Blindando las aplicaciones con IBM Rational Appscan Demostración y Caso de Éxito

Renan Rafael Silva Rubio
Subdirector de Seguridad Informática, Banorte

Ariel Súcari
Director de Operaciones, Itera
ariel.sucari@iteraprocess.com

Innovate2010
The Rational Software Conference

Let's build a smarter planet.

The premiere software and product delivery event.
4 de Noviembre, Madrid

itera
it & business process

Agenda

1. Introducción a la problemática de la seguridad de aplicaciones
2. Estrategia de solución: Procesos + Herramientas + Personas
3. Demostración de la solución
4. Banorte: Caso de éxito
5. Q&A

Robo tradicional

Fraude digital

Titulares

Irán sufre el mayor ataque cibernético de su historia

Israel puede haber creado un virus de una gran potencia, el Stuxnet, diseñado para intentar frenar el programa nuclear iraní

★★★★☆ 18 votos | 25 comentarios

HENRIQUE CYMERMAN | Jerusalén. Corresponsal | 28/09/2010 | Actualizada a las 00:43h | Internacional

Irán sufrió ayer lo que, de confirmarse, sería el **ataque cibernético más grande de la historia**. Los sistemas de control de la central nuclear de Bushehr, así como de otras industrias, se vieron afectados por un **virus de una potencia sin precedentes**, denominado **Stuxnet**.

Un troyano en un lápiz de memoria

Guy Mizrahi, antiguo hacker, afirma que es posible derribar toda una red de ordenadores solamente con un lápiz de memoria. "El virus lanzado sobre Irán penetra en los sistemas informáticos y detecta sus puntos débiles. Luego se multiplica a sí mismo, pasando de un ordenador a otro, instala programas troyanos de espionaje para recoger información, y puede dañar tanto webs como sistemas operativos".

Expertos israelíes consultados por *La Vanguardia* afirman que el **Stuxnet ha sido diseñado para intentar frenar el programa nuclear iraní**. Dada su complejidad sin precedentes es imposible que haya sido creado por un hacker en solitario. Todo apunta a un equipo de profesionales que han tenido medios y dinero suficiente y, al menos, seis meses de tiempo para prepararlo.

Las fuentes consultadas por este diario afirman que sólo Israel y Estados Unidos disponen de los recursos necesarios para crear un virus tan agresivo y complejo como el **Stuxnet**.

Titulares

SON LOS AUTORES DEL ATAQUE A LA PÁGINA DE IZQUIERDA UNIDA

Detenidos en España cinco de los 'hackers' más activos del mundo, dos de ellos menores

- Firmaban sus ataques con los seudónimos 'ka0x, an0de, xarnuz y Piker'
- Dos de ellos son hermanos y otros dos tienen sólo 16 años
- Vivían en Sabadell, Burgos, Málaga y Valencia y se coordinaban a través de Internet
- Habían atacado más de 21.000 páginas y ocupaban el 5º puesto en un ránking mundial

España, Mayo 19, 2008

Titulares

Detenido un hacker en España

A raíz de una denuncia presentada por el Ayuntamiento de Riotinto (Huelva), ha sido detenido un cibercriminal en Huelva que, supuestamente, habría vulnerado la seguridad electrónica de más de un millar de personas.

HUELVA, España, Marzo 27, 2009

Titulares

Filtran datos de 6 millones de chilenos en internet

Hacker sube datos personales de 6 millones de chilenos a internet para demostrar lo mal protegida que está la información en su país

SANTIAGO DE CHILE, Chile, mayo 11, 2008

Titulares

'Hackean' portal de Internet de Hacienda

Hacker de origen turco interviene portal de Internet de la Secretaría de Hacienda; la página conduce a sitios con contenidos en turco

CIUDAD DE MÉXICO, México, mar. 5, 2005

Imagen del portal principal de la SHCP, que fue 'hackeada'.

Titulares

Hacker roba más de 130 millones de números de tarjetas de crédito y débito

"Es el mayor caso de delitos informáticos y de robo de identidad procesado sobre números de tarjetas de crédito y débito"

Los objetivos fueron las redes de Heartland Payment Systems (un procesador de pagos en Princeton), 7-Eleven, Hannaford Brothers, una cadena regional de supermercados y otros dos minoristas.
El robo de tarjetas de crédito y débito números fueron vendidos en línea, y algunos se utilizaron para hacer compras no autorizadas y retirar dinero de bancos.

Los ataques en línea se aprovecharon de las fallas de seguridad en SQL y González utilizaba programas "sniffer" sobre redes corporativas que interceptan transacciones con tarjeta de crédito

Titulares

Durante 17 meses, alguien tenía acceso libre a las computadoras de TJX Companies. Sin que nadie lo notara, más y más código se instaló en los equipos de la cadena minorista de descuentos para descubrir, recolectar y transmitir información de las tarjetas de crédito y débito de sus clientes, que representaban más de **45.7 millones de dólares**.

Amenazas, riesgos e impactos

Amenazas por parte de…

- Empleados
- Proveedores
- Socios de Negocio.
- Hackers
- Competidores
- ¿Enemigos?

Riesgos

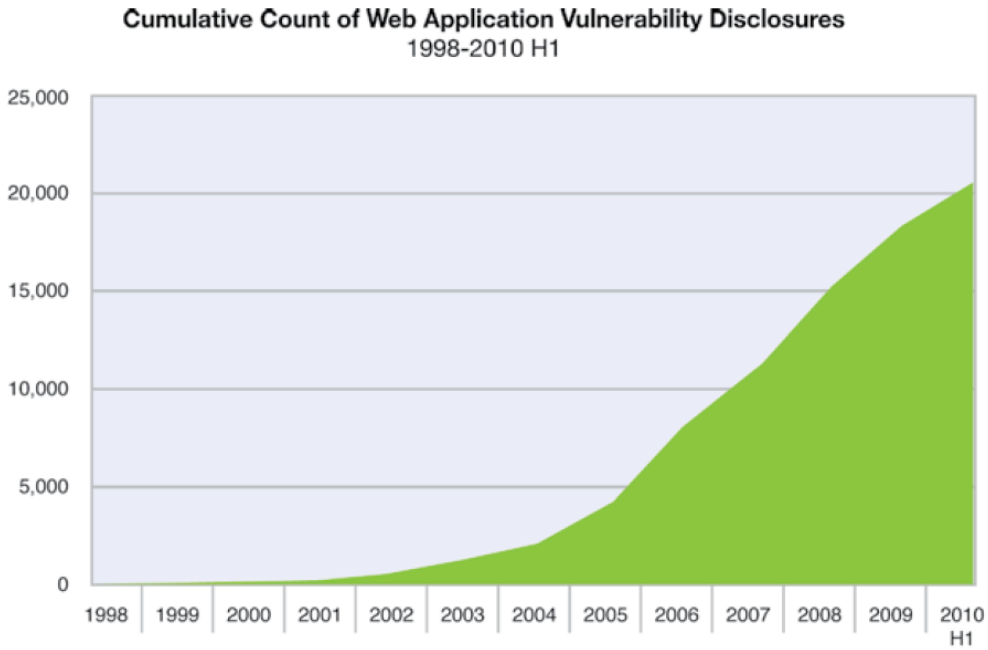
- Robo o alteración de información
- Fuga de información
- Fraudes
- Deterioro de niveles de servicio.
- Imposibilidad para entregar servicios.
- Falta de elementos para fincar responsabilidades
- Robo de identidades

Impactos

- Pérdida de credibilidad o confianza (*imagen*)
- Pérdida de ingresos (*finanzas*)
- Pérdida de oportunidades (*posicionamiento*)
- Incumplimiento de regulaciones (*legalidad*)

Los hackers se enfocan en aplicaciones WEB

- 54.9% de las vulnerabilidades pertenecen a las aplicaciones WEB
- El ataque de SQL injection se ha incrementado 30 veces en los últimos 6 meses
- El 74% de las vulnerabilidades detectadas en 2008 no habían podido solucionarse para el final de ese mismo año.



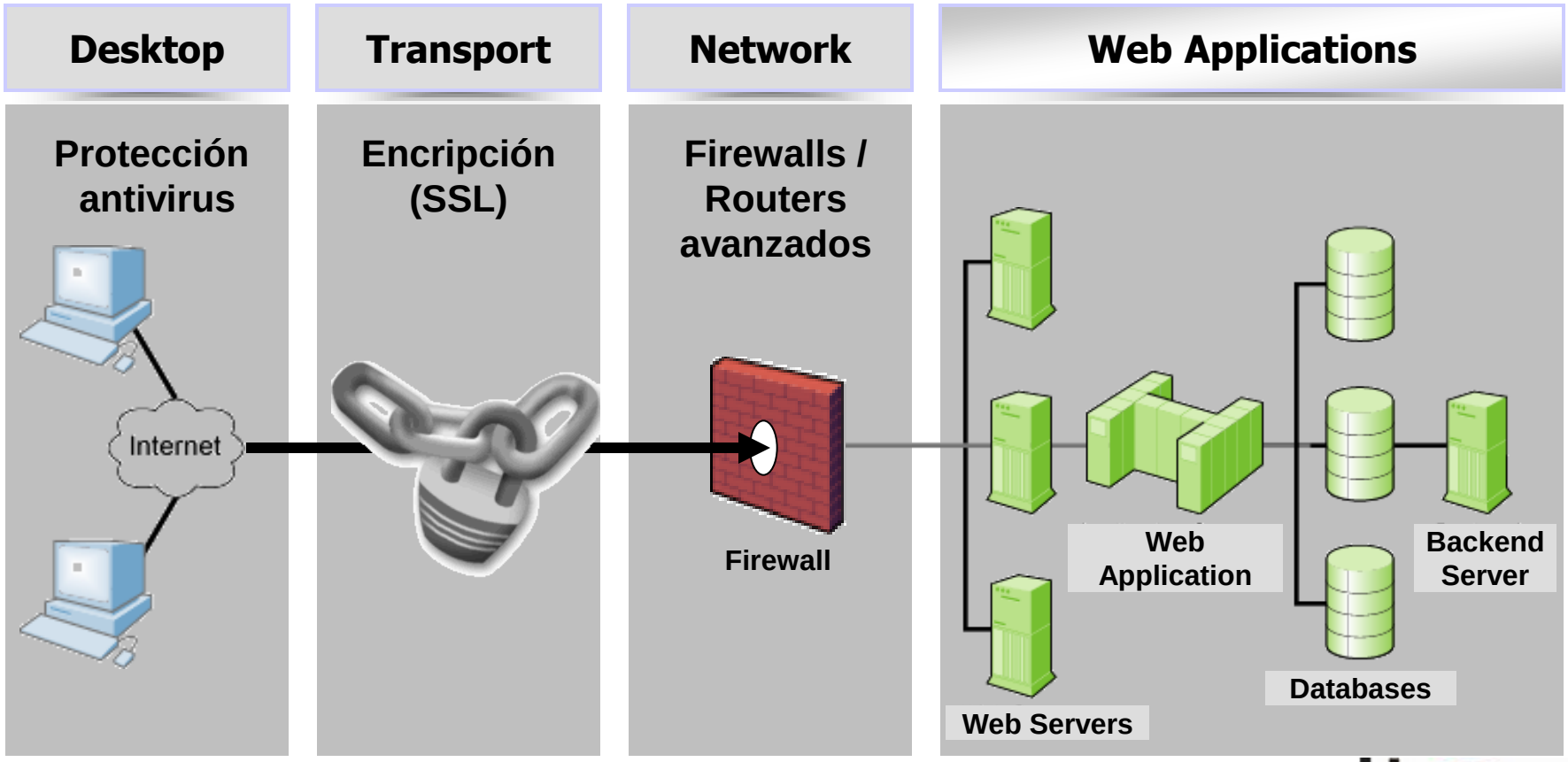
El mito: “Nuestro sitio es seguro”

