

BBK Habia

Incubadora de empresas de
Internet y Nuevas Tecnologías

Jesse James

VS

Wyatt Earp


gaztelanbidean
bbk

BBK Habia

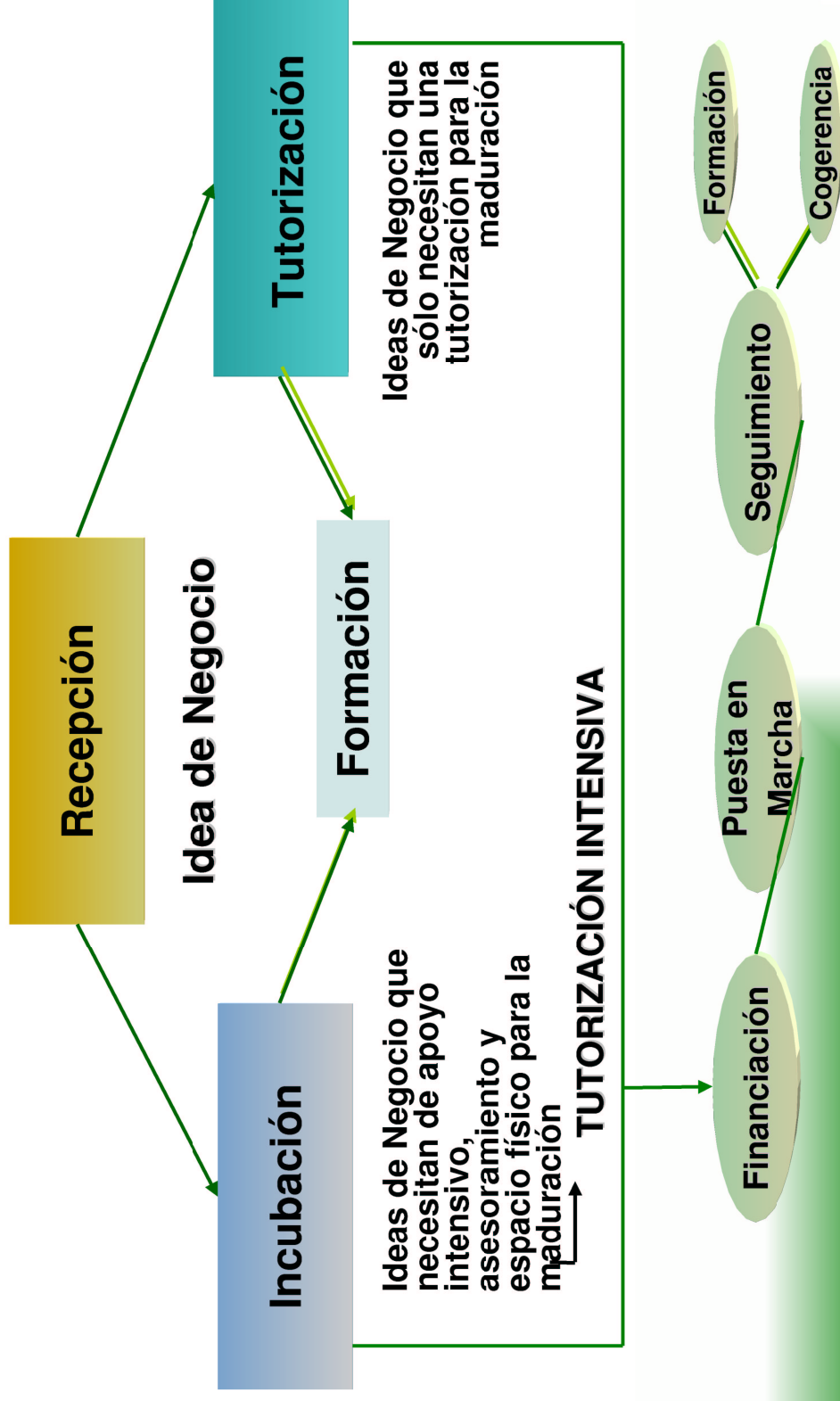
Incubadora de empresas de
Internet y Nuevas Tecnologías



g a z t e l a n b i d e a n

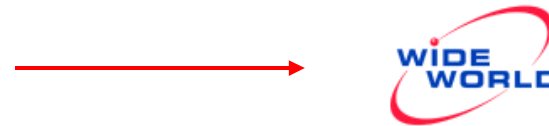
bbk

Esquema del Proceso



Tipología de Proyectos

Proyectos de Nuevas Tecnologías



Proyectos de Internet:

Puros



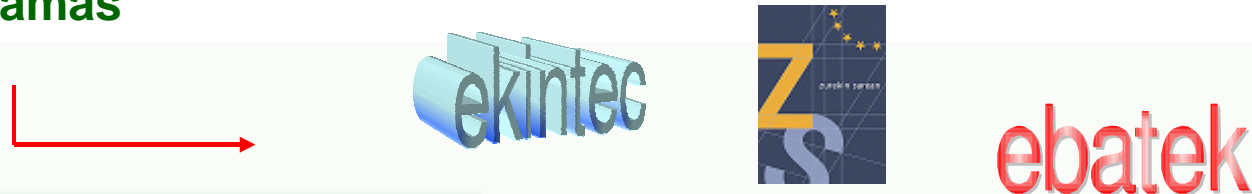
Canal comercializador



Colaterales



Apoyo a programas



BBK Habia

Incubadora de empresas de
Internet y Nuevas Tecnologías

Jesse James

VS

Wyatt Earp


gaztelanbidean
bbk

Jesse James

- Jesse Woodson James
- Kearney (Missouri), Septiembre 5, 1847
- Durante 15 años asaltó y robó trenes, bancos...
- Para algunos fue el Robin Hood del Lejano Oeste y para otros un asesino sanguinario
- Murió con 35 años a manos de sus propios secuaces



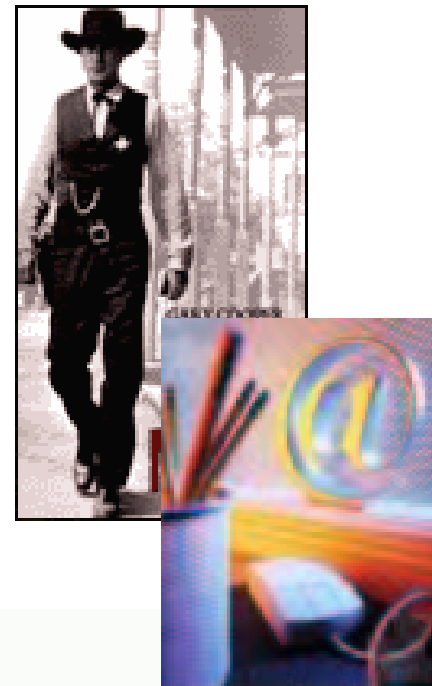
Wyatt Earp

- Wyat Berry Stapp Erap
- Monmouth (Illinois), Marzo 19, 1848
- Durante 23 años fue Marshal en Wichita (Kansas), Dodge City, Tombstone (Arizona) ... Además de ser un incansable viajero y emprendedor
- Una de las leyendas que representaban la ley en el Lejano Oeste
- Murió con 80 años, de viejo y mientras dormía





Far West vs. Internet (I)

- Vasto territorio por explorar
- Innumerables opciones y oportunidades
- Notable deficiencia de normativas legales, mecanismos y agentes que las apliquen
- Propicia la realización de sueños, consecución de grandes éxitos y estrepitosos fracasos
- Proliferan bandidos, delincuentes, marshals y llaneros solitarios



Far West vs. Internet (II)

		
	Wyatt Earp	Administrador de Seguridad
	Jesse James	Hackers Crackers

Jesse James vs Wyatt Earp

¿A qué dedican su tiempo?



Ataques



Ataques
éticos

Prevenir

Detectar

Aislar

Recuperar

2) SEGURIDAD

Firewall, Encriptación, Autenticación
(FW1, IPSEC, TACACS+Radius)



Wyatt Earp
¿A qué dedican su tiempo?

¿Qué ámbitos de seguridad hay que tener en cuenta? (I)

- Política de Seguridad, Documentación y Procedimientos
- Seguridad de Arquitectura y Diseño
- Seguridad de Red
- Seguridad de Sistemas
- Seguridad de Aplicativos
- Seguridad Física



Wyatt Earp

¿Qué ámbitos de seguridad hay que tener en cuenta? (II)

- ¿Qué es?
- ¿Qué aspectos hay que considerar?
- ¿Qué elementos defiende?
- ¿Algún ejemplo práctico?



Wyatt Earp

Política de Seguridad, Documentación y Procedimientos

(¿Qué es?)

Conjunto de ***normas y procedimientos*** que permiten:

- Enumerar y catalogar los elementos a proteger
- Definir y regular los mecanismos y sistemas necesarios para garantizar su seguridad e integridad
- Regular los patrones de conducta de los usuarios de la instalación



Wyatt Earp

¿Qué aspectos de seguridad
hay que considerar?

Política de Seguridad, Documentación y Procedimientos

(¿Qué aspectos hay que considerar?)

