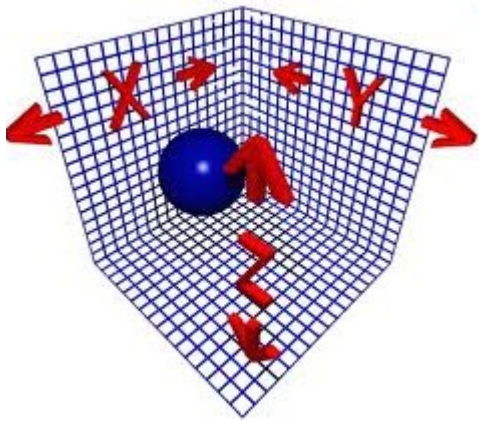
.UBAfiuba
FACULTAD DE INGENIERÍA

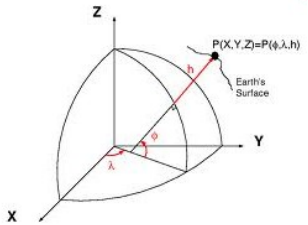
Taller de Criptografía y Seguridad Informática

Trabajo Práctico Sistema XY-Z



Trabajo Practico: Compañía XY Sistema Z

- La compañía XY dedicada a la consultoría legal en litigios comerciales, decide implementar un sistema on-line
- El sistema Z
  - Los clientes puedan realizar el seguimiento de sus trámites y expedientes
  - Desde la WEB.
  - Los mismos contienen información confidencial que sólo debe ser accedida por los involucrados con cada expediente.



Trabajo Practico: Sistema Z

- La dirección involucra al Gerente de Sistemas.
  - Usualmente relacionado con proveedores de tecnología y, a demanda, suele contratar servicios de desarrolladores según sea la necesidad puntual a cubrir.
- Invita a participar al Supervisor de IT.
  - Quien se encuentra principalmente enfocado en la conducción del equipo de Help Desk.

Trabajo Practico: Sistema Z

- En reunión con la dirección
  - Se establece la funcionalidad a nivel muy general del sistema.
  - El Gerente de Sistemas adopta el rol de Project Manager y el supervisor de IT, el rol de Líder Técnico.
  - Debido a cuestiones presupuestarias.
    - Se tratará de utilizar la menor cantidad de personal externo
    - la mayor cantidad de software open-source posible.

Trabajo Practico: Sistema Z

- El desarrollo del sistema Z comienza
  - Un analista y dos desarrolladores externos
  - un administrador de sistemas interno
  - El Líder Técnico hace de facilitador cuando no se encuentra excedido con tareas del equipo de Help Desk.
- Luego de 3 meses…

Sistema Z

- La primera versión del sistema Z se encuentra en producción.
  - Durante una semana varios integrantes de la compañía participan en la carga de los expedientes y trámites en el sistema, asistidos por el analista y uno de los desarrolladores.

Información Disponible

- Minutas de las Reuniones
  - Minuta de Arquitectura del Aplicativo Z
  - minuta de Infraestructura de Aplicativo Z
  - Otras minutas