Tenemos firewalls

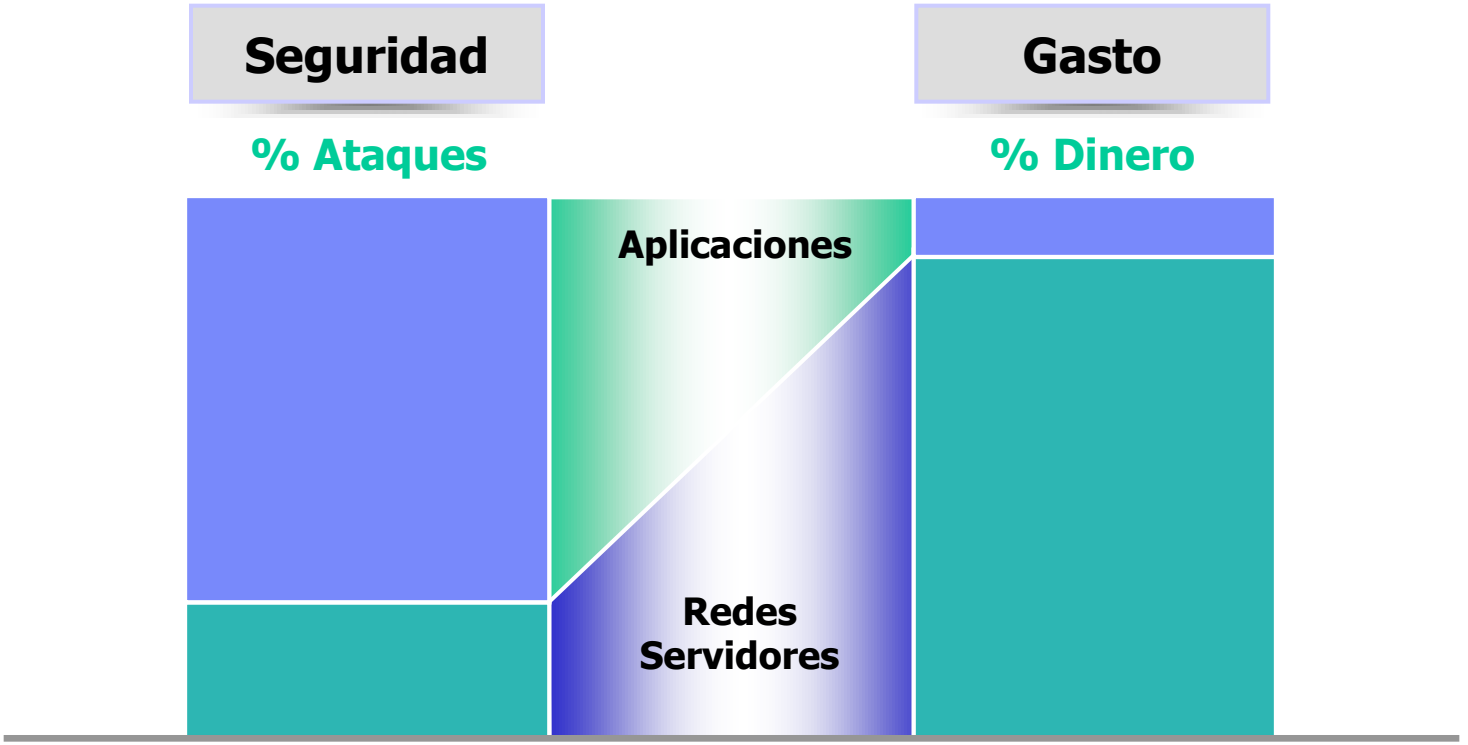
Auditamos cada cuarto con pruebas de penetración

Usamos herramientas para revisar nuestra red

La seguridad de aplicaciones requiere de una estrategia diferente



El gasto en seguridad está desbalanceado



75% De los ataques a la seguridad de la información están dirigidos a la capa WEB

2/3 De las aplicaciones WEB son vulnerables

Problemática

"You know, you can do this just as easily online."

Algunos datos

- **"El 64% de los desarrolladores no confía en sus habilidades para escribir aplicaciones seguras" -** *Microsoft Developer Research*

- ***"El fraude digital crece a tasa del 300% anual, hoy el 94% del monto robado en Estados Unidos es digital"***. – *Federal Trade Commission Identity Test Report*

- **"Las compañías plnean superar los retos en lo que a seguridad de TI respecta:**
  - **Incrementando el entrenamiento (55% de los encuestados)**
  - **Mejorando los procesos (54% de los encuestados)**
  - **Encontrando soluciones de codificación seguras para introducir dentro de sus flujos de trabajo (40% de los encuestados)"** – *Aberdeen Group, May 2007*

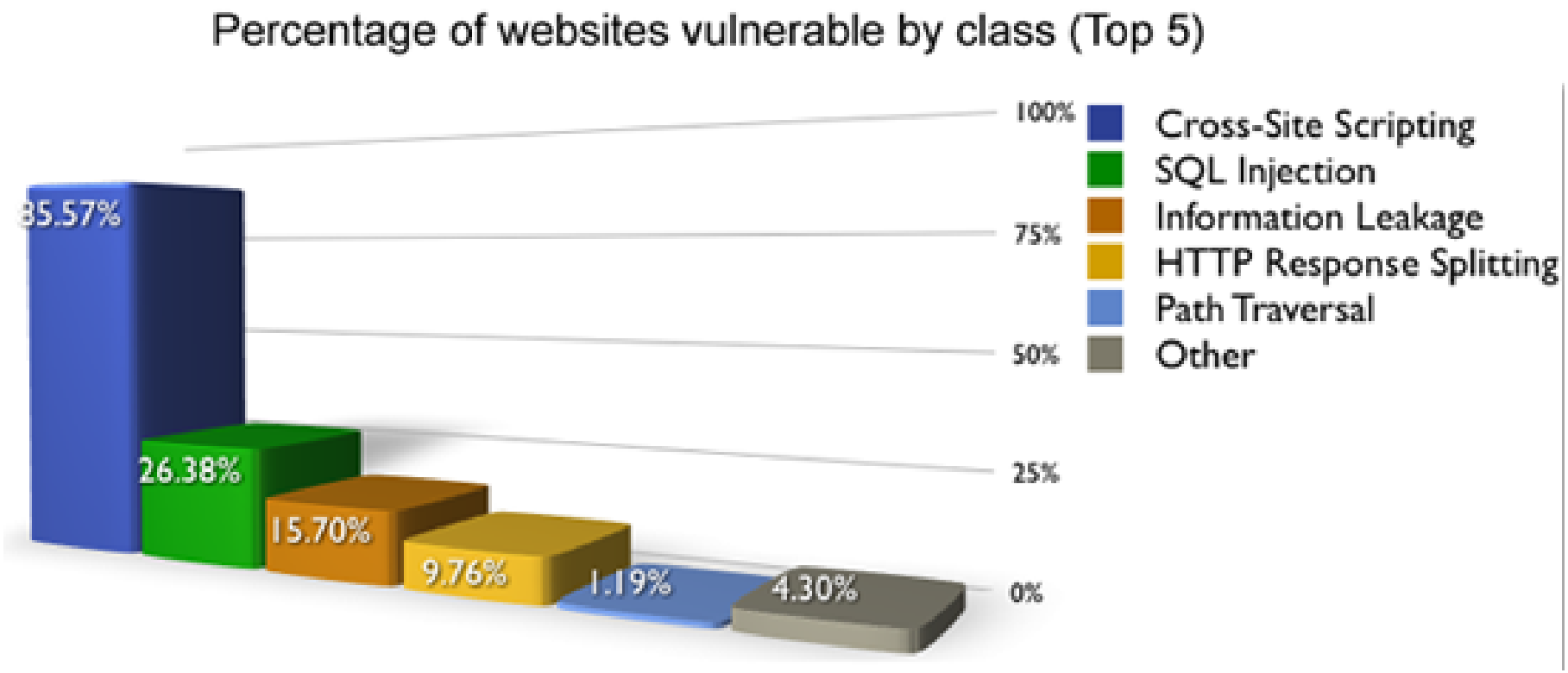
El top 10 de OWASP

- Open Web Application Security Project – una organización abierta dedicada a la lucha contra el Software inseguro.
- El top 10 de OWASP representa un amplio consenso acerca de las principlales vulnerabilidades en cuestión de aplicaciones WEB.
- Usaremos esta lista para cubrir algunos de los más comunes problemas de seguridad de las aplicacioens WEB.

