.2	Referências		3
2. Contextualização do Problema			3
2.1	Descrição do Problema		3
2.2	Oportunidade de Negócio		3
3. Descrição dos Stakeholders e Usuários			3
3.1	Stakeholders Relevantes		3
3.2	Usuários		3
3.3	Principais Necessidades dos Stakeholders ou dos Usuários		3
4. Visão Geral do Produto			3
5. Requisitos Preliminares			3
5.1	Atores		3
5.2	Casos de Uso		3
6. Criticidade, Premissas, Riscos e Restrições			3
6.1	Criticidade		3
6.2	Premissas		3
6.3	Riscos		3
6.4	Restrições		3





Banco do
Nordeste

Especificação Suplementar

3.	Confiabilidade	2
3.1	Maturidade	2
3.2	Tolerância a Falhas	2
3.3	Recuperabilidade	2
3.4	Políticas de Backup	2
3.5	Disponibilidade	2
4.	Desempenho	2
4.1	Tempo de Resposta	2
4.2	Eficiência	2
4.3	Capacidade	2
5.	Suportabilidade	2
5.1	Testabilidade	2
5.2	Manutenibilidade	2
5.3	Extensibilidade	2
5.4	Adaptabilidade	2
5.5	Compatibilidade	2
5.6	Configurabilidade	2
5.7	Instabilidade	2
5.8	Localizabilidade	2
5.9	Padrão de Codificação	2
6.	Segurança	2
6.1	Identificação e Autenticação	2
6.2	Controle de acesso	2
6.3	Integridade de dados	2
6.4	Gerenciamento de exceções	2
6.5	Controle de sessão	2
6.6	Canais de comunicação	2
6.7	Auditoria	2
6.8	Gerência de Configuração	2
6.9	Uso do correio eletrônico pelo aplicativo	2
6.10	Outros	2
7.	Restrições de Design	2
7.1	<Restrição de Design 1>	2



Banco do
Nordeste

Guia de Orientação



Falhas de Segurança em Aplicativos

Página: 1 de 33

Data Alteração:

4-Oct-10

Versão: 02

CONTEÚDO

1. Introdução	4
1.1 Finalidade	4
1.2 Contextualização	4
1.3 Brainstorming	4
1.4 Referências	5
2. Problemas Comuns	5
2.1 Falhas de Autenticação e de Controle de Sessão	5
2.2 Falhas de Injeção de Código	7
2.3 Falhas de Divulgação de Informação	9
2.4 Referência Insegura à Objeto	10
2.5 Criptografia Insegura	11
3. Descrição Geral das Vulnerabilidades Especificadas	12
3.1 Falhas de Autenticação e de Controle de Sessão	12
3.2 Injeção de Código	14
3.3 Falhas de Divulgação de Informação	14
3.4 Referência Insegura à Objeto	15
3.5 Criptografia Insegura	15
3.6 Atores (Invasores ou Atacantes)	17
3.7 Pré-condições	17
3.8 Pós-condições	20
3.9 Considerações gerais	30
4. Correlações e Referências	31
4.1 Correlações	31
4.2 Referências	31



Banco do
Nordeste

Exemplo da Ação de Segurança

The screenshot displays the Banco do Nordeste Intranet interface. At the top, the bank's logo and name are visible. Below the header, a breadcrumb trail reads: RUP_BNB_Revisao > Iniciação > Iteração da Iniciação > Definir o Sistema > Desenvolver Especificações Suplementares. The main heading is 'Tarefa: Desenvolver Especificações Suplementares'. A description states: 'Essa tarefa captura os requisitos não funcionais que não se aplicam a casos de uso específicos.' A list of expandable sections includes: Objetivo, Relacionamentos, Descrição Principal, and Etapas. The 'Etapas' section is expanded, showing a list of tasks: 'Capturar os Requisitos Funcionais que não são específicos de caso de uso', 'Capturar Qualidades do Sistema', 'Capturar Restrições', 'Capturar Requisitos de Conformidade', 'Capturar Requisitos de Documentação', and 'Capturar Requisitos de Segurança'. A red arrow points to the 'Capturar Requisitos de Segurança' item. Below this list, a paragraph explains that categorizing security requirements involves researching protection and prevention techniques, and determining which can be applied to the application architecture. It also mentions a premise that analysts should verify the reference document for additional security requirements.