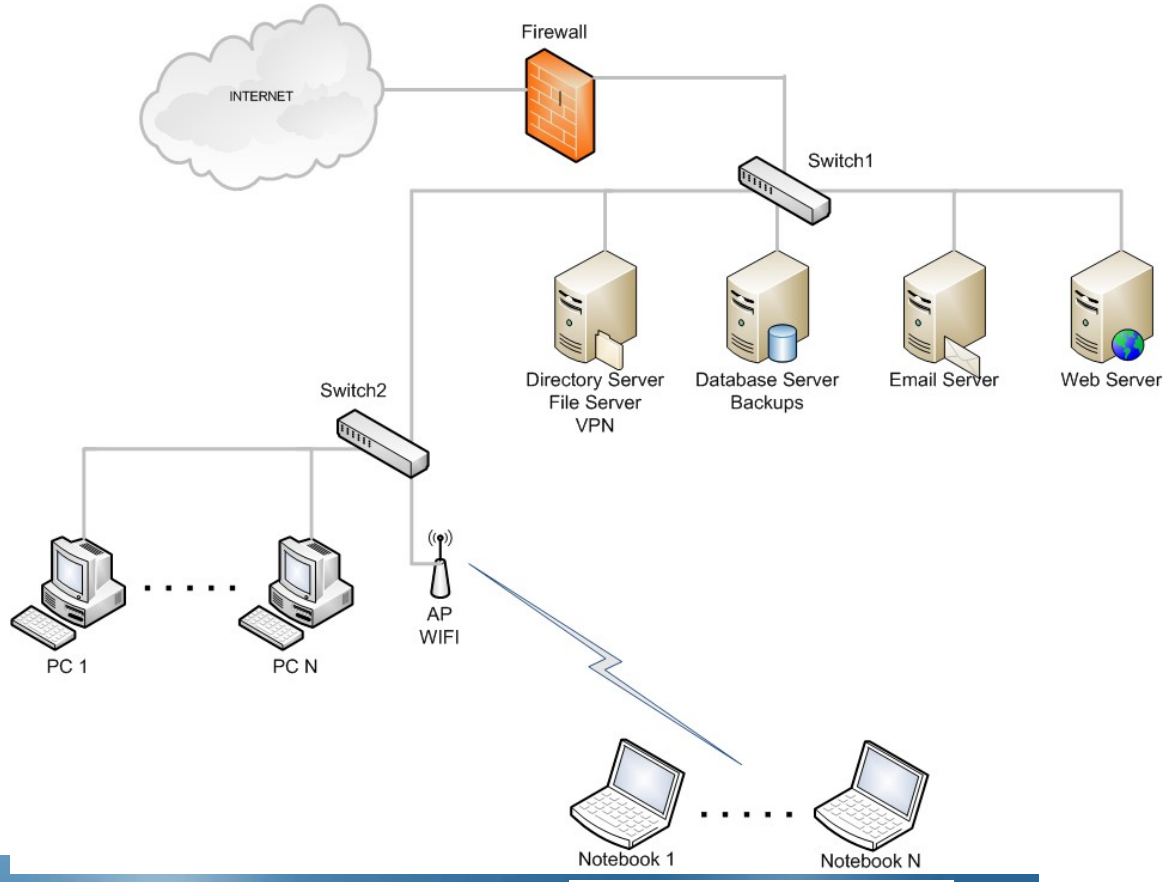
- Diagrama de Arquitectura física de la red
- Documento de Casos de Uso
- Fuentes: El Código fuente de los sistemas no puede ser utilizado en el análisis por razones de seguridad.