Amenaza	Impacto	Ejemplo
Cross Site scripting	Robo de identidad, salida de información delicada	Los hackers pueden hacerse pasar por usuarios legítimos y controlar sus cuentas.
Injection Flaws	El atacante puede manipular consultas a la base de datos, protocolo ligero de acceso a directorios (LDAP), otros sistemas	Hackers can access backend database information, alter it or steal it.
Malicious File Execution	Ejecutar archivos de comando en el servidor hasta lograr control total	El sitio fue modificado para mandar cualquier interacción al hacker.
Insecure Direct Object Reference	El atacante puede acceder cualquier archivo y recurso	La aplicación WEB devuelve información de un archivo importante (en lugar de uno inofensivo)
Cross-Site Request Forgery	El atacante puede enviar transacciones “ciegas” como si fuera un uasuario autorizado	Las peticiones ciegas solicitan transferencias a la cuenta del hacker
Information Leakage and Improper Error Handling	Los atacantes pueden obtener información sobre el sistema detallada	Un error mal escrito o atrapado puede ayudar al hacker en desarrollar futuros ataques.
Broken Authentication & Session Management	Sesiones no guardadas o invalidadas correctamente	El hacker puede forzar a que una sesión pueda reanudarse a pesar de que el usuario haya terminado.
Insecure Cryptographic Storage	Técnicas de encripción débiles pueden ser rotas y descifradas	Información confidencial (SSN, tarjetas) puede ser desencriptada por usuarios mal intencionados
Insecure Communications	Información sensitiva es enviada a traves de canales desencriptados e inseguros	Credenciales desencriptadas pueden ser interceptadas por el hacker para hacerse pasar por el usuario
Failure to Restrict URL Access	El hacker puede acceder recursos no autorizados	El hacker puede acceder cualquier página pasando la de ingreso al sistema


DEMO

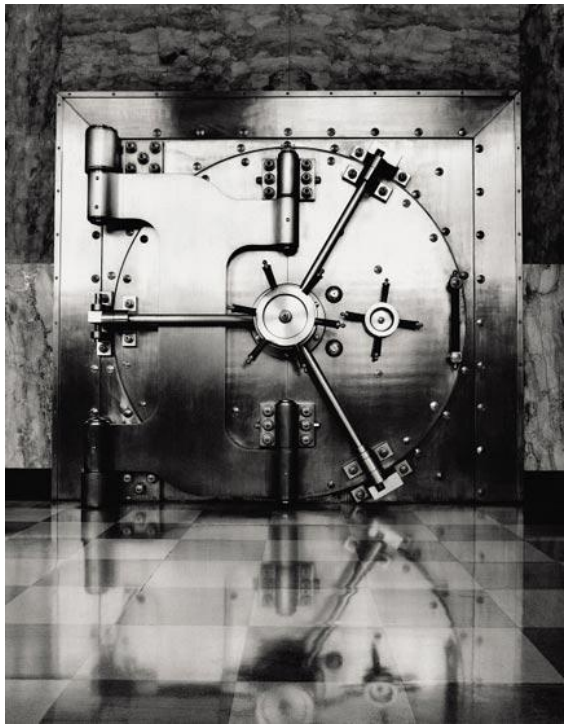
Estadísticas de vulnerabilidades (31,373 Sites)



** http://www.webappsec.org/projects/statistics/

IBM Rational Appscan

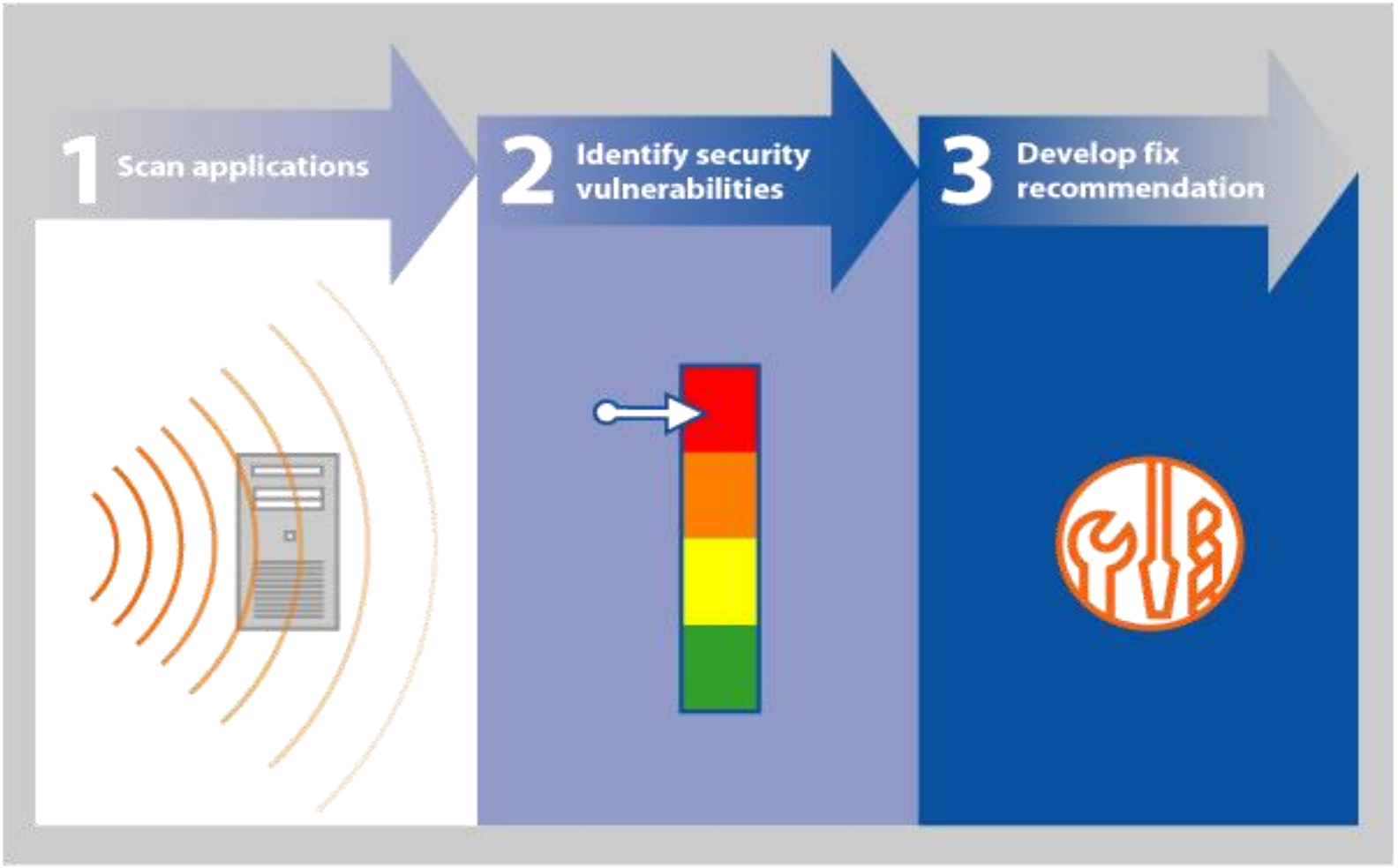
- El líder del mercado indiscutido
  - Ubicado en el #1 del mercado por IDC
  - #1 en numerosas revistas de la industria
- Revisa aplicaciones de manera automática en búsqueda de vulnerabilidades
  - SQL Injection
  - Cross-site Scripting
- Provee recomendaciones acerca de cómo reparar las vulnerabilidades encontradas
  - Limpieza de caracteres



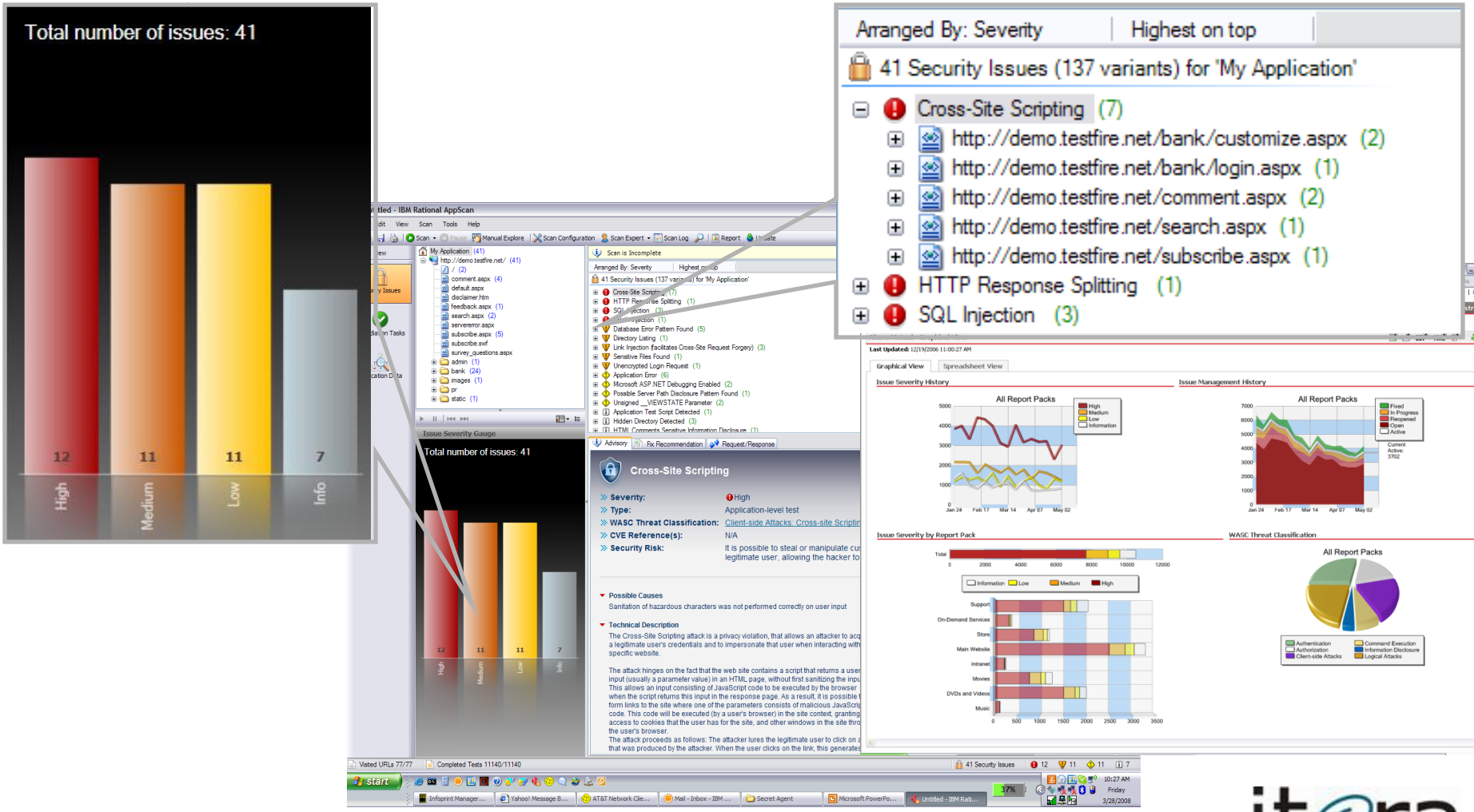
¿El resultado?