RUP_BNB_Revisao > Iniciação > Iteração da Iniciação > Definir o Sistema > Desenvolver Especificações Suplementares

Tarefa: Desenvolver Especificações Suplementares

Essa tarefa captura os requisitos não funcionais que não se aplicam a casos de uso específicos.

- Objetivo
- Relacionamentos
- Descrição Principal
- Etapas
 - Expandir Todas as Etapas / Reduzir Todas as Etapas
 - Capturar os Requisitos Funcionais que não são específicos de caso de uso
 - Capturar Qualidades do Sistema
 - Capturar Restrições
 - Capturar Requisitos de Conformidade
 - Capturar Requisitos de Documentação
 - Capturar Requisitos de Segurança

Categorizar requisitos de segurança pode envolver:

- Pesquisar técnicas de proteção de sistema e de prevenção de ameaça
- Determinar quais técnicas podem ser aplicadas à arquitetura do aplicativo

Uma premissa é que os analistas verifiquem o documento de referência, contendo propostas de requisitos de segurança, na diretriz "Requisitos de Segurança" do RUP-BNB a fim de identificar requisitos adicionais.

Intranet local 100%



Banco do
Nordeste

Diretriz Requisitos de Segurança



Procurar este Site:

Diretriz: Requisitos de Segurança



Relacionamentos

Elementos Relacionados	Desenvolver Especificações Suplementares
------------------------	--

[Voltar ao Início da Página](#)

Descrição Principal

Este documento tem por objetivo prover um conjunto de boas práticas para Requisitos de Segurança, o qual referencia, de forma integral, o Anexo XIII, do [Manual Básico - Segurança da Informação](#).

Posteriormente, e de acordo com uma evolução conjunta dos ambientes de Sistema de Informação e de Segurança Corporativa, serão incorporadas novas orientações e requisitos de segurança, diretamente nas atividades do processo de desenvolvimento. Esses novos aspectos de segurança irão refletir diretamente em adaptações de *templates*, como o documento de Especificação Suplementar, e a inclusão de atividades específicas no processo que deverão ser identificadas conjuntamente pelas duas unidades

O documento PDF está disponível.



Dificuldades

- Sensibilizar gestores sobre a importância de se considerar segurança desde o planejamento do projeto de desenvolvimento.
 - Cultura de segurança é essencial para atingir objetivos de segurança de projetos e evitar atrasos.
- Identificar ações de segurança que deveriam ser realizadas juntamente com as atividades do processo sem causar atraso de projetos.
 - Balancear obrigações extras originadas das novas ações.
- Elevar o nível de conhecimento sobre segurança da informação e segurança de software entre colaboradores envolvidos com o processo de desenvolvimento.
 - Educação em segurança contribui com a execução do projeto e a qualidade dos resultados.



Banco do
Nordeste

Lições aprendidas

- Equipe de desenvolvimento precisa pensar como as funcionalidades poderiam ser comprometidas ou usurpadas;
- O Guia de orientação é ferramenta valiosa de conscientização e de integração de fases, disciplinas e equipes;
- O Guia contribui para a integração do projeto, arquitetura e teste com a estruturação dos requisitos de segurança, permitindo identificar o impacto das vulnerabilidades e ameaças de forma a evitar que problemas de segurança passem despercebidos.

Ambiente de Segurança Corporativa

franzenunes@bnb.gov.br
fcojbn@yahoo.com.br



***Banco do
Nordeste***

Obrigado!