- Enumerar los elementos a proteger
 - Identificación de elementos
 - Identificación de amenazas
 - Identificación de vulnerabilidades
 - Evaluación del ratio de coste de protección/ coste de pérdida
- Definir y regular los mecanismos y sistemas necesarios para garantizar su seguridad e integridad
 - Sistemas de control de acceso
 - Sistemas de recuperación ante desastres
- Regular los patrones de conducta de los usuarios de la instalación
 - Determinar los perfiles y roles del personal
 - Definir sus deberes, derechos, obligaciones y tareas
 - Elaboración y aplicación de procedimientos y manuales



Wyatt Earp

¿Qué aspectos de seguridad
hay que considerar?

Política de Seguridad, Documentación y Procedimientos

(¿Qué elementos defiende?)

- Todos y Ninguno

(Constituye el marco de actuación donde se definen los diferentes subsistemas a implementar pero no controla de forma explícita y directa a nada ni a nadie.)

- Ingeniería Social

- Hay que defenderlo a él

(Dada su naturaleza, resulta extremadamente importante su difusión, control y actualización.)



Wyatt Earp

¿Qué aspectos de seguridad
hay que considerar?

Política de Seguridad, Documentación y Procedimientos

(¿Algún ejemplo práctico?)

•Política de Seguridad

.*****
.*****
.*****
.*****

•Ingeniería social

- Tipo, almacenamiento y gestión de passwords
- PC Portátiles



Wyatt Earp

¿Qué aspectos de seguridad
hay que considerar?

Seguridad de Arquitectura y Diseño

(¿Qué es? ¿Qué aspectos hay que considerar?)

La arquitectura de seguridad y diseño de un lugar, se refiere a **nivel general a la seguridad y estrategias de red y diseño de los sistemas de la organización** en lugar de detalles concretos sobre problemas de seguridad. Incluye importantes temas tales como **confianzas de red, conexiones con el mundo exterior y como estas conexiones interactúan con la organización**. Todo esto tiene un interés especial cuando se analizan cortafuegos y redes. Aunque los detalles técnicos parezcan correctos, puede haber problemas fundamentales con el diseño.



Wyatt Earp
¿Qué aspectos de seguridad
hay que considerar?

Seguridad de Arquitectura y Diseño

(¿Qué elementos defiende?)

- **Todos y Ninguno**

(Constituye el marco de actuación donde se definen los diferentes subsistemas a implementar pero no controla de forma explícita y directa a nada ni a nadie.)

- **Hay que defenderlo a él**

(Dada su naturaleza, resulta extremadamente importante su difusión, control y actualización.)



Wyatt Earp

¿Qué aspectos de seguridad
hay que considerar?

Seguridad de Arquitectura y Diseño

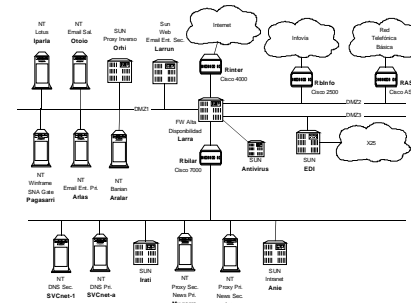
(¿Algún ejemplo práctico?)

- **Back doors**

- Accesos directos a los recursos internos no securizados
- Conexiones extra-empresariales con agentes en los que se confía

- **Segmentación interna en redes departamentales**

- Definición de los roles de los diferentes grupos de usuarios
- Estudio de las relaciones inter-departamentales
 - Interlocutores
 - Dirección de las comunicaciones



Wyatt Earp
¿Qué aspectos de seguridad hay que considerar?

Seguridad de Red

(¿Qué es? ¿Qué aspectos hay que considerar?)

El interés en la seguridad de la red ha crecido rápidamente desde la aparición del gusano (Worm) de Internet en 1988 y la proliferación de los cortafuegos al final de los 90. La seguridad de los sistemas, se eclipsa según **se conectan sistemas juntos, la nueva seguridad se refiere a todos los servicios de la red** que están funcionando para los sistemas en la red (tales como *sendmail*, *ftp*, *telnet*, etc.), confianza entre sistemas y cualquier filtro de acceso controlando el nivel de aplicación y nivel de SO/red y especialmente en **todos aquellos elementos que la configuran y controlan su topología y tráfico**.



Wyatt Earp
¿Qué aspectos de seguridad
hay que considerar?

Seguridad de Red

(¿Qué elementos defiende?)

·Configuración de los elementos de control y gestión de la red y como interactúan

- Firewall
- Routers
- Switches
- Balanceadores de carga
- IDS
- Plataformas y aplicaciones de gestión



Wyatt Earp

¿Qué aspectos de seguridad hay que considerar?

Seguridad de Red

(¿Algún ejemplo práctico?)