Mejora la seguridad, costos menores, y la habilidad de cumplir con PCI, SOX, CNBV y otros estándares

¿Cómo lo hace?


1 Scan applications
2 Identify security vulnerabilities
3 Develop fix recommendation

Reportes


Total number of issues: 41
12
11
11
7
High
Medium
Low
Info
Arranged By: Severity
Highest on top
41 Security Issues (137 variants) for 'My Application'
Cross-Site Scripting (7)
http://demo.testfire.net/bank/customize.aspx (2)
http://demo.testfire.net/bank/login.aspx (1)
http://demo.testfire.net/comment.aspx (2)
http://demo.testfire.net/search.aspx (1)
http://demo.testfire.net/subscribe.aspx (1)
HTTP Response Splitting (1)
SQL Injection (3)
Cross-Site Scripting
Severity: High
Type: Application-level test
WASC Threat Classification: Client-side Attacks: Cross-site Scripting
CVE Reference(s): N/A
Security Risk:
Possible Causes
Technical Description
Issue Severity History
Issue Management History
Issue Severity by Report Pack
WASC Threat Classification
All Report Packs

Entendiendo el problema

Advisory | Fix Recommendation | Request/Response

Cross-Site Scripting

- **Severity:** High
- **Type:** Application-level test
- **WASC Threat Classification:** Client-side Attacks: Cross-site Scripting
- **CVE Reference(s):** N/A
- **Security Risk:** It is possible to steal or manipulate customer session and cookies, which may be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Possible Causes

Sanitation of hazardous characters was not performed correctly on user input

Technical Description

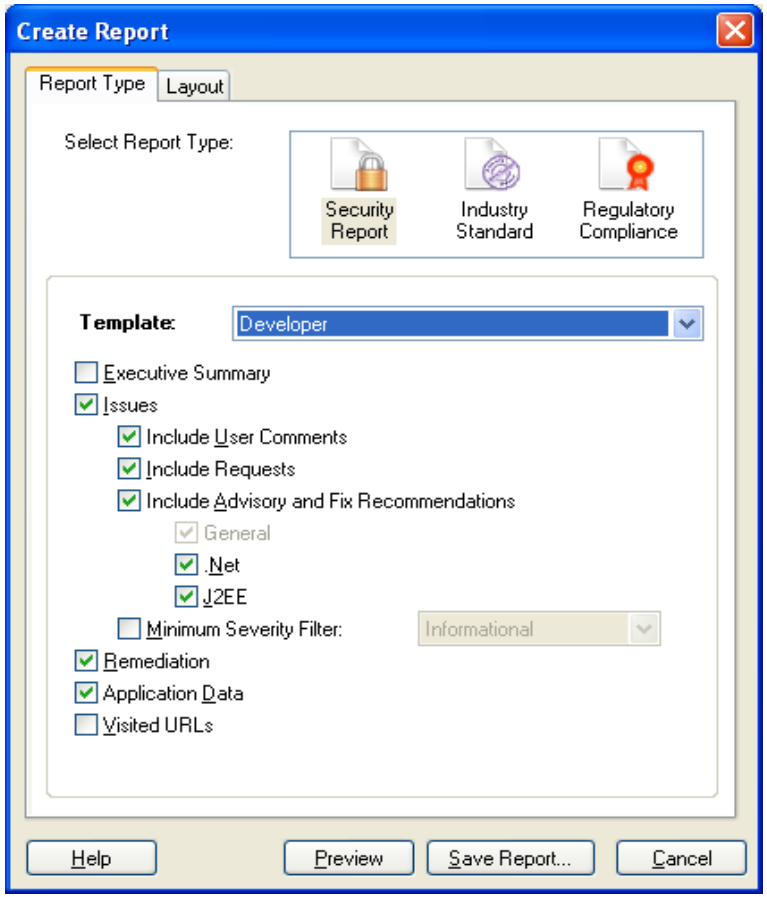
The Cross-Site Scripting attack is a privacy violation, that allows an attacker to acquire a legitimate user's credentials and to impersonate that user when interacting with a specific website.

The attack hinges on the fact that the web site contains a script that returns a user's input (usually a parameter value) in an HTML page, without first sanitizing the input. This allows an input consisting of JavaScript code to be executed by the browser when the script returns this input in the response page. As a result, it is possible to form links to the site where one of the parameters consists of malicious JavaScript code. This code will be executed (by a user's browser) in the site context, granting it access to cookies that the user has for the site, and other windows in the site through the user's browser.
The attack proceeds as follows: The attacker lures the legitimate user to click on a link that was produced by the attacker. When the user clicks on the link, this generates a request to the web-site containing a parameter value with malicious JavaScript code. If the web-site embeds this parameter value into the response HTML page (this is the essence of the site issue), the malicious code will run in the user's browser.

Open in new window

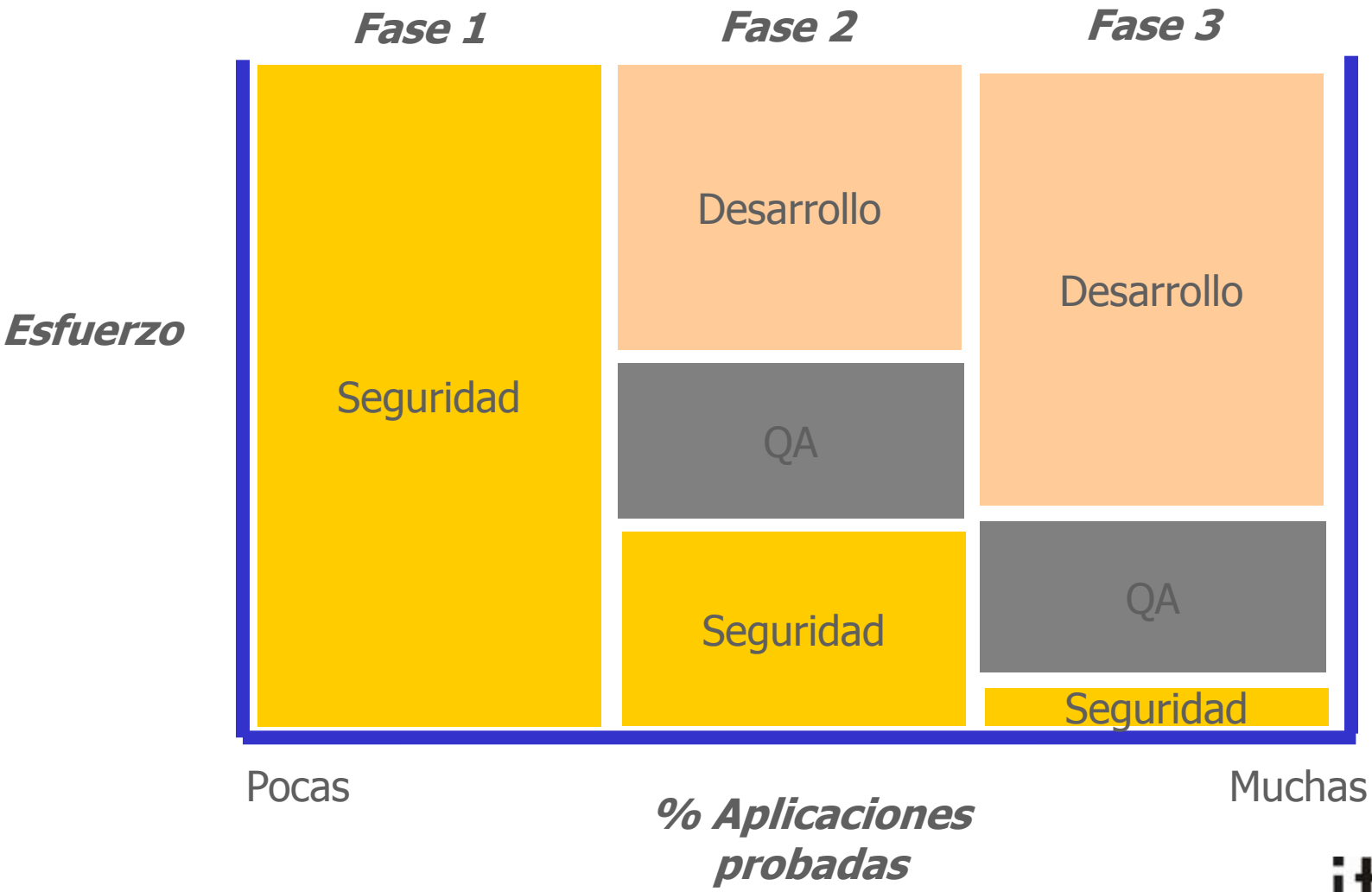
Entrenamiento web Integrado sube el nivel de expertise