minuta de Arquitectura del Aplicativo Z

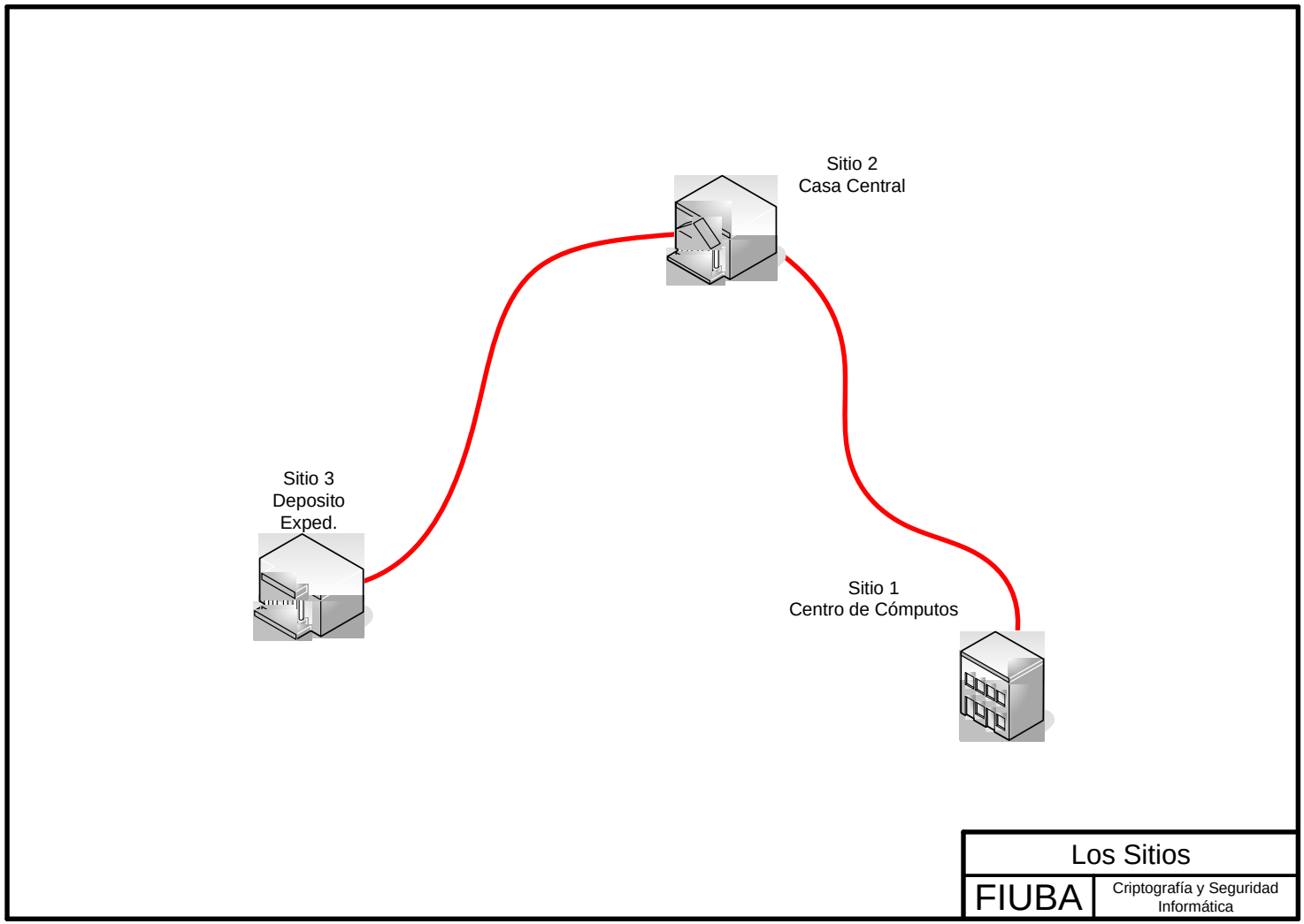
- Sistema Z, desde el punto de vista de infraestructura y aplicaciones se encuentra compuesto por:
  - Un servidor WEB.
    - Tiene un servidor apache de Frontend
    - Con código fuente de la aplicación, el cual contiene también el sitio WEB de la compañía
    - La aplicación tiene un modulo de apache que lo conecta a un tomcat con un aplicativo java denominado BackendZ
    - El BackendZ invoca por WebService unos métodos de manejo de expedientes denominados WS-Expedientes.
  - Un servidor de Base de Datos, el cuál se comparte con otros sistemas de la compañía
    - El servidor de Base de datos tiene los usuarios del aplicativo Z en la base de usuarios.
    - El servidor de Base de datos tiene registros de expedientes consumidos por los WS-Expedientes.
  - Un servidor de Correo Electrónico, el cuál es utilizado como el servidor principal de correo de la compañía.
    - Las notificaciones del Aplicativo Z son enviadas por este medio

minuta de Infraestructura de Aplicativo Z

- La infraestructura final que soporta el aplicativo Z es aproximadamente la que se muestra a continuación:

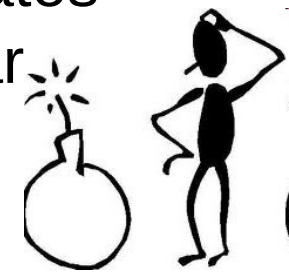


Arquitectura física de la red

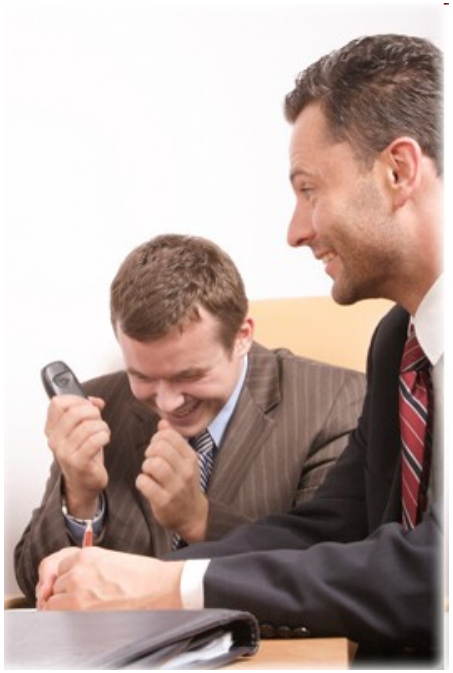


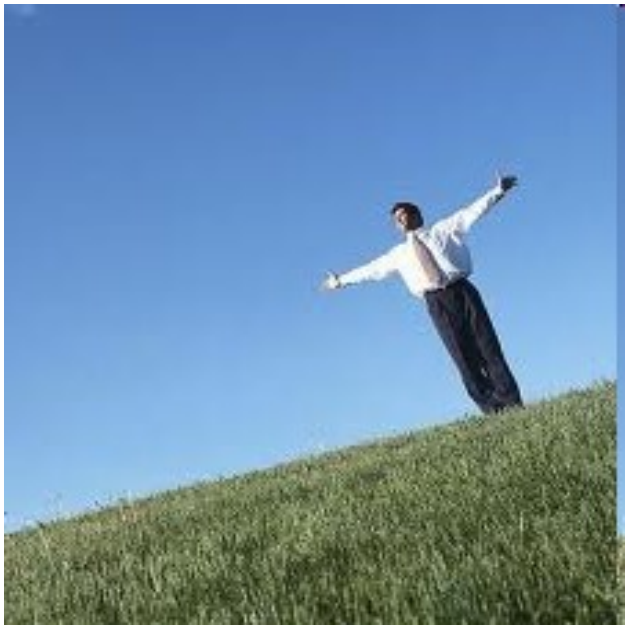
El problema

- Un expediente confidencial tomo estado publico en un programa de noticias de cable.
- A esos datos del expediente tenían acceso desde el sistema 3 personas.
  - El cliente, el abogado y el analista financiero.
- En reunión de emergencia se determina analizar la seguridad del aplicativo Z.
  - Se cree que el punto débil es el acceso a los datos por parte del aplicativo, se propone implementar filtros de aplicación.



- *El dueño de la compañía tiene un amigo que da clases en PUBA.*
- *Este profesor los recomienda a uds.*





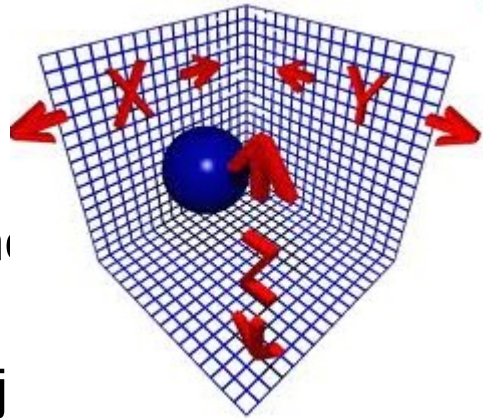
Algunos Objetivos del trabajo

Presentar una propuesta de trabajo con una presentación al dueño de XY respondiendo al RFP que se entrega.

1. Entregables mínimos:
    1. Realizar un Penetration Test de tipo Greybox con el fin de identificar las debilidades que pueda presentar la Aplicación Z y su infraestructura.
    2. Análisis de Factibilidad de Implementación de:Web Application Firewall u Otro elemento a selección del grupo
    3. Analisis de Mejora y reingenieria del sistema con entrega de prototipo.

Se debera entregar como salida del trabajo:

1. Informe Ejecutivo.
2. Informe Técnico, especificando como máxim
vulnerabilidades de mayor importancia.
Presentación del informe al dueño y sus consej



La propuesta debe contener:

- Debe estar separada la propuesta económica de la Técnica. Y estar dirigida al Gerente de Sistemas de XY
- El equipo de trabajo del proyecto se debe presentar con los CV correspondientes que deben ser reales y/o razonables.
- Económica: Mostrar claramente los honorarios profesionales a valores reales de mercado. Condiciones comerciales.
- Técnica: Apartado mostrando el entendimiento de las Necesidades. Objetivo del proyecto. Enfoque y alcance del trabajo. Metodología Propuesta. Actividades que realizaran. Antecedentes y Anexos.

- Etapa de consultas para la propuesta:
  - Es el momento de consultar el alcance y/o cualquier elemento que no este bien especificado en el pedido original
- A los grupos que se le apruebe la propuesta. Se le entregara
  - Minutas del proyecto
  - Fuentes de la aplicación
  - Maqueta del ambiente con maquinas virtuales.
  - Algún otro elemento que pidan en la propuesta de trabajo.