- Protocolos de Enrutamiento no autenticado (OSPF...)
- Errores de configuración de los elementos de control y gestión de la red
 - Firewall
 - Routers
 - Switches
 - Balanceadores de carga
 - IDS
 - Plataformas y aplicaciones de gestión



Wyatt Earp

¿Qué aspectos de seguridad hay que considerar?

Seguridad de Sistemas

(¿Qué es? ¿Qué aspectos hay que considerar?)

La **seguridad de sistemas** se refiere a los problemas que cubren la identificación individual y permisos de los usuarios, sistema de ficheros del sistema, arranque de los sistemas, ficheros de configuración, fichero de logs, bugs y vulnerabilidades que pueden ser explotados por intrusos. En muchos casos (con excepción de los bugs del sistema operativo que se resuelven instalando los parches recomendados), los problemas pueden corregirse fácilmente.



Wyatt Earp
¿Qué aspectos de seguridad
hay que considerar?

Seguridad de Sistemas

(¿Qué elementos defiende?)

•Abastionamiento

- Habilitar puertos utilizados...
- Control de los perfiles y cuentas de usuarios locales
- Actualización sistemática de parches
- Estructura de elementos redundantes intra-extra sistemas

•Gestión de Backups y restauración de datos

- Tipos de soportes
- Periodicidad y alcance
- Almacenamiento y gestión de los soportes



Wyatt Earp

¿Qué aspectos de seguridad
hay que considerar?

Seguridad de Sistemas

(¿Algún ejemplo práctico?)

- **Abastionamiento**

- Instalaciones con valores por defecto

- **Los mismos que en el caso de Seguridad de Aplicativos**

- Buffer overflow
 - Violación en la entrada
 - Condiciones de carrera
 - Inyección de SQL
 - Microsoft



Wyatt Earp

¿Qué aspectos de seguridad
hay que considerar?

Seguridad de Aplicativos

(¿Qué es? ¿Qué aspectos hay que considerar?)

La seguridad de sistemas se refiere a los problemas que cubren el abastionamiento de aplicaciones, saneamiento de sus configuraciones y blindaje del código y recursos de programación que se utilicen para su implementación.



Wyatt Earp
¿Qué aspectos de seguridad
hay que considerar?

Seguridad de Aplicativos

(¿Qué elementos defiende?)

- Datos de usuario
- Control y disponibilidad del propio aplicativo
- Evitar el escalado de permisos y la ejecución de código arbitrario



Wyatt Earp

¿Qué aspectos de seguridad
hay que considerar?

Seguridad de Aplicativos

(¿Algún ejemplo práctico?)

- Buffer overflow
- Violación en la entrada
- Condiciones de carrera
- Inyección de SQL
- Microsoft



Wyatt Earp

¿Qué aspectos de seguridad
hay que considerar?

Seguridad Física

(¿Qué es?)

La seguridad física, es uno de los aspectos **menos considerados** en la seguridad de sistemas de una organización. Se instalan los sistemas y se ponen en una sala con llaves. Sin embargo, **la seguridad física no solo debe cubrir llaves y control de accesos, sino que debe examinar planes de contingencia y equipos para casos de desastres físicos (fuego, inundaciones, tormentas, fallos, etc.)**. La seguridad física es un componente importante en la organización (especialmente considerando que los mayores problemas de seguridad ocurren sobre el sistema por causa de errores y manipulaciones por empleados).



Wyatt Earp

¿Qué aspectos de seguridad
hay que considerar?

Seguridad Física

(¿Qué aspectos hay que considerar?)

- Control de acceso y gestión de todo aquello que esté compuesto por átomos
- Sistemas de detección y extinción de incendios u otros desastres naturales



Wyatt Earp

¿Qué aspectos de seguridad hay que considerar?

Seguridad Física

(¿Qué elementos defiende?)

•ÁTOMOS



Wyatt Earp

¿Qué aspectos de seguridad
hay que considerar?

Seguridad Física

(¿Algún ejemplo práctico?)

- Cajeros Automáticos auto-asistidos
- Puertas abiertas
- Falta de rigurosidad del personal de seguridad
 - Procedimientos
 - Información de Seguridad



Wyatt Earp

¿Qué aspectos de seguridad
hay que considerar?

Información

Nos podéis encontrar en las siguientes direcciones:

www.bbk.es

C Jose M^a Olabarri s/n

48.001 Bilbao

Teléfono: 94 424 38 91

Fax: 94 424 48 24

info@bbk-gaztelanbidean.org

P. T. Zamudio Edificio, 208-A

48.170 Zamudio

Teléfono: 94 431 77 50

Fax: 94 431 70 28

bbkhabia@bbk-gaztelanbidean.org



gaztelanbidean
bbk

¿Y tú quien quieres ser, **Jesse James** o **Wyatt Earp**?