Reportando apego



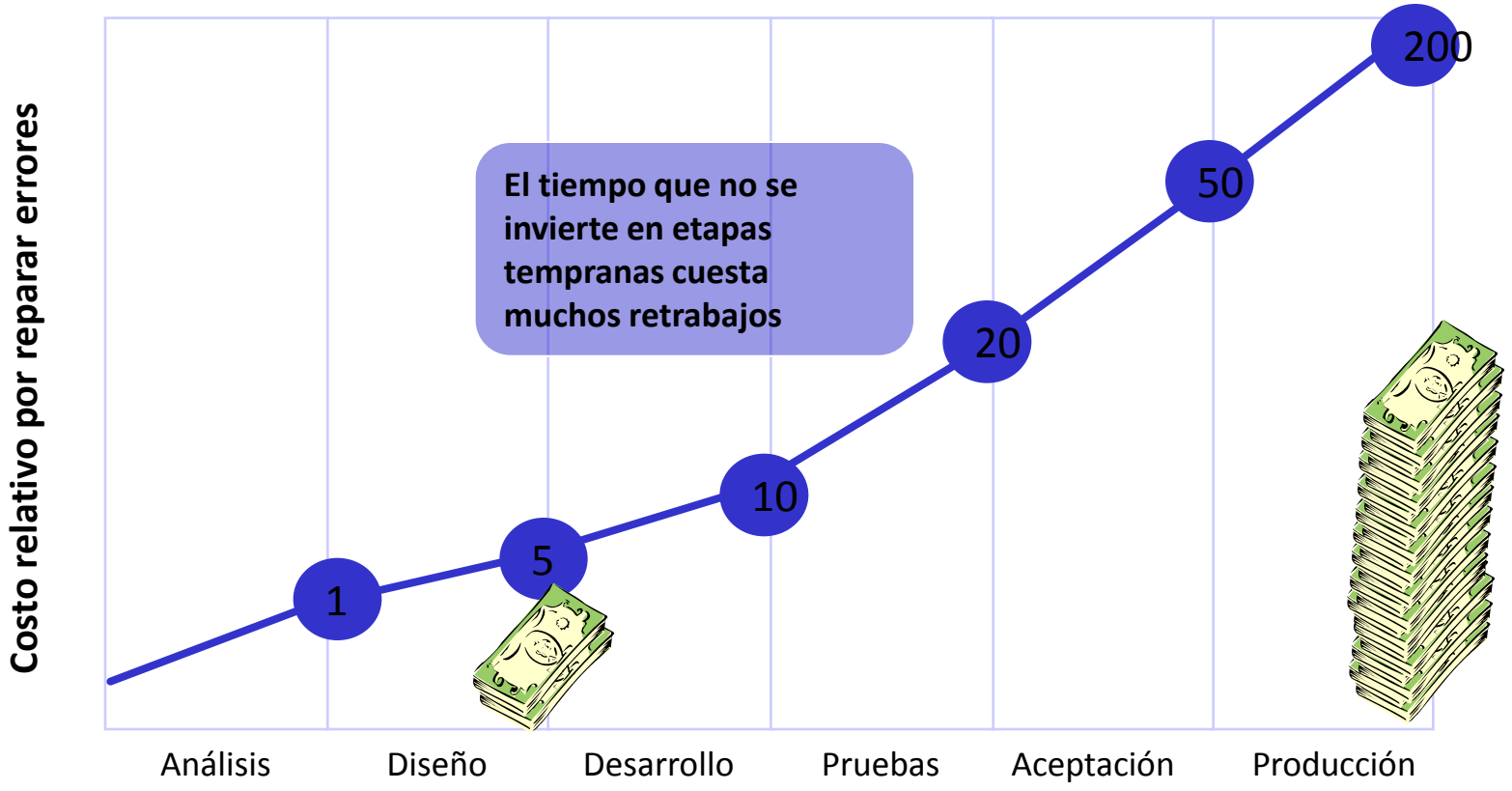
PCI
SOX
HIPAA
GLBA
NERC/ FERC
OWASP
+40 More

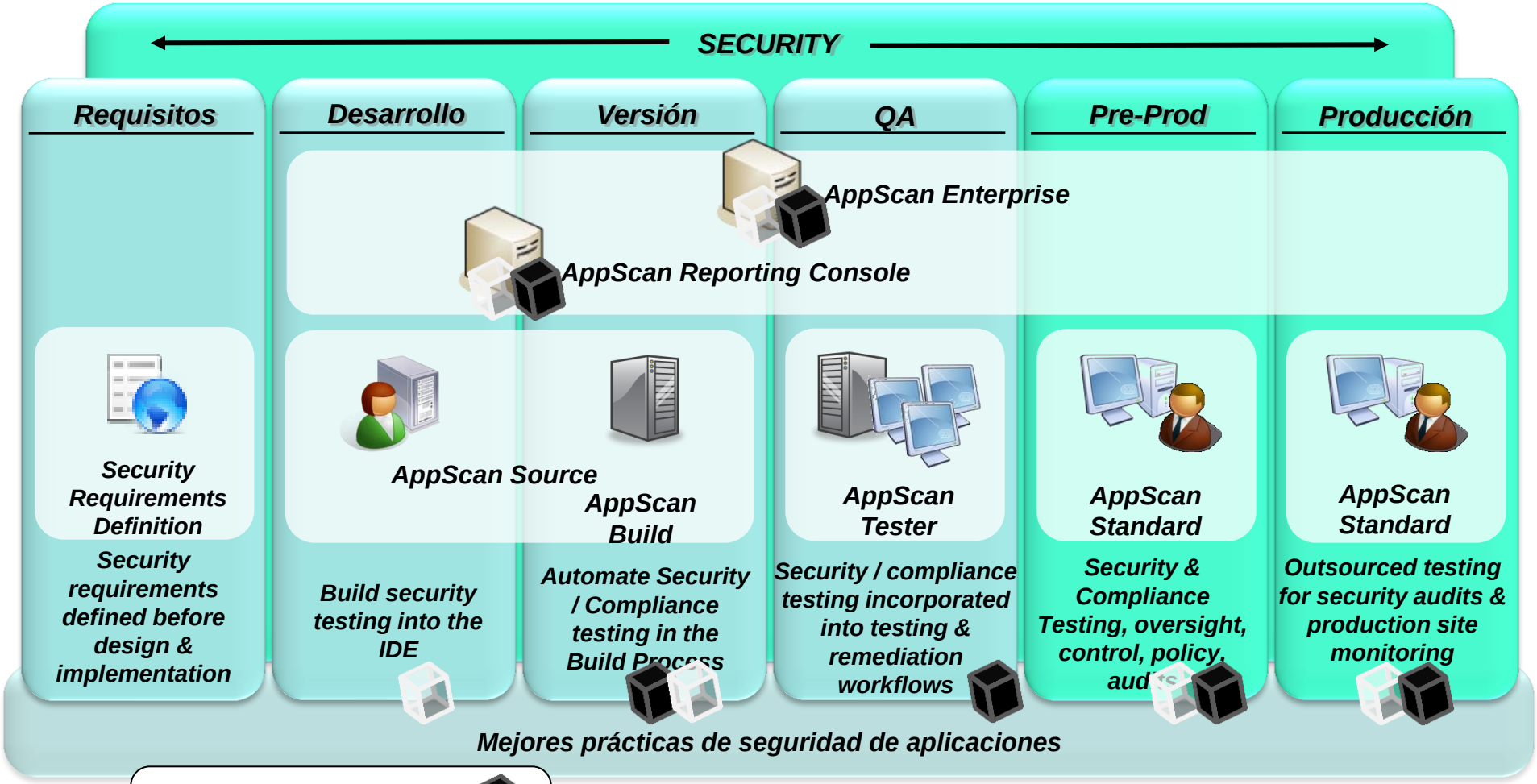
Madurando el proceso



Madurando el proceso

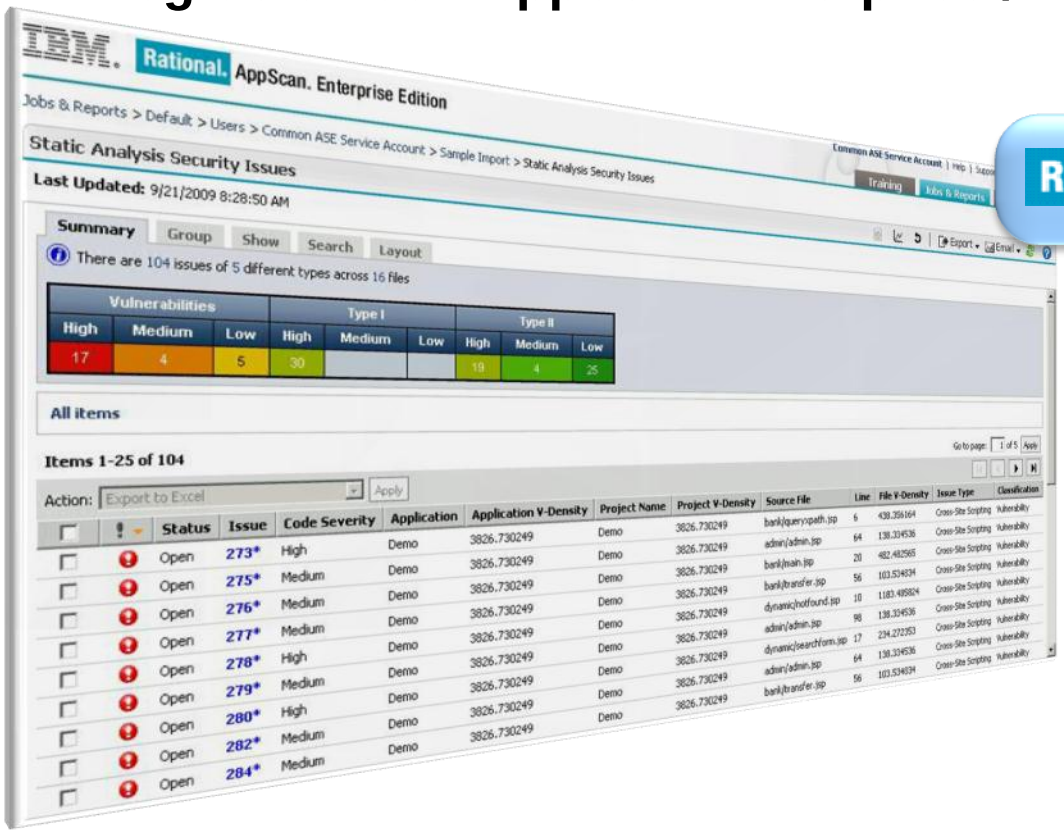
Minimizando costos a través de un ciclo de desarrollo seguro

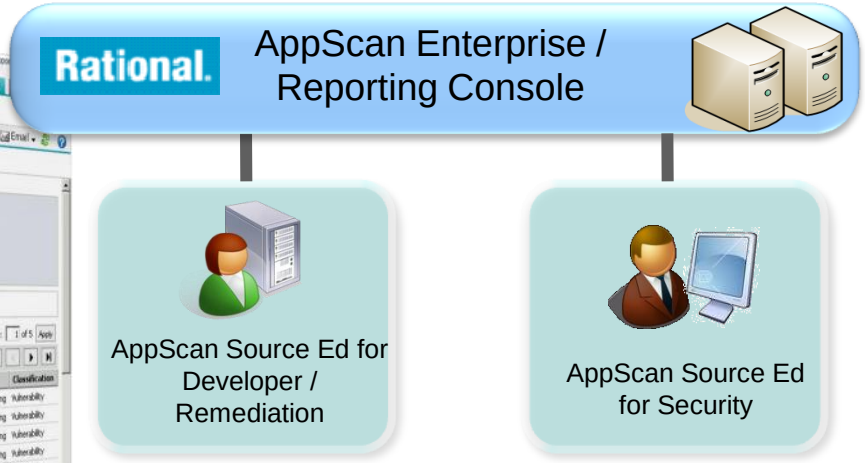




Análisis Dinámico/Blackbox –
Análisis Estático/Whitebox -

- **Integración con AppScan Enterprise / AppScan Reporting Console**

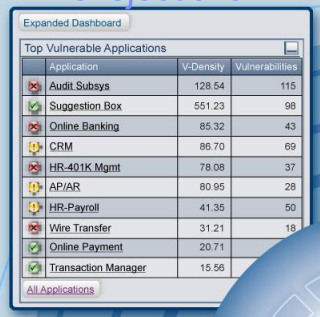




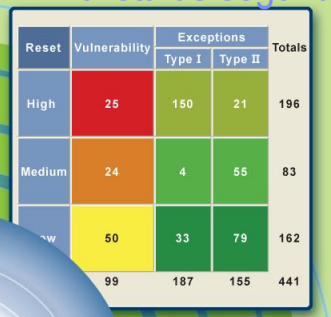
Un tablero para cada interesado

Nivel ejecutivo

- Evaluación
- Soporte para estándares
- Análisis de tendencia
- Priorización rápida de amenazas
- Todos los activos de Software: Internos, externos y open source



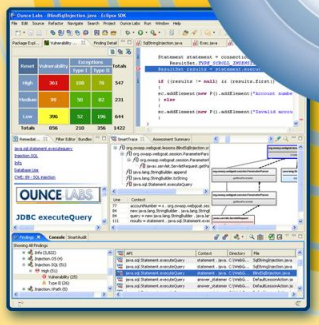
Analista de seguridad



- Análisis simplificado
- Provee guías
- Foco por prioridades
- Aumenta la experiencia en seguridad
- Reporte distribuído
- Resultados consolidados

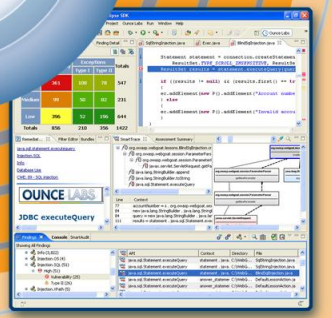
Auditor

- Terminos orientados al auditor
- Reportes centrados en auditoría
- Métricas (Vdensity) para priorizar y dar seguimiento a las correcciones



Desarrollador

- Relación con el analista de seguridad
- Capacidad de diagnósticos
- Simplifica la adquisición de conocimientos sobre seguridad



Asegurar las aplicaciones es un proceso organizacional

- Un cambio de comportamiento
- Requiere más que solo herramientas
- La educación y sensibilización es esencial
- Una visión de las responsabilidades de los resultados de las vulnerabilidades ayuda a encarar el cambio
- Lograr un sentido económico

Banorte

- Inició operaciones en 1899.
- Actualmente al grupo lo conforman:

Banco Mercantil del Norte, Banco del Centro (Fusionado), Casa de Bolsa, Arrendadora-Factor Banorte, Factor Banorte (Fusionado), Almacenadora Banorte, Seguros Banorte-Generali, Afore Banorte-Generali, Pensiones Banorte-Generali, Créditos Pronegocio, Banorte Securities, Inter National Bank, UniTeller, **se anunció la fusión con Banco IXE**.

- Capital contable: aprox. 45.000 millones de pesos
- Activos: aprox. 589.783 millones de pesos
- Margen financiero: aprox. 16.756 millones de pesos

Banorte

- Cuenta con arriba de:
  - 19,500 empleados
  - 1,100 sucursales
  - 1,500 corresponsalías nacionales
  - 4,800 cajeros automáticos

- En TI:
  - Total en TI: aprox 590 personas
  - En Desarrollo: 260 personas
  - En Seguridad Informática: 30 personas
  - 10 fábricas de software

Problemática

- Obligatoriedad en el **cumplimiento de regulaciones** PCI y CNBV
- La dificultad para la obtención de **información** sobre el estado de **seguridad en aplicaciones**.
- Falta de acuerdos con **casas de software** para el cumplimiento de estándares de seguridad en sus entregables.
- Alto grado de **tareas manuales** en seguridad de aplicaciones.

Premisas legales

Comisión Nacional Bancaria y de Valores (CNBV) Anexo 52 Capítulo X:

Artículo 316 Bis 17.- Las Instituciones estarán obligadas a realizar revisiones de seguridad, enfocadas a verificar la suficiencia en los controles aplicables a la infraestructura de cómputo y telecomunicaciones utilizada para la realización de operaciones y prestación de servicios a través de Medios Electrónicos.

VII. El análisis metódico de los aplicativos críticos relacionados con los servicios de Banca Electrónica, con la finalidad de ***detectar errores, funcionalidad no autorizada o cualquier código que ponga o pueda poner en riesgo la información de los Usuarios y de la propia Institución***. (Cualquier nuevo desarrollo de software es un cambio significativo en la infraestructura)

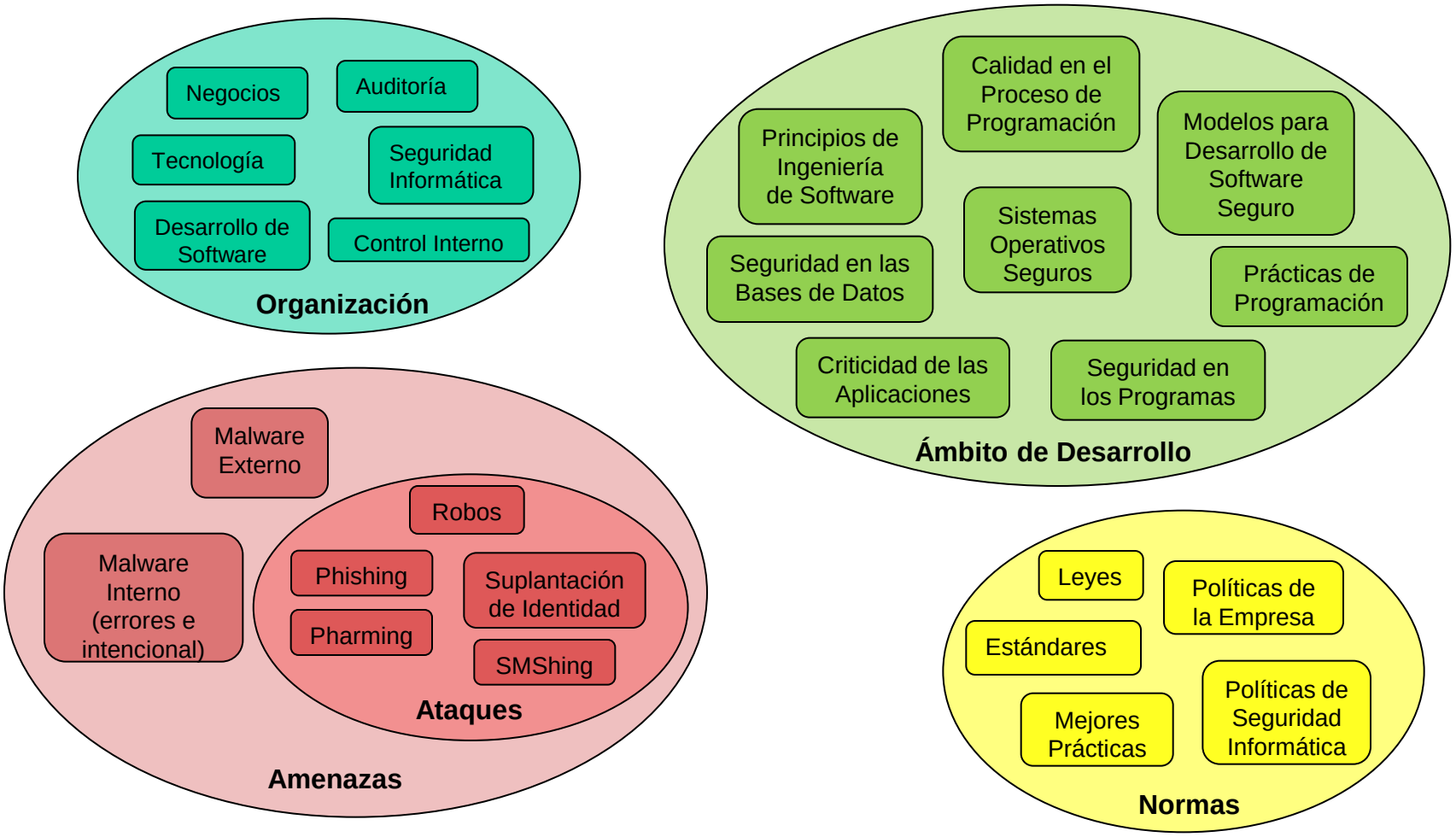
Payment Card Industry Data Security Standards (PCI DSS):

Requisito 6.3 Desarrollar aplicaciones de software basadas en las ***mejores prácticas*** de la industria e incorporar la ***seguridad de la información a través de todo el ciclo de desarrollo de Software***.
Requisito 6.3.7.a Obtener y revisar las políticas documentadas por escrito para confirmar que establecen el requisito de ***revisar los códigos*** y de que la revisión sea realizada por personas que no sean el autor del código.

Objetivos del proyecto

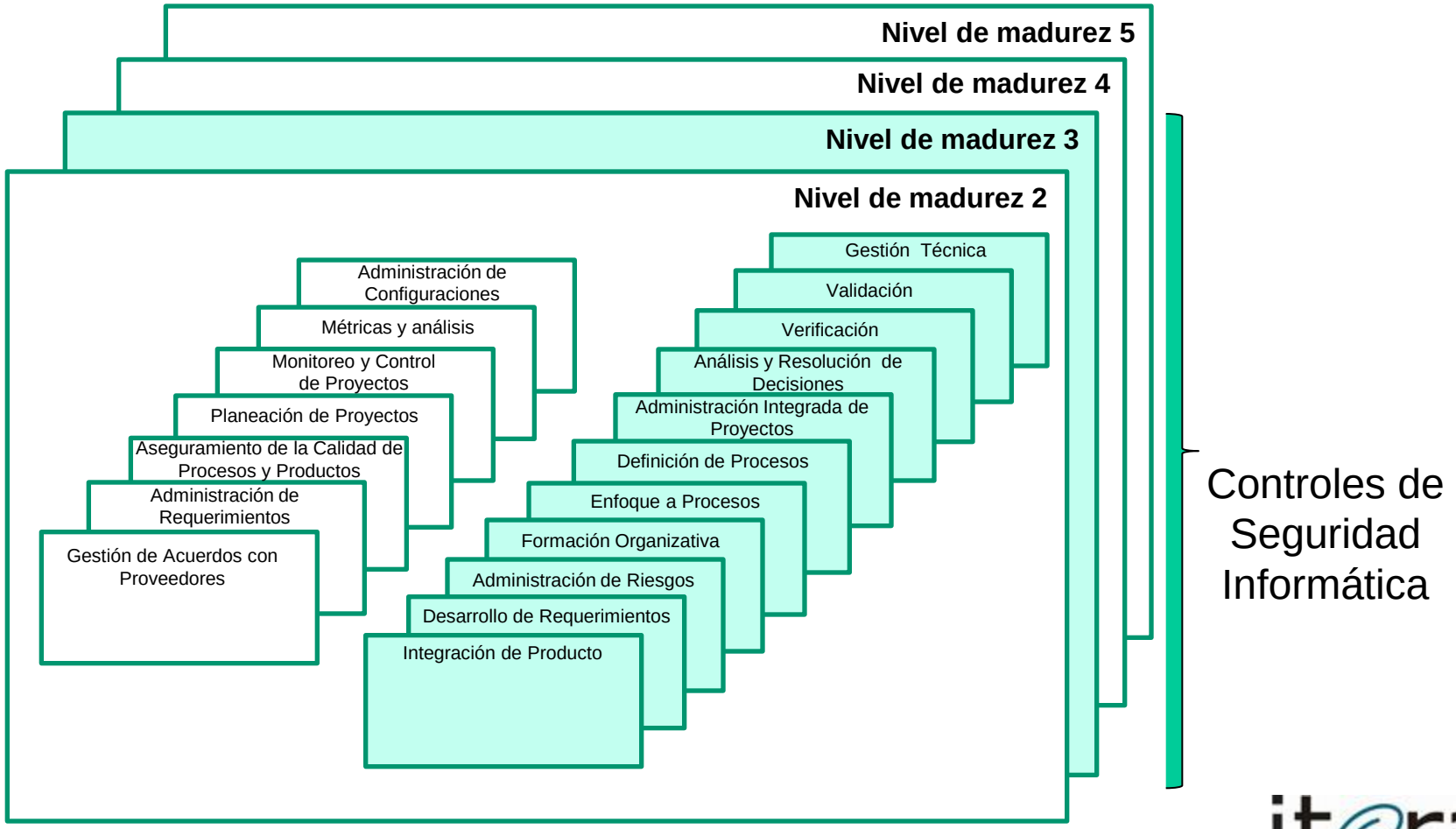
1. Establecer un **modelo integral** de desarrollo seguro a nivel **organizacional**.
2. Contar con un marco de **cumplimiento regulatorio** que permita para los requerimientos establecidos en los estándares o normas de seguridad.
3. Facilitar la detección del **incumplimiento** de los **controles establecidos**.
4. **Integrar** el modelo de **desarrollo seguro** al proceso de desarrollo de software.
5. **Reducir los defectos** de seguridad encontrados en fases de pruebas y producción, minimizando los costos de corrección.
6. Establecer criterios de seguridad para los **proveedores** que participan en servicios.

Factores

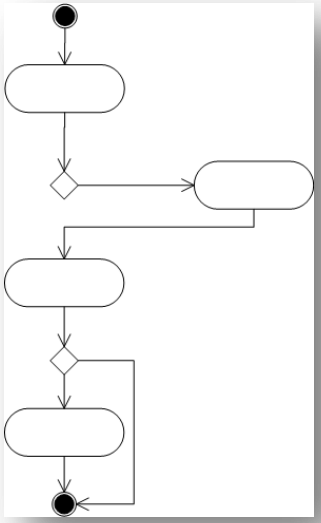

Negocios
Auditoría
Tecnología
Seguridad Informática
Desarrollo de Software
Control Interno
Organización
Calidad en el Proceso de Programación
Principios de Ingeniería de Software
Modelos para Desarrollo de Software Seguro
Sistemas Operativos Seguros
Seguridad en las Bases de Datos
Prácticas de Programación
Criticidad de las Aplicaciones
Seguridad en los Programas
Ámbito de Desarrollo
Malware Externo
Robos
Malware Interno (errores e intencional)
Phishing
Suplantación de Identidad
Pharming
SMShing
Ataques
Amenazas
Leyes
Políticas de la Empresa
Estándares
Políticas de Seguridad Informática
Mejores Prácticas
Normas

CMMI

Software Engineering Institute Capability Maturity Model Integration



Organización para desarrollo de Software seguro



Checklist de Seguridad

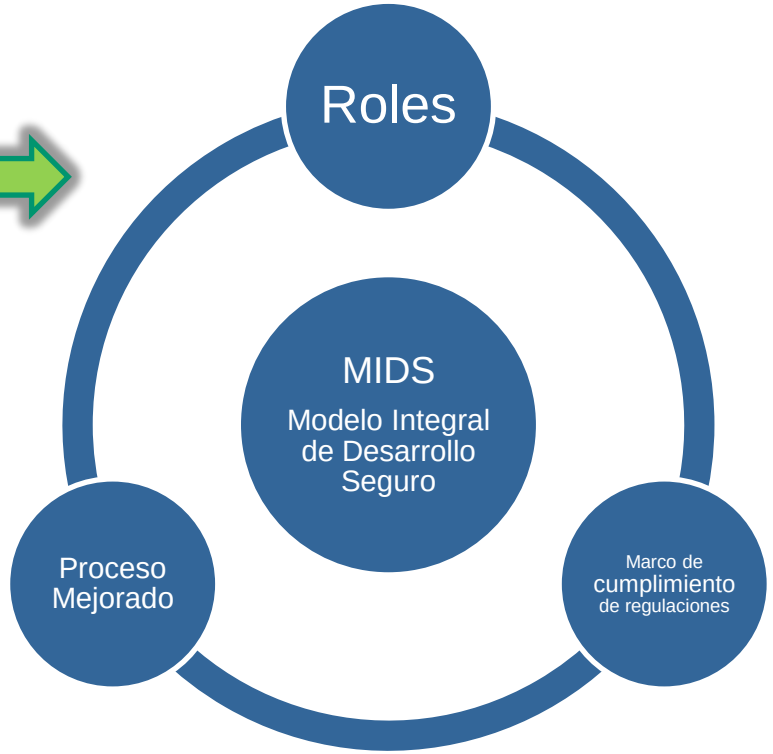
Interacción

Desarrollo

Procesos y Prácticas de Seguridad de Sistemas

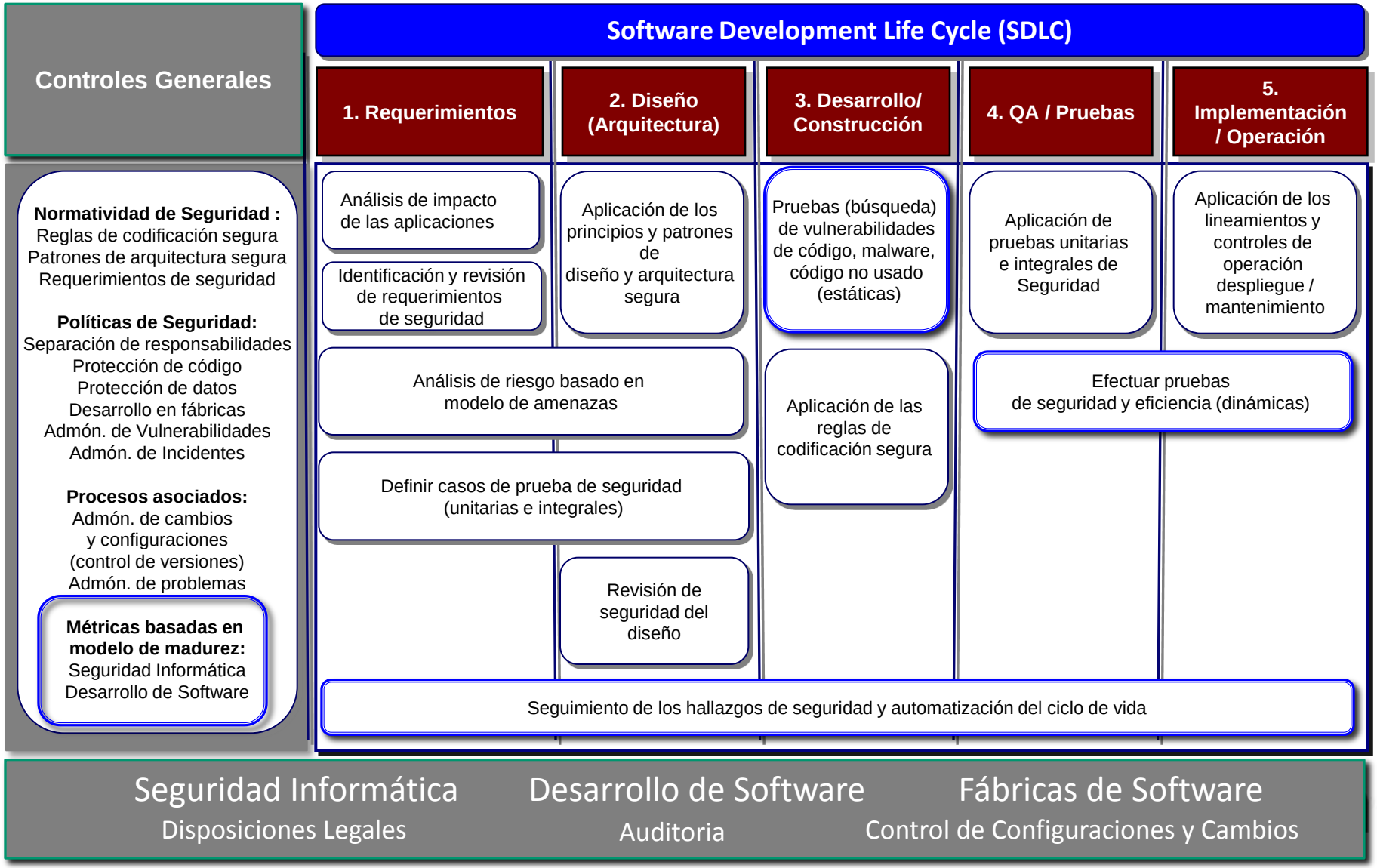
- Gestión Estrategica de Seguridad
- Cumplimiento legal y estandares aplicables
- Identificación, clasificación y evaluación de activos
- Análisis y evaluación de riesgos
- Tratamiento y gestion y riesgos
- Gestión de seguridad operacional

CNBV - Comisión Nacional Bancaria y de Valores
PCI DSS - Payment Card Industry Data Security Standard
WASC - Web Application Security Consortium
OWASP - Open Web Application Security Project
ISO 27000 - International Organization for Standardization. Gestión de Seguridad
COBIT - Control Objectives for Information and related Technology
COSO - Committee of Sponsoring Organizations

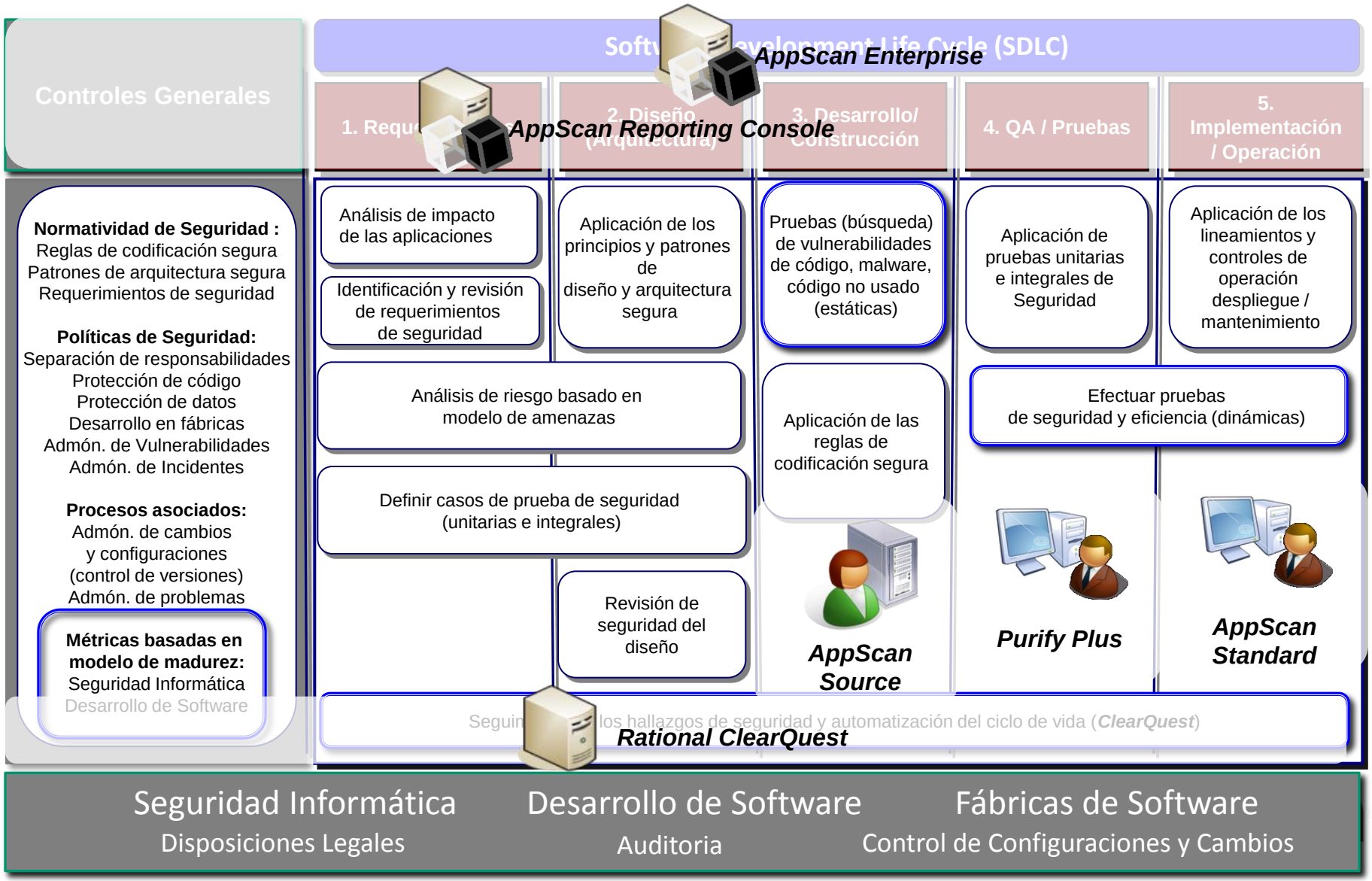


Prácticas, Políticas, Regulaciones, Auditorías, Capacitación

Software Development Life Cycle



Software Development Life Cycle



Tipos de Metodologías de Desarrollo de Software

- En cascada
- Espiral
- Desarrollo iterativo
- Desarrollo de análisis combinado
- Por prototipos
- Desarrollo rápido de aplicaciones (RAD)
- Modelo modificado de prototipos (MPM)
- Modelo de exploración
- Modelo de reuso
- Cleanroom
- Computer Aided Software Engineering (CASE)
- Desarrollo basado en componentes
- Programación estructurada
- Programación extrema

Seguridad en las bases de datos

Riesgos

- Inferencia
- Agregación
- Acceso no autorizado
- Modificación inapropiada de datos
- Disponibilidad de accesos
- Vistas de la base de datos
- Ataques con queries
- Ataques de desviación
- Seguridad del Web
- Contaminación de datos

Objetivos de Seguridad

Para proteger la BD es preciso proteger los recursos, concretamente los datos almacenados, de lecturas y/o actualizaciones accidentales o malintencionadas.

Algunos requisitos de protección a las bases de datos son:
- Protección de accesos indebidos.
- Protección de inferencias.
- Integridad de la BD.
- Integridad operacional de los datos.
- Integridad semántica de los datos.
- Contabilidad y auditoria.
- Autenticación del usuario.
- Gestión y protección de datos sensibles.
- Protección multi-nivel.

Controles en el Diseño

Discrecionalidad
Redundancia
Sobreclasificación
Dominios
Atributos

Beneficios

1. Institucionalización de la solución mediante la utilización de herramientas que lo automatizan, un proceso claro y definido, y personas que se encuentra formadas para utilizarlo.

2. Integración de las casas de Software en el proceso de Desarrollo de Código Seguro de manera natural.

3. Disminución de los riesgos de seguridad informática de la organización.
   - Malware
   - Prácticas de desarrollo
   - La organización
   - Ambientes
   - Ataques (Código dedicado, ingeniería social)

¿A qué nos dedicamos en ItEra?

IT INSTITUTE

Authorized IBM Training

EC-Council

SEIPartner CERT Courses • CMMI • TSP

RMC Project Management, Inc. Authorized Training Provider

exin

Todos reconocemos la importancia de tener un equipo de trabajo de calidad, motivado pero ….

IBM

COBIT

Val IT

Risk IT BASED ON COBIT

BALANCED SCORECARD COLLABORATIVE

PMI

ISO

BPM

ITIL®

PCI Security Standards Council

CMMI®

RUP®

itera it & business process

- ***Renan Rafael Silva Rubio***
- *Subdirector de Seguridad Informática, Banorte*
- *renan.silva.rubio@banorte.com*

- **Ariel Súcari**
- *Director de Operaciones, Itera*
- *ariel.sucari@iteraprocess.com*

- ***Renan Rafael Silva Rubio***
- *Subdirector de Seguridad Informática, Banorte*
- *renan.silva.rubio@banorte.com*

- **Ariel Súcari**
- *Director de Operaciones, Itera*
- *ariel.sucari@iteraprocess.com*